M365 pilviturvallisuus osana markkinointimateriaalia

Jose Junninen

Haaga-Helia ammattikorkeakoulu
Tietojenkäsittely tradenomi
Toiminnallinen opinnäytetyö
2023

Tiivistelmä

Tekijä(t)
Jose Junninen

Tutkinto
Tradenomi

Raportin/Opinnäytetyön nimi
M365 pilviturvallisuus osana markkinointimateriaalia

Sivu- ja liitesivumäärä
28 + 8

Opinnäytetyö on toteutettu toiminnallisena tutkimuksena B2B Solutions:in toimeksiannon mukaisesti. B2B Solutions on pääkaupunkiseudulla toimiva IT-, mobiili- ja tulostuspalveluihin erikoistuva yritys. B2B auttaa asiakkaitaan valitsemaan oikeat palvelut sekä turvalliset työkalut, joilla mahdollistetaan IT:n ja asiakirjahallinnan toimivuus. B2B myyntipalvelu tarjoaa yritysasiakkaillensa myös monitoimilaitteet sekä näihin kuuluvat huollot, koulutukset, asennukset sekä käyttötuen. Heille yritykset pystyvät ulkoistamaan ICT-asiat tai vaan yksittäisen osan näistä. Työn tuloksena syntyy markkinointimateriaalia, joka sisältää tietoa pilvipalveluiden riskeistä ja Microsoftin ratkaisuista näihin riskeihin. Toimeksiantaja voi käyttää materiaalia myynnissä tai henkilöstön koulutuksessa.

Opinnäytetyössä tutkitaan pilviympäristön riskejä sekä Microsoftin ratkaisuja näihin ongelmiin. Tutkimuskysymyksenä on: ”Kuinka säilyttää tietoa turvallisesti Microsoftin pilvessä?”. Työhön on valittu tietoturvariskejä toimeksiantajan näkemyksen perusteella. Tutkimuksen tuloksilla lisätään tietoisuutta tietoturvariskeistä ja näiltä suojautumisesta. Tulokset voivat myös auttaa toimeksiantajaa heidän palvelujen myynnissä.

Tietoperusta muodostuu yleisistä tietoturvariskeistä, kuten käyttäjävirheistä ja haittaohjelmista. Riskien jälkeen tietoperustassa käydään läpi Microsoftin eri ratkaisuja tietoturvan säilyttämiseksi. Ratkaisut ovat valittu toimeksiantajan kanssa. Käsitteitä käydään läpi yleisellä tasolla, jonka jälkeen tarkastellaan Microsoftin tapoja hoitaa nämä tietoturvaratkaisut.

Tutkimusaineiston hankintamenetelminä käytetään observointi- sekä dokumenttianalyysiä. Tutkimuksen päälähteenä on käytetty Microsoftin omaa aineistoa aiheesta, mutta aineistoa on myös etsitty laajasti eri verkkolähteitä hyödyntäen. Microsoft tuottaa luotettavaa sekä tarkkaa aineistoa palveluistaan, joten tätä on käytetty työssä hyväksi.

Työn tuloksena syntyy markkinointimateriaalia, jonka tulokset ovat toimeksiantajan hyödynnettävissä heidän tulevissa projekteissaan. Tulokset auttavat ymmärtämään pilveen sisältyviä riskejä, sekä yleistä tietoa tietoturvasta. Tulosten avulla toimeksiantaja voi mahdollisesti myydä palveluitaan paremmin asiakkaille, tai käyttää aineistoa esimerkiksi henkilöstön koulutukseen.

Opinnäytetyön loppuvaiheilla arvioidaan tutkimuksen tekijän oppimista opinnäytetyöprojektin aikana. Projektin tekeminen on kasvattanut opiskelijan asiantuntevuutta, sekä tietoisuutta pilviympäristön riskeistä sekä näiden ratkaisuista.

Asiasanat
pilvipalvelut, tietoturva, tietoturvariski, Microsoft 365

Sisällys

1 Johdanto

Tietoturva on yksi tärkeistä asioista, joka tulee ottaa huomioon tietojärjestelmien ympäristöissä. Tietoturvan merkitys kasvaa entisestään, kun käsittelyssä on arkaa tietoa, ja kun tietojärjestelmät ovat osa organisaatioiden liiketoimintaa. Pilviympäristöt ovat nykyisin suosittu tekninen alusta, jonka kautta toteutetaan organisaation IT-infrastruktuuri, mutta ovat ne myös yleistyneet yksilöillä. Microsoftin ympäristö on yksi yleisimmistä tietojärjestelmien ympäristöistä, joka tarjoaa paljon erilaisia työkaluja sekä sovelluksia organisaation käyttöön.

Tässä opinnäytetyössä tarkastellaan tietoturvaa Microsoft 365 ympäristössä (myöhemmin M365) ja vain M365-ympäristön näkökulmasta. Tietoperustassa käsitellään tietoturvan käsitteitä sekä suojaustoimenpiteitä, niiden merkitystä sekä Microsoftin omia ratkaisuja tiedostojen turvalliseen säilyttämiseen. Pilven turvallisuutta tarkastellaan organisaation, että myös yksilön näkökulmasta. Microsoft tarjoaa laajan valikoiman palveluita sekä työkaluja, joiden avulla organisaatiot tai yksilöt voivat suojata tietonsa tietoturvauhkilta. (Microsoft s.a)

Opinnäytetyön tavoitteena on tehdä tämän selvityksen tuloksista erillinen markkinointimateriaali toimeksiantajalle, jota voidaan hyödyntää toimeksiantajan organisaatiossa, koska heillä on käytössä Microsoftin ympäristö. Tulokset ja niistä tehty kirjallinen materiaali antaa sisällöllistä M365 tukea ja auttaa yrityksen myyjiä vahvistamaan myyntityötä sisällöllisesti, joka taas mahdollistaa saamaan uusia, potentiaalisia asiakkaita. Opinnäytetyön tietoperusta sekä lopputulos voi myös yleisesti auttaa ymmärtämään tietoturvaa niin Microsoftin ympäristössä, kuin yleisesti. Markkinointimateriaali tehdään selvityksessä saatujen ja analysoitujen tulosten pohjalta, jonka tiedostomuoto on PowerPoint, jolloin tiedoston lukeminen sekä sen käsittely on mukavampaa.

1.1 Toimeksiannon esittely ja tavoitteet

Toimeksianto opinnäytetyön tekemiseen on saatu IT-alan yritykseltä. Toimeksiannon aiheena on luoda yritykselle materiaalia, jonka avulla heidän palveluitaan olisi mahdollista helpommin myydä. Opinnäytetyön tulos tulee olemaan myös ohjeistava esite sekä sisältää informaatiota mahdollisista pilvessä sijaitsevista riskeistä ja vaaroista.

Opinnäytetyön tutkimuskysymyksenä on:

> ”Kuinka säilyttää tietoa turvallisesti Microsoftin pilvessä?”.

Työn tavoitteena on kehittää uutta markkinointimateriaalia, jonka sisältö kertoo selkeästi asiakkaalle pilvialustan tietoturvasta, ja siitä, miten dataa säilytetään turvallisesti pilvessä. Tällöin B2B

Solutions voi käyttää tulevaisuudessa osana yrityksen myyntimateriaaleja, ja siten myös uusien tai vanhojen asiakkaiden hankkimiseen.

1.2 Työn rakenne ja rajaus

Tutkimuksen aiheen valinta on ensimmäinen askel tutkimusprosessissa. On tärkeää valita aihe, joka motivoi tutkijaa ja pitää mielenkiinnon yllä tutkimuksen pitkässä aikajänteessä. Aiheen tuttuus tutkijalle voi helpottaa tutkimusprosessia, sillä täysin uuteen aihepiiriin perehtyminen vie aikaa. (Jyväskylän yliopisto 2021) Tähän aiheeseen olen työharjoitteluni parissa perehtynyt työtehtävissäni. Samalla on kuitenkin hyvä huomioida, että aiheesta ei ole tehty liikaa tutkimusta, jotta on mahdollista löytää omaperäinen näkökulma ja tuottaa uutta tietoa. On myös tärkeää ottaa huomioon aiheen tutkimuksen reunaehdot, kuten mahdollisuus päästä käsiksi tarvittavaan aineistoon ja sen kokoamisen tekniset tai taloudelliset mahdollisuudet. Aiheen liittyminen oman oppiaineen tai laitoksen tutkimuksen painoalueisiin voi helpottaa tutkimuksen tekemistä. Lisäksi on hyvä huomioida, että aiheeseen on saatavilla ohjausta ja tarvittavaa tukea. (Jyväskylän yliopisto 2021)

Aiheen rajaaminen tarkoittaa valitun tutkimusaiheen tarkentamista ja supistamista. Rajaamisen perusteisiin vaikuttavat tutkijan mielenkiinnon kohteet, ja tutkimus tulisi kohdistaa siihen, mikä tutkijaa eniten kiinnostaa. Rajausta voidaan myös perustella tutkijan omilla taidoilla ja osaamisella. Aiheen eri rajaustavat voivat tehdä tutkimuksen joko helpommaksi tai haastavammaksi. Ajan käytettävyys tutkimukseen on myös tärkeä tekijä aiheen rajaamisessa, erityisesti opinnäytetöissä, joissa aihe kannattaa rajata napakasti. (Jyväskylän yliopisto 2021) Tiukalla rajauksella tutkimuksessa voidaan edetä syvällisemmin. Aiheen rajausta voidaan perustella myös tavoitteella tuottaa uutta tietoa aiheesta, jota ei ole aiemmissa tutkimuksissa käsitelty. Tällöin aihe rajataan poikkeuksellisella tavalla verrattuna aiempaan tutkimukseen. Rajausta voi tehdä monin eri tavoin, esimerkiksi rajautumalla tiettyyn ajanjaksoon, tietylle ihmisryhmälle, tiettyyn maantieteelliseen sijaintiin tai tiettyyn aineistotyyppiin. Aiheen rajaamista voidaan myös lähestyä tietyn näkökulman tai käsitteen kautta. Rajaamisen tapoja on lukemattomia. (Jyväskylän yliopisto 2021)

Työ sisältää paljon tietoa pilvestä ja tähän liittyvistä riskeistä. Työ rajataan ja tulee keskittymään vain Microsoftin pilviratkaisuihin sekä palveluihin. Microsoftin omat verkkosivut tulevat toimimaan opinnäytetyön päälähteenä, koska Microsoft jakaa palveluistaan sekä ratkaisuistaan hyvää tietoa omilla verkkosivuillaan. Microsoft on opinnäytetyön tekemiseen luotettava sekä laaja lähde. Yleistä tietoa pilvestä, sekä tämän riskeistä on myös etsitty muistakin lähteistä. Opinnäytetyö ei tule sisältämään perinteisistä palvelimista eikä näiden riskeistä tietoa. Opinnäytetyö ei myöskään vertaile pilven ja palvelimien eroavaisuuksia.

1.3 Tutkimusmenetelmät ja aineistonhankinta

Opinnäytetyön tutkimusmenetelmänä on toiminnallinen tutkimus. Tämä valittiin opinnäytetyön tutkimusmenetelmäksi, koska opinnäytetyön tuloksena on markkinointimateriaalia, jota toimeksiantaja voi tulevaisuudessa käyttää hyväkseen. Toiminnallisesta tutkimuksesta syntyy tuotos, joka voi olla esimerkiksi ohjeistus, tuote tai palvelu. (Karelia Ammattikoulu s.a) Toiminnallinen tutkimus soveltuu erityisesti sellaisiin tutkimuskysymyksiin, joissa tavoitteena on parantaa tai ratkaista käytännön toimintaa tai ongelmia. (Jyväskylän Yliopisto s.a) Tämän perusteella opinnäytetyön tutkimusmenetelmäksi valittiin toiminnallinen tutkimusmenetelmä, jonka avulla toimeksiantaja yritys voi mahdollisesti parantaa myyntityön sisältöä tai tehostaa tietoturvan ymmärrettävyyttä asiakkuussuhteistaan.

Tutkimusaineiston hankintamenetelminä käytetään observointi- sekä dokumenttianalyysiä. Dokumenttianalyysillä tarkoitetaan menetelmää, jolla analysoidaan erilaisia dokumentteja, kuten organisaation verkkosivuja, raportteja tai laskelmia. Dokumenttianalyysissä päätelmät kasataan kirjalliseen muotoon. (Oppariapu s.a) Yleensä kirjallisena muotona toimii raportti, jonka takia dokumenttianalyysi sopii hyvin aineistonhankintamenetelmänä tähän opinnäytetyöhön. Observointimenetelmällä tarkoitetaan menetelmää, jolla voidaan kerätä tietoa suoraan käytännön toiminnasta havainnoimalla tätä. (Jyväskylän Yliopisto s.a) Suoritin työharjoitteluni toimeksiantajalla, joten tutkimuksen aihe on ollut työtehtävieni lähellä päivittäin. Tutkimusaineiston hankinnassa on hyödynnetty paljon Microsoftin omia verkkosivuja, koska nämä ovat luotettavia sekä sisältävät paljon tietoa aiheesta. Lisäksi ainestoa on haettu myös muualta internetistä, kuten kyberturvallisuuskeskuksen verkkosivuilta sekä heidän tuottamista PDF-tiedostoista.

1.4 Käsiteluettelo

Microsoft 365	Microsoftin tarjoama palvelu, joka sisältää erilaisia sovelluksia ja palveluita, kuten Office-sovellukset (Word, Excel, Powerpoint). Microsoft 365 on suunniteltu erityisesti yrityksille ja organisaatioille, jotka haluavat käyttää Microsoftin tuotteita ja palveluita pilvipohjaisesti. Lyhennys ”M365”.
Pilvipalvelu	Pilvipalvelut ovat verkkopohjaisia palveluita, jotka mahdollistavat tietojen tallentamisen, käsittelyn ja jakamisen internetin kautta. Pilvipalvelut ovat yleistyneet viime vuosina, ja ne tarjoavat monia etuja perinteisiin tietokoneisiin verrattuna, kuten skaalautuvuutta, joustavuutta sekä kustannustehokkuutta.

Tietoturva	Tietoturva on tietojen suojaamista haitallisilta hyökkäyksiltä ja vahingoilta, jotka voivat johtaa vuotoihin, varkauksiin tai tiedon tuhoutumiseen. Tietoturva on tärkeää niin yksityiselle, kuin yrityksillekin. Tietojen menetys voi johtaa merkittäviin taloudellisiin ja maineeseen liittyviin vahinkoihin.
Kyberturva	Tietoturvaa laajempi käsite, joka kattaa kaikki digitaaliseen ympäristöön liittyvät turvallisuusasiat. Tähän sisältyy tietokonejärjestelmiin, verkkoihin, ohjelmistoihin, mobiililaitteisiin ja pilvipalveluihin liittyvät riskit.
MFA	MFA (multifactor authentication) tarkoittaa monitekijäistä todennusta, jolla pyritään varmistamaan henkilöllisyys. Tästä lisää tietoperustassa.
Phishing	Phishing on tietojenkalasteluun liittyvä termi, joka tarkoittaa yleisesti ottaen huijausyrityksiä, joissa yritetään hankkia henkilökohtaisia tietoja, kuten salasanoja, pankkitietoja tai luottokorttitietoja. Suomeksi tietojenkalastelu.
Adware	Adware on ohjelmisto, joka näyttää mainoksia käyttäjän tietokoneessa tai mobiililaitteessa. Adwaret yleensä tulevat asennuspakettien mukana.
Ramsonware	Haittaohjelma, joka salaa tai estää käyttäjää käyttämästä tämän tietoja. Yleensä vaatii lunnaita tiedostojen palauttamiseksi. Tästä lisää tietoperustassa.
AIP	Azure Information Protection (AIP) tarjoaa mahdollisuuden määrittää käytäntöjä, jolla tietoa voidaan luokitella sen herkkyyden mukaan. Tästä lisää tietoperustassa.
DLP	Data Loss Prevention (DLP) on käsite, jolla tarkoitetaan tiedon katoamisen estämistä. Tästä lisää tietoperustassa.

2 Tietoturvariskit M365-ympäristössä

Tietoturva on tärkeä osa nykypäiväistä digitaalista maailmaa. Yhä useampi organisaatio on siirtynyt pilvipalveluiden käyttöön. Microsoft 365 on yksi suosituimmista maailmanlaajuisista pilvipalveluista, joka tarjoaa paljon monipuolisia toimintoja organisaatioiden ja yritysten tarpeille. Vaikka tietoturvaominaisuudet kehittyvät ja ovat huippuluokkaa, ei mikään järjestelmä ole täysin immuuni tietoturvariskeille. Tietoturvariskit voivat johtua monesta eri asiasta, kuten haittaohjelmista tai käyttäjävirheistä. Microsoftin (Microsoft 2023) mukaan heillä on kuitenkin monia eri turvallisuusperiaatteita sekä -toimintoja, joiden avulla pystytään suojaamaan tietoa eri uhkilta. On tärkeää ymmärtää tietoturvariskeistä ja näiden mahdollisista haitoista. Tämä mahdollistaa organisaatiota tunnistamaan mahdolliset haavoittuvuudet ja ryhtymään toimenpiteisiin näitä uhkia varten.

2.1 Pilviympäristön riskejä

Tietoturvan riskit ovat kasvaneet huomattavasti viime vuosikymmenien aikana, koska yhteiskuntamme on myös siirtynyt yhä enemmän digitaaliseen maailmaan. Ne ovat todellisia sekä niitä on monenlaisia. Nämä riskit voivat aiheuttaa vakavia seurauksia niin yksilöille, kuin yrityksille. Nykyisin organisaatioilla on hallussaan yhä enemmän tietoa. Samalla, kun tiedon määrä ja merkitys on kasvanut, on myös siihen liittyvät uhkatekijät ovat kasvaneet (Tietoturvariskienarviointi s.a). Tunnistamalla sekä arvioimalla tietoturvan riskejä ja näiden vaikuttavuutta sekä merkittävyyttä organisaation toiminnalle, on myös helpompi vastata näihin uhkiin järkevin kustannuksin. (Tietoturvariskienarviointi.fi s.a)

Opinnäytetyöhön valitut riskit, joista seuraavat kappaleet kertovat, ovat valittu työhön näiden yleisyyden perusteella. Aloituskokouksessa toimeksiantajan kanssa valitsimme myös riskejä, joita olisi opinnäytetyössä hyvä käydä läpi. Riskejä valittiin sen perusteella, mitä mahdolliset toimeksiantajan asiakkaat voisivat pitää ajankohtaisina. Työharjoitteluni aikana työtehtävissä ilmaantui eri tietoturvariskejä, joita myös esitellään opinnäytetyössä. Näiden riskien läpikäynti auttaa lukijaa ymmärtämään erilaisista tietoturvavaaroista, joiden avulla nämä ovat tunnistettavissa ja ehkäistävissä. Riskien läpikäynti on suunniteltu vastaamaan tutkimuskysymykseen: ”Kuinka säilyttää tietoa turvallisesti Microsoftin pilvessä?”. Näiltä riskeiltä voidaan ja pitää suojautua, joka tekee tiedon säilyttämisestä turvallista.

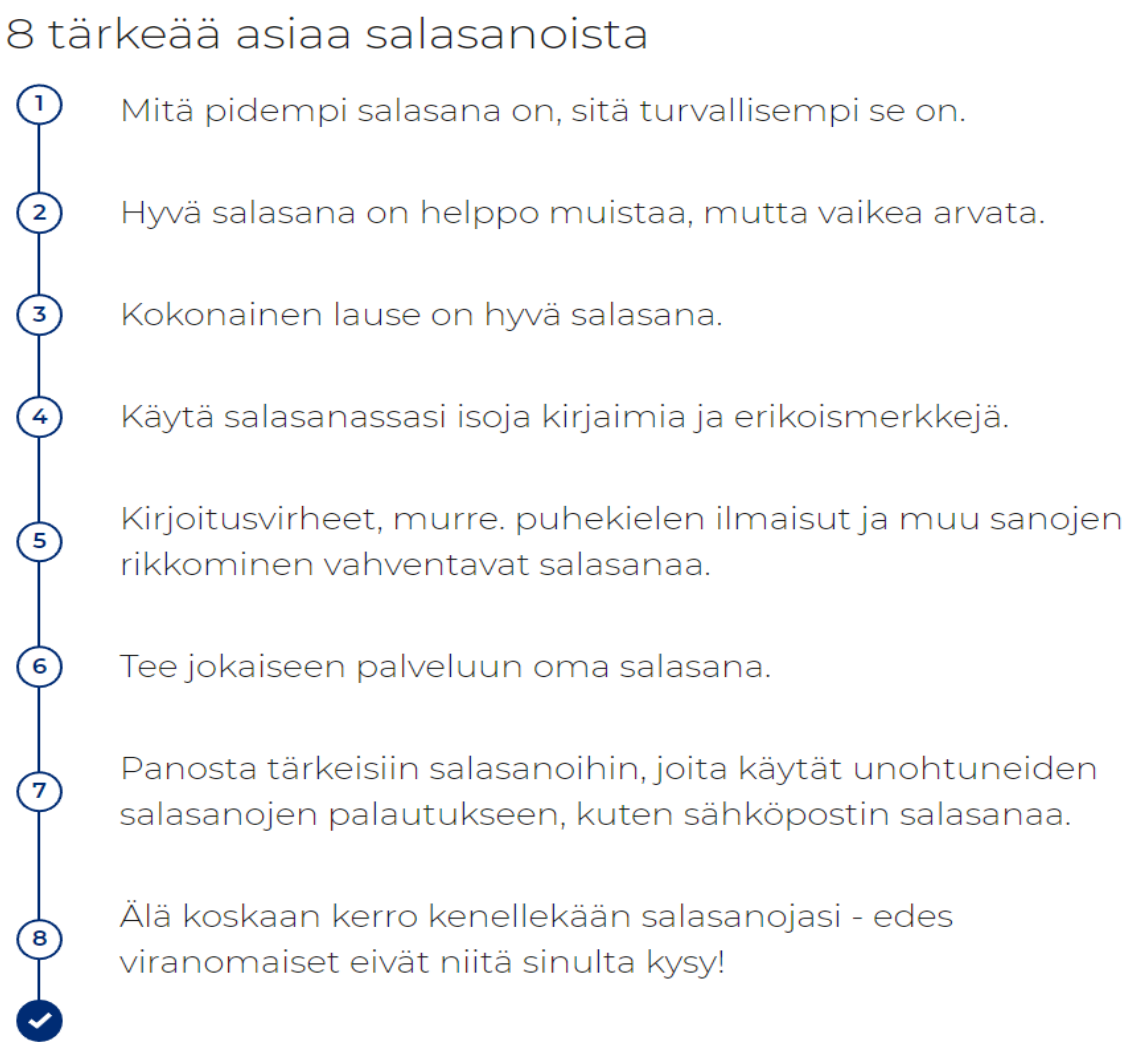
Tietoturvan käyttäjävirheet ovat yleinen syy tietoturvaloukkauksiin tai -murtoihin. Usein käyttäjävirheitä kuitenkin yhdistää yksi asia: huolimattomuus. Esimerkkejä käyttäjävirheistä:

- Salasanat ovat usein heikkoja. Liian yksinkertaiset salasanat, kuten ”Salasana123” ovat helppoja arvata tai murtaa. Käyttäjien tulisi käyttää salasanoja, jotka sisältävät numeroita, kirjaimia

sekä erikoismerkkejä. Huono salasana voi johtaa tietovuotoihin sekä luvattomaan pääsyyn. (Kyberturvallisuuskeskus s.a) Kuvassa 1 on lista hyvästä salasanasta.

- Sähköpostin huolimaton käyttö on yksi yleisistä käyttäjävirheistä. Huijaussähköpostit sisältävät linkkejä tai tiedostoja, jotka yleensä sisältävät haittaohjelmia. Käyttäjien tulisi olla huolellisia sähköpostien avaamisessa sekä olla varovaisia linkkien sekä tiedostojen avaamisessa. (Kyberturvallisuuskeskus 2020)
- Verkkosivut, joilla on epäilyttävä ulkoasu tai ei ole SSL-sertifikaattia, voivat olla haitallisia. Kuitenkin näillä verkkosivuilla oleskelu on yleistä. SSL-sertifikaatit varmistavat, että tiedon siirto verkkosivuston sekä käyttäjän välillä on suojattu sekä salattu. (NordVPN 2021)
- Päivitysten laiminlyönti. Järjestelmäpäivitykset voivat sisältää tietoturvapäivityksiä, ja nämä pitäisi olla ajan tasalla. Käyttäjien tulisi huolehtia päätelaitteensa päivityksistä tai käyttää automaattisia päivityksiä, kun mahdollista. (Kyberturvallisuuskeskus 2020)
- USB-muistitikut voivat sisältää haitallisia ohjelmia, jotka siirtyvät päätelaitteelle, käyttäjän laittaessa tämän tietokoneeseen kiinni.

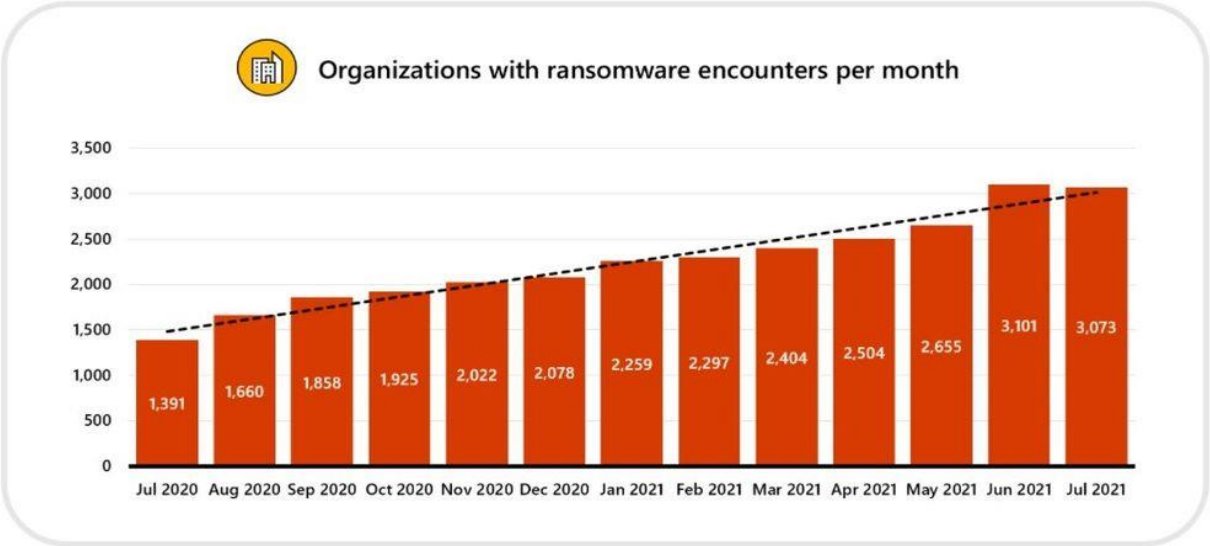
Käyttäjävirheet voivat johtaa ongelmiin, kuten tietovarkauksiin, tietojen menetykseen tai vaikka identiteettivarkauksiin. Käyttäjien tulisi olla tietoisia näistä riskeistä ja noudattaa protokollia, joilla voidaan ehkäistä nämä tietoturvariskit.



Kuva 1. 8 tärkeää asiaa salasanoista (Kyberturvallisuuskeskus 2022)

Englanninkielinen käsite “phishing” on tekniikka, jolla yritetään kalastella tai huijata käyttäjiä antamaan henkilökohtaisia tai arkoja tietoja yleensä sähköpostitse tai puhelimitse. Suomeksi tätä voidaan kutsua tietojenkalasteluksi. Kalastelijat voivat laittaa houkuttelevan tarjouksen tai esiintyä esimerkiksi pankkina, joka pyytää useimmiten napsauttamaan linkin auki tai syöttämään arkaluontoisia tietoja väärennettyyn verkkosivustoon. Tämä on yksi yleisimmistä tietoturva uhkista ja voi johtaa vakaviin seurauksiin. Käyttäjien tulisi olla varovaisia epäilyttävistä viesteistä tai linkeistä. (F-Secure 2023) Organisaatioiden tulisi ottaa käyttöön asianmukaiset tietoturvamenetelmät, kuten tietoturvaohjelmistot tai sähköpostisuodattimet. Usein kalastelusähköpostit sisältävät huonoa suomen kieltä tai erikoismerkkejä.

Ramsonware on haittaohjelma, joka salaa esimerkiksi päätelaitteen tiedostot ja vaatii näiden avaamisesta lunnaita. Suomen kielellä ramsonwarea voi kutsua kiristysohjelmaksi. Kiristysohjelmat yleensä leviävät sähköpostin liitetiedostojen tai haittaohjelmia sisältävän verkkosivun kautta. Parhaita tapoja suojautua ramsonware-hyökkäyksiltä on tiedostojen varmuuskopiointi, virusturva, linkkien sekä sähköpostin varovainen käyttö sekä henkilöstön koulutus tunnistamaan näiden hyökkäysten merkit. (F-Secure 2023) Kuvassa kaksi (kuva 2) visualisoidaan kaaviolla yrityksien kohtaamia kiristysohjelma hyökkäyksiä. Hyökkäyksien määrä on kuukausittain nousussa.



Kuva 2. Organisaatioiden kohtaamat ramsonware hyökkäykset kuukausittain (Barak Klinghofer 2021)

Haittaohjelmat ovat tietokoneohjelmia, joilla pyritään vaikuttamaan päätelaitteen tai verkon toimintaan. Nämä voivat aiheuttaa erilaisia ongelmia, kuten tietojen varkauden, vakoilun, tietojen tuhoamisen tai vaikka laitteen kaatumisen. Haittaohjelmatyyppejä esimerkiksi ovat: virukset, madot, troijalaiset hevoset, adwaret tai vakoiluohjelmat. (Microsoft s.a)

Microsoft 365 tarjoaa useita työkaluja sekä ominaisuuksia, jotka auttavat suojaamaan käyttäjän päätelaitetta ja tietoja. Microsoft Defender on tietoturvaohjelmisto, joka suojaa käyttäjän tietokonetta haittaohjelmilta. Microsoft tarjoaa myös suojatun selaimen, jonka avulla selain estää pääsyn vaarallisille verkkosivuille. Sähköpostiin Microsoft 365 tarjoaa sähköpostisuodatuksen, joka auttaa suodattamaan haitalliset sähköpostiviestit ja estämään näiden pääsyn käyttäjän postilaatikkoon. Tiedostojen varmuuskopiointi onnistuu myös Microsoft Onedrive-palvelun avulla, joka tarjoaa tiedostojen turvallisen tallentamisen pilveen. Tämä mahdollistaa tiedostojen palauttamisen ja niiden turvallisen säilyttämisen. (Microsoft s.a)

Organisaatioiden tietoturvatarpeet ja -vaatimukset vaihtelevat toimialoittain ja organisaation koosta riippuen. (Valtioneuvoston selvitys- ja tutkimustoiminta) Yleisesti ottaen tietoturva on erittäin tärkeä osa organisaation toimintaa, sekä se tulisi ottaa huomioon organisaation strategiassa sekä toimintatavoissa. Kuitenkin tietoturvan tärkeys tulee esille eri lailla, vaikka potilasrekistereistä huolehtivilla yrityksillä, kuin jollain pienyrittäjällä. Tarvetta suurille tietoturvatoimenpiteille ei synny, jos ei ole arkaluontoista tietoa, jota suojata.

2.2 Toimintatavat pilviympäristössä

Tietoturva on tärkeä osa yrityksen toimintaa, koska tämän avulla yritys pystyy suojaamaan liiketoiminnan tärkeitä tietoja sekä vähentää riskejä liittyen tietovuotoihin, tietomurtoihin tai muihin tietoturvauhkiin. Henkilöstön tietoturvatietoisuus ja koulutus ovat keskeisiä tekijöitä yrityksen tietoturvallisuuden kannalta. On tärkeää varmistaa, että työntekijät ymmärtävät tietoturvan merkityksen, noudattavat tietoturvapolitiikkoja ja -ohjeistuksia sekä osaavat tunnistaa potentiaalisia uhkia ja toimia niitä vastaan. Tietoturvakoulutukset ja säännölliset päivitykset auttavat pitämään henkilöstön tietoturvatietoisuuden korkealla tasolla. Lisäksi yrityksen on tärkeää luoda vahva tietoturvakulttuuri, jossa turvallisuus nähdään kaikkien vastuulla. Tietoturvasääntöjen ja -käytäntöjen selkeä viestiminen ja niiden johdonmukainen soveltaminen auttavat edistämään tietoturvanäkökulmaa yrityksen toiminnassa. Henkilöstön tulisi ymmärtää, että tietoturva on osa heidän päivittäistä työtään, ja heidän toimillaan on suora vaikutus yrityksen tietoturvallisuuteen.

Kyperturvallisuuskeskuksen raportin mukaan yrityksen tulisi varmistaa, että kaikilla työntekijöille salasanat ovat vahvoja. Näitä tulisi myös säännöllisesti vaihtaa. Salasanan vaikutus on tietoturvaan suuri, mutta usein vähätelty. Jokaisella käyttäjällä tulisi olla omat tunnukset järjestelmiin eikä yhteisiä käyttäjiä tulisi luoda. Hyvä salasana koostuu vähintään 8–10 merkistä, joka sisältää kirjaimia numeroita sekä erikoismerkkejä. (Kyberturvallisuuskeskus 2022).

Samaa salasanaa ei tulisi käyttää muissa käyttäjätileissä tai palveluissa. Tämä voi johtaa kaikkien käyttäjätunnuksien tietomurtoon. (Marc Dahan 2022) Salasanoja tulisi säilyttää vain näille tarkoitetuissa palveluissa tai paikoissa, eikä näitä tulisi kirjoittaa ylös esim. post-it lapuille työpöydän ääreen. Vahva salasana on merkittävä tapa suojautua tietomurroilta.

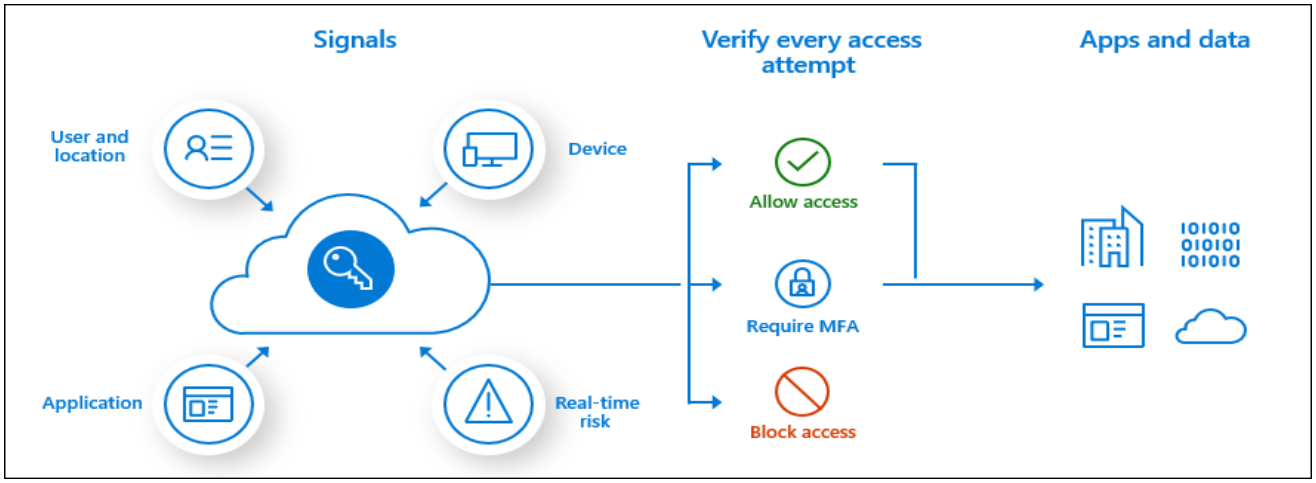
Yrityksissä olevista käyttäytymissäännöistä on pidettävä lujasti kiinni. Yhteisten sääntöjen laiminlyönti voi olla suurikin tietoturvariski. Useimmiten syynä tietoturvakoulutuksen puute tai laiskuus. Käyttäytymissäännöillä tarkoitetaan esimerkiksi tiedostojen varmuuskopiointia oikeaan paikkaan tai salasanojen säilytystä niille kuuluvassa paikassa. Käyttäjätunnuksia ei tulisi lainailla työkavereille

tai päätelaitteen tietoturvapäivityksiä ei saisi laiminlyödä. Pienillä virheillä voi olla suuri vaikutus yrityksen tietoturvaan.

2.3 Tietoturvariskeiltä suojautuminen

Yrityksien tulisi järjestää tietoturvakoulutuksia, jotta työntekijät ymmärtävät tietoturvaan liittyvistä uhkista. Koulutusten tulisi sisältää esimerkiksi tietotekniikan ja tietoturvan perusteita, ennaltaehkäiseviä käytäntöjä, sääntelyvaatimusten noudattamista sekä toimenpiteet tietoturvariskin aiheutuessa. (RSI Security 2021) Koulutusten avulla tietoturvaa pystytään ylläpitämään paremmin, ja turhanpäiväiset virheet eivät jää ainakaan tietämättömyydestä kiinni.

Microsoftin tarjoama Multi-Factor Authentication (myöhemmin MFA) on turvallisuusominaisuus, joka auttaa estämään ei haluttujen henkilöiden pääsyn käyttäjien tileille. (Microsoft s.a) MFA vaatii käyttäjää todentamaan henkilöllisyytensä ennen palveluun päästämistä, jolloin käyttäjä on varmasti tänne sallittu. (Microsoft s.a) MFA auttaa suojatumaan monilta eri tietoturvariskeiltä. Useimmiten nämä kuitenkin ovat phishing-yrityksiä, joissa huijarit yrittävät päästä käyttäjän tilille, tai varastamaan näitä. MFA:n avulla huijarit eivät pääse käyttäjän tilille, vaikka olisivat saaneet tietoonsa tämän salasanan. Kuvassa 3 visualisoidaan MFA:n käyttöä, jossa salasanan lisäksi tarvitaan vielä toinen tunnistautumistapa, ennen kuin käyttäjä pääsee kiinni dataan.



Kuva 3. Multifactor Authentication (Microsoft 2023)

MFA:n käyttöönotto edellyttää, että käyttäjät rekisteröivät vähintään yhden todennusmenetelmän, jolla voidaan todentaa käyttäjän henkilöllisyys. Käyttäjä voi käyttää tähän, vaikka puhelinnumeroa, sähköpostiosoitetta tai Microsoftin omaa autentikointisovellusta. (Microsoft s.a) MFA lisää tiedostojen turvallisuutta huomattavasti. Vaikka kalastelija tietäisi käyttäjätunnuksen salasanan, hän silti tarvitsee vielä toisen tunnistautumistavan, jotta pääsisi tietoon käsiksi. Useimmat sovellukset sekä palvelut myös ilmoittavat, jos joku on yrittänyt kirjautua käyttäjätunnuksellesi, mutta ei ole päässyt sisään.

Virusturva on ohjelmisto, joka suojaa tietokonetta viruksilta tai muilta haittaohjelmilta. Virustorjunta-ohjelmistot perinteisesti skannaavat tietokoneen mahdollisten uhkien varalta, ja ryhtyy toimiin, jos uhkia löytyy. (Ryan Dube 2019) Virusturva ohjelmat ovat nykymaailmassa todella tärkeitä. Nämä lisäävät päätepisteen turvallisuutta suojaamalla tätä haittaohjelmilta, ja varoittamalla huolimattomista toimenpiteistä, joita käyttäjä on mahdollisesti tekemässä.

Microsoftin ratkaisu virusturvalle on Microsoft Defender. Defender on virustorjuntaohjelma, joka tarjoaa suojauksen viruksia, haittaohjelmia sekä muita uhkia vastaan. Defender suorittaa automaattisesti tarkistuksia ja päivittää itsensä uusimpaan versioon turvatakseen, että tietokone on suojattu uusimmilta uhilta. Defenderillä voi suorittaa tarkistuksia, milloin haluaa tai määrittää automaattiset tarkistukset ajastetuiksi. Microsoft Defender myös sisältää verkkosuojauksen, joka varoittaa vaarallisista sivustoista. Tämä myös estää haitalliset lataukset verkkosivuilta. (Microsoft s.a)

EDR eli Endpoint Detection and Response (myöhemmin EDR) tarkoittaa loppukäyttäjien laitteita jatkuvasti valvovaa tietoturvaratkaisua, joka pyrkii havaitsemaan kyberuhkia. (Crowdstrike 2023) EDR tallentaa ja säilyttää loppupisteen käyttäytymistietoja, ja käyttää erilaisia data-analyysitekniikoita epäilyttävän käyttäytymisen havaitsemiseen. EDR tarjoaa tietoturvaan näkyvyyden tapahtumista, joka voisi muuten jäädä huomaamatta. (Crowdstrike 2023) Microsoftin EDR-ratkaisu sisältyy Microsoft Defenderiin, joka myös samalla toimii virusturvana.

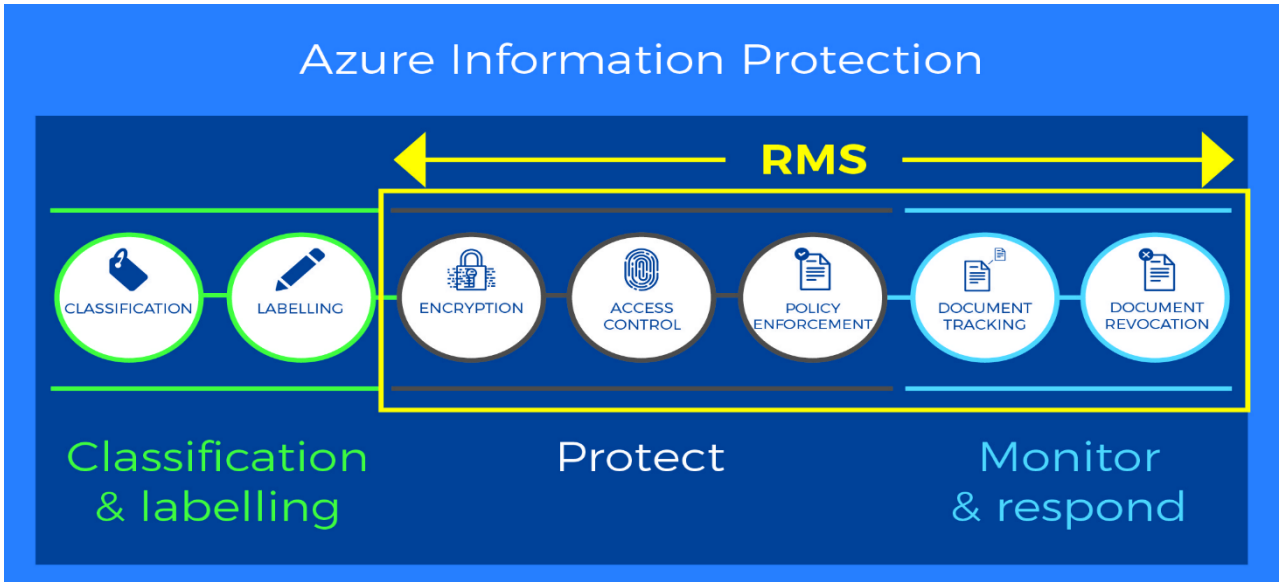
Käyttövaltuushallinta on tietoturvakäytäntö, jolla voidaan hallita käyttäjien pääsyä sovelluksiin tai IT-järjestelmiin. Käyttövaltuushallinta perustuu tunnistautumiseen sekä valtuuttamiseen, joilla voidaan varmistaa, että käyttäjät ovat keitä he ovat sekä, että näille käyttäjille myönnetään asianmukainen käyttöoikeustaso. (Microsoft s.a) Microsoft 365:ssa käyttövaltuushallinta onnistuu Admin Centeristä. Käyttövaltuushallinnalla on suuri merkitys esimerkiksi organisaation tietojen turvallisuuteen.

Käyttäjätilien hallinta ovat osa käyttövaltuushallintaa. Käyttäjätilien tulisi olla yksilöllisiä, jotta näiden seuranta sekä valvominen olisi helpompaa. Jos käyttäjätunnuksella on monta eri käyttäjää, tämän tietoturvaloukkaukset tai väärinkäytökset ovat vaikeampi paikallistaa. Käyttäjätunnuksien yksilöinnillä myös turvataan se, että ei halutut henkilöt eivät pääse heille arkaluonteiseen tietoon. Yksilöllisillä käyttäjillä pystytään varmistamaan myös vastuullisuus. Jos käyttäjät jakavat käyttäjätilejä, on vaikeampi selvittää, kuka on tehnyt mitäkin. Yksilöllisillä käyttäjätunnuksilla on helpompi ja varmempi tapa seurata, että organisaation sisäisiä käytäntöjä sekä vaatimuksia toteutetaan. Yksilölliset käyttäjätilit ovat myös käyttäjän yksityisyyden puolella. Henkilökohtaiset tiedot, kuten nimi, salasana, sähköpostiosoite ovat suojassa muilta käyttäjiltä. Yhteiset käyttäjätunnukset lisäävät myös riskejä tietoturvan kannalta.

Microsoft 365 tarjoaa monia tapoja jakaa tiedostoja turvallisesti ulkoisesti. Microsoft 365:ssa voidaan organisaatiosi tarpeiden mukaisesti rajata oikeuksia. Esimerkiksi Sharepoint-sivuston omistajat voivat jakaa tiedostoja ja kansioita organisaation ulkopuolisten henkilöiden kanssa, mutta sivustolle kutsutut ihmiset eivät. Jakamisen rajoittaminen suojaa organisaation tietoja tietovuodoilta sekä mahdollistaa tiedostojen säilytyksen turvallisesti. Oikeuksien rajoittamisella pyritään estämään tiedon pääsy vääriin käsiin. (Microsoft s.a)

Azure Information Protection (myöhemmin AIP) on Microsoftin tarjoama pilvipohjainen tietoturva- ja tietosuojauspalvelu, jonka avulla voidaan suojata ja hallita organisaation tietoja. (Microsoft s.a) AIP tarjoaa työkaluja tiedon suojaamiseen, luokitteluun, jakamiseen ja seurantaan. (Microsoft s.a) Azure Information Protection sisältyy Microsoft Purviewiin. AIP:n avulla tietoa voidaan luokitella sen arkaluentoisuuden mukaan. Tieto voi olla esimerkiksi julkista, sisäistä tai luottamuksellista. Tämän avulla organisaatiot pystyvät hallita tietoa ja sen jakelua. AIP:n avulla myös tiedon salaaminen ja suojaaminen on mahdollista esimerkiksi käyttöoikeusmäärityksillä ja vesileimoilla. Kuvassa 4 visualisoidaan AIP:n tapoja suojata, valvoa sekä luokitella tietoa. Ensin data luokitellaan, suojataan ja viimeisenä tämän käyttäytymistä tarkkaillaan.

Azure Information Protection vaatii käyttäjiltään lisenssin. Lisenssi sisältyy kuitenkin useisiin Microsoftin lisenssipaketteihin, kuten Microsoft 365 Enterpriseen, Microsoft Mobility + Security-paketteihin ja Microsoft Azure Active Directory Premiumiin. Tarkemmat lisenssiehdot sekä vaatimukset voivat vaihdella käyttäjän sijainnin, organisaation tai käyttötarkoituksen mukaan. (Microsoft s.a)



Kuva 4. Azure Information Protection (Georgina Stockley 2018)

AIP mahdollistaa organisaation luokitella tietonsa sen herkkyyden perusteella. Järjestelmänvalvoja voi esimerkiksi määrittää merkinnän, jolla on säännöt herkkientietojen, kuten luottokorttitietojen

havaitsemiseksi. Merkinnät mahdollistavat tiedon käytön seuraamisen ja hallinnan. Merkinnöillä voidaan myös havaita riskialttiita käyttäytymistä, joiden avulla tietovuodot tai väärinkäytöt voidaan estää. (Microsoft s.a)

Data Loss Prevention eli DLP on osa yrityksen tietoturvaa, joka keskittyy tietojen menetyksen, vuotojen tai väärinkäytön havaitsemiseen ja estämiseen. Organisaatiot käyttävät tätä sisäiseen turvallisuuteen. DLP:n avulla organisaatiot pystyvät estämään luvattoman tiedonsiirron organisaation ulkopuolelle. Tämä myös automaattisesti poistaa ei-toivotut arkaluonteiset tiedot mitä organisaation ulkopuolella voi olla lähtemässä, kuten esimerkiksi henkilötunnuksen tai osoitteen. (Fortinet 2023)

Microsoft toteuttaa DLP:n määrittelemällä ja soveltamalla DLP-käytäntöjä. Käytännöillä voi tunnistaa, valvoa ja suojata automaattisesti arkaluonteisia kohteita eri Microsoft 365 palveluissa, kuten esimerkiksi Teamsissa tai Exchangessa. DLP:n avulla järjestyksenvalvojat saavat hälytyksiä, sen perusteella, jos eri alustoilla jaetaan arkaluontoista tietoa. DLP käytännöillä myös arkaluontoisen tiedon jakaminen voidaan estää. (Microsoft s.a) Microsoft DLP sisältää erilaisia valmiita käytäntöpohjia. Nämä käsittelevät yleisiä vaatimuksia esimerkiksi herkkien tietojen suojaamista eri lakejen mukaisesti. Näitä käytäntöpohjia on mahdollista muokata oman organisaation mukaisiksi. (Microsoft s.a) Esimerkiksi DLP käytäntö voisi estää käyttäjää lähettämästä sähköposteja, jotka sisältä henkilötunnuksia. Toinen käytäntö voisi olla, esimerkiksi sellainen, joka estää käyttäjää lataamasta tietokoneelleen tiedostoja, jotka sisältävät herkkiä tietoja.

Microsoftin DLP sisältyy paketteihin Microsoft 365 E5 Compliance, Microsoft 365 A5 Compliance, Microsoft 365 E5 information protection and governance sekä Microsoft 365 A5 information protection and governance. Yleisimpiin lisenssipaketteihin Microsoft 365 Business Standardiin tai -Premiumiin ei sisälly DLP lisäosaa. Näihin on kuitenkin mahdollista ostaa lisäosa erikseen, joka sisältää DLP:n. (Microsoft s.a)

Varmuuskopiointi on prosessi, jossa tiedot kopioidaan toiseen paikkaan niiden suojaamiseksi. Varmuuskopioinnin avulla pystytään palauttamaan tiedostot, jos näiden alkuperäiset versiot menetetään. Varmuuskopioinnin avulla myös tiedostojen aiempia tiloja voidaan palauttaa, jos tiedot ovat muuttuneet virheelliseksi tai poistettu vahingossa. Pilvikohtaisella varmuuskopioinnilla tarkoitetaan tietojen tallentamista pilvipalveluun, kuten Microsoft OneDriveen. Paikallisella varmuuskopioinnilla tarkoitetaan tietojen tallentamista fyysiselle tallennusvälineelle, kuten USB-muistitikulle tai ulkoiselle kiintolevylle. Tämä tarkoittaa sitä, että varmuuskopiot ovat vain käytössä silloin, kun sinulla on pääsy tallennusvälineelle.

Microsoft ei tarjoa täydellistä varmuuskopiointia. (Microsoft s.a) He tarjoavat oletusasetuksina 30 päivän varmuuskopioinnin, jonka jälkeen tiedostot poistetaan. Tiedostoista luodaan myös

varmuuskopiot, joka 12.tunti. (Microsoft s.a) Tämä voi johtaa ongelmiin, koska usein organisaatiot luulevat järjestelmiensä olevan varmuuskopioituja, mutta näin ei todellisuudessa ole. Olemassa kuitenkin on varmuuskopiointiratkaisuja Microsoft 365 palveluille, jotka ovat säilyttävät varmuuskopiot pidempään.

Lokipalveluilla tarkoitetaan toimintojen seuraamista. Lokitiedot ovat siis tietoa esimerkiksi järjestelmän muutoksista ja käyttötapauksista, mukaan lukien tiedot, että kuka teki, missä teki ja milloin teki. Lokitietoja voidaan käyttää esimerkiksi suorituskyvyn seurantaan, virheiden selvittämiseen tai tietoturvan parantamiseen. Lokitietojen kerääminen ja säilyttäminen voi olla myös lakisääteistä joissakin tapauksissa. (Microsoft s.a)

Security Information and Event Management (myöhemmin SIEM) on turvallisuusratkaisu, joka auttaa organisaatioita havaitsemaan uhkia ennen kuin ne voivat häiritä liiketoimintaa. SIEM yhdistää turvallisuustietojen hallinnan sekä turvallisuustapahtumien hallinnan yhdeksi järjestelmäksi. (Microsoft s.a)

Microsoftin oma SIEM-ratkaisu on nimeltään Microsoft Sentinel. Microsoft Sentinel on pilvipohjainen järjestelmä, joka kerää lokitietoja eri tietolähteistä ja määrittää onko nämä olleet haitallisia. Sentinelin avulla lokitietojen analysointi on siis helpompaa ja järjestelmällistä. Microsoft Sentinel kerää tietoja kaikilta käyttäjiltä, laitteilta, sovelluksilta niin paikan päällä, kuin pilvessä. Tämän avulla pystytään havaitsemaan tuntemattomia uhkia. (Microsoft s.a)

3 M365 Pilviturvallisuus -projektin toteutus

Projektin toteutus on strateginen lähestymistapa liiketoimintalähtöinen eli B2B:n asiakkaiden tietoturvan vahvistamiseen sekä tietojen suojaamiseen Microsoftin sovellusympäristössä. Projektin tavoitteena on hyödyntää tietoperustassa olevaa dataa, jonka avulla Microsoftin ympäristössä oleva turvallisuus paranisi sekä riskienhallinta tehostuisi.

Opinnäyteprojektissa tarkoituksena oli kerätä tietoa Microsoftin tavoista suojata heidän pilvipalvelunsa. Tästä saadun datan perusteella rakennetaan markkinointimateriaalia Microsoftin pilvipalveluista ja, siitä kuinka turvallista datan säilytys heidän pilvipalvelussaan oikeasti on. Tietoperustan rakentamiseen käytettiin internetistä löytyvää dataa, kuten Microsoftin omia verkkosivuja, jotka käyvät perusteellisesti läpi heidän palveluitaan.

3.1 Toimintatutkimuksen toteutus

Opinnäytetyö on tehty B2B Solutions yrityksen toimeksiantona, jossa opinnäytetyöntekijä suoritti kuusi kuukautta kestäneen työharjoittelun. B2B Solutions on pääkaupunkiseudulla toimiva IT-, mobiili- ja tulostuspalveluihin erikoistuva yritys, joka on perustettu vuonna 1993. B2B toimii strategisena IT-kumppanina, josta voi syntyä yrityksesi voimavara. B2B auttaa asiakkaitaan valitsemaan oikeat palvelut sekä turvalliset työkalut, joilla mahdollistetaan IT:n ja asiakirjahallinnan toimivuus. B2B myyntipalvelu tarjoaa yritysasiakkaillensa myös monitoimilaitteet sekä näihin kuuluvat huollot, koulutukset, asennukset sekä käyttötuen. Heille yritykset pystyvät ulkoistamaan ICT-asiat tai vaan yksittäisen osan näistä. (B2B Solutions s.a)

Työtehtävässäni toimeksiantajalla Microsoftin tarjoamien palveluiden sekä työkalujen käyttö oli jokapäiväistä. Työtehtäviin kuului käyttövaltuushallintaa sekä IT-ongelmien ratkontaa. Työtehtävissä myös erilaiset tietoturvariskit, kuten tietojenkalastelut sekä haittaohjelmat tulivat tutuksi. Käyttövaltuushallintaan liittyvissä työtehtävissä käsiteltiin paljon eri Microsoftin lisenssejä, ja eri palveluihin tai työkaluihin kuuluvia oikeuksia. Työtehtäviin kuului myös ohjelmistojen asennuksia sekä mm. MFA:n käyttöönottoja. Ohjelmien sekä työkalujen käytön ohjeistus kuului myös työnkuvaan. Työtehtävien perusteella opinnäytetyön tekemistä on ollut helpompi edistää, koska aihe on tullut tutuksi työn ohella.

Toiminnallisesta tutkimuksesta päätettiin työharjoitteluni loppu päässä. Tätä lähdettäisiin toteuttamaan, kun palaan työharjoittelun loputtua suorittamaan opintoni loppuun. Päätettiin, että työ toteutetaan opinnäytetyöprojektina kevään 2023 aikana, jolloin myös toimeksiantaja, että minä hyötyisin projektista. Projektin toteutus alkoi suunnitteluvaiheella helmikuun lopulla, ja projekti toteutettiin maaliskuun ja huhtikuun 2023 aikana, jossa määriteltiin projektin tavoitteet, laajuus sekä aikataulu.

Tässä myös käytiin läpi B2B:n erityistarpeita ja vaatimuksia, jotta projektin tulevat ratkaisut olisivat räätälöity tarpeiden mukaan. Näitä mm. oli riskien läpi käynti ja Microsoftin ratkaisut ongelmiin.

Kun suunnitteluvaihe oli saatu päätökseen, siirryttiin varsinaiseen toteutusvaiheeseen. Projektin aikataulussa oli varattu aikaa maaliskuun ja huhtikuun 2023 ajalle, jolloin työharjoittelun loppumisen jälkeen palasin opintojen pariin ja keskityin opinnäytetyöprojektin toteuttamiseen. Projektin tavoitteet oli määritelty suunnitteluvaiheessa, mutta toteutusvaiheessa keskityttiin niiden konkreettiseen saavuttamiseen. Toimeksiantajan hyötyjen varmistamiseksi huomioitiin erityisesti B2B-ympäristön erityistarpeet ja vaatimukset. Tämä tarkoitti muun muassa riskien huolellista läpikäyntiä ja tarkastelua sekä Microsoftin ratkaisujen integroimista projektiin. Näin varmistettiin, että tulevat ratkaisut olisivat täysin räätälöityjä vastaamaan tarpeita ja ongelmia.

3.2 Materiaalien läpikäynti

Opinnäytetyön tavoitteena on antaa vastaus pienien tai keskisuurien yrityksien kysymyksiin Microsoft 365 pilven turvallisuudesta. Tuotoksena on siis markkinointimateriaalia, jonka avulla B2B Solutions osoittaa asiakkaillensa tietoturvan sisältö osaamistaan ja siten voi mahdollisesti hankkia uusia asiakkaita tai hoitaa jo olemassa olevia. Markkinointimateriaalien sisällön laajentaminen tietoturva-asian näkökulmasta on tällä hetkellä erittäin ajankohtaista asiakkaille, koko ajan enemmän digitalisoituvassa maailmassa.

Opinnäytetyöprojektin kohderyhmänä ovat pienet ja keskisuuret yritykset, jotka tarvitsevat apua IT-ongelmiinsa. Tämä kohderyhmä koostuu B2B Solutionsin mahdollisista, tai jo olemassa olevista asiakkaista. Nämä yritykset saattavat olla epävarmoja tarvitsemistaan palveluista tai niiden toimivuudesta. Opinnäytetyön tavoitteena on vastata näihin kysymyksiin ja tarjota asiakkaille ratkaisuja heidän nykyisiin ongelmiinsa ja tarpeisiinsa liittyen Microsoftin pilven turvallisuuteen.

Opinnäytetyön lopputulos esittelee B2B Solutionsin tarjoamia palveluita ja samalla vastaa kohderyhmän kysymyksiin. Pienillä ja keskisuurilla yrityksillä voi olla useita syitä ulkoistaa IT-palveluitaan, ja näitä syitä opinnäytetyö voi korostaa. Tällä tavoin se voi houkutella yrityksiä tekemään yhteistyötä B2B Solutionsin kanssa. Yhteistyö mahdollistaa yritysten keskittymisen ydinliiketoimintaansa ja säästää niitä ongelmilta, joihin olisi vaikea löytää ratkaisuja yksin. Markkinointimateriaalin avulla potentiaaliset asiakkaat voivat hyötyä B2B Solutionsin tarjoamista palveluista ja päätyä ratkaisemaan IT-ongelmiaan asiantuntijoiden avulla.

Rajoittavia tekijöitä opinnäytteelle ei ole. Microsoft tarjoaa palveluistaan paljon tietoa, sekä neuvoja, miten näitä tulisi käyttää. Projektin asettamisvaiheessa on määritelty, että markkinointimateriaalin tiedostomuoto on PowerPoint, jota on helppoa jakaa yrityksen sisällä ja sen ulkopuolella.

Opinnäytetyöprojektissa tuottaminen opinnäytetyölle on suunniteltu toteutettavaksi työn ohessa tehtäväksi. Suunnitteilla olisi, että se saataisiin valmiiksi toukokuun loppuun menneeksi.

Resursseja työn tekemiselle on paljon. Internet on täynnä ammatillisia artikkeleita, tiedeartikkeleita sekä muuta yleistä informaatiota, mutta luotettavin lähde on itse näiden palvelun tarjoaja Microsoft. Opinnäytetyössä on suurelta osin hyödynnetty Microsoftin tarjoamia resursseja, jotta varmistetaan luotettavuus ja ajantasaisuus käsiteltävistä aiheista. Näihin resursseihin kuuluvat esimerkiksi Microsoftin tekniset dokumentaatiot, käyttöoppaat ja ohjeet. Niiden avulla on voitu syventyä tarkemmin Microsoftin ratkaisuihin ja niiden käyttöön liittyviin parhaisiin käytäntöihin. He tarjoavat tarkkaa tietämystä, osaamista ja apua palveluistaan sekä palveluilleen. B2B Solutions on tarjoutunut kanssa käymään yhdessä opinnäytetyön etenemistä. Toimeksiantajan kanssa on sovittu viikoittainen palaveri, jossa tarkastellaan työn edistystä ja sisältöä.

Yhteistyö toimeksiantajan kanssa auttaa myös varmistamaan, että työn sisältö vastaa tarkasti toimeksiantajan tarpeita ja odotuksia. Viikoittaiset palaverit tarjoavat tilaisuuden saada palautetta ja ohjausta projektin etenemiselle, mikä edistää työn laadun ja onnistumisen varmistamista. Kaiken kaikkiaan resurssit, kuten Microsoftin tarjoamat lähteet ja B2B Solutionsin asiantuntijuus ja tuki, varmistavat, että opinnäytetyö saa vankan perustan luotettavasta tiedosta ja että työssä käsitellyt aiheet ja ratkaisut vastaavat tarkasti tietoturva-alan vaatimuksia ja tarpeita.

4 Tuloksena markkinointiesite M365 Pilviturvallisuudesta

Opinnäytetyön tuloksena on markkinointimateriaalia yritykselle B2B Solutions. Tämä lopputulos on siis heidän ideansa, kuinka he saisivat opinnäytetyöstä jotain myös itselleen. Myyjät voivat hyödyntää markkinointimateriaalia myyntitapaamisissa, messuilla, seminaareissa ja muissa tapahtumissa. Se auttaa heitä herättämään kiinnostusta potentiaalisissa asiakkaissa ja saamaan heidät harkitsemaan yhteistyötä B2B Solutionsin kanssa. Materiaali voi myös sisältää viittauksia opinnäytetyöhön ja sen tuloksiin, jolloin se lisää yrityksen luotettavuutta ja asiantuntemusta. Näin ollen opinnäytetyön lopputuloksena syntyvä markkinointimateriaali tarjoaa B2B Solutionsille konkreettisen hyödyn omien palveluidensa markkinoinnissa. Se auttaa yritystä hankkimaan uusia asiakkaita ja vahvistamaan asemaansa markkinoilla. Samalla myös opinnäytetyön tekijä hyötyy, sillä hänen työnsä saa käytännön soveltamisen ja näkyvyyden liiketoimintaympäristössä.

4.1 **Projektin eteneminen**

Aihe suunniteltiin yhdessä paikan päällä B2B Solutionsin tiloissa. Tähän päätökseen päästiin melko nopeaa, ja heti aloimme yhdessä suunnitella mitä opinnäytetyön tulisi sisältää. Kirjoitimme ylös muistiinpanot mahdollisesta sisällöstä. Seuraavassa palaverissa kävimme läpi opinnäytetyön sisällysluetteloa, mitä sinne kuuluisi ja mitä ei. Palaverin jälkeen aloin suoraan kirjoittamaan tietoperustaa eri aiheista, joita olimme palaverin aikana suunnitelleet. Tietoperusta oli suunnitelmissa kirjoittaa ensimmäisenä, jotta pohdinta ja empiirinen osuus olisivat helpompia. Itse markkinointimateriaalin teko suunniteltiin, että tämä tehtäisiin koko opinnäytetyön perusteella, eli viimeisenä. Tietoperustaan oli helppo löytää luotettava lähde, koska Microsoft on aiheesta laatinut paljon tietoa omille verkkosivuilleen. Ajatuksena oli siis käyttää näitä.

Opinnäytetyö eteni suunnitellusti ja tavoitteiden mukaisesti. Projektin alussa suoritettiin perusteellinen taustatutkimus tietoperustan aiheista. Näistä oli helpompi kirjoittaa, kun lähteet sekä asia, josta kirjoittaa, oli valmiina. Tietoperustaan suunniteltiin ensimmäisenä kirjoitettavaksi Microsoft 365-ympäristön riskeistä. Tässä vaiheessa käydään läpi eri tietoturvariskejä, ja miten nämä yleensä syntyvät. Lisäksi tutkittiin erilaisia suojaustoimenpiteitä, kuten MFA:ta ja käyttäjätunnusten hallintaa. Seuraavana ajatuksena oli kirjoittaa Microsoftin sisäisiä työkaluja, joiden avulla suojaudutaan tietoturvauhkilta. Näihin kuului esimerkiksi AIP sekä Microsoft Defender. Viimeisenä osa tietoperustaa oli Microsoftin tallennus- ja jakamisratkaisuja, kuten Onedrive.

Opinnäytetyön kirjoittamiseen oli aikaa varattu noin kuukausi, joten työn edistämistä piti tehdä päivittäin. Kuitenkin vaikka aikaa ei ollut varattu hirveästi, ei uskomatonta kiireen tunnetta työtä kirjoittaessa syntynyt. Opinnäytetyön edetessä opettajalle tehtiin välipalautuksia sekä työtä käytiin

näyttämässä toimeksiantajalle Teams videopuheluissa. Näistä saaduilla palautteilla työtä korjailtiin sekä edistettiin.

4.2 Valittu teoria markkinointimateriaalissa

Markkinointimateriaaliin valittiin tietoperustan pohjalta tietoturvariskejä sekä Microsoftin ratkaisuja näihin riskeihin. Toimeksiantaja myös halusi tiettyjä aiheita markkinointimateriaaliin. Näitä aiheita mietittiin markkinointimateriaalin kohderyhmää ajatellen, jotta näistä voisi syntyä mahdollisia asiakkaita. Valitut teoriakohdat auttavat lukijaa ymmärtämään tietoturvanriskejä. Kuitenkin markkinointimateriaalin sisältö perustuu kokonaan tietoperustaan, eikä sisällä tämän ulkopuolelta asioita. Markkinointimateriaali on siis kooste tietoperustasta, joka on tiivistetty PowerPoint kalvoiksi.

Markkinointimateriaali etenee samalla kaavalla, kuin itse opinnäytetyön tietoperusta. Ensin kerrotaan uhkista sekä riskeistä, ja tämän jälkeen mahdollisista toimenpiteistä sekä ratkaisuista. Markkinointimateriaali sisältää siis yleisimmät riskit, kuten käyttäjävirheet ja haittaohjelmat. Tämän jälkeen tarkoituksena on kirjoittaa Microsoftin ratkaisuista sekä yleisistä toimintatavoista, joiden avulla tietoturvauhkia voidaan ehkäistä. Näitä ovat muun muassa Microsoft Defender ja salasana käytännöt. Ideana ei ole käydä PowerPointissa aiheita läpikotaisin läpi, vaan asiakkaalle syntyessä kysymyksiä, voi myyjä mahdollisesti näitä kysymyksiä avata. Markkinointimateriaalilla yritetään luoda mahdolliselle asiakkaalle tarve, jota B2B Solutions voi tarvittaessa täyttää palveluillaan.

5 Pohdinta

Pilvipalvelut ovat yhä suositumpia tapoja tiedon säilyttämiseen, mutta kuitenkin monilla on huoli siitä, onko pilvitallennus turvallista. Tiedon säilyttäminen Microsoftin pilvessä on turvallista sekä hyvä tapa jakaa sekä muokata tietoa, kunhan henkilöstö on koulutettu sekä noudattaa tiettyjä protokollia. Suurin osa tietoturvamurroista johtuu käyttäjävirheistä, jotka olisi helppo kitkeä pois esimerkiksi henkilöstöä kouluttamalla.

5.1 Markkinointimateriaali kohtaa asiakkaan

Opinnäytetyö on ajankohtainen. Koko ajan enemmän digitalisoituneessa maailmassamme, on tärkeää pitää myös turvallisuudesta huolta. Opinnäytetyö käsittelee tietoturvaa, ja osoittaa kuinka tärkeää se on. Lopputuloksena oleva markkinointimateriaali on kuin muistutuslista mahdollisille asiakkaille, joka muistuttaa tietoturvan tärkeydestä. Markkinointimateriaali mahdollisesti luo uusia asiakkuuksia, jos tietoturva asiat eivät ole kunnossa.

Opinnäytetyö tuo esille paljon asiaa tietoturvasta sekä turvallisista toimintatavoista. Nämä ovat tarpeellisia asioita nykypäivän maailmassa. Opinnäytetyö voi markkinointimateriaalin kautta lisätä tietoisuutta tietoturvasta mahdollisille uusille B2B Solutionin asiakkaille. Se tarjoaa myös vastauksia heille ratkaisuista ja helpottaa näiden saavuttamista. Tietoturvamurrot ovat osa melkein jokapäiväistä elämäämme, oli kyseessä jokin huijaussähköposti tai Instagram käyttäjän kaappaus. Opinnäytetyön sisältö voi auttaa tällaisten asioiden ehkäisyssä, antamalla tietoisuutta mahdollisista riskeistä ja vaaroista.

5.2 Tulosten merkittävyys

Opinnäytetyötä voidaan käyttää niin uusien asiakkaiden hankkimiseen, mutta myös oman henkilöstön koulutukseen. Opinnäytetyön sisältö voi mahdollisesti lisätä tietoisuutta myös yrityksen sisällä, jos tätä käyttäisi esimerkiksi koulutusmateriaalina. Opinnäytetyö kuitenkin sisältää paljon asiaa, mitä ei välttämättä, jokapäiväisessä työssä tule vastaan.

Laadulliset kriteerit täyttyvät vasta opinnäytetyön valmistuttua. Opinnäytetyön tavoitteeksi on asetettu asiakashankintaan liittyvä mittari, jolla voidaan mitata työn onnistumista: työn tulos on onnistunut, jos tulosten avulla voidaan edistää mahdollisesti B2B Solutionille uusia asiakkaita. Tällöin opinnäytetyön tuloksena tehty markkinointimateriaali toimii B2B-myyntityössä markkinointimateriaalina, ja jos tästä on myyjille apua uusien asiakkaiden saamisessa, niin siten tiedetään, että markkinointimateriaalin sisältö on onnistunut. Opinnäytetyön tulos myös vastaa mahdollisien asiakkaiden ongelmiin Microsoftin tietoturvasta, joiden avulla nämä pystyvät kartoittamaan ongelmiaan

paremmin. Onnistunut opinnäytetyö tulee käymään läpi Microsoftin palveluita luotettavilla lähteillä ja vastaa asiakkaan kysymyksiin tarvitseeko nämä näitä palveluita.

5.3 Oman oppimisen arviointi

Tämän päivän yhteiskunnassa ja työelämässä tarvitaan koko ajan yhä enemmän jatkuvaa oppimista sekä omaa osaamisen kehittämistä. Oman oppimisen arviointi on tärkeä osa opiskelijan oppimisprosessia, sillä se mahdollistaa tämän kehityksen ja parantamisen. Arviointini perustuu omiin tavoitteisiin, motivaatioon ja oppimistyyliini, mikä mahdollistaa minun tarkastella omaa oppimistani kriittisesti ja kehittää taitojani.

Opinnäytetyön tekemisen aikana oma käsitykseni pilvipalveluista sekä näihin sisältyvistä riskeistä ovat laajentuneet. Riskejä on monia, mutta kuitenkin kyseessä oleva Microsoft 365 pilvipalvelu on turvallinen. Suuri osa virheistä johtuu inhimillisistä virheistä, jotka ei itsessään ole pilvipalveluiden syytä. Myös tiedon etsiminen ja tämän sisältäminen on mielestäni kehittynyt opinnäytetyötä kirjoittaessani. Internet on täynnä tietoa pilvipalveluista ja näihin kuuluvista riskeistä, mutta mielestäni olen valinnut hyvät luotettavat lähteet tietoperustan pohjaksi. Lisäksi projektin aikana tarkasteltiin tarkasti mahdollisia riskejä ja pyrittiin ennakoimaan niihin liittyviä haasteita. Tällainen riskienhallinta auttoi minua oppimaan ja kehittymään projektin aikana.

Oman oppimiseni avulla opinnäytetyön tuloksia voidaan tulla hyödyntämään toimeksiantaja yrityksen tulevissa projekteissa tai muissa oppimisympäristöissä. Tulokset voivat auttaa muitakin oppimaan sekä ymmärtämään paremmin pilvipalveluita ja näiden riskejä. Opinnäytetyö sisältää informaatiota myös yleisesti tietoturvasta, jonka avulla lukija voi mahdollisesti kehittää itseään aiheen parissa. Tämä projekti tarjosi minulle arvokkaan mahdollisuuden soveltaa oppimaani teoriaa käytäntöön ja kehittää käytännön taitojani toiminnallisen tutkimuksen alalla.

Lähteet

Barak Klinghofer. Introducing Microsoft Defender for Endpoint Plan 1. Luettavissa: https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/introducing-microsoft-defender-for-endpoint-plan-1/ba-p/2636641. Luettu 16.5.2023.

Boston University. How To Choose a Strong Password. Luettavissa: https://www.bu.edu/tech/support/information-security/security-for-everyone/how-to-choose-a-strong-password/. Luettu: 22.4.2023.

B2B Solutions. Olemme uuden ajan strateginen IT-kumppani ja yrityksesi voimavara. Luettavissa: https://b2bsolutions.fi/. Luettu 24.5.2023.

Crowdstrike 2022. What is data loss prevention (DLP)? Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 28.4.2023.

Crowdstrike 2023. What is endpoint detection and response (EDR)? Luettavissa: What is EDR? Endpoint Detection & Response Defined (crowdstrike.com). Luettu 27.4.2023.

Fortinet 2023. What is Data Loss Prevention (DLP)? Luettavissa: What is DLP (Data Loss Prevention)? | Fortinet Luettu: 16.5.2023.

F-Secure 2023. Mitä on tietojenkalastelu? Luettavissa: https://www.f-secure.com/fi/articles/what-is-phishing. Luettu: 23.4.2023.

F-Secure 2023. Mikä on ramsonware? Luettavissa: https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack. Luettu: 22.4.2023.

Georgina Stockley 2018. Enhancing Microsoft AIP: What is AIP? Luettavissa: https://www.boldonjames.com/blog/getting-value-from-microsoft-aip-1/. Luettu: 16.5.2023.

Jyväskylän Yliopiston Koppa. Toimintatutkimus. Luettavissa: Toimintatutkimus — Jyväskylän yliopiston Koppa (jyu.fi). Luettu: 24.5.2023.

Jyväskylän Yliopiston Koppa. Havainnointi eli observointi. Luettavissa: Havainnointi eli observointi — Jyväskylän yliopiston Koppa (jyu.fi). Luettu 24.5.2023.

Jyväskylän Yliopiston Koppa. Aiheeseen perehtyminen. Luettavissa: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/tutkimusprosessi/aiheeseen-perehtyminen. Luettu 30.5.2023.

Karelia University. Opinnäytetyön eri muodot. Luettavissa: Opinnäytetyön eri muodot - Karelian opinnäytetyön ohje - LibGuides at Karelia University of Applied Sciences. Luettu 24.5.2023.

Kyberturvallisuuskeskus. Salasanat haltuun. Luettavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf. Luettu 30.5.2023.

Kyberturvallisuuskeskus 2022. Pidempi parempi – Näin teet hyvän salasanan. Luettavissa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan. Luettu 23.4.2023.

Kyberturvallisuuskeskus 2020. 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 24.4.2023.

Kyberturvallisuuskeskus 2020. Muita laitteiden, ohjelmistojen ja sovellusten päivittäminen! Luettavissa: Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen! | Kyberturvallisuuskeskus. Luettu 30.5.2023.

Marc Dahan. Why you should never reuse the same password. Luettavissa: Password Security: Why you should NEVER reuse passwords (comparitech.com). Luettu: 14.5.2023.

Microsoft. What is: Multifactor Authentication. Luettavissa: https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661. Luettu 25.4.2023.

Microsoft. Sovelluksia arjen hallintaan. Luettavissa: https://www.microsoft.com/fi-fi/microsoft-365/buy/compare-all-microsoft-365-products?icid=MSCOM_QL_M365. Luettu 30.5.2023.

Microsoft 2023. Overview of Azure AD Multi-Factor Authentication for your organization. Luettavissa: https://learn.microsoft.com/fi-fi/azure/active-directory/fundamentals/concept-fundamentals-mfa-get-started?view=azurekeyvaultcryptography-2.0.5. Luettu: 16.5.2023.

Microsoft 2023. Set up multifactor authentication for Microsoft 365. Luettavissa: https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide. Luettu: 26.4.2023.

Microsoft. Microsoft Defender for Endpoint. Luettavissa: https://www.microsoft.com/fi-fi/security/business/endpoint-security/microsoft-defender-endpoint. Luettu 27.4.2023.

Microsoft 2023. Microsoft Defender Antivirus in Windows. Luettavissa: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10. Luettu 25.4.2023.

Microsoft 2023. Azure Information Protection (AIP) labeling, classification, and protection. Luettavissa: Identity and Access Management (IAM) Solutions | NordLayer. Luettu: 26.4.2023.

Microsoft 2023. Azure Information Protection service description. Luettavissa: https://learn.microsoft.com/en-us/office365/servicedescriptions/azure-information-protection. Luettu: 28.4.2023.

Microsoft 2023. What is Azure Information Protection? Luettavissa: https://learn.microsoft.com/en-us/office365/servicedescriptions/azure-information-protection. Luettu: 24.3.2023.

Microsoft 2023. DLP policy conditions, exceptions, and actions. Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 25.4.2023.

Microsoft 2023. Lisätietoja tietojen menetyksen estämisestä. Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 29.4.2023.

Microsoft 2023. Securing the Microsoft 365 infrastructure. Luettavissa: Securing the Microsoft 365 infrastructure - Microsoft Service Assurance | Microsoft Learn Luettu: 14.5.2023.

Microsoft 2023. Audit logging and monitoring overview. Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 29.4.2023.

Microsoft 2023. Mikä on SIEM? Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 29.4.2023.

Microsoft. Microsoft Sentinel. Luettavissa: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-conditions-and-exceptions?view=o365-worldwide. Luettu: 29.4.2023.

Microsoft. Mitä haittaohjelmat ovat? Luettavissa: https://www.microsoft.com/fi-fi/security/business/security-101/what-is-malware. Luettu: 23.4.2023.

Microsoft. Mitä on käyttöoikeuksien hallinta?. Luettavissa: Mitä on käyttöoikeuksien hallinta? | Microsoft Security. Luettu 14.5.2023.

Nordlayer. Identity and Acces Management solutions. Luettavissa: Identity and Access Management (IAM) Solutions | NordLayer. Luettu: 25.4.2023.

NordVPN. Mikä on SSL-sertifikaatti? Luettavissa: Mikä on SSL-sertifikaatti? | NordVPN. Luettu: 30.5.2023.

Oppariapu. Dokumenttianalyysi. Luettavissa: DOKUMENTTIANALYYSI – Oppariapu (wordpress.com). Luettu 24.5.2023.

RSI Security. CORE TOPICS FOR EMPLOYEE CYBERSECURITY AWARENESS TRAINING. Luettavissa: Core Topics for Employee Cybersecurity Awareness Training | RSI Security. Luettu: 14.5.2023.

Ryan Dube 2019. What is Antivirus? Luettavissa: What Is Antivirus and What Does It Do? (lifewire.com). Luettu: 14.5.2023

Tammidigital 2022. Käyttäjälähtöiset tietoturvariskit. Luettavissa: https://tammidigital.fi/kayttajalahtoiset-tietoturvariskit/. Luettu: 22.4.2023.

Tietoturvariskienarviointi. Yleistä tietoturvariskeistä. Luettavissa: https://www.tietoturvariskienarviointi.fi/. Luettu: 14.5.2023.

Valtioneuvoston selvitys- ja tutkimustoiminta. Tietojohtaminen ja sen kehittäminen: tietojohtamisen arviointimalli ja suosituksia maakuntavalmistelun pohjalta. Luettavissa: Tietojohtaminen ja sen kehittäminen: tietojohtamisen arviointimalli ja suosituksia maakuntavalmistelun pohjalta (valtioneuvosto.fi). Luettu: 30.5.2023.

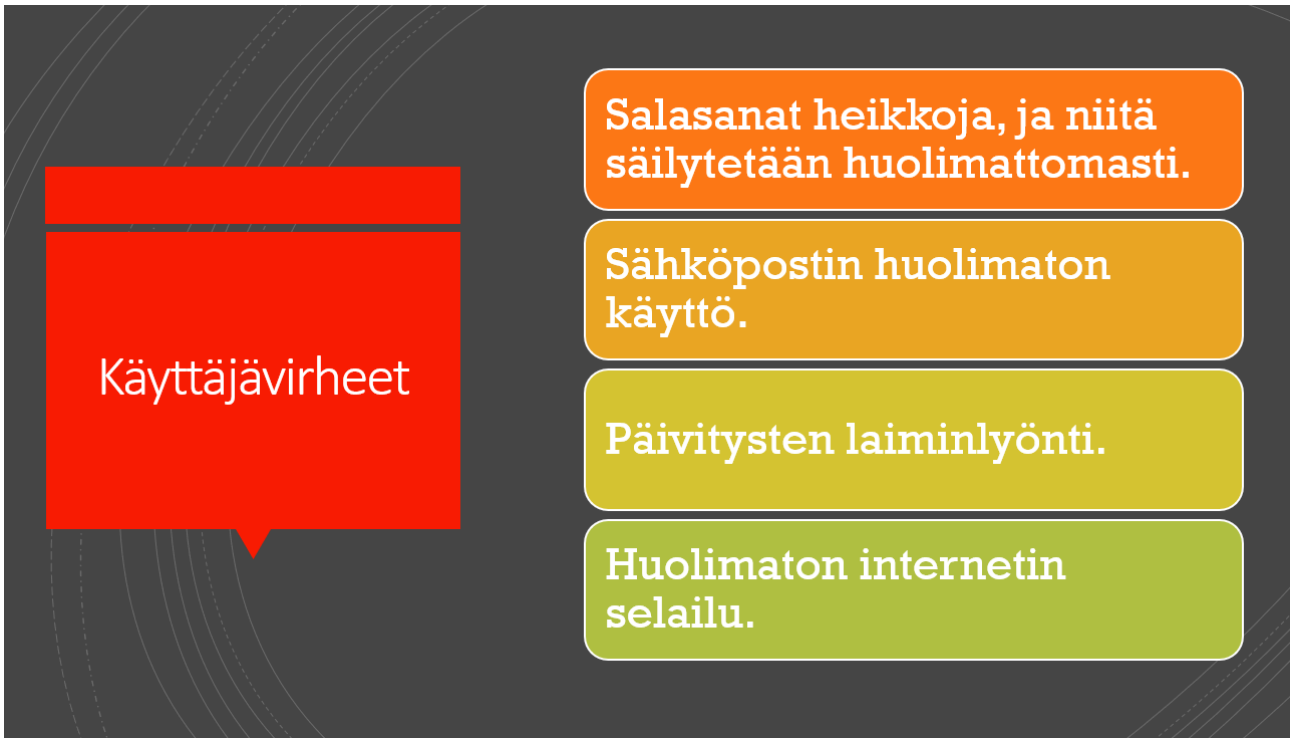
Liitteet

Liite 1. Microsoft 365 pilviturvallisuus (16)

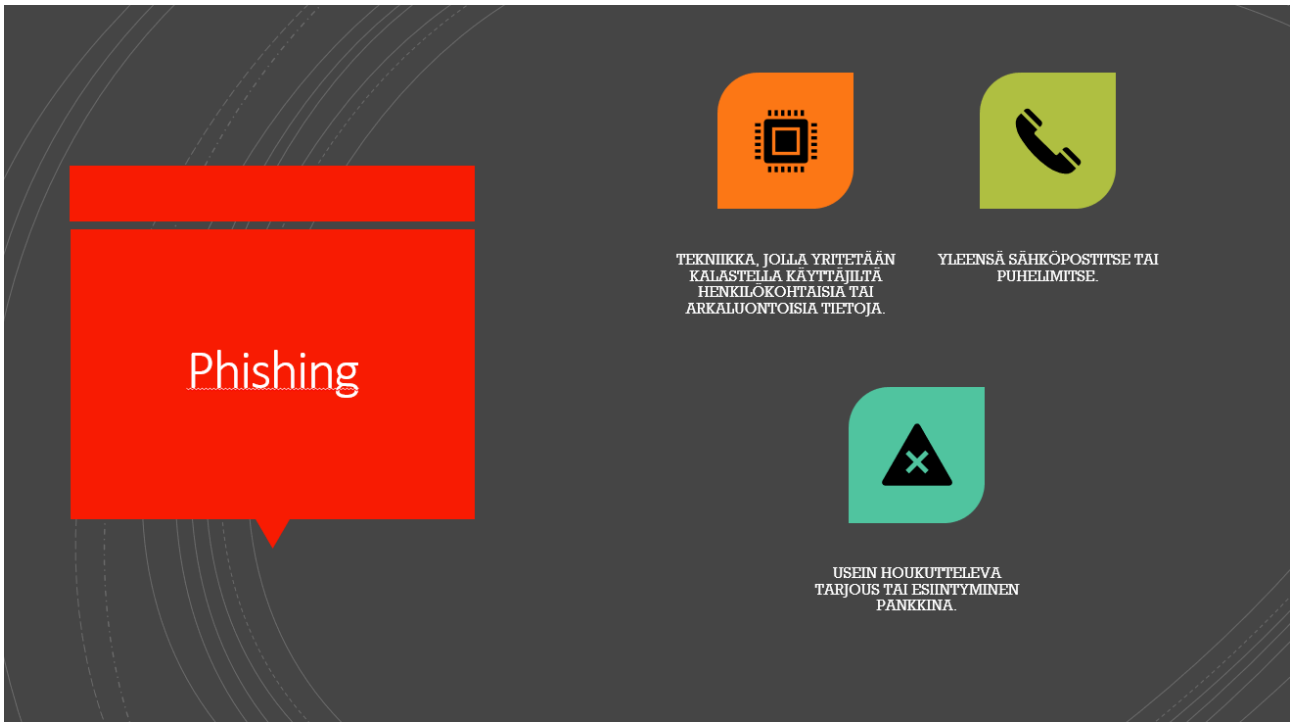
Liite 1. Ensimmäinen kalvo

Liite 1. Toinen kalvo

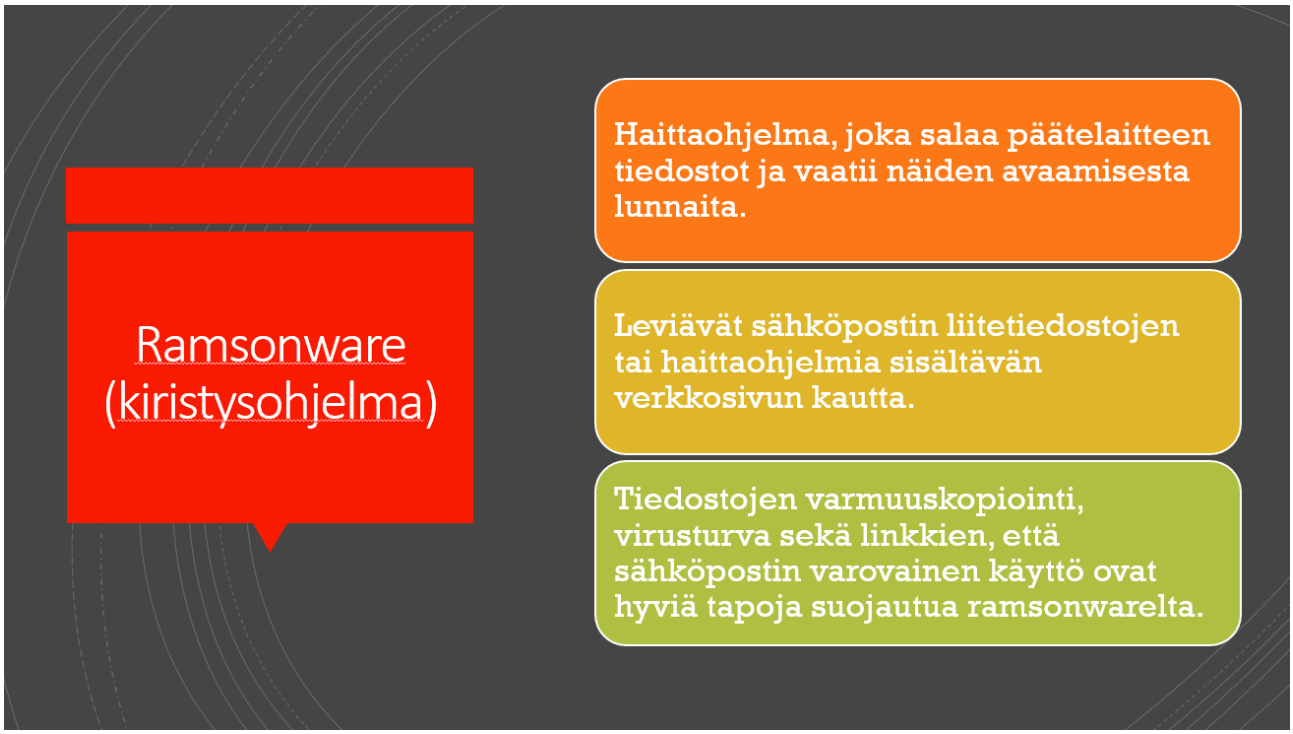
Liite 1. Kolmas kalvo



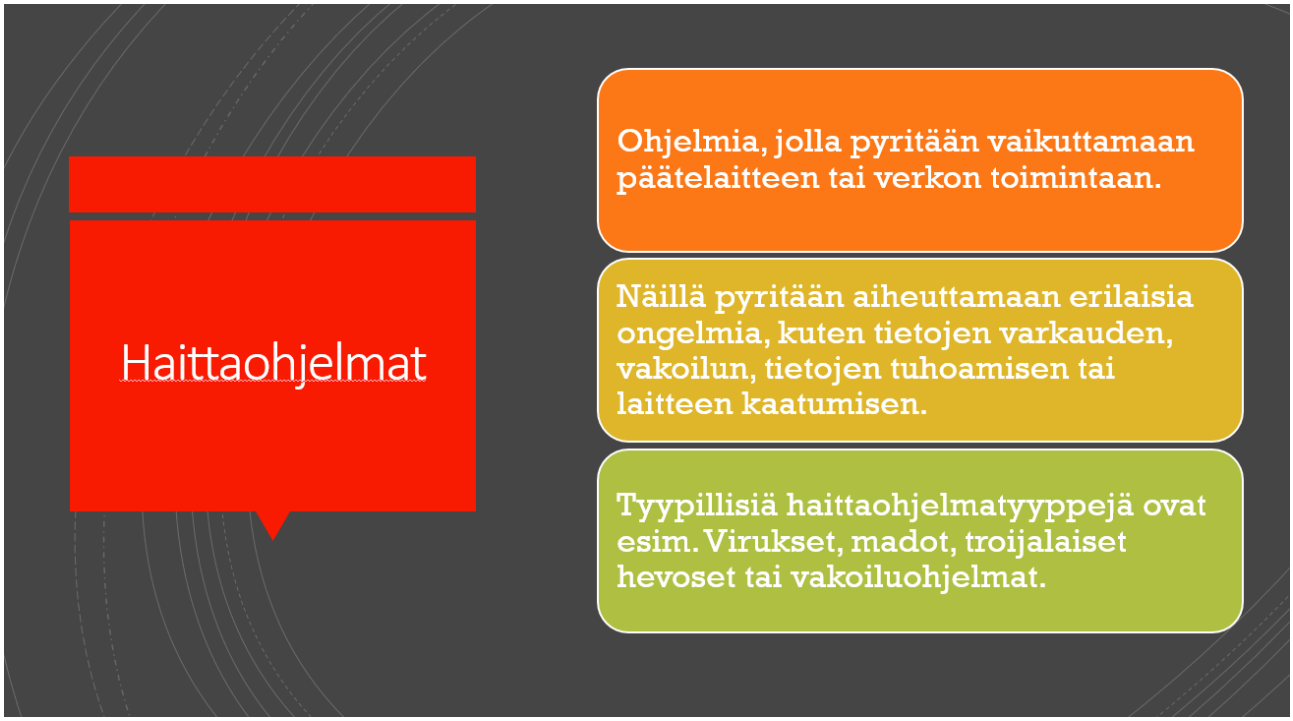
Liite 1. Neljäs kalvo



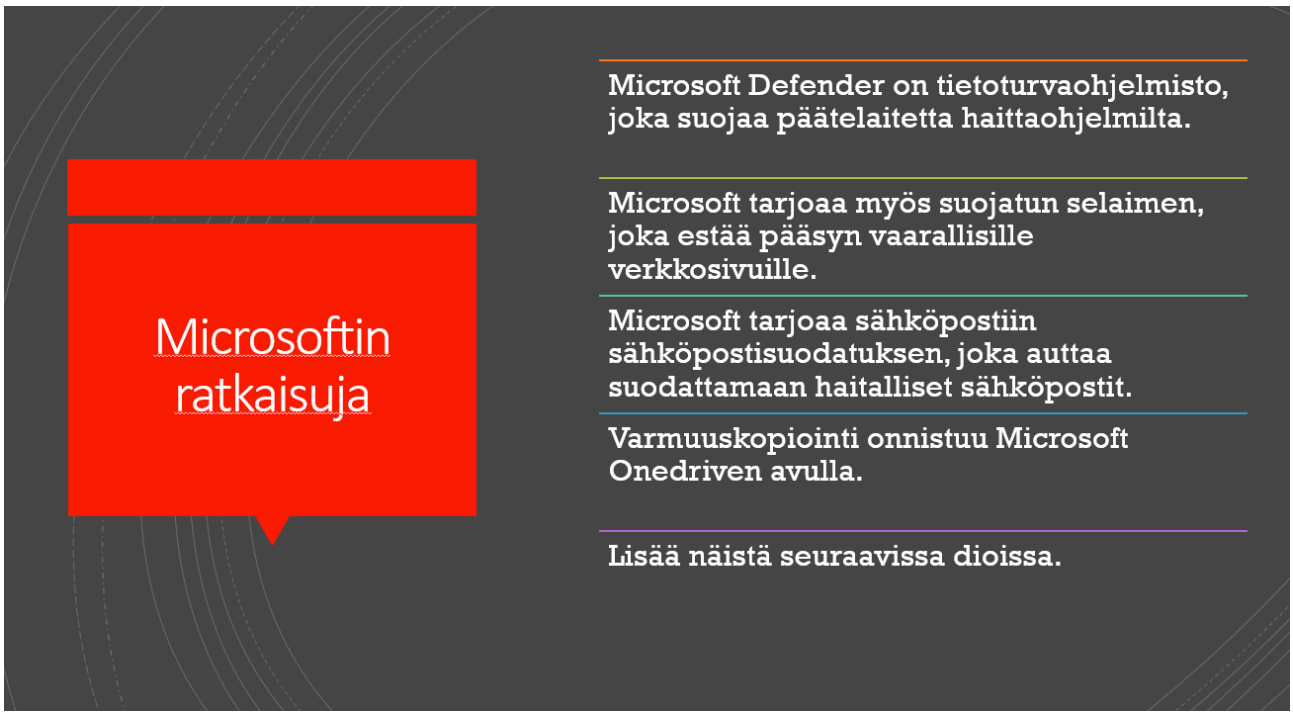
Liite 1. Viides kalvo



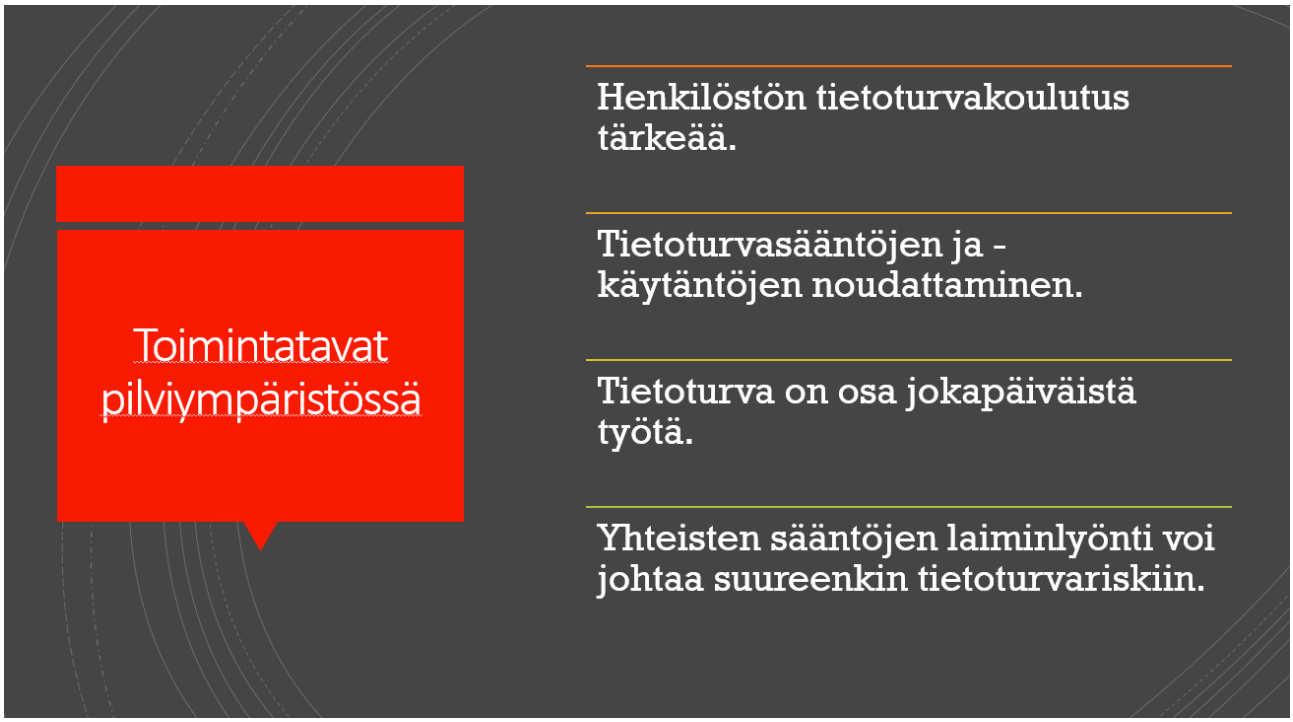
Liite 1. Kuudes kalvo



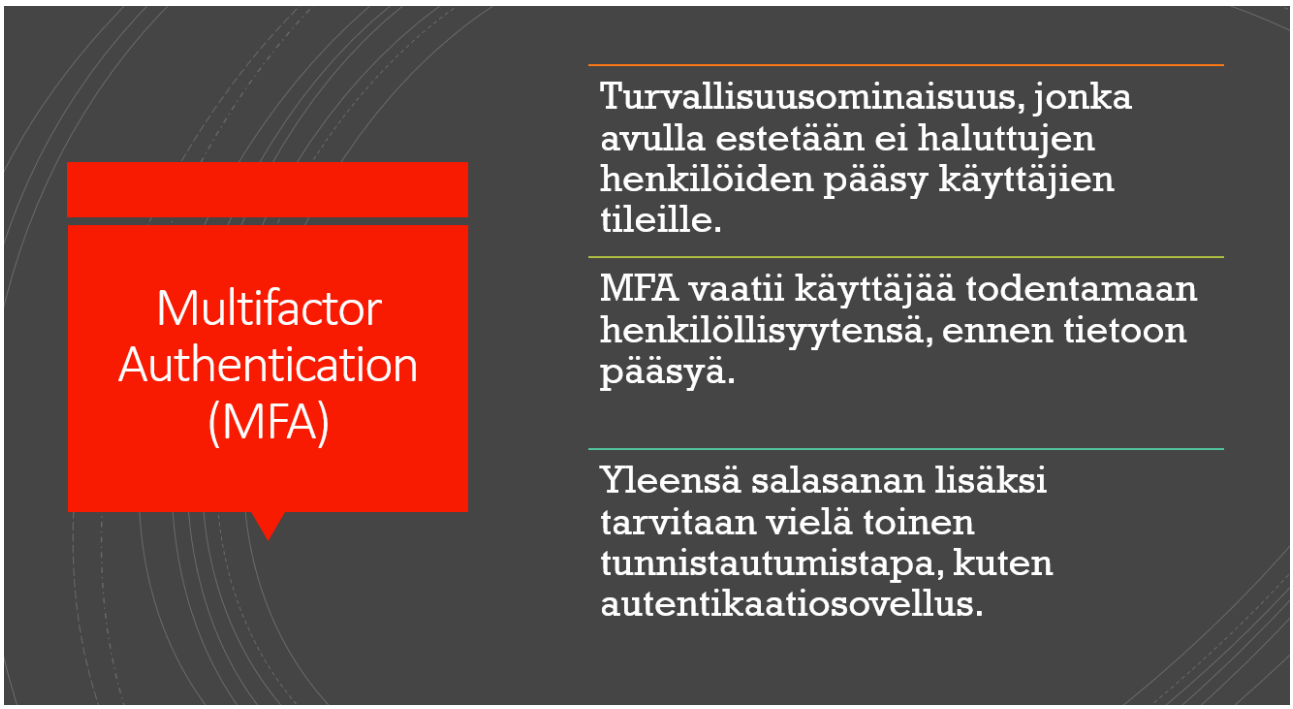
Liite 1. Seitsemäs kalvo



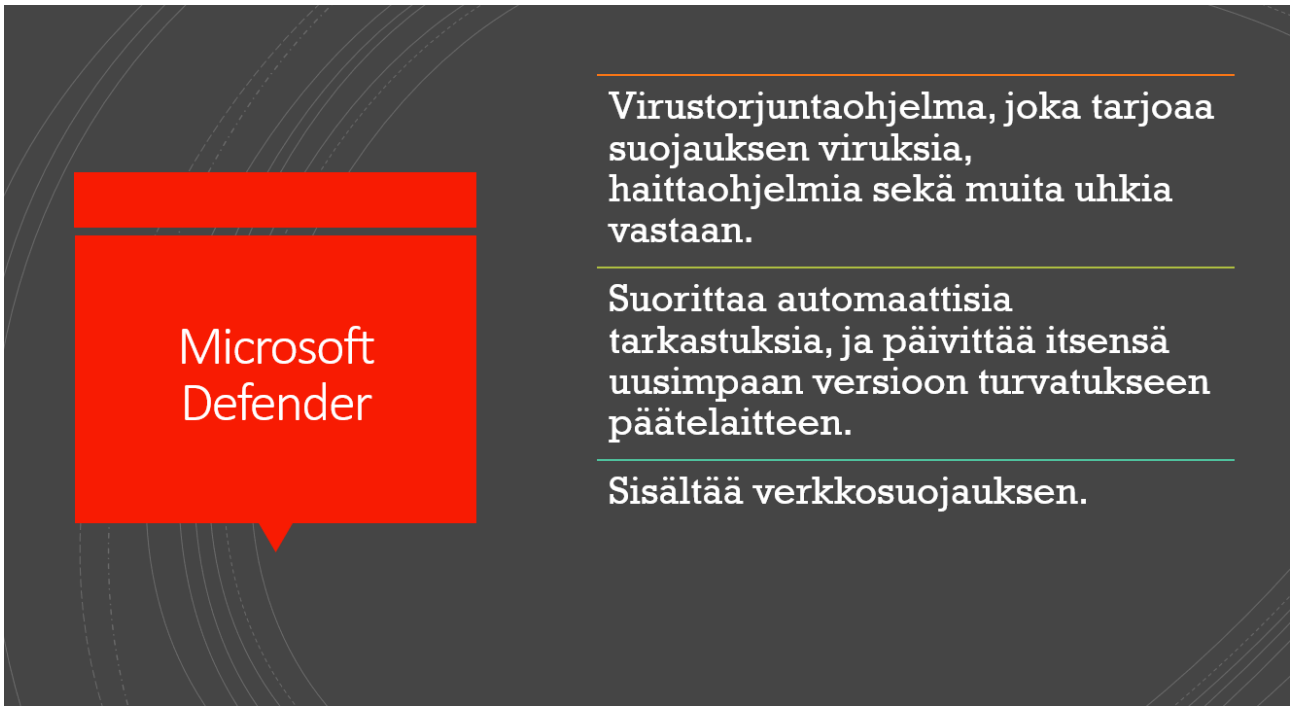
Liite 1. Kahdeksas kalvo



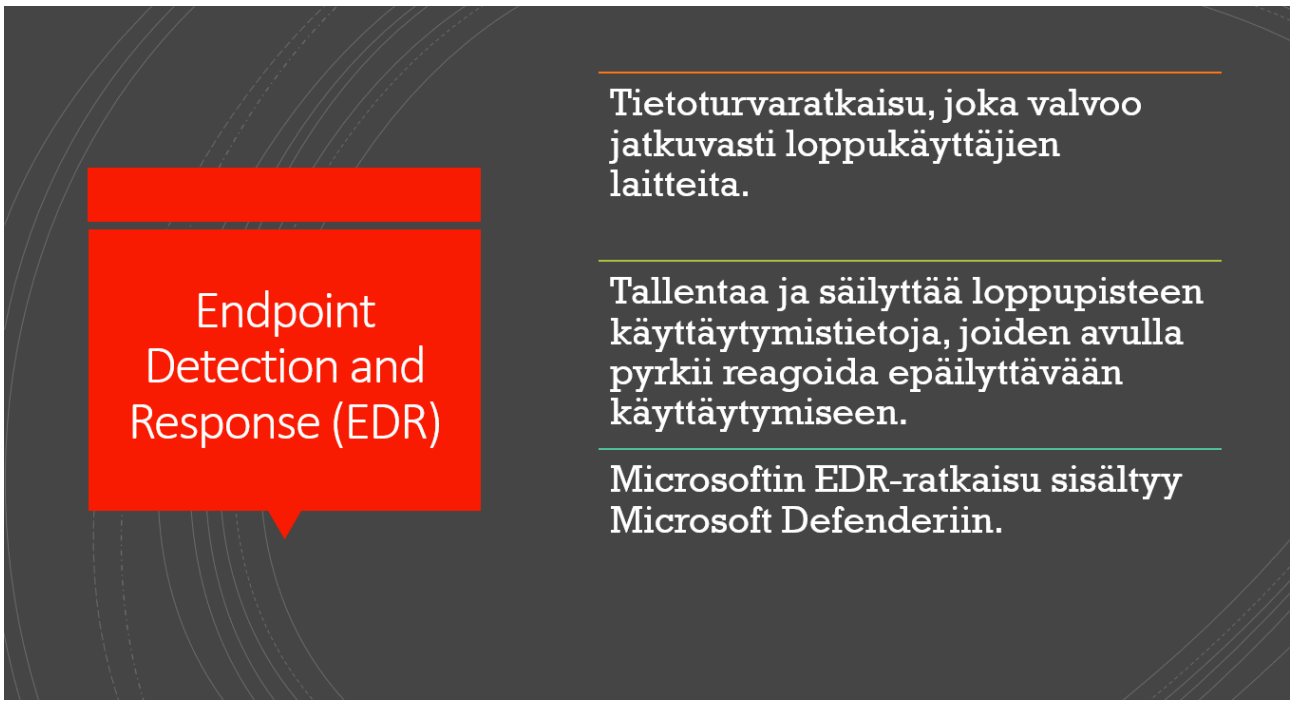
Liite 1. Yhdeksäs kalvo



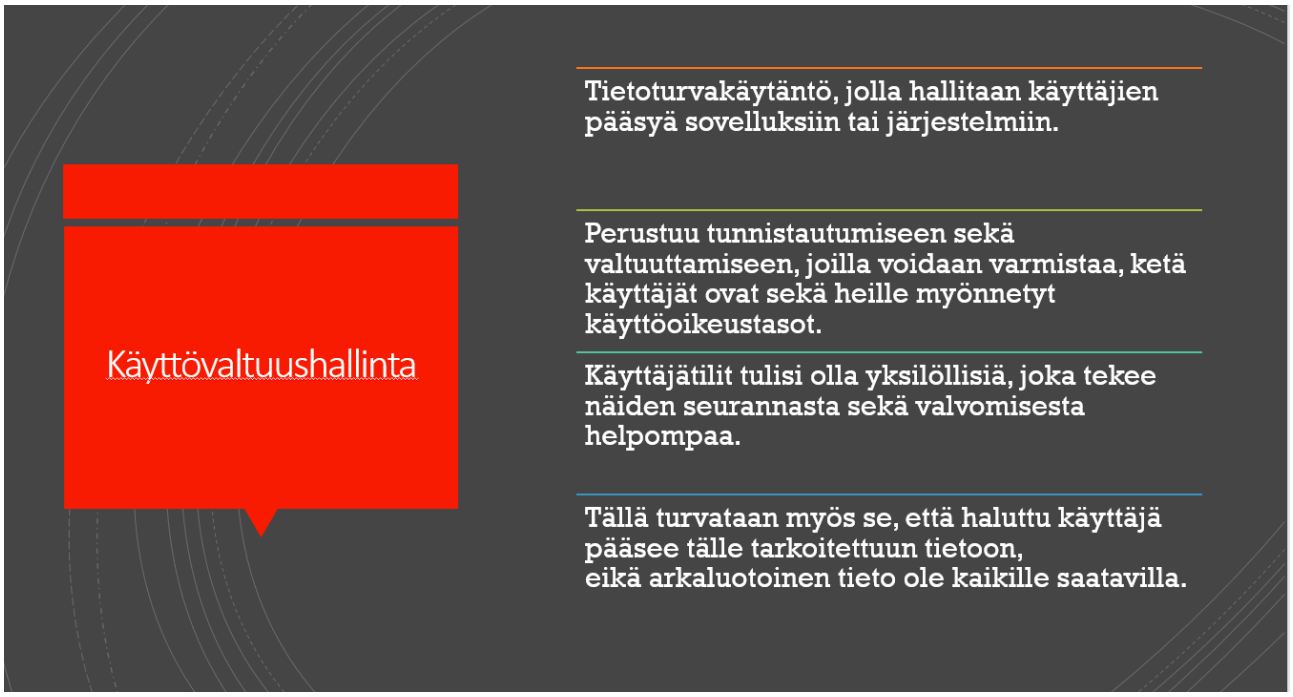
Liite 1. 10. kalvo



Liite 1. 11. kalvo

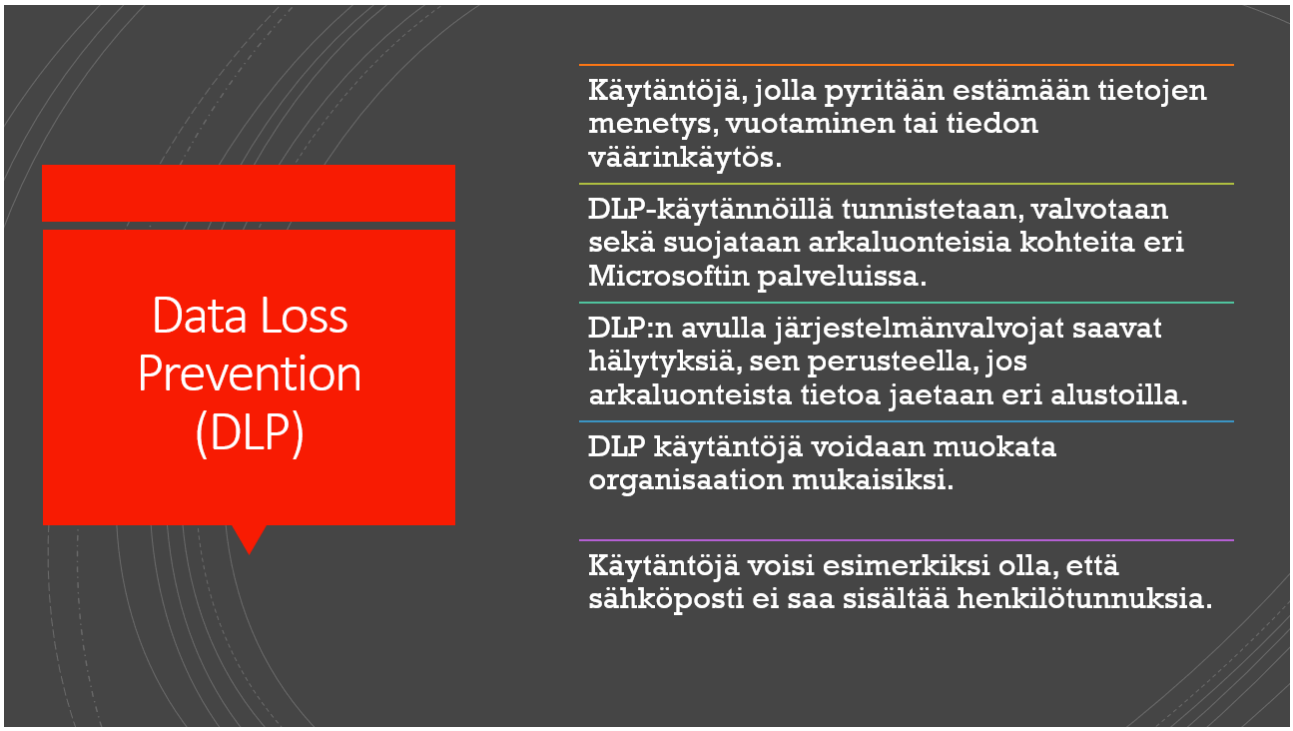


Liite 1. 12. kalvo

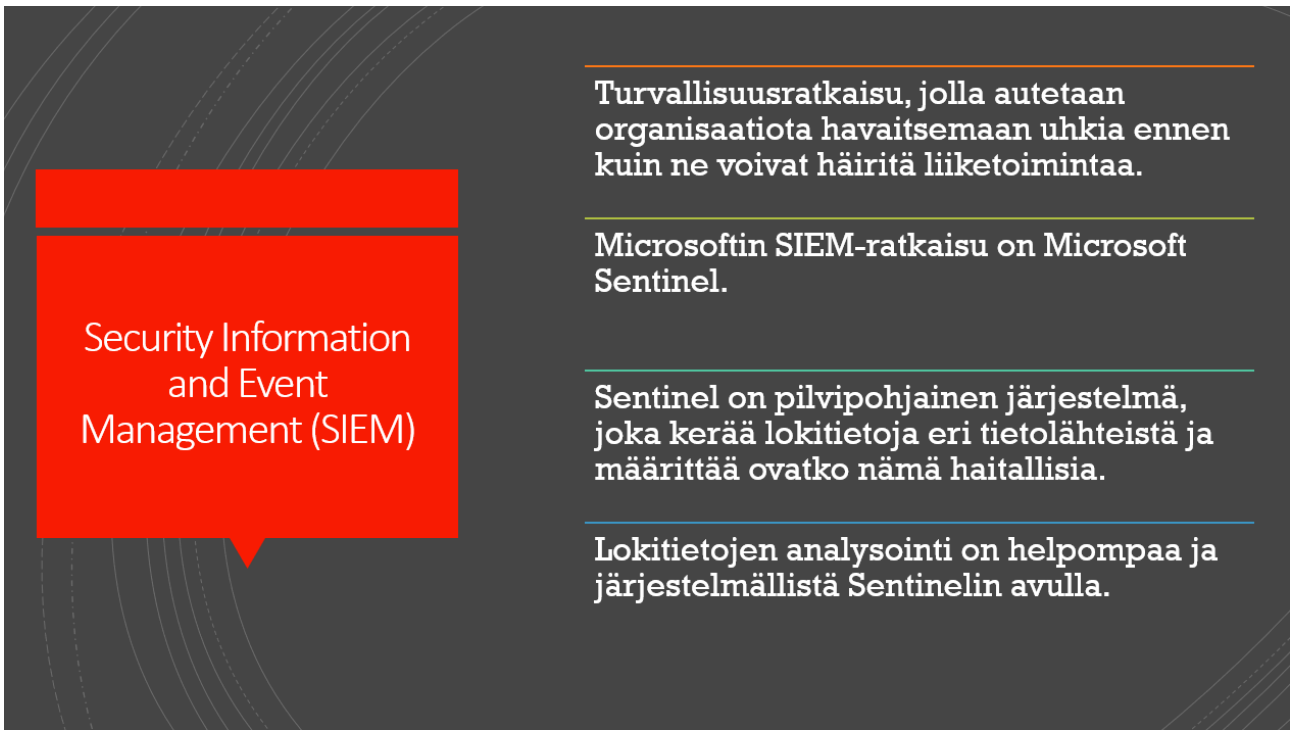


Liite 1. 13. kalvo

Liite 1. 14. kalvo



Liite 1. 15. kalvo



Liite 1. 16. kalvo