



Tiedon luokittelumalli, case elintarviketeollisuus

Mika Arvonen

2020 Laurea

Laurea-ammattikorkeakoulu



Tiedon luokittelumalli, case elintarviketeollisuus

Mika Arvonen
Tulevaisuuden innovatiiviset
digitaaliset palvelut
Opinnäytetyö
Joulukuu, 2020

Mika Arvonon

Tiedon luokittelumalli, case elintarviketeollisuus

Vuosi

2020

Sivumäärä

47

Opinnäytetyön tavoitteena oli kehittää elintarviketeollisuudessa toimivalle organisaatiolle tiedon luokittelumalli perustuen teknologian hyväksikäyttöön.

Kehittämistehtävässä kartoitettiin haastatteluilla kerätyn aineiston sekä tutkimuskirjallisuuden avulla tunnistamaan parhaat käytännöt luokittelumallin tueksi. Tutkimusstrategiana oli tapaustutkimus, jonka tiedonkeruumenetelmänä olivat haastattelut. Tutkimuksen tueksi haastateltiin kuutta konsulttia kolmesta eri IT palvelualan yrityksestä. Haastateltavat valittiin sillä perusteella, että tunsivat riittävästi kohde organisaation liiketoimintaa ja prosesseja.

Työ nosti esiin kokemuksia muiden organisaation luokittelumallien hyviä ja huonoja ominaisuuksia ja kokemuksia niiden käyttöönotosta. Haastattelujen myötä myös selvisi, että monissa organisaatioissa tiedon luokittelu on jo käytössä. Tämä korostaa työn merkitystä ja tarpeellisuutta entisestään kohde organisaatiossa.

Opinnäytetyön kehittämis ehdotuksena on luokittelumalli kohde organisaation käyttöön. Mallissa on pyritty mahdollisimman kattavasti huomioimaan haastattelujen perusteella kootut parhaat käytännöt.

Mika Arvonien

Data Classification Model, Case Food Industry

Year

2020

Pages

47

The aim of the thesis was to develop a technology-based information classification model for an organization operating in the food industry.

In this development work, the material collected through interviews and research literature were mapped to identify best practices to support the classification model. The research strategy was a case study based on interviews. To support the study, six consultants from three different IT service companies were interviewed. Interviewees were selected on the basis that they had enough knowledge of the target organization 's business and processes.

The work highlighted experiences with the good and bad features of other organizations' classification models and experiences with their implementation. The interviews also revealed that the classification of information is already in use in many organizations. This further emphasizes the importance and necessity of the work in the target organization.

The proposal for the development of the thesis is a classification model for the use of the organization. In the model, the best practices gathered based on the interviews have tried to be considered as comprehensively as possible.

Keywords: cyber security, data classification, data labeling

Sisällys

1	Johdanto.....	7
2	Case yritys, nykytila ja tutkimuksen tavoitteet.....	7
2.1	Tutkimus- ja kehitystehtävän määrittely	8
2.2	Nykytila	8
2.3	Tavoitteet	8
2.4	Tutkimuskysymykset ja rajaukset.....	8
2.5	Opinnäytetyön rakenne	9
3	Tutkimusstrategia - tapaustutkimus	9
3.1	Perustelut menetelmävalinnalle	10
3.2	Haastateltavien valitseminen	10
3.3	Haastatteluiden toteutus	10
3.4	Analyysi ja tulkinta	11
4	Tietoturvan peruskäsitteet.....	11
4.1	Saatavuus.....	11
4.2	Eheys.....	12
4.3	Luottamuksellisuus.....	13
4.4	Todennus	13
4.5	Kiistämättömyys.....	14
5	Tieto suojattavana kohteena	14
5.1	Mitä tieto on	14
5.2	Miksi tietoa on suojeltava.....	15
5.3	Millaista tietoa on suojeltava.....	15
5.4	Tiedon elinkaari	16
5.5	Lainsäädännön ja asetusten vaikutus tietojen suojaukseen	16
5.6	Liike- ja ammattisalaisuudet	18
6	Tiedon luvattoman käytön seurauksia.....	19
6.1	Tiedon yksinoikeuden menetys.....	19
6.2	Tiedon luottamuksellisuuden menetys	19
6.3	Rikoksen tekijän saama taloudellinen hyöty	19
6.4	Tietomurron seurauksena kuluva aika, raha ja maineen menetys	20
7	Suojattavien tietojen luokittelu	20
7.1	Tiedon luokat	20
7.2	Microsoftin oletusluokat tiedolle	21
8	Teknologia luokittelun tukena.....	23
8.1	Azure Information Protection	23
8.2	Azure Information Protection luokkinen käyttäminen	26
9	Haastattelututkimus	29

9.1	Tiedon luokittelumallin käyttöönoton tarpeellisuus kohde organisaatiossa.	30
9.2	Muiden organisaatioiden tiedon luokittelun tilanne.....	31
9.3	Teknologian hyväksi käyttäminen tiedon luokittelussa	32
9.4	Automaattinen luokkien salaus.....	33
9.5	Suosittelut tiedon luokat	35
9.6	Tutkimuksen validiteetti ja reliabiliteetti.....	37
10	Luokittelumalli kohdeorganisaation käyttöön	38
10.1	Tiedon luokat	38
10.2	Luokan merkitseminen	39
10.3	Luokkien käsittelysäännöt	39
10.4	Jatkotutkimusehdotukset	40
	Kuviot	44
	Taulukot	44
	Liitteet	45

1 Johdanto

Kaikkien yritysten tavoitteena on kannattava liiketoiminta. Yritysten toimintaympäristö on muuttunut haasteellisemmaksi globalisaation myötä. Tietoturvan osalta yritysten tietojen siirtyminen pilvipalveluihin on osaltaan muuttanut perinteisiä suojauskäytäntöjä sekä tuonut lisävaatimuksia tiedon ja tietoturvan hallintaan. Turvallisuus on entistään tärkeämpää parannettaessa tuottavuutta, kehittäessä yrityksen kilpailukykyä ja asettaessa liiketoiminnan tavoitteita. Liiketoiminnan tavoitteiden tulee aina ohjata yrityksen turvallisuustyötä. Kilpailukyky ja turvallisuus eivät ole toistensa vastakohtia, vaan turvallisuus on kilpailukyvyn keskeinen ja tärkeä edellytys ja osa laadukasta liiketoimintaa ja sen johtamista.

Yrityksen tietopääomasta huolehtiminen kuvaa yrityksen hyvää tietojenkäsittelytapaa ja -kulttuuria. Kaikille yrityksille tieto ja siitä huolehtiminen asianmukaisesti on ensiluokkaisen tärkeää. Ongelman saattaa muodostaa se, että tietoihin ja tietojen käsittelyyn liittyviä riskejä ei tunnisteta riittävällä tarkkuudella.

Tietoturvallisen toiminnan edellytyksenä on se, että yrityksessä tunnistetaan toiminnan kannalta merkitykselliset ja suojeltavat tiedot ja kohteet. Kohteita ovat muun muassa yrityksen tuottamat ja käsittelemät tietoa-aineistot, sen käyttämät tietotekniset ohjelmistot ja palvelut, tietojenkäsittelylaitteet ja tilat, joissa edellä mainittuja kohteita käsitellään ja säilytetään. Kohteiden tunnistamisen jälkeen on mietittävä ja sovittava, miten kohteet suojataan, kuka miten kohteita saa käsitellä, miten ja koska kohteiden tulee olla saatavilla ja varmistetaan, että kohteiden sisältämä tieto pysyy oikeellisena ja muuttamattomana.

2 Case yritys, nykytila ja tutkimuksen tavoitteet

Kehityskohteeksi valittu yritys on merkittävä kotimainen elintarviketeollisuuden toimija. Yrityksellä on tuotantolaitoksia Suomessa 12 paikkakunnalla sekä tytäryhtiöt Ruotsissa, Venäjällä, Virossa, Yhdysvalloissa ja Kiinassa. Yrityksen Suomessa myytävät tuotteet ovat aina valmistettu Suomessa ja niihin käytetään vain suomalaista pääraaka-ainetta. Yrityksen liikevaihto vuonna 2018 oli noin 1 800 miljoonaa euroa. Suomessa yritys työllistää noin 3400 eri alojen ammattilaista ja tytäryhtiöissä työskentelee noin 1000 henkilöä kolmessa eri tuotantolaitoksessa ja myyntikonttoreissa. Yrityksen tuotteita viedään noin 60 maahan ympäri maailman, ja vienti kattaa noin neljänneksen koko Suomen elintarvikeviennistä. Vienti sisältää kuluttajalle suunnattujen kaupassa myytävien elintarviketuotteiden lisäksi elintarviketeollisuudelle suunnattuja raaka-aineita.

Yrityksen tuotekehityksellä on pitkät ja vahvat perinteet, joiden vakiintuneena ajatuksena on ihmisten hyvinvoinnin lisääminen. Yritys tekee tieteestä arkea ja elämää parantavia tuotteita.

Yrityksen innovaatioilla on 350 patenttia ympäri maailman. Yrityksen tuotevalikoimaan kuuluu noin 1000 tuotetta ja vuosittain se lanseeraa yli 100 uutuustuotetta.

2.1 Tutkimus- ja kehitystehtävän määrittely

Yrityksessä on käynnissä tietojen luokitteluhanke. Tämä tutkimustyö on osa hanketta ja tutkimustyön tuotoksena syntyy ehdotus tietojen luokittelumallista yritykselle.

Projektityössä otetaan myös kantaa tiedon omistajan tehtäviin ja vastuisiin, turvallisuusluokkien määrittelyyn ja niiden nimeämiseen ja merkitsemiseen sekä luokkien mukaiseen käsittelyyn ja periaatteisiin.

2.2 Nykytila

Viimeisten vuosien kuluessa yrityksessä on otettu laajasti käyttöön pilviteknologioihin perustuvia tiedonkäsittelyn ja -hallinnan palveluita. Nämä modernit teknologiat ovat muuttaneet olennaisilta osin perinteisiä tiedon suojaamisen menetelmiä. Aiemmin yrityksen käsittelemä ja hallinnoima tieto on pääsääntöisesti sijainnut sisäverkossa ja sen suojaaminen ulkopuolisilta on ollut helposti toteutettavissa perinteisillä palomureilla. Pilvipalveluissa tietoa tallennetaan yrityksen sisäverkon ulkopuolelle palveluntarjoajien kapasiteettiin. Myös tiedon jakaminen ulkopuolisille on entistäkin yksinkertaisempaa pilvipalveluissa. Tästä syystä on äärimmäisen tärkeää, että yrityksen tietopääoma on luokiteltu sen kriittisyyden mukaan ja eri luokille on olemassa erilaiset käsittelysäännöt. Yrityksessä on ollut käytössä erilaisia tiedon luokittelua ja niiden merkitsemisen käytäntöjä. Näitä ei kuitenkaan ole ohjeistettu riittävällä laajuudella tietojä käsittelyäälle henkilöstölle.

2.3 Tavoitteet

Ennen opinnäytetyön aloittamista keskustelin aiheesta tietohallintojohtajan kanssa ja tulimme siihen tulokseen, että ehdotus tietojen luokittelumallista on hyvä aihe kehittämistehtävälle sekä yritykselle tärkeä ja ajankohtainen aihe. Tavoitteeksi asetin riittävän yksinkertaisen mallin tuottamisen, joka perustuu käytössä oleviin osittain automatisoituihin teknologioihin helpottaen tiedon luoja ja tietojen käsittelijöiden vastuita ja velvollisuuksia. Tavoitteena on luoda kaikkia yrityksen toimintoja palveleva malli, joka on käyttöönotettavissa kaikissa toimintamaissa. Lisäksi tavoitteena on yrityksen toiminnan jatkuvuuden suojaaminen ja sen tietopääoman turvaaminen alati muuttuvassa ja nopeasti uusiutuvassa maailmassa.

2.4 Tutkimuskysymykset ja rajaukset

Tutkimuksen ongelmana on:

- Millaisilla tiedon luokilla ja käsittelysäännöillä voidaan turvata yrityksen tietopääoma?

Tutkimusongelmaa selvitetään tarkemmalla tutkimuskysymyksellä:

- Miten käytössä oleva teknologia auttaa ja helpottaa tiedon luokittelua ja tiedon käsittelysääntöjä?

Tämä tutkimustyö ei ota kantaa ehdotetun luokittelumallin käytön jalkautukseen organisaatiossa. Tämän tutkimustyön tuotos painottuu suurimmaksi osaksi pilviympäristöissä sijaitsevien tietojen luokitteluun perustuen Microsoftin teknologioihin. Osa käsiteltävistä teknologioista saattaa vaatia käyttäjäkohtaisia lisenssejä, joita organisaatiolla ei toistaiseksi ole käytössä.

2.5 Opinnäytetyön rakenne

Opinnäytetyön strategiana on tapaustutkimus. Opinnäytetyö koostuu teoreettisesta tietopohjasta (kappaleet 3-8) sekä empiirisestä osuudessa haastatteluihin perustuvasta tutkimusanalyysistä (kappale 9) sekä analyysin perusteella tuotetusta kohdeorganisaation luokittelumalliehdotuksesta, joka esitetään kappaleessa 10. Tietopohjassa käsitellään tutkimusmenetelmän valinta, tietoturvan peruskäsitteet, tiedon elinkaari ja olomuodot sekä käytössä olevan teknologian mahdollisuudet. Analyysiosassa käsitellään haastattelujen tuloksia ja kappaleessa 10 tutkimustyön tuloksena syntyvä tietojen luokittelumalli ja työn johtopäätökset sekä jatkotutkimusehdotukset.

3 Tutkimusstrategia - tapaustutkimus

Opinnäytetyössä on kyseessä yrityksen tietoturvan ja tiedonhallinnan kehittäminen. Opinnäytetyöprosessin aluksi etsittiin tietoturvaan ja tietojen luokitteluun liittyvää teoreettista ja kirjoitettua tietoa sekä tutustuttiin käytettävissä oleviin teknologioihin ja automatisoituihin ratkaisuihin. Näin kehittämiskohteeksi valittuun tiedon luokitteluun, tietoturvan peruskäsitteisiin ja tietoon itseensä tutustuttiin sekä teoriassa, että käytännössä. Tämän jälkeen kehittämiskohde määriteltiin ja tehtiin tarvittavat rajaukset. Tiedonkeruumenetelmäksi valikoitui haastattelututkimus. Tähän päädyttiin muun muassa siitä syystä, että yrityksen IT-palvelukumppaneiden joukossa oli tarjolla useita konsultteja, jotka tuntevat teknologian tarjoamat mahdollisuudet ja ovat olleet mukana useiden eri organisaatioiden tiedonluokitteluhankkeissa. Heitä haastattelemassa oli mahdollisuus kartoittaa parhaat käytännöt analyysia ja kehittämistehtävän lopputulosta varten.

Haastateltavaksi valikoitui yhteensä kuusi kokenutta kehittämiskohteena olevan yrityksen tuntevaa konsulttia kolmesta eri IT-palveluyrityksestä. Haastattelut pyrittiin toteuttamaan marraskuussa online-kokouksissa mutta aikatauluhaasteiden vuoksi muutamia haastatteluja tehtiin sähköpostilla puhelimesta tapahtuneen alustuksen ja taustoituksen jälkeen. Haastateltavilta kysyttiin etukäteen rakennetun kysymyslomakkeen mukaiset kysymykset

(Liite 1). Konsulttien haastatteluissa pyrittiin selvittämään heidän käsityksensä tiedonluokittelun tarpeellisuudesta kohdeyrityksessä, muiden asiakasyritysten tilanne tiedonluokittelun ja teknologian käyttämisestä sekä parhaat kokemuksen kautta opitut käytännöt. Jokaisen kysymyksen osalta haastattelulla oli myös mahdollistaa antaa vapaamuotoinen avoin kommentti tai näkemys.

3.1 Perustelut menetelmävalinnalle

Opinnäytetyön läpinäkyvyyden ja luotettavuuden takaamiseksi siinä pitää kuvata menetelmävalinta perusteluineen (Kananen 2012, 25). Näin ulkopuoliset työn arvioitsijat ja lukijat voivat arvioida tulosten luotettavuutta ja työn eri vaiheita.

Tämän opinnäytetyön perustuu laadulliseen tutkimukseen, jossa siirrytään teoriasta käytäntöön. Tutkimustavoitteena on muodostaa ymmärrys kehittämiskohteesta ja siihen liittyvästä teoriasta. Lopputuloksena koottu aineisto muodostaa opinnäytetyön sisältäen tutkimusongelman, menettelytapojen kuvaamisen, tutkimustulosten arvioinnin ja raportoinnin jatkokehitysehdotuksineen (Kananen 2012, 46-47).

Tässä opinnäytetyössä käytettiin liitteen 1 mukaista strukturoitua haastattelua ja kyselylomaketta. Pyrkimyksenä oli käytännönläheisesti luoda uusi rakenne käsittelyssä olevaan ongelmaan. Tähän tarvittiin jo olemassa olevaa sekä haastattelujen muodossa kerättyä uutta tietoa. Tutkimuksen tuloksena toivottiin syntyvän teoreettisesti perusteltu uusi ratkaisu kohdeorganisaation ja tiedeyhteisön käyttöön. Strukturoitu haastattelu perustuu valmiiseen kyselylomakkeeseen ja haastattelussa kysymykset esitetään kaikille haastateltaville samassa järjestyksessä ja saman muotoisina. Valmiiden määrämuotoisten kysymysten käyttäminen takaa sen, ettei haastattelija vaikuta vastauksiin omilla mielipiteillään. (Ojasalo, Moilanen & Ritalahti 2014, 65.)

3.2 Haastateltavien valitseminen

Tässä tutkimuksessa valintakriteerinä oli, se että valikoidut konsultit ovat työskennelleet IT-palveluntarjoajalla kohdeyrityksen asiakkuudessa. Heillä kaikilla oli laajasti kokemusta teknologian tukemista tiedonluokittelun ja -hallinnan toteutuksista, ja he tunsivat entuudestaan kohdeyrityksen toimintamalleja, liiketoiminnan erityispiirteitä sekä tiedonhallinnan ja -varastoinnin prosesseja. Lisäksi heillä oli tieto kohdeyrityksessä käytössä olevista ohjelmistoista sekä lisensseistä. Kaikki haastatteluun pyydetty konsultit osallistuivat haastatteluun ja paneutuivat vastauksiinsa kiitettävällä tasolla.

3.3 Haastatteluiden toteutus

Haastattelututkimuksessa tärkeää ja merkityksellistä on luottamuksen rakentaminen haastattelijan ja haastateltavan välille (Ruusuvuori & Tiitula 2015, 41). Tämän tutkimuksen haastattelutilanteissa ei ollut mahdollista kohdata haastateltavia kasvatusten vallitsevien

poikkeusolojen vuoksi. Haastatteluista sovittaessa haastateltaville kuitenkin kerrottiin kattavasti opinnäytetyön ja haastatteluiden merkitys ja tarkoitus. Heille myös kerrottiin, että vastaukset käsitellään anonyymisti sekä haastateltavan, että hänen edustamansa yrityksen osalta.

3.4 Analyysi ja tulkinta

Haastattelut pyrittiin asettamaan osaksi tutkimusongelmaa ja tutkimuksen analyysivaiheessa tehtiin aineistosta nousevia johtopäätöksiä, suosituksia ja koettuja parhaimpia käytäntöjä lopulliseen ehdotukseen luokittelumallista kohde organisaatiolle. Haastateltujen vastaukset luokiteltiin ja jokaiselle haastatellulle määriteltiin kirjain hänen edustamansa yrityksen mukaisesti. Luokat olivat Yritys A, B ja C. Yrityksen sisällä haastatellut konsultit luokiteltiin numeerisesti A1, A2, A3, B1, B2 ja C1.

4 Tietoturvan peruskäsitteet

Tietoturvalla tarkoitetaan tietojen, tietojärjestelmien ja palveluiden suojaamista erilaisilta sisäisiltä ja ulkoisilta riskeiltä. Tietoturva on läsnä yrityksen ja sidosryhmien päivittäisessä toiminnassa. Tiedon eri tallennusmuodoista huolimatta tieto on suojattava asianmukaisesti niin, että sitä ei voida käyttää väärin eivätkä tiedot voi aiheuttaa vahinkoa yrityksen toiminnalle. (Miettinen 1999, 23-24.)

Tietoturvan perustavoitteet pyritään takaamaan erilaisin hallinnollisin ja teknisin toimenpitein. Perustavoitteet ovat saatavuus (availability), eheys (integrity), luottamuksellisuus (confidentiality), todennus (authentication) ja kiistämättömyys (non-repudiation). (Rousku 2014, 47.)

Erilaiset kansalliset lait ottavat kantaa tieto-omaisuuden turvallisuuteen ja valtuuttavat viranomaisia valvomaan niiden toteutumista. Lait määrittelevät yksityisyyden suoja, tietojen luottamuksellisuutta, eheyttä ja saatavuutta. Lakien noudattamatta jättäminen tulkitaan rikkomukseksi, jonka rangaistukset vaihtelevat maittain. Niin sanotun hyvän hallintomallin mukaisesti paineet lisääntyvät kaikilla vastuullisilla toimijoilla lakien huomioon ottamiseksi sekä henkilökohtaisen vastuun kantamiseksi. Lakien, direktiivien ja sääntöjen noudattaminen eroaa eheydestä, luottamuksellisuudesta ja saatavuudesta, sillä ne määrittelevät yrityksen tieto-omaisuuden muodot ja suojaamiseen liittyvät seikat, joita yrityksen on pakko noudattaa eri liiketoiminta-alueillaan. (Jordan & Silcock 2005, 169).

4.1 Saatavuus

Saatavuudella tarkoitetaan yksinkertaisimmillaan sitä, että yrityksen tiedot ovat tarvittaessa niiden henkilöiden käytettävissä keillä on oikeus ja tarve niiden käyttöön. Monet yrityksen

päivittäiset työrutiinit ja päätökset edellyttävät tietojen olevan käytettävissä. Saatavuuteen vaikuttavat eniten yrityksen IT-resurssien määrä, järjestelmien toimintavarmuus ja laatutaso. Saatavuus saatetaan menettää myös yhä useammin ulkopuolisten syiden vuoksi. Tällaisia ovat muun muassa:

- Häiriöt kansallisissa tai kansainvälisissä Internet-yhteyksissä
- Luonnonmullistukset, tahallinen haitanteko kuten palvelunestohyökkäykset tai sabotaasi
- Toimittajan tai palveluntarjoajan häiriöt ja virheet palveluissa
(Jordan & Silcock 2005, 168.)

Perinteisiä toimintatapoja saatavuuden varmistamiseksi on kaikkien resurssien kahdentaminen mukaan lukien IT-laitteet, verkkoyhteydet, virtalähteet, kuormantasaus ja fyysiset toimitilat. Pilvi-palveluiden myötä osa näistä saatavuuden varmistustavoista on muuttunut palveluun kuuluvaksi automaattiseksi osaksi. (Jordan & Silcock 2005, 168.)

4.2 Eheys

Tietojen eheydellä tarkoitetaan sitä, että tiedot ja järjestelmät ovat luetettavia, oikeita ja ajantasaisia, eivätkä ne ole hallitsemattomasti muutettavissa laitteisto- tai ohjelmistovirheiden, häiriöiden, sabotaasin tai inhimillisen toiminnan seurauksena (Digi- ja väestötietovirasto 2020). Tietojen eheys on kunnossa, kun tiedot ovat siinä tilassa kuin niiden alun perin on tarkoitettu ja suunniteltu olevan, eikä niitä ole muutettu tahallisesti tai tahottomasti ei toivottuun muotoon (Miettinen 1999, 26). Mikäli samaa asiaa kuvaava tieto on tallennettu useampaan yleisesti saatavilla olevaan paikkaan, tulee niiden sisällön olla sama (Virtanen 1995, 8).

Tietojen tahaton eheyden menetys, korruptoituminen tai tietojen häviäminen johtuu yleensä seuraavista asioista:

- Tietokoneen tai palvelimen laitteistovika
- Erilaiset ohjelmistoviat tai virheet koodissa, jotka sallivat käyttäjiltä toimenpiteitä, joissa tietoa menetetään tai muutetaan
- Infrastruktuurin häiriöt, kuten sähkö- tai verkkokatkokset
- Käyttäjille suunnattujen ohjeiden huomioimatta jättäminen
- Konfigurointivirheet käyttöoikeuksissa
(Jordan & Silcock 2005, 167.)

Hyväksi todettuja keinoja eheyden säilyttämiseksi ovat muun muassa vikasietoiset ja kahdennetut palvelut, automatisoitu varmuuskopiointi tai palvelun tarjoajan tietojen hajautus sekä varmuuskopioiden palautusten testaaminen. Myös tietojärjestelmiin

tunkeutumisen esto ja havaitseminen ovat tärkeitä elementtejä eheyden varmistuksessa. (Jordan & Silcock 2005, 167.)

4.3 Luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan, että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen henkilöiden ja tahojen käytettävissä. Ulkopuolisille ei anneta mahdollisuutta muuttaa tai tuhota tietoja, eikä käsitellä tietoja millään keinoilla. Toisin sanoen luottamuksellisuuden varmistaminen on tietojen suojaamista lavatonta käyttöä vastaan. (Digi- ja väestötietovirasto 2020.)

Luottamuksellisuus korostuu henkilötietojen ja henkilökisterien, tuotekehitystietojen, yrityksen taloudellista tilaa koskevien tietojen ja liikesalaisuuksiin liittyvien tietojen käsittelyssä ja suojauksessa. Luottamuksellisuuden menettäminen saattaa aiheuttaa yritykselle merkittäviä taloudellisia sekä yritysimagea vahingoittavia tilanteita. (Miettinen 1999, 26.)

Luottamuksellisuuden menettämiselle mahdollisia tilanteita ovat:

- Rikollinen toiminta muun muassa tietojenkalastelu
 - Kilpailijoiden tai mahdollisesti tiettyjen maiden harjoittama yritysvakoilu
 - Työntekijöiden uteliaisuus esimerkiksi palkkatietoja tai työntekijöiden henkilötietoja kohtaan
 - Työntekijän siirtyessä kilpailijalle
- (Jordan & Silcock 2005, 167.)

Yleisiä luottamuksellisuuden turvaamiseksi käytössä olevia keinoja ovat muun muassa riittävän pitkät salasanat, eriytetyt verkkoratkaisut, ajantasainen ja hallittu käyttöoikeuspolitiikka, kriittisen tiedon tekninen suojaaminen, kaksivaiheisen tunnistautumisen käyttäminen sekä erilaisten teknisten valvontatyökalujen käyttö ja niiden hälytyksiin reagointi. (Jordan & Silcock 2005, 167.)

4.4 Todennus

Todennusta suoritetaan, jotta saadaan selville osapuolten aitous ja oikeellisuus.

Todentaminen edellyttää aina jotain yksilöllistä ominaisuutta, esimerkiksi salasanaa tai fyysistä ominaisuutta, kuten sormenjälkeä tai kasvojen tunnistusta. Todentaminen voi olla myös vahvaa. Tällöin käyttäjältä vaaditaan salasanan ja käyttäjätunnuksen lisäksi jotain fyysistä yksilöllistä tunnistusvälinettä. Yleisesti käytössä olevia vahvan todentamisen välineitä ovat sirukortit ja mobiiliapplikaatiot. (Järvinen 2013, 36.)

Todennusta voidaan käyttää periaatteessa kahdessa eri tilanteessa. Sitä käytetään silloin, kun henkilö kirjautuu palveluun tai kaksi erillistä tietoteknistä palvelua kommunikoivat

keskenään. Todennus käyttäjän ja palvelun välillä voidaan hoitaa eri tavoin muun muassa kryptattujen salasanojen avulla tai asymmetrisellä salauksella. Tietoteknisten palveluiden kesken todennuksessa käytetään esimerkiksi digitaalista allekirjoitusta tai symmetristä salausta yhdessä asymmetrisen salauksen kanssa. (Järvinen 2013, 38.)

4.5 Kiistämättömyys

Kiistämättömyydellä tarkoitetaan juridisen sitovuuden luomista sen varmistamiseksi, ettei tietojen käsittelyssä tai niiden siirrossa osallisena ollut taho voi jälkikäteen kiistää osuuttaan. Tietojen ja tietoa-aineistojen osalta kiistämättömyys koskee tietoa siitä, kuka on muokannut tietoja. Sähköisessä viestinnässä kiistämättömyydellä tarkoitetaan niitä toimenpiteitä, joilla varmistutaan viestin lähettäjältä ja viestin vastaanottajasta. (Valtioneuvosto 2018, 17.)

Kiistämättömyys todennetaan varmenteilla sekä aikaleimoilla. Se tarkoittaa, ettei henkilö voi kiistää lähettäneensä jotain viestiä. Kiistämättömyyden periaatteet liittyvät vahvasti todennukseen ja eheyteen. (Savolainen 2013, 8.)

5 Tieto suojattavana kohteena

Useimmissa tapauksissa tiedot ovat yrityksen tärkein suojausta vaativa omaisuus. Tiedot sijaitsevat yrityksen tietojärjestelmissä, tietokannoissa ja tiedostoissa perinteisissä datakeskuksissa tai pilvipalveluissa sekä erilaisina tulosteina ja fyysisinä dokumentteina. Tietojen turvaluokkajärjestelmissä määritellään yksityiskohtaisesti, miten arvokkaita tiedot ovat ja millainen suojaustaso kunkin turvaluokan tiedoilla on oltava.

5.1 Mitä tieto on

Tieto on informaatiota, jolla on arvoa ja merkitystä yrityksen tavoitteiden täyttymisessä. Informaatio koostuu datasta eli yksittäisistä merkityksellisistä merkeistä, jotka kokonaisuutena muodostavat informaation. Data muodostuu sellaisista merkeistä, joita voidaan tulkita tietyn yhtenäisen mallin mukaan. Tiedon käsite voidaan myös esittää seuraavasti: Data on muokkaamaton raakatiieto kaikista tapahtumista ja ympärillämme olevista asioista. Vain osalle datasta on informatiivinen arvo. (Paavilainen 1998, 17,)

- Informaatio on dataa, joka antaa meille uutta tietoa ympärillämme olevista asioista. Mitä yllätyksellisempää ja uudempaa informaatio on, sitä suurempi sen on sen informatiivinen arvo. Mitä paremmin se on asiayhteyteensä sopivaa, sitä helpommin se on muutettavissa tiedoksi.
- Tieto vähentää epätietoisuutta jostakin asiasta ja erottaa päätöksen arvauksesta. Tietomäärän kasvaessa kokemus vanhenee yhä nopeammin ja lisää informaatiota

tarvitaan päätösten perustaksi. Tällöin oikea-aikainen tiedonsaanti ja tietojenkäsittelyprosessin tehokkuus on ensiarvoisen tärkeää.

- Tietämys on kaiken käytettävissä olevan tiedon kokonaismäärä, joka ihmisellä on hallussaan.

(Paavilainen 1998, 17.)

5.2 Miksi tietoa on suojeltava

Yrityksen sijainti, ympäristö, toimiala ja toiminnan laajuus asettavat vaatimuksia liiketoiminnan jatkuvuuden hallinnan kehittämiseksi. Yritys käsittelee monenlaista tietoa, josta merkittävä osa on tarkoitettu ainoastaan yrityksen sisäiseen käyttöön. yrityksen mahdolliset tuotekehityksen hankkeet kiinnostavat kilpailijoita ja monenlaiset tiedot ja tunnukset kiinnostavat hakkereita ympäri maailmaa. Uhat saattavat olla yrityksen sisällä, lähipiirissä tai toisella puolella maailmaa mutta tietoverkkojen kautta vain muutaman sekunnin päässä (Kyrölä 2001, 37-40).

Tietojen hallitsematon muuttuminen, tahoton paljastuminen, häviäminen tai käytön estyminen saattavat merkittävästi vaikuttaa yrityksen liiketoimintaan. Tiedon määrä myös kasvaa jatkuvasti. Sitä on asiakirjoina, sähköpostiviesteissä, pilvitallennustiloissa, Teams-keskusteluissa, tietokannoissa ja muilla tallennusmedioilla. Kaikissa yrityksen toiminnoissa pitää selvittää mitä tietoa ja missä järjestelmissä tietoa säilytetään ja miten tärkeää ja kriittistä tietoa käsitellään. Tällöin arvioidaan normaalin tuotannon ja toiminnan tuottavuuden ja sujuvuuden kannalta se, miten oikeina, muuttumattomina, luottamuksellisina ja suojattuina tietojen pitää säilyä. Syyt tiedon suojaamiseksi asettaa se ovatko tiedot omia vai asiakkaiden, liittykö niiden käsittely asiakkaille suunnattuun palveluun, velvoittavatko lait tai viranomaiset tietojen suojaamista vai ovatko tiedot yleisesti yrityksen salaiseksi tai kriittiseksi luokittelemia. Jos esimerkiksi yritys käsittelee asiakkaiden tai työntekijöiden arkaluontoisia tietoja kuten henkilö- tai terveystietoja, henkilötietolaki ja GDPR-asetus asettaa vaatimukset tietojen suojaukselle. Mikäli käsitellään palkanmaksuun liittyviä tietoja, asetetaan yrityksen palkanmaksumenettelyille ja -järjestelmille oikeellisuus- luottamuksellisuus- ja oikea-aikaisuusvaatimuksia. (Kyrölä 2001, 37-40.)

5.3 Millaista tietoa on suojeltava

Yrityksen tieto-omaisuutta on kaikki yrityksessä luotu ja muokattu tieto. Se koostuu yrityksen, asiakkaiden ja yhteistyökumppaneiden toimintaan liittyvistä asioista. tietoa on tulosteina, tallennettuna ja yrityksen työntekijöiden muistissa. Tietopääomaa ovat työntekijöiden tiedossa olevat tiedot muun muassa yrityksen käytännöistä, suojauksista, strategiasta ja niiden heikkouksista. Yrityksen tieto-omaisuuden suojauksessa on otettava huomioon myös työntekijöiden mahdollisuus väärinkäyttää tietojaan. Näitä tietoja ja tieto-omaisuutta pitää suojata sen mukaan, miten arvokasta ja tärkeää tieto on yrityksen liiketoiminnalle. (Kyrölä 2001, 67.)

Yrityksen on tärkeää tunnistaa ne tiedot, joiden oikeellisuudesta, käytettävyydestä ja luottamuksellisuudesta pitää huolehtia tiedon elinkaaren eri vaiheissa. On myös huomioitava, että tiedon tärkeys ja kriittisyys saattavat muuttua sen elinkaaren aikana. (Kyrölä 2001, 68-69.)

5.4 Tiedon elinkaari

Kaikella tiedolla on elinkaari, jonka aikana tieto syntyy, sitä käsitellään ja lopuksi tieto hävitetään. Elinkaaren aikana tiedon luottamuksellisuusvaatimukset saattavat muuttua. Esimerkiksi pörssiyhtiön tilinpäätöstietoja koostettaessa, tieto on aluksi luottamuksellista. Kun tulos julkaistaan, se muuttuu julkiseksi tiedoksi. Osa yrityksen käsittelemistä tiedoista ovat koko tiedon elinkaaren ajan luottamuksellisia, kuten palkkatiedot, asiakkaiden henkilötiedot ja ohjelmalliset koodit. (Kyrölä 2001, 68.)

Tiedon elinkaari jakaantuu seuraavasti:

- tiedon syntyminen
- tiedon levitys sekä jakaminen, tulostaminen, säilytys ja käsittely
- tiedon hävittäminen ja poistaminen.

Tiedolla ja mediallylla joka tiedon sisältää, saattaa olla eri pituiset elinkaaret. Esimerkiksi arkaluonteinen tieto voidaan määritellä poistettavaksi järjestelmästä tai rekisteristä heti, kun perusteita tiedon säilyttämiselle ei enää ole. GDPR-asetuksen vaatimusten mukaisesti henkilö voi myös pyytää poistettavaksi kaikki häntä koskeva tieto. Ihmismuistista ei tietoa voi kuitenkaan poistaa kuten järjestelmistä. Eli tiedon elinkaari jatkuu muistissa, vaikka järjestelmästä arkaluontoinen tieto olisi hävitetty (Leppänen 2006, 256).

5.5 Lainsäädännön ja asetusten vaikutus tietojen suojaukseen

Lakeja ja asetuksia, jotka liittyvät tavalla tai toisella tietojenkäsittelyyn ja suojaustarpeisiin edellyttäen tiedoilta esimerkiksi luottamuksellisuutta ovat muun muassa:

- perustuslaki
- henkilötietolaki
- sähköisen viestinnän tietosuojalaki
- työsopimuslaki
- arvopaperimarkkinalaki
- laki sopimattomasta menettelystä liiketoiminnassa
- teletoiminnan tietosuojalaki
- tekijänoikeuslaki
- patenttilaki
- valmiuslaki

- EU:n yleinen tietosuoja-asetus (GDPR)
(Kyrölä 2001, 55)

Tietojen suojaamisen ja luottamuksellisuuden kannalta tärkeimmät lait ja asetukset ovat:

Perustuslaki

Koska Suomessa ei ole erityistä tietoturvalakia, siihen liittyvät lait ovat erilaisina osina useammissa yksittäisissä laeissa. Suomessa tietoturvan lainsäädännöllinen kehys alkaa perustuslaista, jossa on määritelty kansalaisten perusoikeudet. Oikeus yksityisyyden suojaan turvataan perustuslaissa ja tämä asettaa kriteerit myös yritysten tietoturvatoimiin sekä tietojen suojaukseen. (Laaksonen, Nevasalo & Tomula 2006 27-28.) Perustuslain 10§ määrittelee yksityisyydensuojan seuraavasti: Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta tai kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa, vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Eli perustuslaki määrittelee yksityiselle kansalaiselle viestinnän suojan, joka on mahdollista menettää esimerkiksi esitutkinta- tai tiedustelulain nojalla. (Oikeusministeriö 2020.)

Tietosuoja laki

Henkilötieto on peruskäsite, joka liittyy lähes kaikkiin tietoturvana sääteleviin lakeihin. Sillä tarkoitetaan kaikenlaisia yksilöiviä merkintöjä, jotka kuvaavat luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan sekä tietoja, jotka liittyvät henkilön perheeseen tai yhteisessä taloudessa asuviin henkilöihin. Näin ollen lain mukaan voidaan tulkita henkilötiedoiksi mikä tahansa tieto, jonka perusteella henkilö voidaan yksilöidä. Tieto voi olla esimerkiksi henkilön nimi tai osoite. Lisäksi laki velvoittaa, että henkilötietorekisterin ylläpitäjän on suunniteltava ja toteutettava rekisteri tietoturvallisesti niin, että yksittäinen henkilötieto voidaan poistaa ja tuhota järjestelmästä turvallisesti. (Oikeusministeriö 2020.) Näillä tiedoilla voidaan todeta, että lähes jokaisen yrityksen tietojärjestelmät sisältävät tietoja, jotka katsotaan henkilötiedoiksi. Sähköisen viestinnän tietosuojalaissa mainittu tunnistamistietokäsite eroaa henkilötiedoista siten, että henkilötieto koskee aina luonnollista henkilöä, kun tunnistetieto voi koskea myös oikeushenkilöä, kuten esimerkiksi yritystä tai yhdistystä. (Laaksonen ym. 2006, 32.)

Tietosuojalaki (1050/2018) korvasi aiemman henkilötietolain 5. joulukuuta 2018, Tietosuojalakia sovelletaan henkilötietojen käsittelyyn. Sen tarkoituksena on toteuttaa

yksityiseeden suojaa sen perusoikeuksia henkilötietoja käsiteltäessä ja edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Lakia sovelletaan yritysten, viranomaisten, järjestöjen ja yhteisöjen sekä osittain yksityishenkilöiden suorittamaan henkilötietojen käsittelyyn. Sitä sovelletaan käytännössä jokaiseen yritykseen, jossa käsitellään yksittäisten henkilöiden tietoja kuten nimeä tai henkilötunnusta.

Yleinen tietosuojasetus GDPR

EU-maissa vuonna 2018 voimaan tulleen yleisen tietosuojasetuksen (General Data Protection Regulation GDPR) taustalla on halu yhtenäistää henkilötietojen käsittelyä EU alueella ja hallita niiden käsittelyä eri jäsenmaissa. Se ohjaa jäsenmaita käsittelemään yhtenäisesti henkilötietoja turvallisemmin ja huolellisemmin sekä edistää digitaalisten sisämarkkinoiden kehittymistä EU alueella. Se myös antaa EU alueen kansalaisille yhtenäisiä oikeuksia henkilötietojen käsittelyn suhteen. Keskeisimmät oikeudet ovat: Henkilön oikeus saada tietää mitä tietoja hänestä on rekisteröity ja oikeus tietää miten ja mihin tarkoitukseen henkilötiedot on kerätty. Se antaa oikeuden pyytää virheellisten henkilötietojen korjausta tai vaihtoehtoisesti niiden poistamista kokonaan rekisterin pitäjän järjestelmästä. Henkilöllä on myös oikeus pyytää henkilötietojen käsittelyn rajoittamista ja pyytää niiden siirtämistä toiselle organisaatiolle. (Tietosuojavaltuutetun toimisto 2020.)

5.6 Liike- ja ammattisalaisuudet

Yrityksen liike- ja ammattisalaisuudet ovat tietoja, jotka eivät ole yleisesti saatavilla. yrityksen liiketoiminnan kannalta niiden suojaaminen edellyttää aktiivisia toimenpiteitä, jotta tiedot pysyvät yrityksen sisäisinä ja mahdollistavat esimerkiksi kilpailuedun. Yrityssalaisuudet voivat olla muun muassa tuotekehitystietoja, tutkimustietoja, reseptejä tai tietoja prototyypeistä- Jossain tapauksissa yritys voi luovuttaa salaisia tietoja esimerkiksi yhteistyökumppanille. Näissä tapauksissa on tärkeää, että yrityssalaisuuksia saavat taho veloitetaan noudattamaan salassapito- ja käyttökieltosopimuksia. (Laaksonen ym. 2006, 75-76.)

Liike-, ammattisalaisuus- ja yritysturvallisuus termejä ei ole suoranaisesti määritelty missään laissa. Lähtökohtana voidaan pitää sitä, että edellä mainituilla termeillä tarkoitetaan samaa asiaa. Laissa sopimattomasta menettelystä liiketoiminnassa ja työlaissa määritellään ammatti- ja liikesalaisuuden salassapitovelvollisuudet. Myös rikoslain 30:11§ määrittelee käsitteenä yrityssalaisuuden. Sen mukaan yrityssalaisuudella tarkoitetaan liike- tai ammattisalaisuutta tai muuta vastaava elinkeinotoimintaa koskevaa tietoa, jonka elinkeinoharjoittaja pitää salassa ja jonka ilmaiseminen olisi omiaan aiheuttamaan taloudellista vahinkoa joko hänelle tai toiselle elinkeinoharjoittajalle, joka on uskonut tiedon hänelle. Lähtökohtana on se, että yrityssalaisuudella pitää olla taloudellista arvoa omistajilleen ja omistajalla tulee olla pyrkimys tiedon salassa pitämiseksi. Yrityksen kaikki työntekijätkään eivät näin ollen voi olla oikeutettuja kaikkeen tietoon. Tästä syystä yrityksen

tulisi luokitella tietonsa ja ohjeistaa asianmukaiset käsittelysäännötluokitellulle tiedolleen. (Laaksonen ym.2006, 75-76).

6 Tiedon luvattoman käytön seurauksia

Tietoa syntyy suoraan ja välillisesti monissa yrityksen erilaisissa prosesseissa ja syntynyt tieto tulisi käyttää mahdollisimman tuottavasti yrityksen hyväksi. Jos sisäiseen käyttöön ja erityisesti tuotekehitykseen kuuluva tieto vuotaa ulkopuolisille syynä saattaa olla tietovarkaus. (Jordan & Silcock 2005, 158.)

Tiedon väärinkäytön vaikutuksia yrityksille voidaan tarkastella esimerkiksi seuraavasti:

6.1 Tiedon yksinoikeuden menetys

Konkreettisen, fyysisen omaisuuden kanssa on usein selvää, jos joku ulkopuolinen käyttää sitä luvatta tai on ottanut sen haltuunsa. Sen sijaan tieto-omaisuuden suhteen uhri ei välttämättä aina ole tietoinen, jos tiedon yksinoikeus on menetetty. Kun yrityksellä on yksinoikeus tiedon käyttöön se voi oman harkintansa mukaan päättää miten tietoaan käyttää ja miten sen avulla saa parhaan mahdollisen hyödyn. (Jordan & Silcock 2005, 159.) Yleisesti voidaan todeta, että yritys omistaa tiedon, jonka luomisen se on kustantanut ja joka sisältää yrityksen toimintaan liittyviä asioita. Esimerkiksi työntekijän työaikanaan tekemä keksintö, joka ei liity yrityksen toimialaan tai työntekijän työasioihin, ei anna työnantajalle oikeutta keksintöön. Mikäli keksintö kuitenkin liittyy olennaisesti työssä tehtyyn tutkimukseen, jonka sivutuotteena keksintö on syntynyt, on työnantajalla oikeus tietoon. (Leppänen 2006, 67.)

6.2 Tiedon luottamuksellisuuden menetys

Termiä luottamuksellisuuden menetys käytetään silloin, kun tietoa on päässyt käyttämään kuka tahansa muu kuin henkilö tai taho, joiden käyttöön tieto on tarkoitettu. (Jordan & Silcock 2005, 159) On monia tilanteita, joissa yksityishenkilöt luovuttavat henkilökohtaisia tietoja yritysten ja viranomaisten erilaisiin rekistereihin. Kyseisten tietojen väärinkäyttö suunnitelmallisesti, virka- tai järjestelmävirheen seurauksena vahingoittaa organisaatiota ja saa asiakkaat ja käyttäjät vakuuttuneeksi siitä, että kyseinen organisaatio ei ole heidän luottamuksensa arvoinen (Jordan & Silcock 2005, 160).

6.3 Rikoksen tekijän saama taloudellinen hyöty

Esimerkiksi etukäteistieto pörssiyhtiön tuloksesta, sen hankkeista tai fuusioista mahdollistaa taloudellisen voiton pörssin osakemarkkinoilla. Rikollisen saavuttama taloudellinen hyöty koituu yritykselle ja muille osakkeenomistajille kustannuksiksi. (Jordan & Silcock 2005, 158.)

6.4 Tietomurron seurauksena kuluva aika, raha ja maineen menetys

Tietomurron havaitsemisen jälkeen saattaa yrityksessä alkaa pitkä ja kallis työ, jotta menetetty tieto-omaisuus saadaan jälleen alkuperäiselle tasolle. Yleensä uudesta järjestelmästä halutaan tehdä edellistä turvallisempi ja näin aikaa saattaa kulua huomattavasti. Tietomurron myötä mahdollisesti menetettyä asiakkaiden luottamusta on vaikea mitata rahassa. (Jordan & Silcock 2005, 159-160). Sosiaalisessa mediassa myös asiakkaiden negatiiviset kokemukset saattavat elää keskusteluissa useita vuosia.

7 Suojattavien tietojen luokittelu

Jotta kappaleessa 6 esitetyt tiedon luvattoman käytön seuraukset sekä tietoturvaluustoimenpiteiden oikeaksi mitoittamiseksi suojattavat tiedot on luokiteltava. Luokittelun myötä toimenpiteet voidaan mitoittaa oikein ottaen huomioon tiedon merkitys ja käyttötarkoitus sekä tietoon mahdollisesti kohdistuvat uhkatekijät ja riskit. (Digi- ja väestötietovirasto 2020.)

Tietoa käsitteleville työntekijöille pitää tehdä selväksi, että heidän käsittelemä tieto on yrityksen toiminnan kannalta arvokasta ja suojeltavaa. Tietojen luokitteluun liittyvissä ohjeistuksissa tulee käsitellä seuraavia asioita:

- Tiedon luokka. Luokittelu voi olla yksinkertaisimmillaan luottamuksellinen ja julkinen mutta luokkia voi olla myös useampia. Ohjeistuksessa tulee selittää eri luokkien merkitys ja esimerkit eri luokkien mahdollisesta sisällöstä. Julkisella sektorilla pitää huomioida julkisuuslain asettamat vaatimukset ja velvoitteet.
 - Tiedon käsittelyn periaatteet. Ohjeistuksessa pitää huomioida miten eri luokkien materiaalia tulee käsitellä. Käytännössä tiedoston jakamisen, sähköpostin ja puhelimen käyttö pitää ohjeistaa niin, että työntekijä on tietoinen siitä, että minkälaista tietoa voidaan antaa ja jakaa eteenpäin.
 - Tiedon salaamisen edellyttämät toimenpiteet ja määrittelyt sille, milloin salaaminen on pakollista.
 - Tiedon hävittämiseen liittyvien toimenpiteiden kuvaus. Ohjeesta pitää selvittää miten tarpeettomaksi muuttunut tieto pitää hävittää.
- (Laaksonen ym. 2006, 161.)

7.1 Tiedon luokat

Luokiteltu tieto kertoo tietojen tärkeyden yritykselle, selkeyttää tiedon käsittelytapoja ja korostaa henkilöstölle tietojenkäsittelyn huolellisuusvelvoitetta. Luokittelu ilmaisee myös yrityksen tietosuojatahdon sekä vaitiolo- ja salassapitovelvollisuuden merkityksen. Tiedot tulee luokitella riippumatta niiden tallennus- tai olomuodosta. Paperitulosteissa, tiedostoissa

ja esityksissä pitää tiedon luokka olla selkeästi esillä. Luokitellulle materiaalille pitää sopia ja ohjeistaa käyttöoikeuksien hallintaa, salausmenettelyjä ja toiminta tiedonsiirrossa, jakamisessa ja lähettämisessä. (Leppänen 2006, 263.)

Valtionvarainministeriön tuottaman valtiohallinnon tietoaineistojen käsittelyn tietoturvallisuusohjeen mukaisesti valtion virastot luokittelevat tiedot omalla tavallaan. Tätä luokittelumallia on mahdollista noudattaa yrityksissä mutta myös omia malleja on mahdollista luoda. Mikäli liiketoiminnan toisena osapuolena on valtion tai kuntien laitoksia, yrityksen on noudatettava valtionhallinnon tietoturvallisuusohjeita (Digi- ja väestötietovirasto 2020).

7.2 Microsoftin oletusluokat tiedolle

Useiden yritysten siirryttyä käyttämään loppukäyttäjien pilvipalveluita tiedon luokittelussa on mahdollista käyttää Microsoftin oletusluokkia:

- Henkilökohtainen - Personal
- Julkinen - Public
- Yleinen tai sisäinen - General
- Luottamuksellinen - Confidential
- Erittäin luottamuksellinen - Highly Confidential

Henkilökohtainen tieto on henkilökunnan omia yksityisiä ja henkilökohtaisia tiedostoja ja tietoja. Tällaisia saattavat olla esimerkiksi valokuvat, videot, erilaiset asiakirjat, todistukset ja matkaliput.

Julkinen tieto on kaikkien saatavilla sitä saa vapaasti jakaa ja käyttää. Yrityksissä julkista tietoa ovat esimerkiksi Internetsivuilla ja mainosmateriaalissa oleva tieto. Julkista tietoa on myös yrityksen jakama markkinointimateriaali, tiedotusvälineille jaettava materiaali sekä erilaiset tutkimuksiin jaettavat materiaalit. Kun yrityksen tuotteet ja palvelut ovat vapaasti saatavilla myös niitä koskeva tieto on julkista. Mahdolliset tuotteisiin liittyvät patentit, rekisteröidyt tavaramerkit ja tekijänoikeudet rajaavat kuitenkin tietojen julkisuutta. Julkista tietoa on myös yrityksen itsensä julkaisemat tiedot, joiden sisältö perustuu lakeihin tai asetuksiin. (Leppänen 2006, 269-270.)

Sisäistä tietoa on sellainen yrityksen tieto, joka on tarkoitettu ainoastaan omalle henkilöstölle. Sisäiselle materiaalille on tyypillistä laaja käsittelytarve, korkea päivittäinen käytettävyys ja mahdollinen julkitulon aiheuttama pieni vahingollisuus. Sisäiseksi tiedoksi tyypillisesti katsotaan seuraavat tiedot ja asiakirjat esimerkiksi sisäinen puhelinluettelo, organisaatiokaaviot ja vastualueet, prosessivastuut ja tehtävät, yrityksen tuotteet ja palvelut, hinnat ja toimitusehdot, sopimus pohjat ja asiakirjamallit, itse tuotetut ja ulkopuolisilta hankitut raportit, selvitykset sekä dokumentit ja tietojärjestelmien arkkitehtuurikuvaukset. Yksittäisen sisäisen tiedon vuotaminen yrityksen ulkopuolelle ei ole

useinkaan erityisen vahingollista. Mutta mikäli tietoa valuu ulos useampina yksittäisinä puroina, siihen mahdollisesti investoidut kustannukset saattavat aiheuttaa suurempia tappioita tai mainehaittoja. Sisäisen tiedon kannalta merkityksellistä on se, ettei sitä koske samanlainen lainsuoja kuin esimerkiksi salaista tietoa. Tosin sisäisten tietojen laajamittainen ja määrätietoinen kerääminen ja ulkopuolisille luovuttaminen taloudellista tai ammatillista hyötyä vastaan saattaa täyttää yrityssalaisuuden rikkomisen tai muun rikoksen tunnusmerkit. (Leppänen 2006, 270-271)

Luottamuksellista tietoa on sellaista tietoa, joka voi ilmi tullessaan vahingoittaa yritystä, henkilöstöä, asiakasta tai yhteistyökumppania. Yrityksissä luottamuksellinen tieto liittyy oleellisesti asiakassuhteisiin sekä taloudellisiin ja operatiivisiin toimintoihin. Kun sisäiseksi merkittyihin materiaaleihin lisätään tarkentavia ja yksilöiviä tietoja se muuttuu luottamukselliseksi. Luottamukselliseksi määritellään tyypillisesti esimerkiksi seuraavat tiedot:

- kannattavuus- ja katelaskelmat
- investoinnit
- henkilöstön palkkatiedot ja työsopimukset
- alihankinta- ja yhteistyösopimukset
- asiakastiedot
- markkinointisuunnitelmat
- myyntilaskelmat ja erittelyt
- kassavirrat ja rahaliikenne
- turvallisuusjärjestelyt
- tuotekehityssuunnitelmat- ja yhteenvedot
- hallitukset- ja johtoryhmän pöytäkirjat
- asiakasmateriaalit
- tuotteiden ja palveluiden prosessikuvaukset
- tuotteiden piirustukset ja reseptiikka
- hakemukset, valitukset ja riita-asiat
- kilpailijatiedot ja -analyysit

(Leppänen 2006, 271-272.)

Erittäin luottamuksellista tietoa on sellainen tieto, joka ilmi tullessaan vaarantaa yrityksen toimintoja ja voi aiheuttaa merkittävää vahinkoa yritykselle, yhteistyökumppaneille tai kolmannelle osapuolelle. Yrityksissä erittäin luottamukselliseksi määritellään yleisesti seuraavat tiedot:

- merkittävät asiakas- ja yhteistyö- ja osakassopimukset
- liiketoiminnan strategiset suunnitelmat

- asiakkaiden ja yhteistyökumppaneiden salaiseksi tai erittäin luottamukselliseksi luokittelema tieto
- yrityskauppoihin ja patenttihakemuksiin liittyvä materiaali

(Leppänen 2006, 274.)

8 Teknologia luokittelun tukena

Yrityksissä laajasti käytössä olevat Microsoftin palvelut mahdollistavat helposti käyttöönotettavat tiedon luokittelun työkalut. Azure Information Protection (AIP) toiminnallisuus suojaa yrityksen ja käyttäjien tietoja monella erilaisella mekanismilla muun muassa estämällä luottamuksellisen sähköpostin lähettämisen edelleen, suorittamalla sisällön perusteella automaattista luokittelua sekä salaamalla tiedot ja tiedostot automaattisesti perustuen käyttäjän valitsemaan luokkaan.

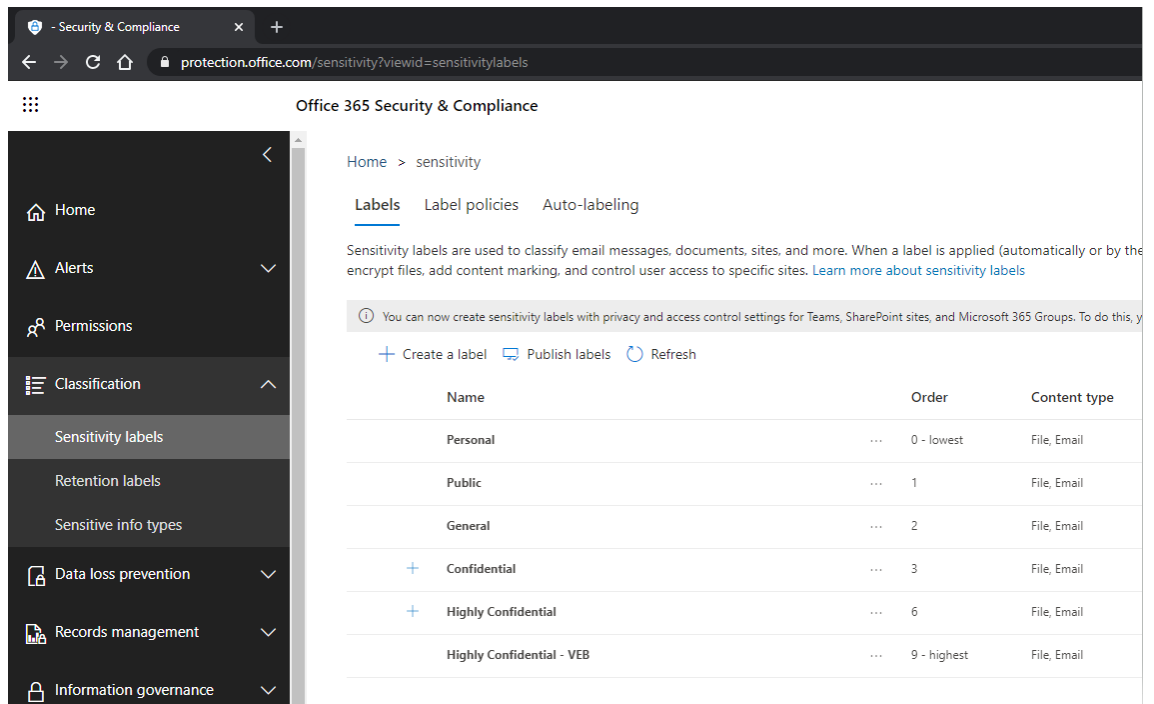
Microsoft Information Protection:

- Suojaa organisaatiota tietovuodoilta estämällä käyttäjien virheellisiä toimia sekä suojaamalla tiedon ulkopuolisten luvattomalta pääsylvä.
- Raportoi kuka käyttäjä käsittelee tietoja.
- Mahdollistaa tehokkaan ja luottamuksellisen tietojen yhteiskäytön.
- Ohjaa käyttäjiä toimimaan organisaation tiedonkäsittelyn - ja luokittelun mukaisesti.
- Raportoi käyttäjälle havaitsemistaan häiriöistä tiedonkäsittelyssä ja luottamuksellisuudessa.
- Raportoi ylläpitäjälle organisaation tiedon käsittelystä sekä luottamuksellisen tiedon jakamisesta.

(Microsoft 2020)

8.1 Azure Information Protection

Azure Information Protection koostuu useammasta luokittelun-, merkitsemisen- ja suojaustuotteen yhdistelmästä, kuten Office 365, Azure Information Protection ja Windows Information Protection tuotteista. Sen konfigurointi ja hallinta tapahtuu kuvio 1 mukaisessa Microsoftin Office 365 tietoturva ja yhteensopivuus (Office 365 Security & Compliance) portaaliassa <https://protection.office.com/>. (Microsoft 2020).



Kuvio 1 Luottamuksellisuustunnistet protection.microsoft.com portaalissa

Luokkien peruskäyttö vaatii Azure Information Protection lisenssin, jonka voi hankkia yksittäisenä tuotteena vuoden 2020 listahinnalla 20,28 €/käyttäjä/vuosi. Tyypillisin tilanne organisaatioissa on se, että Azure Information Protection on käytettävissä osana Microsoft 365 E3, E5 tai Enterprise Mobility + Security E3 tai E5 paketteja. (Microsoft 2020.)

Jatkuvasti päivittyvän pilvimallin ansiosta luokkien hallinta ja julkaisu on nykyään suhteellisen helppoa. Kuvio 2 mukaisesti esimerkissä luodaan uusi Highly Confidential - Special luokka. Kuvio 3 esittämässä näkymässä uudelle luokalle määritellään pakollinen salaus, käyttöoikeus yksittäisille käyttäjille, käyttäjäryhmille tai koko organisaatiolle. Käyttöoikeudelle on mahdollisuus määritellä päättymisajankohta, mutta esimerkissä käyttöoikeus määritellään pysyväksi. Luokalle määritellään kolmen vuorokauden offline työskentely, jolloin luokan mukaista tiedostoa voi käsitellä ilman Internet yhteyttä. (Sulava 2020.)

Lopuksi luokalle määritellään sen merkitsemiskäytännöt. Kuviossa 4 asetetaan luokan nimi vesileimalla keskelle dokumenttia sekä dokumentin ylätunnisteseen.

New sensitivity label

Name & description

Scope

Files & emails

Groups & sites

Finish

Name and create a tooltip for your label

The protection settings you choose for this label will be immediately enforced on the files, encrypted wherever they go, whether they're saved in the cloud or downloaded to a computer.

Name *

Highly Confidential - Special

Description for users *

Highly Confidential label for special use

Description for admins

Highly Confidential label for special use

Kuvio 2 Highly Confidential - Special luokan nimeäminen

New sensitivity label

Name & description

Scope

Files & emails

Encryption

Content marking

Auto-labeling for Office apps

Groups & sites

Finish

Encryption

Control who can access files and email messages that have this label applied. [Learn more about](#)

☐ Remove encryption if the file is encrypted

☒ Configure encryption settings

Turning on encryption impacts Office files (Word, PowerPoint, Excel) that have this label applied. Because they are opened or saved, and some SharePoint and OneDrive features will be limited or unavailable. [Learn more](#)

Assign permissions now or let users decide?

Assign permissions now

The encryption settings you choose will be automatically enforced when the label is applied

User access to content expires

Never

Allow offline access

Only for a number of days

Users have offline access to the content for this many days

3

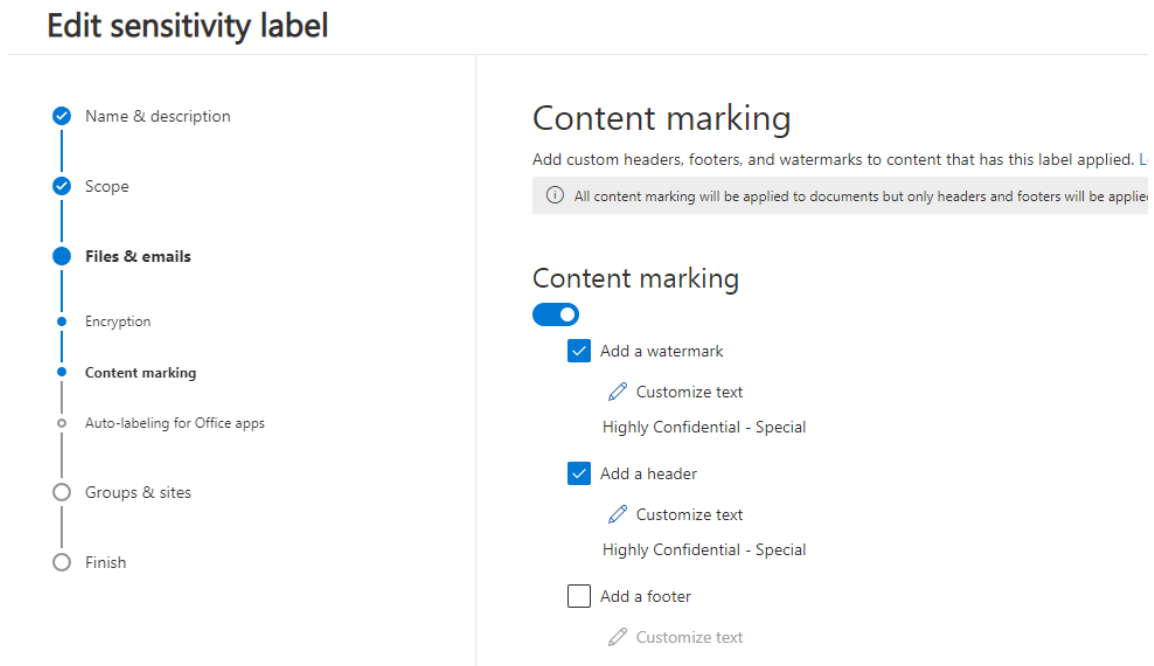
Assign permissions to specific users and groups *

[Assign permissions](#)

Users and groups	Permissions
...@05.onmicrosoft.com	Co-Author

☐ Use Double Key Encryption

Kuvio 3 Salauksen, käyttöoikeuden, offline käytön ja käyttäjäryhmän määrittäminen

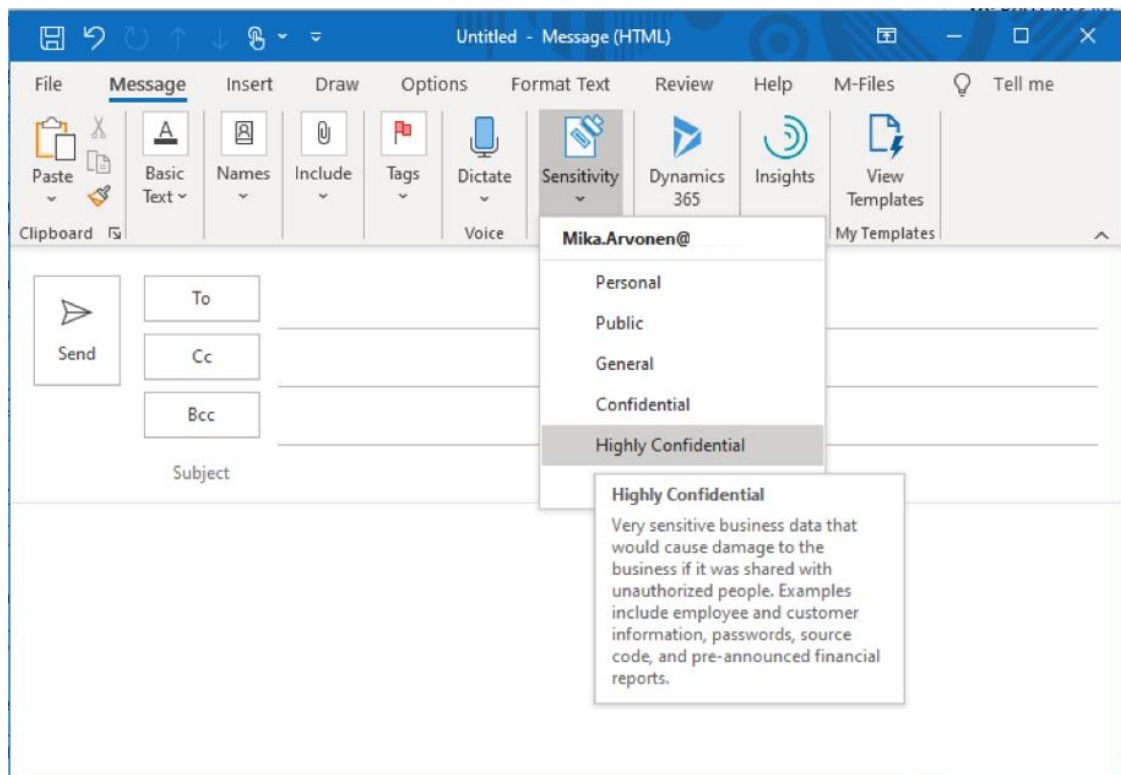


Kuvio 4 Luokan merkitseminen vesileimalla ja ylätunnisteella

Luokalle olisi mahdollista lisätä automaattisia tunnisteita, joiden esiintyminen asiakirjassa muuttaa automaattisesti luokituksen ja mahdollisesti pakottaa tiedoston tai sähköpostin salauksen. Tällaisia tunnisteita ovat muun muassa eri maiden passinumero, pankkitilien numerot, sosiaaliturvatunnukset ja erilaiset Microsoftin palveluihin liittyvät tilaukset tai salaukset tunnisteet. Koska Highly Confidential - Special ryhmässä on jo oletuksena määritelty salaus, automaattisia tunnisteita ei ole tarve tässä ryhmässä käyttää. Lopuksi luokka julkaistaan halutuille käyttäjille tai ryhmille. (Sulava 2020.)

8.2 Azure Information Protection luokkinen käyttäminen


Azure Information Protection luokat ovat julkaisuehtojen mukaisesti käytettävissä organisaation kaikissa Office 365 tuotteissa esimerkiksi Outlook sähköpostissa, Word-, PowerPoint-, ja Teams-tiedostoissa, käytettiin niitä sitten asennetuilla työpöytäversioina, selaimella Online-versioina Windows- ja macOS-käyttöjärjestelmissä tai mobiililaitteiden applikaatioina Adnroid- ja iOS-käyttöjärjestelmissä. (Sulava 2020.)



Kuvio 5 Luokkien valinta Outlook työpöytäsovelluksessa

Käyttäjille julkaistut luokat ovat valittavissa Outlook työpöytäsovelluksen Sensitivity painikkeella kuvio 5 mukaisesti. Mobiilisovelluksessa luokan valinta tapahtuu Add Sensitivity valinnalla (kuvio 7). Luokan merkitseminen dokumenteissa on vapaasti pääkäyttäjän määriteltävissä sijainnin, vesileiman, fontin, fontin koon ja fontin värin osalta. Kuviossa 6 luokka on määritelty näkymään Word dokumentin oikeassa yläkulmassa sekä vesileimalla keskellä dokumenttia. (Sulava 2020.)

Highly Confidential -



[First Name]
[Surname]

Date


[Recipient Name]	[Recipient Street Address]
[Title]	[Recipient City, ST Zip]
[Company]	

Dear [Recipient Name]


[If you're ready to write, select a line or paragraph of tip text and start typing to replace it with your own. Don't include space to the right of the characters in your selection.]

[It's easy to match any of the text formatting you see here. On the Home tab of the ribbon, check out the Styles gallery for all styles used in this letter.]


Sincerely,
[Your Name]




[Your Address]
[City, ST ZIP Code]



[Your Phone]

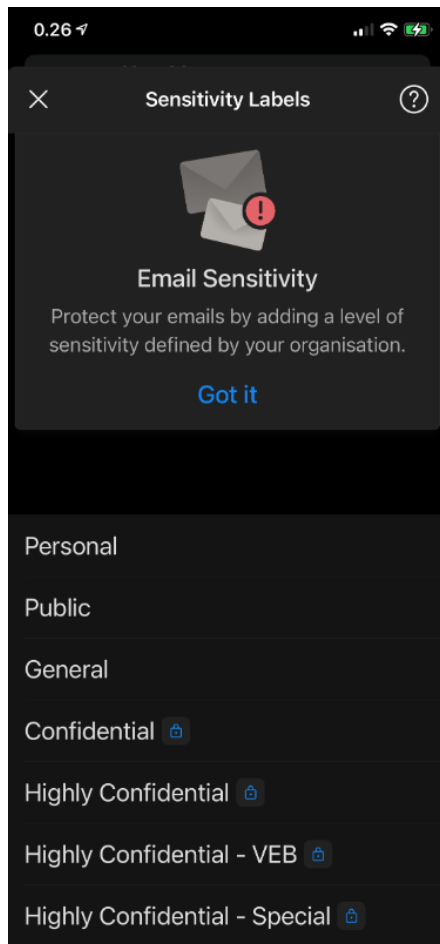


[Your Email]



[Your Website]

Kuvio 6 Highly Confidential luokan vesileima Word dokumentissa



Kuvio 7 Luokan valinta iOS mobiilikäyttöjärjestelmän Word applikaatiossa

Luokan asetuksista ja salauksen pakotuksesta riippuen, Office ohjelmistot tekevät automaattisia suojaustoimintoja. Näitä ovat muun muassa:

- salatun sähköpostin edelleen välittämisen estäminen
- salatun sähköpostin avaaminen organisaation ulkopuolella, vaatii avaajalta vahvan tunnistautumisen Microsoftin lähettämällä kertakäyttöisellä koodilla
- salatun materiaalin kuvaruutukaappauksen estäminen
- salatun materiaalin jakaminen Teams onlinepalaverissa
- salatun materiaalin tulostuksen estäminen

(Sulava 2020)

9 Haastattelututkimus

Opinnäytetyön tavoitteena on haastattelun perusteella saada näkökulmia ja kokemuksia parhaista käytännöistä ja kerättyä tietopohjaa ja haastattelun analysoinnilla luoda toimiva tiedon luokittelumalli kohde organisaation käyttöön. Tavoitteena on luoda luokittelumalli,

joka on lähtökohtaisesti helppokäyttöinen ja käyttöönotettavissa kaikissa kohde organisaation toimintamaissa. Haastattelujen tulokset perustuvat kuuden kokeneen ja kohde organisaation liiketoimintaa tuntevan konsultin vastauksiin. Konsultit edustivat kolmea eri IT-palvelutoimittajaa. Vastauksia ja tuloksia käsiteltäessä haastateltavat erotellaan toisistaan yrityksen A, B ja C kirjaimella sekä konsulttinumerolla 1,2 ja 3. Tulosten analysoinnissa vastauksista etsittiin säännönmukaisuuksia ja näitä käytettiin johdettujen päätelmien muodostamiseen. Haastattelu kysymyksistä perusteella hahmoteltiin kuusi eri aihekokonaisuutta, joita tarkastellaan tässä luvussa sellaisina kuin ne haastattelujen perusteella hahmottuivat. Kappaleessa 10 esitellään luokittelumalli sellaisena kuin se haastattelujen mukaisesti muodostui perustuen konsulttien aiempiin kokemuksiin ja parhaisiin käytäntöihin kohde yrityksen liiketoimintaan soveltuen.

9.1 Tiedon luokittelumallin käyttöönoton tarpeellisuus kohde organisaatiossa.

Ensimmäisessä kysymyksessä haastateltavilta kysyttiin miten tärkeänä he kokevat tiedon luokittelun käyttöönoton kohde organisaatiossa. Vastaukset on kuvattu kuviossa 8.

Haastattelu vastausten perusteella konsultit näkivät tiedon luokittelun pääsääntöisesti erittäin tärkeäksi kohde organisaatiossa. Neljä vastaajaa koki tiedon luokittelun käyttöönoton erittäin tärkeäksi, yksi melko tärkeäksi ja yksi jonkin verran tärkeäksi.



Kuvio 8 Vastaajien näkemys tiedon luokittelun tarpeellisuudesta kohde organisaatiossa

Avoimien vastausten osalta nousee esiin, että tiedon suojaamisen on luokittelua tärkeämpää sekä miten luokittelu osaltaan edesauttaa tunnistamaan suojattavat tiedot.

”Tiedon suojaamisen on luokittelua tärkeämpää”. (A1.)

”Tiedonluokittelu auttaa osaltaan organisaatiota ymmärtämään millaista ja minkä arvoista tietoa organisaatiossa on. Kun tieto luokitellaan, organisaation on helpompaa kohdistaa suojaustoimenpiteet arkaluontoiseen ja liiketoimintakriittiseen tietoon. Näin pystytään kohdistamaan suojaustoimenpiteet kustannustehokkaasti arvokkaimpaan tietoon.” (A2.)

9.2 Muiden organisaatioiden tiedon luokittelun tilanne

Kysymys kaksi käsitteli konsulttien näkemyksiä siitä, miten laajasti muissa organisaatioissa on otettu tiedon luokittelu käyttöön. Vastauksissa ei otettu huomioon minkä kokoisten organisaatioiden kanssa konsultit tekevät yhteistyötä tai edustavatko organisaatiot yksityistä tai julkista puolta. Näin ollen vastaukset eivät välttämättä ole täysin verrattavissa kohdeorganisaation tilanteeseen. Vastausten perusteella (kuvio 9) on kuitenkin huomioitavissa, että luokittelu on melko laajasti käytössä yrityksissä ainakin jollain tasolla. Eniten vastauksia (kolme kappaletta) keräsi vaihtoehto 50-75%, kaksi vastaaja arvioi luokittelun olevan käytössä 25-50% yrityksistä ja yksi arvioi luokittelun olevan käytössä 75-100% asiakaista.



Kuvio 9 Vastaajien arviot tiedon luokittelun yleisyydestä asiakasorganisaatioissa

Avoimissa vastauksissa nousee esiin eroja riippuen organisaatioiden koosta ja toimintakentästä sekä lievää kriittisyyttä siitä, että ainoastaan luokittelumallit ja -käytännöt eivät sinällään vielä tuo mitään suojaa tiedoille.

”Tällä hetkellä tiedonluokittelu on käytössä jollain tasolla suurimmassa osassa organisaatioita, joiden kanssa työskentelen. Uutena ilmiönä ovat pienet ja keskisuuret organisaatiot, jotka ovat heränneet tiedonluokittelun ja -suojauksen tarpeeseen esimerkiksi viimeaikaisten kiristyshaittaohjelmiin yms. perustuvien tietoturvahyökkäysten takia.” (A2.)

”Julkisen puolen asiakkailla tiedonluokittelu on ollut käytössä pitkään. Viime vuosina Microsoftin palveluiden kehittymisen ja yritysten pilvilisenssien hyödyntämisen myötä luokittelu on yhä yleisempää isoissa ja keskisuurissa yrityksissä.” (B1.)

”Valtaosassa organisaatioita, keillä on mielestään käytössä tiedon luokittelu, ei todellisuudessa kuitenkaan käytä tai seuraa tiedonluokittelun käyttöä. Tämä tarkoittaa sitä, että joihinkin organisaatioihin on syntynyt mielikuva siitä, että luokittelu on käytössä ja se suojaa tietoa, vaikka todellisuudessa mielikuvan takia tiedonluokittelussa ei tapahdu mitään”. (C1.)

9.3 Teknologian hyväksi käyttäminen tiedon luokittelussa

Kysymys kolme koski teknologisten ratkaisujen hyödyntämistä luokittelussa. Vastausten perusteella (kuvio 10) automaatio ja teknologia on vahvasti otettu mukaan tiedon luokitteluun. Vastanneista neljän mukaan teknologia avustaa yli 50% organisaatiossa luokittelua. Yhden vastaajan näkemyksen mukaan teknologia on mukana 25-50% yritysten luokittelukäytännöistä.



Kuvio 10 Teknologian hyväksikäyttö organisaatioiden tietojen luokittelussa

Avoimissa vastauksissa korostuu lähinnä Microsoftin tuotteiden hyväksikäyttö luokittelussa.

”Lähes kaikissa tuntemissani organisaatioissa on käytössä Microsoftin tiedonluokittelun ja -suojauksen työvälineet. Jotkin organisaatiot käyttävät vielä pelkkiä tekstikenttiä, mutta ovat pyrkimässä teknisten apuvälineiden käyttöön ja siihen, että luokittelutieto tallentuu metadataan joko automaattisesti tai käsin luokittelemalla.” (A2.)

”Azure Information Protection alkaa olemaan markkinassa käytännössä oletustuote tietojen suojaamisessa ja luokittelussa” (C1.)

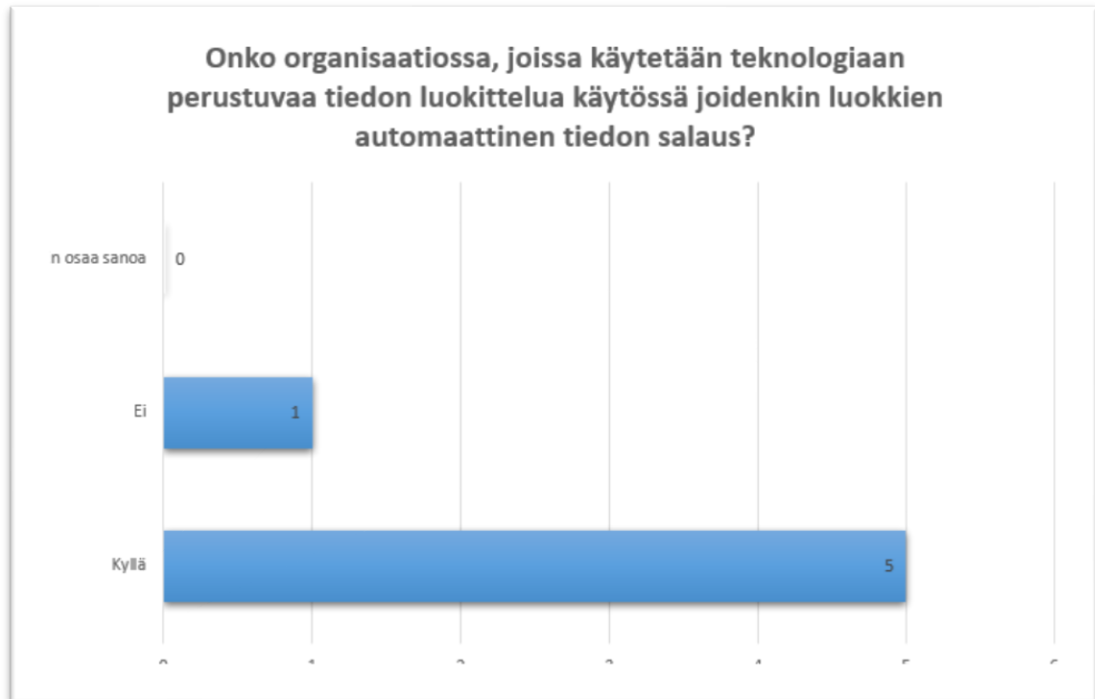
Teknologiaa on mahdollista myös hyödyntää pienissäkin määrin eli esimerkiksi oletusluokan automaattisella valinnalla tai tiedon sijainnin perusteella määräytyvän järjestelmän mukaisesti.

”Melko on paljon käytössä joko automaattista tai oletukseksi määriteltyä luokkaa. Jossain tapauksissa on tehty niin, että tietyssä järjestelmässä oleva tiedot ovat automaattisesti esim. luottamuksellisia.” (A1.)

9.4 Automaattinen luokkien salaus

Kysymys neljä käsitteli tiettyjen luokkien automaattista salausta niiden organisaatioiden osalta, joissa luokitteluun käytetään hyväksi jotain teknologiaan perustuvaa tuotetta.

Vastauksen on esitetty kuviossa 11. Niiden perusteella on tulkittavissa, että tiedon automaattinen salaaminen tiettyjen luokkien osalta on erittäin laajasti käytössä.



Kuvio 11 Automaattisen salauksen käyttäminen tietyissä luokissa

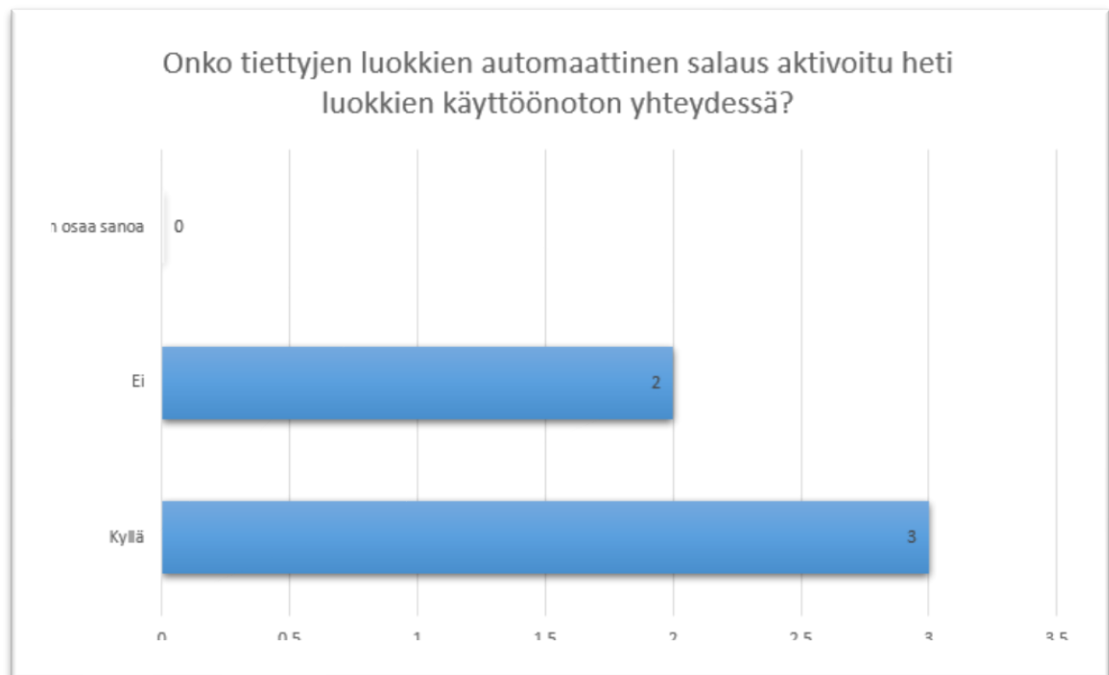
Avoimien vastausten osalta esiin tulevia asioita ovat mm. lisenssiriippuvuudet sekä salauksen myötä mahdolliset myöhemmin ilmenevät haasteet.

"Salausta käytetään usein mm. luottamuksellisen tiedon suojaamisessa. Kannattaa kuitenkin aina muistaa, että lisenssien kanssa saattaa tulla haasteita, jos vähintään E3 ei ole käytössä" (B2.)

"Salauksen kanssa kehotan aina olemaan vähän varovainen. Salauksen purkaminen on nimittäin todella työlästä, jos tenantteja pitää myöhemmin yhdistää vaikkapa yrityskauppojen yhteydessä" (C1.)

"Automaatiikka on yleensä käytössä tai ainakin sitä on kokeiltu, mikäli organisaation lisenssitaso sen sallii. Tiedonluokittelun tietoluokkien ylemmissä tietoluokissa kuten Confidential tai Secret salaukset ovat yleensä mukana kaikissa tuntemissani organisaatioissa." (A2.)

Viidestä vastaajasta, jotka kertoivat automaattisen salauksen olleen käytössä, kolme kertoo salauksen olleen käytössä heti luokkien käyttöönottojen yhteydessä (kuvio 12).



Kuvio 12 Automaattisen salauksen käyttöönoton ajankohta

Avoimissa vastauksissa esiin nousevat vahvasti testauksen ja pilotoinnin merkitys.

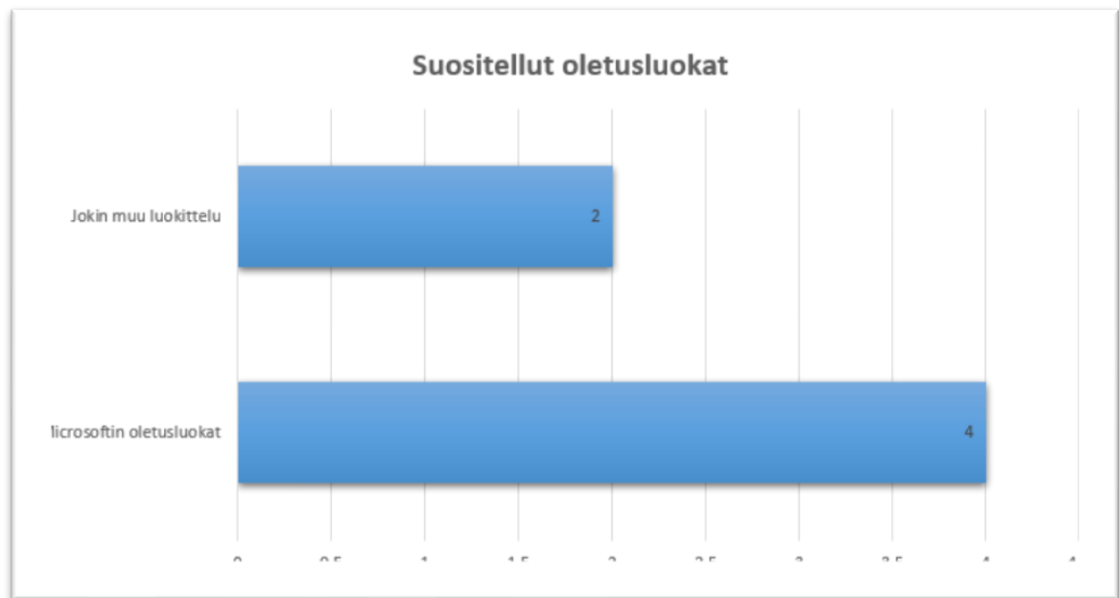
”Suositukseni on, että ensin tehdään luokittelumalli, jossa on muutama salauksen sisältävä testileima. Näitä leimoja testataan pilotointivaiheessa mahdollisimman laajasti erityyppisillä käyttötapauksilla. Mikäli pilotointivaiheessa ei tule show stoppereita, tiedonluokittelumalli salattuine leimoineen otetaan käyttöön koko organisaatiossa.” (A2.)

”Salausta kannattaa testata ja pilotoida todellakin perusteellisesti ennen käyttöönottoa” (C1.)

”En suosittele salauksen käyttöönottoa alku vaiheessa. Käyttäjille kannattaa antaa ensin riittävästi aikaa tutustua luokitteluun ja se vaikutuksiin. Salauksen vaikutukset saattavat olla osalle käyttäjistä hieman haasteellisia hahmottaa. Outlookin osalta tilanne on helpompi hahmottaa, koska salaus koskee lähtökohtaisesti just sitä yhtä liitettä, jota käyttäjä on lähettämässä.” (B1.)

9.5 Suositellut tiedon luokat

Kysymyksessä kuusi vastaajilta pyydettiin ehdotusta kohdeorganisaation luokitteluksi. Vastaajista neljä suosittelee lähtökohtaisesti käyttöönotettavaksi Microsoftin oletusluokkia (kuvio 13).



Kuvio 13 Jakauma oletusluokka suosituksesta

Avoimissa vastauksissa esiin nousee myös vaihtoehto lisätä alaluokkia.

”Lähtökohtaisesti suosittelen Microsoftin oletusluokkia, jotka ovat riittävän yksinkertaisia. Tarvittaessa voidaan ottaa käyttöön alaluokkia.” (A1.)

”Microsoftin parhaiden käytänteiden mukainen malli, johon lisätään organisaatiokohtaisia mausteita, sopii useimmille yksityisen puolen organisaatioille.” (A2.)

”Microsoftin malli on ihan hyvä vaikkakaan itse en näe perusteluja henkilökohtainen luokalle. Mielestäni yrityksessä käsiteltävät tiedot eivät tarvitse tätä luokkaa.” (B2.)

Kaksi vastaajista suosittelee Microsoftin oletusluokista poikkeavaa mallia. Toinen suosituksesta on huomattavan yksinkertainen ja toinen laajempi.

”Suosittelen yksinkertaista mallia, joka on käyttäjille helpompi. Luokat voisivat olla ulkoinen, sisäinen ja luottamuksellinen.” (B1.)

”Julkaistavissa oleva tieto esim. julkinen nettisivu, joka ei sisällä salassa pidettävää tietoa, Julkinen tieto (pyydettyäessä julkinen), Julkisuuslain perusteella salassa pidettävä tieto, liiketoiminnan salaiset tiedot (suunnitelmat, IPR, jne), asiakastieto, henkilötieto (EU:n tietosuoja-asetuksen 4 artikla), arkaluontoinen henkilötieto (EU:n tietosuoja-asetuksen 9 artikla), TLIII tason tieto ja turvakieltoasiakkaan yhteystiedot (ei luokka itsessään).” (C1.)

Muut huomioitavat suositukset

Viimeisessä kysymyksissä vastaajilta tiedusteltiin yleisiä suosituksia kohde organisaation luokittelumallille. Vastauksissa korostuu automaatio, käytön helppous, pilotointi ja

käyttöönoton yhteydessä tapahtuva loppukäyttäjien ohjeistus sekä käyttäjien sitouttaminen luokitteluun.

”Mahdollisimman automaattinen luokittelu.” (A1.)

”Microsoftin parhaiden käytänteiden noudattaminen. Käytännön kokemuksista oppiminen ja ulkopuolisen avun käyttäminen. Mahdollisimman laaja testaus pilotointivaiheessa. Organisaation sitouttaminen, viestintä- ja koulutus ovat keskeisiä.” (A2.)

”Huolellisien suunnittelun ja pilotoinnin merkitystä ei pidä aliarvioida. Käyttäjille pitää selkeästi viestiä ohjeet ja luokkien merkitykset. Ohjesivut on myös syytä julkaista esim. Intrassa.” (B1.)

”Jos käyttäjät eivät ymmärrä miksi luokat on olemassa, niiden käyttäminen ei koskaan tule onnistumaan riittävällä tasolla.” (B2.)

”Teknologia on väline, jonka avulla voidaan tietoa luokitella sen perusteella, miten luokat on määritelty organisaatioissa. Jos organisaation jäsenet eivät noudata sovittuja luokitteluun liittyviä ohjeita, ei teknologia voi pätevästi luokitella tietoa. Itse näen, että tässä on syy siihen, miksi tiedonluokitteluun suhtaudutaan negatiivisesti, koska organisaatioilta puuttuu kyvykyys saada ihmiset mukaan muutokseen, jonka päämääränä on toimiva tiedonluokittelumalli.” (C1.)

9.6 Tutkimuksen validiteetti ja reliabiliteetti

Kun arvioidaan tutkimusmenetelmien luotettavuutta, voidaan käyttää termejä validiteetti ja reliabiliteetti. Validiteetti tarkoittaa, että tutkimuksessa on tutkittu sitä mitä on kerrottu suunnitelmassa. Reliabiliteetilla sen sijaan tarkoitetaan sitä, että tutkimuksessa saadut tulokset ovat myöhemmin toistettavissa. (Tuomi & Sarajärvi 2018, 161.) Laadullisessa tutkimuksessa aineiston analyysivaihetta ja luotettavuuden arviointia on haasteellisempaa erottaa verrattuna määrälliseen tutkimukseen. Laadullisessa tutkimuksessa tutkijalla on enemmän liikkumavaraa analyysin, tulkintojen ja tutkimuksellisen tekstin välillä. laadullisen tutkimuksen luotettavuutta arvioitaessa joudutaan kuitenkin usein pohtimaan tehdyn analyysin kattavuutta sekä tutkijan omia ratkaisuja. (Eskola & Suoranta 1998, 209.)

Hyvä muistisääntö laadullisen tutkimuksen luotettavuutta tarkasteltaessa on se, että tutkija pyrkii kuvaamaan mahdollisimman tarkasti tutkimuksen toteutuksen eri vaiheet (Hirsjärvi, Remes & Sajavaara 2007, 226). On kuitenkin syytä muistaa, että kun tutkimuksen tai tarkastelun kohteena on ihmisten toiminta tai ajattelu, on tutkimuksen toistettavuus tai tilanteen vakiona pitäminen haasteellista (Kananen 2014, 145). Pitää myös huomioida, että haastatteluissa kerätyn aineiston laatu vaikuttaa paljon tutkimuksen luotettavuuteen (Hirsjärvi & Hurme 2004, 185).

Tämän työn alkukappaleissa tuotiin esiin tutkimuksen aihe, tarkoitus ja tutkimuskysymykset. Aiheen tarpeellisuutta ja valintaa perusteltiin ja avattiin työssä käytetyt tutkimusmenetelmät ja -prosessit. Aineisto kerättiin kuuden haastattelun perusteella saadusta materiaalista sekä tietoturvan, tiedonluokittelun ja tiedon teoreettista tietopohjaa tutkimalla. Haastatteluita ei nauhoitettu mutta niiden sisältä pyrittiin tarkasti dokumentoimaan vastauslomakkeisiin. Haastatteluvastauksista koostettiin taulukot, jotka on dokumentoitu tässä kappaleessa. Työn lopputuloksena muodostettu ehdotus luokittelumallista kohdeorganisaation käyttöön on esitetty kappaleessa 10. Tutkimuksen tekijän aikaisemmat kokemukset tiedon luokittelusta ja haastateltavien konsulttien asiakkuuksien jakautuminen yksityisen ja julkisen sektorin välillä ovat saattaneet vaikuttaa tutkimukseen ja sen tuloksiin.

10 Luokittelumalli kohdeorganisaation käyttöön

Tämän työn lopputuloksena on ehdotus case yritykselle tiedon luokittelumallista. Ehdotus perustuu haastattelujen ja tietopohjan perusteella analysoituihin malleihin ja käytäntöihin. Haastattelun perusteella on pääteltävissä, että teknologiaan perustuva luokittelu on laajasti käytössä eri organisaatioissa eikä sen käytössä ole ilmennyt merkittäviä haasteita. Suurin osa haastatelluista suositteli tiedon luokiksi Microsoftin oletusluokkia, joten ne ovat luonteva vaihtoehto myös kohde organisaation mallin perustaksi. Kappaleessa 10.4 esitellään myös suositeltavia jatkotutkimusten ehdotuksia kohde organisaatiolle mallin ja sen toimivuuden sekä käytettävyyden kehittämiseksi.

10.1 Tiedon luokat

Tiedot ja asiakirjat luokitellaan seuraavasti:

- **Personal** Tiedot ovat työntekijöiden yksityisiä tietoja esimerkiksi valokuvia, varausvahvistuksia ja opiskeluun liittyviä asiakirjoja.
- **Public** Tiedot ovat tarkoitettu julkaistuksi yrityksen ulkopuolella. Tiedot ovat esimerkiksi tutkimustuloksia, uutisia ja markkinointiin ja viestintään liittyvää materiaalia.
- **General** Tiedot on tarkoitettu yrityksen sisäiseen käyttöön eikä niiden suojaamiseen tarvita salausta.
- **Confidential** Tiedot ovat yritykselle arkaluontoisia ja erityisesti suojeltavia tietoja tai ne ovat tietoja, joiden erityiseen suojaukseen on lakien tai asetusten mukainen erityinen vaatimus. Luokan tiedot salataan automaattisesti. Salauksen purkuun on oikeus Domain Users AD-ryhmän jäsenillä. Luokan sähköpostin vastaanottaja ei voi edelleen lähettää sähköpostia ja yrityksen ulkopuoliselta vastaanottajalta vaaditaan vahva tunnistautuminen.

- **Highly Confidential** Tiedot ovat erityisen arkaluontoisia ja salaisia. Luokan kaikki tiedot salataan. Tiedon omistaja ja luokituksen asettaja määrittelee käyttöoikeudet tarpeen mukaan. Luokan dokumentit merkitään punaisella Highly Confidential vesileimalla asiakirjan sivuille. Luokan dokumentteja ei ole mahdollista tulostaa. Dokumenteista ei ole mahdollista ottaa kuvaruutukopioita Windows käyttöjärjestelmässä ja niiden jakaminen Teams onlinekokouksissa on estetty.

10.2 Luokan merkitseminen

Merkitseminen otetaan käyttöön kaikissa uusissa Microsoft ekosysteemin dokumenteissa, ohjelmissa ja viesteissä, jotka tukevat Azure Information Protection automaattista luokittelua. Tiedon oletusluokaksi määritellään General ja kaikki uudet dokumentit saavat tämän luokan, kun dokumentti luodaan. Tiedon luoja eli dokumentin ensimmäisen tallentajan vastuulla on arvioida tiedolle oikea luokka ja luokan asetusten mukaisesti tarvittaessa käyttöoikeudet salaukselle. Personal ja Public luokan dokumentteja ei erikseen nimetä ylä- tai alatunnisteessa. General luokan dokumenteissa luokka merkitään automaattisesti dokumentin oikeaan yläreunaan mustalla fonttikoon 12 tekstillä. Confidential luokan tunniste merkitään vastaavasti punaisella fonttikoon 12 tekstillä. Highly Confidential luokan dokumentit merkitään oikeaan yläreunaan fonttikoon 12 tekstillä sekä sivun keskelle punaisella fonttikoon 14 vesileimalla.

10.3 Luokkien käsittelysäännöt

Luokkien käsittelysäännöt on kuvattu alla olevassa taulukossa.

	Personal	Public	General	Confidential	Highly Confidential
Tiedon omistajan ja luoja vastuu	Luokan valinta	Luokan valinta	Luokan valinta	Luokan valinta	Luokan valinta, käyttöoikeuden määrittely
Käsittelypaikka	Ei rajoituksia	Ei rajoituksia	Käsittelyssä huimoitava, ettei tieto ole ulkopuolisten nähtävissä tai kuultavissa	Käsittelyssä huimoitava, ettei tieto ole ulkopuolisten nähtävissä tai kuultavissa	Käsittelyssä huimoitava, ettei tieto ole ulkopuolisten nähtävissä tai kuultavissa
Tallennus ja arkistointi	Ei rajoituksia	Ei rajoituksia	Ei julkisesti saatavilla	Salattuna	Salattuna
Tulostus	Ei rajoituksia	Ei rajoituksia	Ei rajoituksia	Teknisesti estetty	Teknisesti estetty
Merkintä	Sähköpostiviestin yläbannerissa	[Yrityksen nimi] - Public musta 12 koon fontti sivun ylätunnisteessa keskellä tai sliden oikeassa yläkulmassa, sähköpostiviestin yläbannerissa.	[Yrityksen nimi] - General musta 12 koon fontti sivun ylätunnisteessa keskellä tai sliden oikeassa yläkulmassa, sähköpostiviestin yläbannerissa.	[Yrityksen nimi] - Confidential punainen 12 koon fontti sivun ylätunnisteessa keskellä tai sliden oikeassa yläkulmassa, sähköpostiviestin yläbannerissa.	[Yrityksen nimi] - Highly Confidential punainen 12 koon fontti sivun ylätunnisteessa keskellä tai sliden oikeassa yläkulmassa sekä punainen 14 fontti koon vesileima sivun, sliden tai taulukon keskellä, sähköpostiviestin yläbannerissa.
Salaus	Ei määritelty	Ei määritelty	Ei määritelty	Vahva salaus, käyttöoikeus Domain Users -ryhmällä tai tiedon luoja määrittelemänä.	Vahva salaus tiedon luoja määrittelemänä.
Matkustaminen	Ei rajoituksia	Ei rajoituksia	Käsimatkatavarana	Käsimatkatavarana, PC ja puhelimen säilytys aina valvottuna.	Käsimatkatavarana, PC ja puhelimen säilytys aina valvottuna.

Taulukko 1 Luokkien käsittelysäännöt

10.4 Jatkotutkimusehdotukset

Luokittelumallin käyttöönoton jälkeen, kun käyttötilanteista on enemmän tietoa ja luokkien käytöstä on tullut rutiinia, ehdotetaan arvioitavaksi osastokohtaisten alaluokkien käyttöönottoa. Esimerkkejä suositeltavista alaluokista ovat Confidential luokan alle perustettavat Confidential HR ja Confidential Legal ja Confidential R&D alaluokat, joiden käyttöoikeudet perustuvat edellä mainittujen osastojen käyttäjien AD-ryhmiin.

Myöhemmässä vaiheessa myös kehittämissuunnitelmana on DLP (Data Loss Prevention) sääntöjen käyttöönottoa. Säännöillä on mahdollista automaattisesti tunnistaa ja suojata

esimerkiksi EU alueen henkilötunnuksia, luottokorttien numeroita tai pankkitilien tietoja. Sääntöihin on myös mahdollista tehdä yrityskohtaisia sääntöjä esimerkiksi erityisesti suojattavien projektien nimillä tai muilla avainsanoilla.

Lähteet

Painetut

Eskola, J. & Suoranta, J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino.

Heikkinen, H., Rovio, E. & Syrjälä, L. 2007. Toiminnasta tietoon. Toimintatutkimuksen menetelmät ja lähestymistavat. Dark Oy, Vantaa

Hirsjärvi, S. & Hurme, H. 2004. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. Helsinki: Tammi.

Jordan, E. & Silcock L. 2006. Strateginen IT-riskien hallinta. Edita Publishing Oy. Helsinki.

Järvinen, P. 2003. Salausmenetelmät. Jyväskylä: Docendo Finland Oy.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä: kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylän ammattikorkeakoulu. Jyväskylä.

Kananen, J. 2014. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylän ammattikorkeakoulun julkaisuja 176. Jyväskylä: Juvenes Print.

Kerko, P. 2001. Turvallisuusjohtaminen, PS-kustannus. Jyväskylä.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. WSOY. Juva.

Laaksonen, M. & Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy. Helsinki.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio. Gummerus Oy. Jyväskylä.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen: Näin suojaat yrityksesi toiminnan. Kauppakaari. Jyväskylä. Enterprise Adviser kirjasarja.

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Talentum Media Oy. Jyväskylä.

Ojasalo, K., Moilanen, T & Ritalahti, J. 2014. Sanoma Pro Oy. Helsinki.

Paavilainen, J. 1998. Tietoturva. Suomen ATK kustannus Oy. Jyväskylä.

Rousku, K. 2014. Kyberturvaopas Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Ruusuvuosi, J. & Tiitula L. 2015. Haastattelu - Tutkimus, tilanteet ja vuorovaikutus. Tampere. Vastapaino Oy.

Tuomi, J. & Sarajärvi, A. 2002. Laadullinen tutkimus ja sisällönanalyysi. Helsinki: Tammi.

Virtanen T. 1995. Johtajan tietoturvallisuusopas. Julkisen tietohallinnon neuvottelukunta. Helsinki.

Sähköiset

Digi- ja väestötietovirasto 2020. Viitattu 1.10.2020 <https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet>

Microsoft 2020. Viitattu 10.11.2020 <https://azure.microsoft.com/en-us/pricing/details/information-protection/>

Oikeusministeriö 2020. Edita Publishing Oy. Viitattu 11.10.2020. <https://www.finlex.fi/fi/laki/ajantasa/1999/19990731>

Oikeusministeriö 2020. Edita Publishing Oy. Viitattu 11.10.2020. <https://www.finlex.fi/fi/laki/alkup/2018/20181050>

Savolainen, Petri. 2013. Viitattu 2.10.2020. Kertakäyttösalausanajärjestelmä Yritysverkkoon kirjautumisessa. https://www.theseus.fi/bitstream/handle/10024/61587/Savolainen_Petri.pdf?sequence=1

Tietosuojavaltuutetun toimisto. 2020. Viitattu 5.11.2020 <https://tietosuoja.fi/gdpr>

Valtioneuvosto 2018. Viitattu 9.10.2020. Sähköisen viestinnän salaus- ja suojausmenetelmät. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160614/LVM_02_2018_Sahkoisen_viestinnan%20salaus_ja_suojaus.pdf

Julkaisemattomat

Sulava Oy. Azure Information Protection koulutus 1.7.2020

Kuviot

Kuvio 1 Luottamuksellisuustunnistet protection.microsoft.com portaalissa	24
Kuvio 2 Highly Confidential - Special luokan nimeäminen	25
Kuvio 3 Salauksen, käyttöoikeuden, offline käytön ja käyttäjäryhmän määrittäminen	25
Kuvio 4 Luokan merkitseminen vesileimalla ja ylätunnisteella	26
Kuvio 5 Luokkien valinta Outlook työpöytäsovelluksessa	27
Kuvio 6 Highly Confidential luokan vesileima Word dokumentissa	28
Kuvio 7 Luokan valinta iOS mobiilikäyttöjärjestelmän Word applikaatiossa	29
Kuvio 8 Vastaajien näkemys tiedon luokittelun tarpeellisuudesta kohde organisaatiossa	30
Kuvio 9 Vastaajien arviot tiedon luokittelun yleisyydestä asiakasorganisaatioissa.....	31
Kuvio 10 Teknologian hyväksikäyttö organisaatioiden tietojen luokittelussa	33
Kuvio 11 Automaattisen salauksen käyttäminen tietyissä luokissa	34
Kuvio 12 Automaattisen salauksen käyttöönoton ajankohta.....	35
Kuvio 13 Jakauma oletusluokka suosituksesta	36

Taulukot

Taulukko 1 Luokkien käsittelysäännöt	40
--	----

Liitteet

Liite 1: Haastattelukysymykset	46
--------------------------------------	----

Liite 1: Haastattelukysymykset

1. Kuinka tärkeänä näet organisaatiossa X tiedon luokittelun käyttöönoton?

Erittäin tärkeänä	<input type="checkbox"/>
Melko tärkeänä	<input type="checkbox"/>
Jonkin verran tärkeänä	<input type="checkbox"/>
En lainkaan tärkeänä	<input type="checkbox"/>
En osaa sanoa	<input type="checkbox"/>

Avoin vastaus:

2. Kuinka monessa organisaatiossa kenen kanssa teet yhteistyötä on käytössä tiedon luokittelu?

0-25%	<input type="checkbox"/>
25-50% x	<input type="checkbox"/>
50-75%	<input type="checkbox"/>
75-100%	<input type="checkbox"/>
En osaa sanoa	<input type="checkbox"/>

Avoin vastaus:

3. Kuinka monessa organisaatiossa, jonka kanssa teet yhteistyötä on käytössä teknologiaan perustuva tiedon luokittelu?

0-25%	<input type="checkbox"/>
25-50%	<input type="checkbox"/>
50-75%	<input type="checkbox"/>
75-100%	<input type="checkbox"/>
En osaa sanoa	<input type="checkbox"/>

Avoin vastaus:

4. Onko organisaatiossa, joissa käytetään teknologiaan perustuvaa tiedon luokittelua käytössä joidenkin luokkien automaattinen tiedon salaus?

Kyllä	<input type="checkbox"/>
Ei	<input type="checkbox"/>
En osaa sanoa	<input type="checkbox"/>

Avoin vastaus:

5. Onko tiettyjen luokkien automaattinen salaus aktivoitu heti luokkien käyttöönoton yhteydessä vai myöhemmässä vaiheessa?

Kyllä	<input type="checkbox"/>
Ei	<input type="checkbox"/>
En osaa sanoa	<input type="checkbox"/>

Avoin vastaus:

6. Millaisia tiedon luokkia suosittelet organisaation käyttöön?

7. Avoimet kommentit tai suositukset teknologiaan perustuvasta tiedon luokittelusta?