Opinnäytetyö (AMK)

Tieto- ja viestintätekniikka

2019

Patrik Jyränti

GDPR JA TIETOTURVATUOTTEISTUS PIENYRITYSYMPÄRISTÖSSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 29 sivua

Patrik Jyränti

GDPR JA TIETOTURVATUOTTEISTUS PIENYRITYSYMPÄRISTÖSSÄ

Euroopan yleinen tietosuoja-asetus 2016/679 (GDPR, General Data Protection Regulation) on vuoden verran voimassa ollut henkilötietojen oikea oppiseen ja tietoturvalliseen käsittelyyn keskittynyt säädös. Tietosuoja-asetus on tuonut monia muutoksia yrityksille ja yhteisöille siitä, miten henkilötietoja kuuluu käsitellä, miksi näin tehdään ja millä tavoin se toteutetaan. Vaikka tietosuoja-asetus hyväksyttiin vuonna 2016 ja otettiin täysin käyttöön 2018 kahden vuoden siirtymäajan jälkeen, on se kuitenkin vaikealukuista ja sisältää paljon lakiteknistä termistöä.

Opinnäytetyö on toteutettu yhteistyössä Admia IT-Palveluiden sekä Elda Oy LKV & Valokuvauksen kanssa palvelemaan mikro- ja pienyrityksiä sekä avustamaan mikro- ja pienyrityksiä implementoimaan valmiita tietoturvatuotteita olemassa oleviin järjestelmiinsä. Opinnäytetyön tavoitteena oli luoda helppolukuinen tietopaketti, jossa avataan Euroopan unionin yleistä tietosuoja-asetusta 2016/679 (*GDPR, General Data Protection Regulation*).

Opinnäytetyö on suoritettu kahdessa osassa. Ensimmäisenä oli varsinainen tutkimus, jossa määriteltiin yrityksen toimivuuden kannalta, millaisia ohjelmistoja ja palveluja yritykset tarvitsevat toimiakseen. Tällaisia voivat olla laskutustyökalut tai asiakasrekisterien ylläpitoon ja hallintaan liittyvät työkalut ja ohjelmistot. Toisena osuutena oli varsinainen käytännön työ, jonka tarkoituksena oli tutkia, onnistuuko tietoturvaratkaisujen siirtäminen yritysten välillä, vaikka yritykset toimivat eri aloilla.

Opinnäytetyö voi tällaisenaan toimia yleiskäytännöllisenä oppaana, minkä avulla voidaan arvioida yritysten tietoturvatasoja, sekä se lisää tietämystä yritysten kesken tietosuoja-asetuksesta.

ASIASANAT:

GDPR, tietoturva, yrittäjyys, auditointi

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and communications technology

2019 | 29 pages

Patrik Jyränti

GDPR AND INFORMATION SECURITY PRODUCTIZATION IN A SMALL BUSINESS ENVIRONMENT

The European General Data Protection Regulation 2016/679 is a legal act, that came in effect in 2018 and is the foundation for the correct usage and safe handling of personal data. The Data Protection Regulation has brought many changes to companies and communities on how personal data should be handled why and how it is implemented. Although the Data Protection Regulation was adopted in 2016 and was fully implemented in 2018 after a two-year transition period, it is cumbersome and contains a great amount of legal terminology.

The thesis has been produced in co-operation with Admia IT-Palvelut, and Elda Oy LKV & Valokuvaus to serve micro and small businesses, and to assist micro and small companies to implement ready-made security products into their existing systems. The aim of this thesis was to create an easy-to-read information package which explains the European Union General Data Protection Regulation 2016/679 (GDPR). The thesis has divided in two parts.

The first part of the thesis introduces, what factor determines the kind of software and services that companies need in order to comply with the act. The knowledge of this comes from the author's own experience as an entrepreneur. The very basic software and service needs are common and in daily use for most small business environments. These include billing tools or tools and software related to maintaining and managing customer registers. The second part describes the actual practical work which examine whether the transfer of security solutions between companies was successful, even though the companies were operating in different sectors. The second part was mostly based on literature researching and interviewing Elda's employees.

The actual result in the thesis was achieved. The work, which was carried out previously by Admia IT-Palvelut, could be simulated by another company. The thesis concludes that at the small enterprise level it is possible to transfer security solutions between companies, regardless of the field in which companies work.

As such, the thesis can serve as a general practice guide for evaluating the security levels of companies, as well as increasing awareness among companies of the privacy regulation.

KEYWORDS:

GDPR, information security, entrepreneurship, audit

SISÄLTÖ

KUVAT

1 JOHDANTO

1.1 Opinnäytetyön tausta

Olen itse yrittäjä ja tästä syystä opinnäytetyön aiheen valinta oli helppoa. Euroopan unionin yleinen tietosuoja-asetus 2016/679, eli tutummin GDPR, oli suurin yksittäinen muutos yritystasolla vuosiin ja halusinkin erityisesti juuri siitä syystä keskittyä tähän aiheeseen. Itse olin oman työni puolesta joutunut jo paljon ennen varsinaista voimaan tuloa tutustua aiheeseen, joten omassa yritystoiminnassani oli muutamia asioita, joita piti parantaa. Jäljelle jäi mm. rekisteriselosteiden valmistus käytettyjen ohjelmistojen osalta ja olemassa olevien tietoturvaratkaisujen tutkiminen ja mahdollinen vaihto parempiin ratkaisuihin. Koska opinnäytetyön on tarkoitus toimia ohjeistuksena pienyrityksille ja työn on tarkoitus olla yleispätevä, ja monella alalla toimiva, niin valitsin toisen pienyrityksen, Elda Oy LKV & Valokuvauksen yhteistyökumppaniksi opinnäytetyöhön. Eldalla oli jo olemassa olevat ratkaisut omaan tietoturvaansa, mutta katsoimme tämän työn yhteydessä, löytyykö työstäni jotain, millä olemassa olevia suojia voisi parantaa. Yritys on valittu mukaan siitä syystä, että se poikkeaa täysin oman yritykseni alasta. Lisäksi vaikuttavina tekijöinä oli suuri asiakastietojen määrä, jota yritys kerää.

1.2 Opinnäytetyön tavoitteet

Opinnäytetyön päätavoitteena on luoda helppolukuinen tietopaketti siitä, mitä GDPR on, mitä tietoturvallisuus tarkoittaa käytännössä, mitä vaaditaan tietosuoja-asetuksen, tietoturvan toteuttamiseksi ja miten se käytännössä toteutetaan. Opinnäytetyön on tarkoitus muodostaa kokonaisuus, jonka avulla jokainen alkava ja jo toimiva mikro- ja pienyritys voi tehdä oman GDPR-selosteensa, hankkia asianmukaiset tietoturvaratkaisunsa tietomurtojen varalle ja tutkia millaisia vakuutuksia yrityksille on tietomurtojen varalle. Lisäksi käydään pintapuolisesti läpi, mitä tehdään tietomurron sattuessa ja miten jatketaan siitä eteenpäin.

2 GDPR:N MERKITYS

GDPR, muodollisemmin Euroopan unionin yleinen tietosuoja-asetus 2016/679, on vuonna 2016 voimaan tullut, ja vuonna 2018 kahden vuoden siirtymäajan jälkeen täysin voimaan astunut tietosuoja-asetus EU:n kansalaisten henkilötietojen käsittelystä. Monet pienyritykset kamppailevat tämän aiheensa kanssa, eikä suotta, sillä aihe on tuore ja selkokielistä tekstiä on tuotettu vain vähän.

General Data Protection Regulation, eli GDPR, on EU:n tietosuoja-asetus. Asetus korvaa ja yhtenäistää eri maiden nykyiset säännöt. Se määrittelee, miten henkilötietoja saa käsitellä EU:ssa. Koko direktiivi on varsin pitkä ja sisältää paljon jo nyt Suomessa voimassa olevia säännöksiä. Vuoden 2018 käyttöönoton jälkeen kaikkien yritysten ja organisaatioiden on noudatettava uutta asetusta tuntuvien sakkojen uhalla. Asetus herättää huomattavasti kysymyksiä siitä, mitä tulee tehdä. Koko alueen kattava yhtenäistetty toimintapolitiikka tarkoittaa kuitenkin sitä, että kaikki ovat samojen sääntöjen edessä. (Findwise 2018.)

Tämän hetkiset rangaistukset tietosuoja-asetuksen seuraamatta jättämisestä ovat kovat. Tällä hetkelle rahallisesti määrätyt rangaistukset ovat 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. (EUR-Lex 2016.)

Uusi asetus korvaa EU:n aiemman asettaman henkilötietodirektiivin 95/46/EY sekä osittain Suomen lainsäädännössä henkilötietolain 523/1999. (EUR-Lex 2016.)

GDPR toi yritysmaailmaan käsitteet mm. rekisterinpitäjä, henkilötietojen käsittelijä, rekisteröity. Kaikilla näillä on omat merkityksenä ja omat erityispiirteensä. Näitä erityispiirteitä ovat esimerkiksi vastuualueet ja oikeudet. Tämä on hyvä tapa erotella työtehtävät ja toimintatavat eri toimijoiden kesken.

2.1 Rekisteröity ja rekisteröidyn oikeudet

Rekisteröidyllä tarkoitetaan luonnollista henkilöä/yksilöä, joka on tunnistettava tai tunnistettavissa oleva, joka on antanut luvan tallentaa omia henkilötietojaan yrityksen järjestelmiin.

Tietosuoja-asetus ei toistaiseksi päde yrityksiin itsenään, sillä yrityksiä ei lasketa luonnollisiksi yksilöiksi. Jos yritykselle on nimetty yhteyshenkilö, niin yhteyshenkilön osalta tietosuoja-asetukset puolestaan pätevät. Tällä tarkoitetaan esimerkiksi referenssi tapauksia yritysten välillä.

Rekisteröidyn oikeuksiin kuuluu seuraavat asiat:

- Rekisteröity saa tietää, että miten rekisterinpitäjät käyttävät ja käsittelevät hänen henkilötietojaan. Hänellä on myös oikeus nähdä täydellisesti hänen henkilötietoihinsa rekisterinpitäjien tietokannoissa ja saada tietoon, että mitä dataa rekisterinpitäjillä on hänestä tallessa. Näihin lukeutuvat myöskin muistiinpanot asiakkaasta, vaikka ne olisivat vain rekisterinpitäjän sisäiseen käyttöön. Rekisteröidyn esittäessä pyyntö saada tietoonsa, että mitä henkilötietoja hänestä on kerättynä, on rekisterinpitäjällä tietosuoja-asetuksen mukainen velvoite toimittaa koneluettava (yleensä .pdf- tai .csv-tiedosto) kuukauden kuluessa. Poikkeuksia löytyy, jos rekisteröidyn pyyntö on mittavan laaja tai monimutkainen, niin rekisterinpitäjällä on oikeus saada lisäaikaa kahden (2) kuukauden verran. Viivästyminen ja lisäajasta ilmoittaminen pitää kuitenkin aina olla perusteltua.
- Rekisteröidyllä on oikeus oikaista häntä koskevia, virheellisiä, henkilötietoja. Lisäksi rekisteröidyllä on halutessaan oikeus täydentää puuttuvia henkilötietoja.

- Rekisteröidyllä on oikeus tulla unohdetuksi. Tämä tarkoittaa sitä, että rekisterinpitäjä on velvoitettu poistamaan rekisteröidyn tiedot järjestelmistään kuukauden aikana niiltä osin, kun se on lain puitteissa mahdollista. Poikkeuksena on esimerkiksi laskutustiedot ja vanhat laskut, jotka kirjanpitolain mukaan pitää säilyttää kuusi (6) vuotta. Myöskin mikäli henkilö on historiallisesti tai tieteellisesti merkittävä persoona ja hänestä kerätään henkilötietoja tutkimustarkoituksia varten, on henkilötietojen poisto mahdollista evätä. Myöskin, mikäli rekisteröity on syyllistynyt rikokseen ja haluaa poistaa henkilötietonsa oikeudellisen vaateen estämiseksi, puolustamiseksi tai laatimiseksi on pyyntö henkilötietojen poistosta mahdollista evätä.
- Rekisteröidyllä on oikeus rajoittaa tai estää häntä koskeva henkilötietojen käsittely. Syitä tähän voivat olla esimerkiksi yleisen edun vuoksi tai toisen henkilön oikeuksien suojelemiseksi. Lisäksi rekisteröidyllä on oikeus kieltäytyä suoramarkkinoinnista. Rekisteröity voi kieltää yhden tai useamman suoramarkkinointitavan kerralla. Suoramarkkinoinniksi lasketaan tekstiviesti-, puhelu- ja sähköpostimarkkinointi, sekä yrityksen sisäinen profilointi, jolloin rekisteröidylle tarjotaan tietyn tyyppisiä tai tuotteita. Profilointi voi tapahtua iän, sukupuolen tai mielenkiinnonkohteiden kautta. (Tietosuojavaltuutetun toimisto 2018.)

2.2 Henkilötieto

Henkilötiedoiksi luetaan kaikki tiedot, joilla voidaan identifioida tai yksilöidä yksittäinen rekisteröity. Näitä tieto voivat olla esimerkiksi nimi, puhelinnumero, sähköposti, osoite tai erilaiset verkkotunnistetiedot.

Myös erilaiset biometriset tunnisteet, kuten sormenjälki, iiriskuva tai kuva henkilöstä lasketaan henkilötiedoiksi ja näitä koskee samat tietosuoja-asetuksen määräykset.

Lähtökohtaisesti henkilötiedot eivät saa pitää sisällään arkaluontoisia merkintöjä tai tietoja. Näiksi luetellaan esimerkiksi etnisyys, uskonnollisuus, poliittinen kanta tai seksuaalinen suuntautuminen. (Tietosuojavaltuutetun toimisto 2018.)

2.3 Rekisterinpitäjä

Rekisterinpitäjäksi kutsutaan tahoa, joka omistaa, sekä määrittelee ja hallinnoi sitä, että millä tavalla henkilötietoja käsitellään ja mihin tarkoitukseen henkilötietoja kerätään. Rekisterinpitäjiä voivat olla esimerkiksi yritykset ja organisaatiot, mutta myös potilastietoja käsittelevä sairaala tai sosiaalisen median palvelu. (Tietosuojavaltuutetun toimisto 2018.)

2.4 Henkilötietojen käsittelijä

Henkilötietojen käsittelijäksi kutsutaan tahoa, joka käsittelee henkilötietoja rekisterinpitäjän määrittelemällä tavalla. Näitä voivat olla yrityksessä esimerkiksi työntekijä, joka tarvitsee työssään henkilötietoja ja käsittelee niitä sitä kautta. Myöskin toinen yritys voi olla henkilötietojen käsittelijä. Tällaisia voivat olla esimerkiksi ulkoistettu laskutuspalvelu tai tilitoimisto, joka tekee palkanlaskentaa rekisterinpitäjän yrityksen työntekijöille.

Henkilötietojen käsittelyn vaadittava ohjeistus pitää olla tietosuoja-asetuksen mukainen. Tästä ohjeistuksesta vastaa rekisterinpitäjä. Myöskin henkilötietojen käsittelijän on varmistettava, että hänen omat työskentelytapansa täyttävät tietosuoja-asetuksen määräykset, vaikka tätä ei olisi erikseen määritetty rekisterinpitäjän ohjeistuksessa. (Tietosuojavaltuutetun toimisto 2018.)

2.5 Tietosuojavastaava

Tietosuojavastaava on erityisasiantuntija, joka on rekisterinpitäjän nimeämä henkilö, yleensä rekisterinpitäjän työllistämä, mutta tarvittaessa ostopalvelun kautta myös ulkopuoliselta taholta hankittua palvelua. Tietosuojavastaavan tehtäviin kuuluu avun antaminen rekisterinpitäjän yrityksen / organisaation henkilöstölle ja johdolle, sekä auttaa rekisterinpitäjää lakisääteisten velvoitteiden toteuttamisessa. Tietosuojavastaava toimii yrityksessä henkilötietojen käsittelyä valvovana tahona, sekä yhteyshenkilönä valvontaviranomaisiin, kuten tietosuojavaltuutettuun.

Tietosuojavastaava vaaditaan yrityksessä, mikäli käsiteltävä henkilötieto on erityisen arkaluontoista, tai henkilötietojen käsittely on yrityksen pääasiallinen tehtävä.

Käsitteinä ”säännöllinen” tai ”järjestelmällinen” ei ole avattu tietosuoja-asetuksessa, mutta voidaan tehdä olettamus, että mikäli henkilötietojen käsittely on jatkuvaa, henkilötietoja kerätään keskeytyksettä osana henkilötietojen keruustrategiaa, tai profilointi internetin kautta tehtynä edes satunnaisesti, on nämä tietosuoja-asetuksen mukaisia perusteita nimetä erillinen tietosuojavastaava. (Tietosuojavaltuutetun toimisto 2018.)

2.6 Tietosuoja- ja rekisteriseloste

Tietosuoja- ja rekisteriselosteet toimivat parhaina tapoina tiedottaa rekisteröityä ja valvontaviranomaisia siitä, miten rekisterinpitäjä hallinnoi ja vartioi henkilötietojen käsittelyä. Lisäksi nämä rekisteritiedot ovat tapa osoittaa rekisteröidylle, että millaisia henkilötietoja heistä kerätään, jonka kautta rekisteröity voi vaatia poistoa tai korjauksia omille henkilötiedoilleen. Tietosuojaselosteen on tarkoitus kattaa kaikki rekisterit, jotka rekisterinpitäjällä on käytössä, kun puolestaan rekisteriseloste tehdään jokaisesta rekisteristä erikseen. Tietosuoja- ja rekisteriselosteiden tekeminen on vaatimus jokaisella yrityksellä, joiden henkilöstömäärät ovat 250 henkeä tai yli. Lisäksi pienyrityksille samaiset selosteet ovat pakollisia, jos

- Henkilötietojen käsittely ei ole satunnaista
- Henkilötiedot käsittelevät arkaluontoista tietoa tai erityisryhmiin kuuluvien ihmisten tietoja. Näitä voivat olla esimerkiksi potilastiedot tai oikeuden määräämät tuomiot tai rikostutkintaan liittyvät tiedot
- Henkilötietojen käsittely voi aiheuttaa tai aiheuttaa riskin rekisteröidyn oikeuksille tai rekisteröidyn vapauksille. Näitä voivat olla esimerkiksi rekisteröidyn kehitykseen ja tai terveyteen liittyvät syyt

Tietosuojaseloste pitää olla saatavana pyynnöstä, sekä se pitää esittää asiakkaalle tai rekisteröidylle pyydettäessä, mikäli asiakkaasta kerätään henkilötietoja.

Tietosuojaselosteelle ei ole standardipohjaa, mutta sen on hyvä vastata ainakin seuraaviin kysymyksiin:

- Rekisterinpitäjä. Lisää myös rekisterinpitäjän yhteystiedot.
- Yhteyshenkilö rekisteriä koskevissa asioissa. Yleensä tämä on rekisterinpitäjälle toimiva tietosuojavastaava. Lisää myös tietosuojavastaavan yhteystiedot.

- Rekisterin nimi. Listaa tietosuojaselosteessa kaikki rekisterit, jotka rekisterinpitäjällä on käytössä. Näitä voivat olla esimerkiksi asiakas-, markkinointi- ja laskutusrekisteri.
- Henkilötietojen käsittelyn tarkoitus. Tähän avataan, että miksi rekisteriä tarvitaan, sekä miten ja mitä sillä tehdään. Esimerkiksi onko kyseessä uutiskirjeille tarkoitettu mainos- ja markkinointirekisteri vai suoramainontarekisteri, vai kerätäänkö tietoja yhteisen hyvän edun vuoksi, kuten tieteelliseen tarkoitukseen.
- Rekisterin tietosisältö. Millaista tietoa rekisterinpitäjä kerää? Onko tarkoituksen mukaista, että rekisteröidyn henkilötiedot kerätään täydellisenä, eli sisältäen esimerkiksi vahvaan tunnistukseen riittävät tuntomerkit, kuten henkilötunnuksen, vai riittääkö rekisteröidystä pelkkä nimi tai vastaava henkilötieto?
- Säännönmukaiset tietolähteet. Mistä rekisterinpitäjä hankkii tiedot?
- Tietojen säännönmukainen luovutus. Myydäänkö tietoja eteenpäin vai luovutetaanko nämä esimerkiksi vain viranomaismääräyksestä, eli käräjäoikeuden määräyksestä eteenpäin.
- Tietojen siirrosta EU:n tai ETA:n ulkopuolelle. Tarvitseeko näitä tietoja siirtää? Onko rekisterinpitäjällä käytössä asiakasrekisteri, jonka palvelimet sijaitsevat esimerkiksi USA:ssa, jolloin tietojen säilytys tapahtuu EU/ETA-alueiden ulkopuolella?
- Rekistereiden suojauksen periaatteet. Miten henkilötietojen käsittelyä suojataan. Tietoturva ei ole riittävä vastaus tähän kysymykseen. Lisäksi on hyvä eritellä, että miten rekisterinpitäjä käsittelee manuaalista, eli paperilla olevaa henkilötietoa, ja automaattista, eli tietokoneella käsiteltäviä henkilötietoja. Vastauksia voivat olla esimerkiksi, että rekisterinpitäjällä on hallussaan arkaluontoisille papereille tarkoitettu oma, lukollinen, jäteastia, mihin henkilötiedot, mitä ei enää käsitellä, laitetaan. Tietokoneella tapahtuvasta henkilötietojen käsittelystä puolestaan varmistuu siitä, että tietoturva kaikilla tietokoneilla, millä tätä tehdään, on tietoturva kunnossa. Lisäksi on hyvä tarkastaa, että käytössä olevissa ohjelmistossa on uusimmat lisenssit/versiot asennettuna. Sovellus- ja ohjelmatuottajat vastaavat siitä, jos tuote on aktiivisesti kehityksessä, että se on myös tietoturvallinen.

  Lisäksi voit esimerkiksi mainita, että yrityksenne sähköpostipalvelimelta lähtevät kaikki kaksi vuotta vanhat sähköpostit automaattisesti roskakoriin.

- Tietojen tarkastusoikeus. Millaisilla ehdoilla rekisterinpitäjä antaa tietoja tarkastettavaksi? Onko se paperinen kopio, joka lähetetään asiakkaalle, vai onko kyseessä koneluettava painos henkilötiedoista? Sallitut tiedostomuodot ovat .pdf ja .cvs.
- Tietojen oikeellisuuden korjaaminen. Miten nopeasti rekisterinpitäjä reagoi tietojen muutospyyntöihin. Onko se esimerkiksi 7 vuorokautta tai 30 vuorokautta. Tällä hetkellä tietosuoja-asetuksen määrittelemä suurin aikamääre on yksi kuukausi, eli 30 vuorokautta.
- Muita henkilötietojen käsittelyyn liittyviä oikeuksia. Tähän listataan, mikäli rekisterinpitäjällä on ylimääräisiä oikeuksia henkilötietojen käsittelyssä. Esimerkiksi potilastietojen käsittely, jolloin toimitaan toisten etujen mukaisesti. (Admia IT-Palvelut 2018.)

Rekisteriseloste pääasiassa samat kysymykset sisällään. Poikkeuksena on, että jos tietojen oikeellisuuden korjaaminen tai muita henkilötietojen käsittelyyn liittyviä oikeuksia on muutettu rekisterin osalta, niin myös näihin kysymyksiin vastataan. Rekisteriseloste tehdään koskien jokaista rekisteriä ja ohjelmistoa erikseen. Eli esimerkiksi asiakas- ja markkinointirekisteristä pitää olla rekisteriseloste, samoin sosiaalisen median palveluista ja laskutuksesta. Mikäli rekisterinpitäjällä on käytössään laajempia ohjelmistokokonaisuuksia, kuten CRM ja SAP-ohjelmistot, niin näistä ja niiden osa-alueista tulee tehdä myöskin omat rekisteriseloteet.

2.7 GDPR – ketä tämä koskettaa?

Euroopan unionin yleinen tietosuoja-asetus koskee kaikkia Euroopan unionin asukkaita ja säädöksen tarkoituksena on saattaa eri EU:n jäsenmaiden henkilötietojen käsittelyyn liittyvät lait ja tietosuojalait lähemmäksi toisiaan muodostaen yhden, identtisen, tavan käsitellä tietoja.

Tietosuoja-asetuksen on tarkoituksena suojata EU:n asukkaita, joten tietosuoja-asetus koskettaa myös EU:n ulkopuolella olevien maiden, yrityksien ja toimijoiden henkilötietojen käsittelyä. Euroopan unionin yleisen tietosuoja-asetuksen mukaan jokaiselle EU:n kansalaiselle on taattava samanlainen henkilötietojen käsittely, riippumatta, että mistä henkilökäsittelyä tehdään.

Yhdysvalloissa on lukemattomia yrityksiä joutunut sulkemaan omat verkkosivunsa ihmisiltä, jotka yrittävät ottaa niihin yhteyden EU:n sisältä. Tällaisia toimijoita ovat esimerkiksi Tronc and Lee Enterprises media publishing groups -konserni, joka on sulkenut seuraavat sivut (BBC 2018.)

- New York Daily News
- Chicago Tribune
- LA Times
- Orlando Sentinel
- Baltimore Sun

3 TIETOTURVA JA TIETOMURTO

Usein sekoitettavat termit tietosuoja ja tietoturva kuulostavat samalta, mutta tarkoittavat kahta eri asiaa. Tietoturva on oma osansa tietosuojan alla, vaikka tietoturva kattaa myös paljon muuta, mikä ulottuu tietosuojan ulkopuolelle.

Tietoturva ja tietosuoja voidaan jakaa moneen alakategoriaan, joiden kanssa tarkoitetaan tiettyä osa-aluetta. Tämän tekstin osuudessa käsitellään vain tietoteknistä osuutta tietoturvasta ja tietosuojasta.

3.1 Tietoturva

Tietoturvalla ja tietoturvallisuudella tarkoitetaan tiedon saatavuutta (*availability*), luottamuksellisuutta (*confidentiality*) ja eheyttä (*integrity*) tiedon ylläpidollisessa mielessä. Kun puhutaan tietoteknisestä tietoturvasta, niin näitä lauseita on tuotu täydentämään käsitteet tunnistus (*detection*), todennus (*authentication*) ja kiistämättömyys (*non-repudiation*). (Hakala ym. 2016)

Tietoturvan päätarkoituksena yritysmaailmassa on rajata tietoa sisäiseen käyttöön ja valvontatoimilla huolehtia siitä, että ulkopuoliset eivät pääse tätä tietoa käsittelemään. Tämä johtaa siihen, että on todennettavissa kuka tietoa saa käsitellä. Kun todennus on tapahtunut, luo tämä kiistämättömyyden, jonka kautta käsittelijä ei voi kiistää omaa osallisuuttaan tietyn datan virheelliseen, tai virheettömään, käsittelyyn. Tällä tavoin tarvittu data ovat saatavilla, luottamuksellisia ja ehyitä.

Tietoturvalla tarkoitetaan yleisimmin tietokonemaailmassa sitä, että koneet ovat suojattuna virustorjuntaohjelmistoilla, mutta tämä ei välttämättä riitä yritysmaailmassa. Virustorjuntaohjelmistojen lisäksi yrityksillä on lukuisia muita vaihtoehtoja suojautua erilaisilta haittaohjelmilta, viruksilta tai tietomurroilta. Jos lähdetään rakentamaan tietoturvaa, niin ensimmäinen askel on ottaa tietokoneeseen ym. virustorjuntaohjelmisto, mutta myöskin varmistua siitä, että käyttöjärjestelmä, sekä käytössä olevat ohjelmistot ovat päivitetty uusimpiin ohjelmistoversioihin. Tällä pääsee pienyritystasolla jo hyvin pitkälle, mutta jos yrityksessä työskentelee useampi henkilö ja päätelaitteita alkaa olla enemmän, on suotavaa jatkaa tietoturvan kehittämistä. Mahdollisia ratkaisuja tietoturvan kehittämiseen voivat olla jotkin seuraavista

3.2 Palomuuri

Palomuurit ovat kuin portinvartijoita, joiden tarkoituksena on estää asiaton liikenne internetistä sisäverkkoon ja sisäverkosta internetiin. Nämä ovat itsessään hyvin suosittuja ratkaisuja pienten yritysten sisäverkkoratkaisuissa ja näiden kautta saavutetaan seuraavan asteen tietoturvataso pienellä sijoituksella. Palomuurin toimintaperiaate perustuu TCP/UDP-porttien seurantaan ja niistä lähtevän datan käsittelyyn. Palomuuri seuraa tarkasti TCP-paketin kulkua sisäverkossa ja tutkii sisältääkö lähtevät tai saapuvat paketit komentoja, jotka ovat kiellettyjä. Näitä voivat olla esimerkiksi erilaiset kyselyt (*request*) laitteista, millä määritetään koneen IP-osoite.

3.3 Virtuaalinen erillisverkko

Virtuaalinen erillisverkko (VPN (*Virtual Private Network*), on tapa yhdistää erilliset tietokoneet ja palvelimet julkisen verkon yli luoden yksityisen verkon. Virtuaalisen erillisverkon edut ovat sen tekniikassa. Kun VPN-palvelua käytetään, muodostaa se palveluntarjoajan palvelimen ja tietokoneen välille siis oman yksityisen verkkonsa. Tässä välissä verkon pakettitiedot salataan erilaisten algoritmien kanssa, luoden yhteyden datankäsittelystä anonyymiä. Myöskin maininnan arvoista on se, että kun palvelu on koneilla käytössä, piilottaa se koneen oman IP-osoitteen ja siirtyy käyttämään palveluntarjoajan palvelimen määräämää IP-osoitetta. Tällä tavoin saadaan luotua lisäharhautus muille palveluntarjoajille, kuten verkko-operaattoreille, jotka tutkivat ja valvovat verkkoliikennettä laittomuuksien varalta. VPN-palvelu ei itsessään ole laitoin, eikä sitä käytetä yksinomaan laittomuuksien tekemiseen, vaan juurikin verkon lisäturvallisuuden luomiseen.

Suosituimpia, maksullisia, palveluntarjoajia VPN-palveluista Suomessa ovat F-Secure ja NordVPN.

3.4 Käyttäjän luomat tietoturvariskit

Yksi suurimmista tietoturvariskeistä tällä hetkellä on käyttäjän itse luomat tietoturvaongelmat. Tällaisiksi voidaan luetella huolimaton käyttäytyminen netissä, sekä saastuneiden ohjelmien lataaminen suoraan työasemalle tai palvelimelle.

Koko ajan suositummaksi tulevat phishing-kalastelut, joko sähköpostitse tai verkkosivujen ponnahdusikkunoiden kautta tulevat tarjoukset, ilmaisista tuotekokeiluista, jotka yrittävät kalastella luottokorttitietoja tai henkilötietoja, joita myydään eteenpäin.

Phishing-hyökkäykseksi voidaan myös kutsua sähköposteja, jotka ovat esimerkiksi tulleet näennäisesti pankilta ja viestissä pyydetään käyttäjätunnusta ja salasanaa tai kirjautumaan pankin sivuille sähköpostin linkin kautta, koska viestin mukaan verkkopankissa on ”vakava virhe, joka pitää korjata ensi tilassa”. Yleensä viestit on kirjattu verrattain hyvällä suomen kielellä ja sähköposti on tullut osoitteesta turva.<pankin nimi. Esimerkiksi Nordea tai Säästöpankki>.fi, joka saa ihmiset epäileväisemmiksi, että onko kyseessä todella ongelma, joka pitää korjata.

Toinen yleinen tapa luoda tietoturva aukko käyttäjän toimimesta, on ladata toisen luoma tiedosto. Tässä esimerkissä lataus on Microsoft Office Word-pohja tuntemattomalta alusta ja antaa ohjelman avautua muokattavassa tilassa, jolloin siihen mahdollisesti sisällytetty haittaohjelma pääsee vapaasti kulkemana koneen sisällä, koska käyttäjä on itse antanut sille luvan avautua tietokoneella.

3.5 Tietomurron sattuessa

Kuten FBI:n edellinen johtaja Robert Mueller jo tiesi, niin on olemassa kahdenlaisia yrityksiä ja organisaatioita. On hakkeroituja yrityksiä ja sitten on yrityksiä, jotka tullaan hakkeroimaan. Uuden tietosuoja-asetuksen myötä tietomurtoihin suhtaudutaan yhä vakavammin.

Tietomurrolla tai henkilötietojen tietoturvaloukkauksella tarkoitetaan erilaisia tapahtumia, joiden vuoksi henkilötietoja tuhoutuu, muuttuu, häviää, luovutetaan asianosattomille luvattomasti tai ne päätyvät käsiin, joille ei ole oikeutta käsitellä rekisterinpitäjän henkilötietoja. (Tietosuojavaltuutetun toimisto 2018.)

Tietomurto tai henkilötietojen tietoturvaloukkauksellisia asioita voivat olla esimerkiksi

- Varastettu tietokone
- Haittaohjelmatartunta tai virus
- Hävinnyt datamedia, kuten ulkoinen kovalevy
- Hakkerointi järjestelmiin (Tietosuojavaltuutetun toimisto 2018.)

Tietomurron sattuessa Suomen tietosuojavaltuutettu, Reijo Aarnio, on antanut selkeät toimintaohjeet, miten toimia

- Selvitetään tietomurron / tietoturvaloukkauksen laajuus ja vakavuus. Käsitteleekö rekisterinpitäjä henkilötietoja? Miten arkaluontoista järjestelmissä olevat henkilötiedot ovat? Esimerkiksi onko kyseessä asiakkaan aikakausilehden tilaustiedot, joiden arkaluontoisuus on huomattavasti vähäisempää, kuin samaisen aikakausilehden maksutiedot. On hyvä ymmärtää, että rekisterinpitäjän ja henkilötietojen käsittelijän on suojattava järjestelmät niin, että suojaustoimet ovat linjassa henkilötietojen käsittelyyn liittyvien riskien kanssa.
- Dokumentoidaan kaikki tietoturvaloukkaukset ja arvioidaan vahinkojen määrä. kuinka paljon henkilötietoja ja muuta dataa on viety tai saatettu viedä?
- Tee ilmoitus valvontaviranomaisille 72 tunnin kuluessa huomatusta murrosta. Mikäli aikamääreeseen ei pystytä, pitää valvontaviranomaisille tehdä kirjallinen ja perusteltu selvitys tapahtumasta ja syistä, jotka estivät ilmoittamisen.
- Henkilötietojen arkaluontoisuus määrittelee, että miten nopeasti rekisterinpitäjän pitää ilmoittaa rekisteröidylle tietomurrosta ja henkilötietojen kaappauksesta. Jos tiedot pitivät sisällään esimerkiksi luottokorttitiedot, on aiheellista ilmoittaa viipymättä rekisteröidylle, että kortti pitää sulkea. Lisäksi rekisteröidylle pitää ilmoittaa yhteystiedot henkilöstä (esimerkiksi tietosuojavastaava), joka antaa lisätietoja tietomurrosta ja varastetusta henkilötiedosta. (Tietosuojavaltuutetun toimisto 2018.)

4 TIETOTURVATUOTTEISTUS PIENYRITYKSILLE

Opinnäytetyön teknisenä ja käytännöllisenä osuutena oli uudelleen mallintaa toimivat tuotevalinnat oman yritykseni tietoturvaratkaisuista ja määrittää ne toiseen pienyritykseen, joka toimii täysin eri alalla, kuin yritykseni. Tämän testauksen ansiosta loin olettamuksen, että kyseisiä tietoturvaratkaisuja voidaan hyödyntää myös muissa yrityksissä ilman, että tämän ohjeistuksen pitää olla alakohtainen. Yhteistyökumppanilla, Elda Oy LKV & Valokuvauksella (jäljempänä ”Elda), oli käytössään jo omat tietoturvaratkaisunsa. Tietoturvallisuus syistä opinnäytetyö ei avaa sitä, otettiinko jotain alla olevista tuotteista ja ratkaisuista, tai niiden osista varsinaiseen tuotantoon asti. Opinnäytetyö on tehty olettamuksella, että lähdemme uudelle yritykselle rakentamaan koko tietoturvan alusta.

4.1 GDPR

Alkuselvitykseen kuuluu selite siitä, minkälaisten ohjelmistojen kanssa toimitaan ja miten ohjelmistot ovat tuotettu sekä kenellä on vastuu mahdollisen tietomurron yhteydessä. Alalla on vain muutama vallitseva ohjelmisto, jonka pohjalle välitystoiminta on helppoa perustaa. Tämä johtuu niiden helppokäyttöisyydestä ja monipuolisuudesta. Tuotteet ovat Alma Media Oyj:n tuottama eKivi-pilvipalvelu sekä Oikotie Asunnot Oy:n kehittämä PDX+–ohjelmisto. Tässä tapauksessa Elda käyttää Alma Median tuottamaa eKivi-palvelua.

Ensimmäinen selvityksen kohde oli, onko eKivi/Alma Media vai Elda rekisterinpitäjänä. Vaikka eKivi sisältää asiakastietoja ei sitä yksiselitteisesti voi luokitella rekisterin pitäjäksi. Asia ei ole ihan yksikertainen ja vaatii vähän tarkennusta.

Alma Media Oyj ylläpitää rekistereitä ja se tekee siitä myös rekisterinpitäjän. Normaalisti Alma Median suoria asiakkaita ovat kiinteistönvälitysyritykset ja kiinteistönvälittäjät. Mutta koska Elda on tuottanut varsinaisen rekisterin eKivi-palveluun, niin tämä tekee myös Eldasta rekisterinpitäjän. Kun kyseessä on tilanne, jossa yrityksiä on kaksi tai useampia ja yksi alusta, jonka sisällä tiedot ovat, kutsutaan näitä yhteisrekisterinpitäjiksi ja nämä puolestaan tuo rekisterinpitäjän vastuut molemmille yrityksille.

Kun Eldan oikeudet ja vastuut oli selvitetty, piti selvittää, että miten eKivi on hoitanut oman osuutensa ylläpidosta ja tietoturvasta. Varsinaisesta tietoturvatasosta löytyy hyvin vähän tietoja, mutta mainoksen mukaan heidän järjestelmänsä sähköisen arkistoinnin osalta on AVI:n (Aluehallintovirasto) hyväksymä, joka voidaan asettaa tässä vertailussa sopivaksi rajaksi.

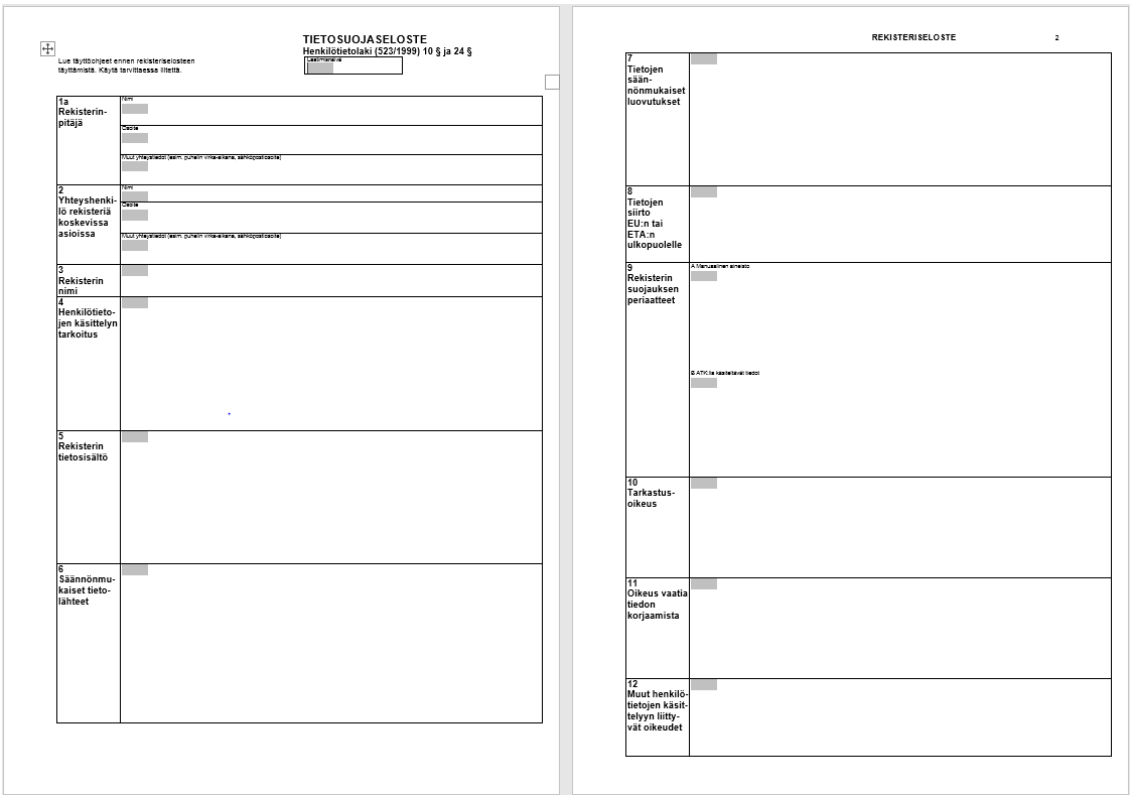
ASIAKASHALLINTA	eKIVI
GDPR-asetuksen mukainen henkilötietojen hallinta	☑
Asiakastietojen ylläpito ja hyödyntäminen lomakkeilla	☑
Asiakashistoria ja asiakkaiden luokittelu	☑
Yhteydenottojen hallinta, sähköpostien, tekstiviestien ja PDF-esitteiden lähettäminen	☑
TOIMEKSIANNOT	
Sähköinen arkistointi (AVIn hyväksymä)	☑
Toimeksiantosopimukset (PDF), selostusliitteet (PDF), kuluseuranta, taloyhtiötiedot	☑
Toimeksiantosopimuksen sähköinen allekirjoitus (myynti ja vuokraus)	☑
Ostotarjoukset (PDF), kauppakirjat (RTF) ja vuokrasopimukset (RTF)	☑
Ostotarjouksen sähköinen allekirjoitus	☑
Varainsiirtoverolaskelmat, laskut ja tilisiirrot (PDF)	☑
Ostotoimeksiantosopimukset (PDF) ja kohteen tiedot	☑
Ostotoimeksiantosopimuksen sähköinen allekirjoitus	☑
Vahdin liittäminen ostotoimeksiantoon	☑
Tarjouskauppa*	☑
Arviolausunnot (PDF) / arviokirjojen arkistointi	☑
KOHTEET	
Kohteen tiedot, kuvat, video- ja virtuaaliesittelyt	☑
Myyntiesitteet (PDF) ja ikkunakortit (PDF)	☑
Kohde-esitys (sähköinen ikkunakortti)	☑
Paremmat kuvat*	☑
SIIRROT MARKKINAPAIKOILLE (Huom. edellyttää voimassaolevaa erillistä sopimusta ko. markkinapaikalle)	
Etuovi.com, Vuokraovi.com, Oikotie.fi -siirrot sisältyvät hintaan, muut sopimuksen mukaan*	☑
Kohdetietojen siirtäminen omille kotisivuille / Wordpress pluginiin*, REST	☑
Mindworking-esitesiirto*	☑
Netvisor-laskusiirto*	☑
RAPORTOINTI	
Päiväkirjat	☑
Myynti-, palkkio-, toimeksiantovarasto- ja hankintaraportit	☑
Raportointitasot: henkilö, yritys, alue, konserni	☑
VAHDIT	
Myynti-, palkkio-, toimeksiantovarasto- ja hankintaraportit	☑
Raportointitasot: henkilö, yritys, alue, konserni	☑
DOKUMENTTIPANKKI	
Tiedostojen lisääminen toimeksiantojen yhteyteen	☑
Yhteisten mallipohjien ja tiedostojen hallinta	☑

Kuva 1. eKivi-pilvipalvelun tuoteominaisuudet

Eldalla on käytössään myös muita ohjelmistoja ja tuotteita, kuten tilit sosiaalisessa mediassa, sekä kolmannelta osapuolelta ostettu pilvipalvelu tallennustilaksi. Kaikista tehtiin erikseen vielä rekisteriselosteet.

4.2 Tietosuoja- ja rekisteriselosteiden valmistus

Koska yritys käsittelee runsaasti henkilötietoja, jotka ovat osittain arkaluonteisia, pitää tietosuoja-asetuksen mukaiset selosteet valmistaa. Pohjat ovat olleet käytössä jo ennen tietosuoja-asetusta ja ovat alun perin suunniteltu Suomen henkilötietolain 523/1999 mukaisiksi, mutta varsinaisen sisältönsä puolesta toimivat edelleen pienyrityksille täyttäen GDPR-vaatimukset.



TIETOSUOJASELOSTE
Henkilötietolaki (523/1999) 10 § ja 24 §

Lue täyttöohjeet ennen rekisteriselosteen täyttämistä. Käytä tarvittaessa liitettä.

1a Rekisterinpitäjä	Nimi Osoite Muut yhteystiedot (esim. puhelin virka-aikana, sähköpostiosoite)
2 Yhteyshenkilö rekisteriä koskevissa asioissa	Nimi Osoite Muut yhteystiedot (esim. puhelin virka-aikana, sähköpostiosoite)
3 Rekisterin nimi	
4 Henkilötietojen käsittelyn tarkoitus	
5 Rekisterin tietosisältö	
6 Säännönmukaiset tietolähteet	

REKISTERISELOSTE 2

7 Tietojen säännönmukaiset luovutukset	
8 Tietojen siirto EU:n tai ETA:n ulkopuolelle	
9 Rekisterin suojauksen periaatteet	A Manuaalinen aineisto B ATK:lla käsiteltävät tiedot
10 Tarkastusoikeus	
11 Oikeus vaatia tiedon korjaamista	
12 Muut henkilötietojen käsittelyyn liittyvät oikeudet	

Kuva 2. Tietosuojaseloste

4.3 Tietoturvaohjelmistojen yleiskatsaus

Tietoturva on monialainen käsite ja vaatii toimiakseen monta erilaista elementtiä. Opinnäytetyötä varten vertailtiin useita eri tietoturvatoimittajien tuotteita. Tässä vertailussa käytetty kokoonpanona kymmentä tietokonetta ja kymmentä älypuhelinta tai tablettitietokonetta. Toiminta pääasiassa yksittäisessä toimistossa ja sisäverkossa, sekä älypuhelimet tai tablettitietokoneet mukana asiakaskäynneillä.

Koska pelkkien virustorjuntaohjelmistojen osalta valinta on suuri, niin vertailut opinnäytetyössä on rajattu kolmeen.

4.3.1 F-Secure

F-Secure Oyj on vuonna 1988 Helsingissä perustettu tietoturvatuotteita ja ratkaisuja loppulaitteille tarjoava yritys. Vuoteen 1999 asti yritys tunnettiin nimellä Data Fellows Oyj. Käyttäjämäärästä ei ole tarkkaa selostusta. (Wikipedia 2019.)

F-Securen päätuote yrityksille on PSB (Protection Service for Business), joka sisältää hallintaportaalin, Computer Protectionin, Mobile Protectionin ja Server Securityn. (F-Secure 2019.)

F-Secure ei itse myy omia tuotteitaan, vaan on jalkauttanut eri jälleenmyyjille. Tässä tapauksessa hintatiedot on tarkastettu Telia Finland Oyj:ltä.

F-Secure Computer Protection-palvelu sisältää

- DeepGuard 6
- Tietojen suojaaminen
- Sisällön suodatus
- Selauksen suojaus
- Sovellushallinta
- Laitehallinta
- Ohjelmistopäivitysten hallinta
- Hallittava palomuuri
- Haittaohjelmien torjunta (Telia Finland, 2019)

F-Secure Mobile Protection-palvelu sisältää

- VPN
- Sovellusten suojaus
- Selauksen suojaus
- Hallittu varkaudenesto
- Tietoturvan seuranta
- Salasanan pakotus
- Laitetiedot
- Seurannan esto
- Virtuaalinen sijainti (Telia Finland 2019.)

Hinnat laitetta kohden ovat 3,50 euroa kuukaudessa. (Telia Finland, 2019) ja tämä tuo kustannukseksi 840 euroa vuodessa. Laskukaavassa on 10 tietokonetta ja 10 mobiililaitetta.

Hinnat eivät silti F-Securen osalta ole täysin vertailukelpoisia muihin nähden, sillä F-Securella ei ole erillistä tuotetta pienyrityksille, vaan samat tuotteet käyvät mikro- ja pienyrityksistä aina pk-tason yrityksille asti. Toisin sanoen suojaus on samalla tasolla, kuin isoissa yrityksissä, mutta hinnan määrittelee loppulaitteiden lukumäärä.

4.3.2 Bitdefender

Bitdefender on vuonna 2001 Romanian Bukarestissa perustettu tietoturvaohjelmistoja tuottava yritys. Vuonna 2018 Bitdefenderin tuotteitta oli asennettuna yli 500 miljoonaan loppulaitteeseen. Bitdefenderillä tunnetuin pienyrityksille suunnattu suojausohjelmisto on Small Office Security. Rajoitettujen tuoteominaisuuksien vuoksi emme voi kuitenkaan ottaa tätä tuotetta mukaan vertailuun, vaan valitsemme Bitdefender GravityZone Advanced Business Security -tietoturvatuotteen. (Bitdefender 2019.)

Bitdefender GravityZone Advanced Business Securityn -tietoturvatuote sisältää seuraavat ominaisuudet

- Tuki Windows, Mac ja Linux käyttöjärjestelmille
- Tuki Windows ja Linux palvelinkäyttöjärjestelmille
- Tuki mobiililaitteille

- Virustorjunta
- Palomuuri
- Laitehallinta
- Sovellushallinta
- Koko kovalevyn salaus
- Verkkosivustojen suojaus
- Laajat raportointimahdollisuudet
- SIEM-integraatiot
- Päivitysten hallinta
- Ilmoitukset
- Prosessien valvonta ja keskeytys virusepäilyjen vuoksi (Bitdefender 2019.)

Bitdefender GravityZone Advanced Business Security on kattava tietoturvatuote, mutta samalla vertailujen tuotteista ehdottomasti kallein. Bitdefender GravityZone Advanced Business Security kustantaa vuodeksi 939,99 euroa 20 laitteelle. (Bitdefender 2019.)

4.3.3 Kaspersky Lab ZAO

Laboratoriya Kasperskogo, tai tutummin Kaspersky Lab ZAO, on vuonna 1997 Moskovassa perustettu tietoturvayhtiö. Kasperskyn tuotteita käyttää 400 miljoonaa kotikäyttäjää ja yritystuotteilla on 270 000. Tunnetuin pienyrityksille suunnattu suojausohjelmisto on nimeltään Small Office Security.

Kaspersky Small Office Security -tietoturvaratkaisu sisältää seuraavat ominaisuudet

- Tuki Windows ja Mac käyttöjärjestelmille
- Tuki Windows-pohjaiselle tallennuspalvelimelle
- Tuki Android puhelimille ja tableteille (ei iOS tukea)
- Virustorjunta
- Roskapostisuodatin
- Salasanojen hallintaohjelmisto
- Verkkosivustojen suojaus
- Suojaus verkkopankin käyttöön
- Tietojen varmuuskopiointi
- Verkkosivustojen hallinta

- Tiedostojen salaus (Kaspersky 2019.)

Tuotepaketti ei itsessään ole niin kattava, kuin ylemmät vaihtoehdot, mutta tämä puolestaan kompensoituu hinnassa. Kaspersky Small Office Securityn kustannukset ovat 390 euroa vuodessa. (Kaspersky 2019.)

4.4 Tietoturvaohjelmiston vertailu ja valinta

Tietoturvaohjelmistoista on nyt esiteltynä kärki kolmikko, joiden pohjalta lähdetään selvittämään, että mitä palveluita yritykset todellisuudessa tarvitsevat ja mitkä osat tuotteista jäävät toiselle sijalle.

Lähtökohtaisesti yritykset tarvitsevat virustorjuntaohjelmiston, joka kaikista tietoturvaratkaisuista löytyy. Muita tarvittavia tuotteita ovat VPN. VPN löytyy vain F-Securen tarjoamasta paketista valmiina ominaisuutena. Bitdefender tarjoaa myöskin VPN-palvelua, mutta tämä tulee lisämaksullisena tuotteena tuoden 119,99 euroa lisälaskua vuosittain (bitdefender.com) Kaspersky ei tarjoa VPN-palvelua edes lisämaksusta Small Office Securityyn. Huomionarvoista on se, että F-Secure tarjoaa omassa paketissaan hallittavan palomuurin, joka on toteutettu suoraan ohjelmiston sisään, näin eliminoiden erillisen palomuurin tarpeen – aluksi. F-Securen palomuuri toimii palomuurina vain yksittäisten laitteiden osalta, eikä näin tuo turvaa varsinaiselle verkolle.

Muita haluttuja turva-asetuksia ovat selauksen suojaus, joka on integroituna kaikkiin tietoturvaratkaisuihin. Lisäksi laitehallinta, sovellushallinta ja päivitysten hallinta on integroituna F-Securen ja Bitdefenderin tuotteisiin.

Varsinaisen vertailun perusteella on päädytty F-Securen tuoteperheeseen, joka on kattava ominaisuuksillaan, helppokäyttöinen, mutta myöskin skaalautuva ja pilvipohjaisella hallintapaneelilla, jolloin yrityksen ei tarvitse huolehtia tietoturvan asentamisesta ja ylläpitämisestä omalla palvelimellaan. Lisäksi kyseessä on kotimainen tuote, joten sekin tuo oman lisänsä tuotteen arvoon.

4.5 Mekaaniset tietoturvaratkaisut

Tietoturvaohjelmistojen lisäksi kannattaa miettiä ratkaisuja yrityksen omaan verkkoon. Näitä voivat olla hallittavat laitteet, kuten kytkimet, palomuurit ja reitittimet, joilla lisätään varsinaisen verkon turvaa ja yrityksen sisäisen tekemisen turvaa eri toimijoiden välillä. Yrityksen kasvaessa on myös mahdollista harkita vaihtoehdoiksi erilaisia SIEM-palvelut (*Security information and Event Management*), joiden kanssa kerätään lokitietoja yrityksen verkon tapahtumista ja varmistetaan, että ylimääräisiä laitteita ei pääse käsiksi yrityksen sisäverkkoon. SIEM ohjelmistot eivät kuitenkaan ole kohdennettu suoraan pienyrityksille, sekä ovat niin laajoja, että niitä ei käsitellä erikseen.

Vaikka tietoturvaohjelmistot ovatkin tarkoitettu helpoksi käyttää ja käyttöönottaa, niin on suositeltavaa kääntyä asiantuntijan puoleen, mikäli käytetään tai asennetaan suuria verkkoratkaisuja tai verkkoon liitettäviä laitteita, jotka ovat tarkoitettu tietoturvan parantamiseen tai omaavat tietoturvaan liittyviä hallinnollisia konfigurointeja. Tällaisia laitteita ovat esimerkiksi hallittavat palomuurit ja kytkimet. Väärin konfiguroituna tällaiset laitteet voivat olla itsessään verkon suurin tietoturvariski.

4.6 Yrityksen vakuutukset

Vaikka yrityksillä on käytössään tietoturvaratkaisut, ei se automaattisesti tarkoita, että yritys ei voi tulla hakkeroiduksi. Tätä varten yrityksille on kehitetty erilaiset tietoturva- ja kybervakuutukset, jotka auttavat taloudellisesti, mikäli yritys joutuu tietomurron uhriksi. Suomessa suurimmat vakuutusyhtiöt, jotka tämän tyyppisiä vakuutuksia tarjoaa, ovat OP Pohjola Oyj ja If Vahinkovakuutus Oyj.

Millaisissa asioissa tietoturva- ja kybervakuutukset korvaavat?

Alla yleisimpiä tapauksia, mitä vakuutus korvaa tietomurron sattuessa. On kuitenkin hyvä ymmärtää, että vaikka vakuutukset ovat olemassa, näiden hankkimisen vaatimuksena on, että yrityksen tietoturva on lähtökohtaisestikin kunnossa.

- Mikäli yrityksen toiminta keskeytyy ja tästä aiheutuu vahinkoja. Esimerkiksi jos verkkokauppa joudutaan sulkemaan tietomurron vuoksi ja tällöin tuotteita tai palveluja ei voida myydä, auttaa vakuutus kattamaan tästä koituneet tappiot.

- Jumiutuneista järjestelmistä johtuvat kulut esimerkiksi hakkeroinnin tai palvelunestohyökkäyksien tilanteessa.
- Saastuneiden järjestelmien puhdistuksesta aiheutuvia kuluja viruksen tai haitallisen koodin aiheuttamissa tilanteissa.
- Järjestelmien, ohjelmien tai verkkojen palauttamisesta aiheutuvia kuluja.
- IT-laitteiden ja ohjelmistojen rikkoutuminen, joka voidaan osoittaa johtuneen tietomurrosta. (If Vahinkovakuutus 2019.)
- Teollisuusrobotin hakkerointi pysäyttämän tuotannon liiketoiminta menetyksien korvaaminen (OP Pohjola Oyj 2019.)

Vakuutukset ovat hyviä ja edullisia tapoja lisäämään turvaa tietomurron kohdalla, sillä varsinaisen tietomurron sattuessa, voivat kulut nousta todella korkeiksi pienissäkin yrityksissä.

5 LOPUKSI

Opinnäytetyön tavoitteena oli avata helppolukuisessa muodossa Euroopan yleistä tietosuoja-asetusta 2016/679 ja siihen liittyviä, tarvittavia, toimenpiteitä. Samalla avattiin lyhyesti, mitä tapoja on parantaa yrityksien tietoturvaa niin ohjelmistoilla kuin varsinaisilla verkkoon liitettävillä laitteilla.

Vaikka varsinainen tietosuoja-asetus on ollut käytössä jo vuoden verran, on siinä silti paljon tulkinnanvaraisia asioita, kuten todelliset vastuut kahden yrityksen välillä. Opinnäytetyön tarkoituksena oli avata tietosuoja-asetuksen määrittämiä tiettyjä reunaehtoja, miten yrityksien pitää vähimmissäkin määrin toimia. Jos kokonaiskuvaa katsotaan, niin suurempi ajatus tietosuoja-asetuksen takana on yritysten varsinainen herättäminen tietosuojaan, tai valitettavan usein sen puutteeseen. Tietosuoja-asetuksen suurempi tarkoitus on asettaa yritykset tilaan, jossa niiden pitää pohtia omaa prosessiaan tietoturvan ja tietosuojan kannalta ja uudistaa se vaaditulle tasolle. Suomessa on kuitenkin edelleen valitettavan monta yritystä, jotka eivät välttämättä ole tehneet mitään tietosuoja-asetuksen tai henkilötietojen käsittelyn parantamisen hyväksi. Kokemukseni mukaan tämä piirre korostuu erityisesti taajama-alueella sijaitsevissa ja toimivissa yrityksissä.

Opinnäytetyössä tarkastellut tietoturvaohjelmistot ja -laitteet ovat ensimmäisiä asioita, jotka yritysten tulisi ottaa huomioon. Tuotteet ja palvelut on vertailtu niin, että jokaisessa on selkeä peruste tuotteen valitsemiselle tai valitsematta jättämiselle.

Opinnäytetyöhön kuului myös varsinainen tekninen osuus, joka toteutettiin yhteistyössä oman yritykseni, Admia IT-Palveluiden, sekä Elda Oy LKV & Valokuvauksen kanssa. Tarkoituksena oli mallintaa oman yritykseni alkuperäinen tietoturvaratkaisu ja verrata, voiko tämän kopioida suoraan toiselle, eri alalla toimivalle pienyritykselle. Elda Oy LKV & Valokuvauksen kanssa oli helppo toimia, sillä Eldalle oli myös tärkeää, että pienyrittäjät pitävät huolta toisistaan ja tällöin edistävät tietämystä vaikeistakin asioista. Täältä sain käyttööni uskomattoman määrän tietoa LKV-toiminnasta ja siihen liittyvästä lainsäädännöstä. Tietoturvallisuussyistä en kuitenkaan avaa opinnäytetyössä tarkemmin, oliko varsinaisesta työstä Eldalle itsessään hyötyä, tai otettiinko jotain ehdotuksistani käyttöön yrityksessä. Elda Oy LKV & Valokuvaus oli tyytyväinen antamaani panokseen. Eldan koki, että työ on helppolukuinen ja juuri sellaisessa

muodossa kirjoitettu, tietoa saavat myös muut pienyritykset, jotka, jotka kamppailevat samojen asioiden kanssa.

LÄHTEET

Admia IT-Palvelut. Tietosuoja- ja rekisteriseloteet 2018. Viitattu 24.3.2019

BBC, GDPR: US news sites unavailable to EU users under new rules. Viitattu 17.3.2019 https://www.bbc.com/news/world-europe-44248448

Bitdefender Small Office Security. Viitattu 26.3.2019 - https://www.bitdefender.com/solutions/small-office-security.html

EUR-Lex, Access to European Union law; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 9.3.2019 https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679

Euroopan komissio, Mikä on rekisterinpitäjä tai tietojen käsittelijä? Viitattu 9.3.2019 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi

FindWise, Mitä jokaisen kuuluu tietää EU:n uudesta tietosuoja-asetuksesta GDPR? Viitattu 9.3.2019 https://findwise.com/en/gdpr-fi

F-Secure. Viitattu 26.3.2019. https://www.f-secure.com/fi_FI/web/home_fi/home

Hakala, Mika & Vainio, Mika & Vuorinen, Olli: Tietoturvallisuuden käsikirja, 2006. Docendo Finland Oy. ISBN 951-846-273-9.

If Vahinkovakuutus Oyj, tietoturvavakuutus Viitattu 27.3.2019 https://www.if.fi/yritysasiakkaat/vakuutukset/vastuuvakuutukset/tietoturvavakuutus/tietomurto

Kaspersky Zao LAB. Viitattu 26.3.2019 https://www.kaspersky.com/small-business-security/small-office-security

OP Pohjola Oyj, Kybervakuutus Viitattu 27.3.2019 https://www.op.fi/yritykset/riskienhallinta/vakuutukset/toiminta/kybervakuutus

Opi Tietosuojaa, Viitattu 10.3.2019 https://opitietosuojaa.fi/fi/aloitus/tietosuoja

Tietosuojavaltuutetun toimisto, 2018. Viitattu 13.3.2019 https://tietosuoja.fi

Tietosuojavaltuutetun toimisto, 2018 Viitattu 13.3.2019 https://tietosuoja.fi/tietosuoja

Wikipedia, F-Secure. Viitattu 24.3. https://fi.wikipedia.org/wiki/F-Secure

Wikipedia, TCP. Viitattu 18.3.2019 https://fi.wikipedia.org/wiki/TCP

Wikipedia, Tietosuoja. Viitattu 18.3.2019 https://fi.wikipedia.org/wiki/Tietosuoja

Wikipedia, Tietoturva. Viitattu 18.3.2019 https://fi.wikipedia.org/wiki/Tietoturva