Opinnäytetyö (AMK)

Tietojenkäsittely

2022

Teemu Järvi

KULJETUSYRITYKSEN SIIRTYMINEN VERKKOLASKUTUKSEEN TIETOTURVALLISESTI

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2022 | 35 sivua, 1 liitesivu

Teemu Järvi

KULJETUSYRITYKSEN SIIRTYMINEN VERKKOLASKUTUKSEEN TIETOTURVALLISESTI

Vuoden 2020 huhtikuusta alkaen on laki sähköisestä laskutuksesta (241/2019) velvoittanut yrityksiä käsittelemään verkkolaskuja. Yrityksillä on oikeus saada pyynnöstä toiselta yritykseltä lasku sähköisessä muodossa eli verkkolaskuna. Yrityksellä on oikeus jättää lasku suorittamatta, mikäli se ei pyynnöstä huolimatta saa sitä sähköisessä muodossa.

Opinnäytetyön tavoitteena oli tutkia erään kuljetusyrityksen nykyisen tietoturvan toteutusta, EU:n yleisen tietosuoja-asetuksen noudattamista ja varmistua henkilöstön riittävästä tietoturvatietoisuudesta ennen siirtymistä manuaalisesta laskuttamisesta verkkolaskuttamiseen.

Kuljetusyrityksen tietoturvan toteuttaminen, EU:n yleisen tietosuoja-asetuksen noudattaminen ja henkilöstön tietoturvatietoisuus tutkittiin haastatteluilla ja tutustumalla mm. yrityksen työtilaan, laitteisiin ja dokumentteihin.

Yrityksen tietoturvan toteuttamisessa ja EU:n yleisen tietosuoja-asetuksen noudattamisessa havaittiin korjattavaa ja puutteita. Havaitut puutteet ja epäkohdat korjattiin tai poistettiin ennen siirtymisprosessia manuaalisesta laskuttamisesta verkkolaskuttamiseen. Henkilöstön tietoturvatietoisuus oli alun perinkin kohtalaisella tasolla, mutta säännöllistä tietoturvakoulutusta voidaan kuitenkin suositella.

Yrityksen siirtyminen verkkolaskuttamiseen onnistui hyvin. Verkkolaskuttamisen useat hyödyt tulivat nopeasti ilmi, ja yrityksen laskutusprosessi on merkittävästi ryhdistynyt.

ASIASANAT:

laskutusohjelma, tietoturva, tietosuoja-asetus, verkkolaskutus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2022 | 35 of pages, 1 page appendix

Teemu Järvi

A TRANSPORT COMPANY'S INFORMATION SECURE TRANSITION TO E-INVOICING

Since April 2020, the Act on Electronic Invoicing (241/2019) has required companies to process e-invoices. Companies have the right to receive an invoice from another company in an electronic form, for example as an e-invoice. A company has the right not to pay an invoice if, despite the request, it does not receive it electronically.

The aim of the thesis was to study the implementation of the current information security of a transport company, the compliance with the EU's General Data Protection Regulation and to ensure that the personnel have sufficient information security awareness before transition from manual invoicing to e-invoicing.

The implementation of the transport company's information security, compliance with the EU's General Data Protection Regulation and the personnel's information security awareness were examined through interviews and by the thesis a becoming acquainted with company workspace, equipment, and documents.

Corrections and shortcomings were identified in the implementation of the company's information security and compliance with the EU's General Data Protection Regulation. Identified deficiencies and inconveniences were corrected or eliminated prior to the transition from manual invoicing to e-invoicing. Staff security awareness was initially moderate, but regular information security training can be recommended.

The transport company's transition to e-invoicing was successful. Many benefits of e-invoicing quickly became apparent, and the company's invoicing process has improved significantly.

KEYWORDS:

invoicing software, information security, data protection, e-invoicing

SANASTO

Pilvipalvelu	Pilvipalvelussa ohjelmat tai tiedot ovat pilvipalvelun tarjoavan yrityksen palvelimella, ne eivät ole yrityksen tietokoneella tai omalla palvelimella (Elisa 2017).
Sähköinen lasku	Sähköisellä laskulla tarkoitetaan laskua, joka on luotu ja vastaanotettu rakenteisessa sähköisessä muodossa, ja joka on käsiteltävissä automaattisesti eli verkkolaskuna (Isolta 2021g).
Sähköpostilasku	Sähköpostilaskut PDF-tiedostoineen eivät ole verkkolaskulain mukaan sähköisiä laskuja, koska ne vaativat manuaalista työtä (Isolta 2021g).
Verkkolasku	Verkkolaskulla tarkoitetaan yritykselle tai muulle organisaatiolle lähetettävää sähköistä laskua, joka välittyy digitaalisessa ja koneluettavassa muodossa vastaanottajalle (Isolta 2021g).
Verkkolaskulaki	Verkkolaskulailla tarkoitetaan lakia hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta (Laki hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta 241/2019).

SISÄLTÖ

LIITTEET

KUVAT

1 JOHDANTO

Eduskunnassa hyväksyttiin vuonna 2019 laki hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta koskien valtion keskushallintoviranomaisia ja yhteishankintayksiköitä (241/2019). Vuoden 2020 huhtikuusta alkaen laki on laajentunut koskemaan myös muitakin hankintayksiköitä. Lain mukaan hankintayksiköllä ja elinkeinonharjoittajalla on oikeus saada pyynnöstä lasku toiselta hankintayksiköltä tai elinkeinonharjoittajalta sähköisen laskun muodossa. Verkkolaskulain tavoitteena on nopeuttaa siirtymistä kokonaan automatisoituun taloushallintoon julkisella ja yksityisellä sektorilla. Automatisoinnilla saavutetaan monia hyötyjä. (Valtiokonttori 2019.)

Opinnäytetyön tavoitteena on tutkia erään kuljetusyrityksen nykyisen tietoturvan toteutusta, EU:n yleisen tietosuoja-asetuksen asettamien vaatimusten noudattamista, varmistua henkilöstön riittävästä tietoturvatietoisuudesta, ja varmistaa verkkolaskuttamiseen siirtyminen onnistuneesti. Vuoden 2020 huhtikuussa voimaan tulleen uuden verkkolaskulain myötä kuljetusyrityksessä siirrytään manuaalisesta laskuttamisesta sähköiseen laskuttamiseen eli verkkolaskutukseen. Yrityksen verkkolaskuttamiseen siirtymisen tavoitteena on vähentää laskuttamiseen käytettävää aikaa, helpottaa laskuttamista ja saatavien seurantaa, poistaa laskuvirheet, ja nopeuttaa asiakkaalla laskun käsittelyä ja maksamista.

Opinnäytetyön teoriaosuus muodostuu tietoturvallisuudesta, EU:n yleisestä tietosuoja-asetuksesta sekä verkkolaskutuksesta annetuista lainsäädännöstä, ohjeista, oppaista, kirjallisuudesta ja verkkomateriaaleista. Tutkimusmenetelmänä on tapaustutkimus, ja se on toimintatutkimuksellinen.

Opinnäytetyön soveltavassa osuudessa tutkitaan yrityksen tietoturvallisuuden toteutumista ja EU:n yleisen tietosuoja-asetuksen asettamien vaatimusten noudattamista sisältäen mm. asiakastietojen käsittelyprosessi, toimintaperiaatteet, ohjeet, sopimukset, selosteet ja dokumentit. Yrityksen manuaalisen laskutusprosessin nykykäytäntö ja verkkolaskutuksen olennaisia piirteitä käydään läpi.

Kuljetusyrityksen tietoturvan toteutus, tietosuoja-asetuksen noudattaminen ja henkilöstön tietoturvatietoisuus tutkitaan haastatteluilla ja tutustumalla mm. yrityksen työtiloihin, laitteisiin ja dokumentteihin. Yrityksen siirtyminen onnistuneesti verkkolaskutukseen varmistetaan tarvittaessa osallistumalla muutosprosessiin.

2 TIETOTURVALLISUUDEN PERUSTEITA JA OHJEITA

2.1 Tietoturvan määritelmä

Tietoturvassa on kyse tietojen, järjestelmien, palveluiden ja tietoliikenteen asianmukaisesta suojaamisesta (Helsingin yliopisto 2020).

Tietoturva on hallinnollisia ja teknisiä toimia, joilla varmistetaan tiedon luottamuksellisuus, eheys ja käytettävyys (Traficom 2020a).

Klassisessa tiedon arvoon perustuvassa määritelmässä tietoturvallisuus muodostuu kolmesta osatekijästä. Luottamuksellisuudella (engl. confidentiality) tarkoitetaan sitä, että tietojärjestelmässä olevat tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä. Eheydellä (engl. integrity) tarkoitetaan sitä, että tieto on oikeaa eikä siinä ole tahallisia tai tahattomia virheitä. Käytettävyydellä (engl. availability) tarkoitetaan sitä, että tietojärjestelmän tiedot ovat saatavissa oikeassa muodossa ja kohtuunopeasti. (Hakala ym. 2006, 4.)

Perinteiseen määritelmään on myöhemmin lisätty kolme osatekijää: kiistämättömyys, pääsynvalvonta ja todentaminen. Kiistämättömyydellä (engl. non-repudiation) tarkoitetaan sitä, että tietojärjestelmällä on kyky tunnistaa ja tallentaa luotettavasti järjestelmäkäyttäjän tiedot. Pääsynvalvonnalla (engl. access control) tarkoitetaan menetelmiä, joilla rajataan tietoteknisen ympäristön käyttöä. Todentamisella (engl. authentication) tarkoitetaan tietojärjestelmäkäyttäjän ja laitteiden tunnistamista luotettavasti. (Hakala ym. 2006, 5–6.)

Tietoturvan tavoitteiden saavuttamisen edellytyksenä on osapuolten todentaminen, joka on haasteellista. Ihmisten henkilöllisyyden, laitteiden ja verkkopalveluiden aitouden helppo ja aukoton varmistaminen on vaikeaa. Useat tietoturvaongelmat johtuvat todentamisen ongelmista eivätkä mm. heikosta salauksesta tai epäluotettavista laitteista. (Järvinen 2012, 12.)

2.2 Tietoturvallisuuden osa-alueet

Tässä luvussa esitellyt seuraavat määritelmät perustuvat Hakalan ym. (2006, 10–12) lähteeseen. Tietoturvallisuuden laaja kokonaisuus voidaan jakaa fyysiseen ja hallinnolliseen turvallisuuteen sekä henkilö-, käyttö-, laitteisto-, ohjelmisto-, tietoaineisto- ja tietoliikenneturvallisuuteen.

Fyysisen turvallisuuden tavoitteena on suojata toimitilat, laitteet ja henkilöt fyysiseltä uhalta (esim. ilkivallalta tai murtautumiselta) ja sähkö-, vesi- ja tulipalovahingoilta.

Hallinnollisen turvallisuuden tavoitteena on varmistaa tietoturvan kehittämistä ja johtamista, ylläpitää myös yhteyksiä turvallisuudesta vastaaviin viranomaisiin ja arvioida esim. lisenssi- ja palvelusopimusten vaikutusta yrityksen tietoturvalinjauksiin.

Henkilöturvallisuuden tavoitteena on varmistua järjestelmänkäyttäjien toimintakyvystä sekä käyttöoikeuksista tietoihin ja tietojärjestelmiin. Toimiin kuuluvat mm. sijaisjärjestelyt, koulutukset, vastuiden ja oikeuksien määrittely ja tarvittaessa työntekijän taustatietojen selvittäminen.

Käyttöturvallisuuden tavoitteena on tunnistaa tietojärjestelmän käytöstä aiheutuvia riskejä ja varautua niihin.

Laitteistoturvallisuudella tarkoitetaan tietojenkäsittelylaitteiden testaamista, huoltamista, suojaamista ja vanhentuneiden laitteiden poistoa.

Ohjelmistoturvallisuudella tarkoitetaan esim. varmistamista ohjelmistojen testauksella ohjelmistojen yhteensopivuutta, sovellusten tarkoituksenmukaisuutta, luotettavaa ja virheetöntä toimintaa, ja ohjelmistoversioiden ja lisenssien kontrollointia.

Tietoaineistoturvallisuudella tarkoitetaan tietojen, asiakirjojen ym. hallittua säilyttämistä, varmistamista, palauttamista ja tuhoamista.

Tietoliikenneturvallisuuden tavoitteena on varmistaa tiedonsiirtoratkaisujen (esim. lähi- ja laajaverkkoyhteyksien) ja viestintäjärjestelmien turvallisuus.

2.3 Tietoturvauhkia

Tietoturvauhista puhuttaessa moni nostaa heti esille, että ihminen on pahin tietoturvauhka. Mikäli työntekijällä ei esimerkiksi ole osaamista, motivaatiota eikä hän tiedosta tietoturvan tärkeyttä, väite on totta. Myös kovassa kiireessä ja väsyneessä olotilassa tehdyt nopeat ratkaisut voivat olla tietoturvauhkia. Tietoturvauhkien minimoinnissa tärkeässä roolissa ovat tietoturvakoulutus (perustaitojen osaaminen), huolellisuus ja jos mahdollista, tietoturvaa koskevien uutisten jatkuva seuranta.

Traficom on listannut ”Kybersää heinäkuu 2020” -raportissaan top 5 -kyberuhat yrityksiä kohtaan. Ajankohtaisimpana on nostettu esille laajavaikutteiset kiristyshaittaohjelmat, jotka vaikuttavat yritysten liiketoiminnan jatkuvuuteen. Tietojenkalastelu on yhä rikollisten aktiivisessa käytössä verkkohuijauksissa, lisäksi puhelinhuijausten määrä on kasvanut. Haavoittuvuuksien nopean hyväksikäytön riski on lisääntynyt. (Traficom 2020b.)

2.3.1 Kiristyshaittaohjelmat

Kiristyshaittaohjelma (engl. ransomware) lukitsee tiedostoja tai mahdollisesti koko tietokoneen ja vaatii rahallista korvausta lukitusten poistamiseksi. Ohjelma lupaa lunnaiden maksamisen jälkeen avata vahvalla salauksella lukitut tiedostot. Yleinen sääntö on, että maksua ei kannata suorittaa. Kiristyshaittaohjelmat ovat rikollisten levittämiä ja lunnailla rahoitetaan rikollista toimintaa. Jos uhri päättäisikin maksaa lunnaat, ei ole mitään varmuutta siitä, että lunnaiden vaatija pitää sanansa ja vapauttaa tiedostot. (Viestintävirasto, 2016.)

Uusi ilmiö kiristyshyökkäyksissä on lunnasvaatimusten tehostaminen: hyökkääjä uhkaa kohdetta saamiensa tietojen myymisellä, vuotamisella tai julkaisemisella (Traficom 2020c).

Haittaohjelmat tarttuvat verkkoon kytkettyihin laitteisiin, kuten mobiililaitteisiin ja tietokoneisiin. Sähköpostin mukana on voinut tulla liitetiedosto, jonka avaamisen jälkeen tietokoneelle latautuu vahingollista sisältöä tai käyttäjä on ollut jollakin epämääräisellä sivustolla ja klikannut siellä olevaa haitallista linkkiä. (Viestintävirasto 2016.)

2.3.2 Tietojenkalastelu

Tietojenkalastelu (engl. phishing) ja muu käyttäjien manipulointi (engl. social engineering) on nykyään yleistä. Tietojenkalastelun tavoitteena on saada kerättyä pankkitunnuksia, henkilötietoja, käyttäjätunnuksia, salasanoja ja tietoja organisaatiorakenteista, joita voidaan hyödyntää tietomurroissa. Pankkitietojen kalastelussa hyödynnetään huijaussähköpostia, jossa pyydetään kirjautumista linkin kautta tietylle sivustolle. Tietojenkalastelu Office 365 -tuotteiden, sähköpostin käyttäjätunnusten ja salasanojen osalta on Suomessa aktiivista. (Traficom 2020b.)

2.3.3 Haavoittuvuudet

Haavoittuvuudessa (engl. vulnerability) on kyse mistä tahansa heikkoudesta, joka mahdollistaa vahingon toteutumisen tai käyttämisen vahingon aiheuttamisessa. Haavoittuvuuksia voi olla mm. prosesseissa ja tietojärjestelmissä. (Turvallisuuskomitea 2018.)

Nollapäivällä (engl. zero-day tai 0day) tarkoitetaan sitä hetkeä, jolloin ohjelmistosta tai tietojärjestelmästä vastuussa oleva taho tulee tietoiseksi haavoittuvuudesta. Ongelma on voinut olla olemassa jo useita vuosia, vaikka sitä ei ole kukaan havainnut aikaisemmin, mutta on myös mahdollista, että ongelmaa on hyväksikäytetty ja asia ei ole paljastunut aiemmin. (Mikrobitti 2019.)

Haavoittuvuuksien hyväksikäyttö on nykyään nopeaa, joka edellyttää nopeita päivityksiä ja muitakin toimenpiteitä. Rikolliset ovat kehittäneet hyväksikäyttömenetelmiä nopeasti heti ohjelmapäivitysten ilmestyttyä ja tunnistavat päivittämättömät kohteet. Mitä pidempään haavoittuvuuden korjaaminen kestää tai korjausta siirretään myöhempään ajankohtaan, sitä korkeammaksi hyväksikäytön riski nousee. (Traficom 2020b.)

2.4 Tietomurroilta suojautuminen

Tietomurrolla tarkoitetaan luvatonta tunkeutumista laitteeseen, palveluun, tietojärjestelmään tai sovelluksen luvatonta käyttöä. Rikoslaissa tietomurto on määritelty rangaistavaksi teoksi, ja jo tietomurron yritys on rangaistava teko eli järjestelmään tunkeutuminen luvatta täyttää rikoksen tuntomerkit. Tietomurrot aiheuttavat yrityksille taloudellisten tap-

pioiden lisäksi myös maineen menetyksiä. Yrityksen normaalitoiminta voi pysähtyä pitkäksikin aikaa, kun pitää tehdä korjauksia tai ympäristön uudelleenasennuksia. Tietomurtoja voidaan hyödyntää esim. laskutuspetoksissa. (Traficom 2020d.)

Seuraavat esitellyt menetelmät tietomurroilta suojautumiseen perustuvat Traficomin (2020d, 2020e) lähteisiin: ohjelmistojen ja järjestelmien päivittäminen, monivaiheisen tunnistautumisen käyttäminen, ei samoja salasanoja useissa eri palveluissa ja varmuuskopioiden ottaminen.

Ohjelmistojen ja järjestelmien päivittämisellä tarkoitetaan sitä, että järjestelmät ja laitteet tulee pitää ajan tasalla. Pitää muistaa, että suurin osa ohjelmapäivityksistä sisältää haavoittuvuuksien korjauksia, jotka tulee asentaa mahdollisimman nopeasti, kun ne ovat julkaistu.

Useimmissa ohjelmissa on mahdollisuus automaattisiin päivityksiin, jolloin käyttäjän ei tarvitse etsiä päivityspaketteja tai muistaa tarkastaa päivityksiä aika ajoin. Käyttäjän tulisi huolehtia säännöllisesti seuraavista päivityksistä: Tietoturvaohjelmisto (sisältäen mm. palomuuri ja virustorjunta), internet-selain ja selaimen liitännäiset, käyttöjärjestelmä, sovellukset, ohjelmistot, mobiililaitteet, modeemi, reititin ja muut mahdolliset älylaitteet.

Kun palvelun käyttäjän tunnistamiseen käytetään käyttäjätunnuksen ja salasanan käytön täydentävää tunnistamistapaa, sillä tarkoitetaan **monivaiheista tunnistautumista**. Esim. nettipankkiin kirjauduttaessa käyttäjän puhelimeen tulee vielä tekstiviestillä kertakäyttökoodi. Vaikka hyökkääjällä olisi käyttäjätunnus ja salasana, niin tietomurtoon tarvitaan lisäksi käyttäjän puhelin.

Ei samoja salasanoja useissa eri palveluissa, jolloin voidaan estää jo mahdollisesti vuotaneiden tunnusten laajempi hyväksikäyttö, koska useisiin internetissä käytettyihin palveluihin on kohdistunut salasanavuotoja (käyttäjätunnus-salasana parit). Hyvä ohje laadukkaasta salasanasta on, että sen tulisi olla riittävän pitkä (väh. 15 merkkiä), käytetään lausetta eikä yhtä sanaa ja käytetään merkkejä (numeroita, eri kokoisia kirjaimia ja erikoismerkkejä). Yksi suositus on, että käyttäjän tulisi hyödyntää salasanojen hallintaohjelmaa.

Varmuuskopioiden ottamisella tarkoitetaan sitä, että käyttäjän tulee tehdä tärkeimmistä tiedoista ja palveluista varmuuskopiot ja säilyttää ne erillään suojattavista järjestelmistä ja tiedoista, jolloin esim. kiristyshaittaohjelma ei tee varmuuskopioista käyttökelvottomia. Varmuuskopioiden palauttamista tulee kokeilla säännöllisesti, jotta voidaan

varmistua palauttamisten onnistumisesta ja tarvittavien järjestelmäasetusten varmuuskopioinnista.

2.5 Toimenpiteet tietomurron kohteeksi joutumisen jälkeen

Seuraavat esitellyt toimenpiteet tietomurron kohteeksi joutumisen jälkeen perustuvat Traficomin (2020d) lähteeseen: ilmoitus, eristys, salasanojen vaihto, lokien varmistus, varmuuskopioiden palautus ja viestintä.

Jos on epäilys tai havainto, että on joutunut tietomurron kohteeksi, niin tulee aina tehdä **ilmoitus** Kyberturvallisuuskeskukseen lomakkeella tai sähköpostitse (cert@traficom.fi) ja tehdä myös rikosilmoitus. Jos murtautuja on saanut tietomurron seurauksena suojattavia tai salassa pidettäviä tietoja, on kyse tietovuodosta. Jos on epäilys, että tietovuodossa on mukana myös muiden ihmisten henkilötietoja, on kyse tietosuojarikkomuksesta, jolloin tulee tehdä **ilmoitus** tietosuojavaltuutetulle.

Lisähaittojen estämiseksi tulee murrettu **kohde eristää** muusta toimintaympäristöstä.

Murretuissa järjestelmissä käytetyt **salasanat tulee vaihtaa** tai lukita käytetyt tunnukset murretun ympäristön osalta.

Tietomurtoa edeltävät ja sen aikaiset **lokitiedot tulee varmistaa,** ja ettei niiden sijainti ole murretussa ympäristössä. Murtautujalla on mahdollisuus muokkailla lokitietoja, mikäli ne sijaitsevat murretussa ympäristössä.

Ennen kuin voidaan **palauttaa murrettujen järjestelmien varmuuskopiot**, tulee varmistua, ettei hyökkääjällä ole enää toimintaedellytyksiä verkossa ja huolehtia järjestelmäpäivityksistä. Lisäksi tulee varmistua, ettei palautetussa ympäristössä ole haittaohjelmia.

Jos on kyse laajasta tietomurrosta, tulee huolehtia **viestinnästä** asiakkaille, julkisuuteen ja yhteistyötahoille.

2.6 Tietoturvan riskienhallinta lyhyesti

Yksi tärkeimmistä asioista tietoturvassa on riskienhallinta. Tietoturvallisuuden ja jatkuvuuden hallinnan kehittämistyö on riskienhallintaa. Kun organisaatio arvioi riskit, niin se voi kohdistaa käytettävissä olevat voimavarat niihin kohteisiin, joissa uhkan toteutuminen on todennäköisintä ja vaikutus mahdollisimman suurta. (Rousku 2014, 61.)

Riskienhallintaprosessin voi toteuttaa monella eri tavalla erilaisia riskienhallintamalleja tai teorioita hyödyntäen. Yksi esimerkki riskienhallintaprosessista on seuraavanlainen: Riskikartoitus → Riskianalyysi → Toimenpide-ehdotukset → Riskienhallinta → Riskienhallinnan seuranta. (Valtiovarainministeriö 2017.)

Organisaation tulee ensimmäiseksi **kartoittaa** siihen mahdollisesti kohdistuvat erilaiset tietoturvauhat. Tietoturvariskit tulee kerätä kaikista tietoturvan osa-alueista. Kun ne ovat tunnistettu, organisaation tulee suorittaa riskianalyysi. (Pro Tietosuoja 2020.)

Riskianalyysissä määritellään riskien vakavuus ja todennäköisyys, mikä on nykyinen riskitaso, riskien syyt, riskien seuraukset ja tavoiteltu riskitaso. (Valtiovarainministeriö 2017).

Riskien tunnistamisen ja arvioinnin jälkeen tulee suunnitella **riskienhallinnan toimenpide-ehdotukset**. Riskienhallintakeinot voidaan jakaa neljään osa-alueeseen: riskin välttäminen (poistaminen), riskin pienentäminen, riskin siirtäminen (esim. vakuutus) ja riskin pitäminen (jäännösriski). (Suomen Riskienhallintayhdistys 2020.)

Riskienhallinnassa sovitaan riskienhallintatoimenpiteistä ja vastuutuksesta, ja määritellään myös toimenpiteiden toteuttamisaikataulu. **Riskienhallinnan seurannassa** suoritetaan hallintatoimenpiteiden seurantaa 1–4 kertaa vuodessa ja tarvittaessa uudelleenarviointia. (Valtiovarainministeriö 2017.)

3 EU:N YLEINEN TIETOSUOJA-ASETUS

Euroopan unionin yleistä tietosuoja-asetusta (engl. GDPR, General Data Protection Regulation) on aloitettu soveltamaan toukokuusta 2018, ja se koskee kaikkea sen soveltamisalaan kuuluvaa henkilötietojen käsittelyä EU:ssa. Sen tavoitteena on vahvistaa kansalaisten yksityisyydensuojaa ja yhtenäistää eurooppalaista tietosuojasääntelyä, ja se on suoraan sovellettavaa lainsäädäntöä. Lisäksi yhtenä tavoitteena on parantaa luottamusta online-palveluihin. (Andreasson ym. 2019, 27.)

3.1 Tietosuoja-asetuksen periaatteita

3.1.1 Riskiperusteinen lähestymistapa

Tietosuoja-asetusta tulee soveltaa sekä automaattiseen että manuaaliseen henkilötietojen käsittelyyn. Tietosuoja-asetuksen velvoitteita ja asianmukaisia suojaustoimia tulee suhteuttaa henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille aiheutuviin riskeihin. Tavoitteena on välttää vähäisten riskien toiminnan ylimitoitusta, mutta toisaalta turvata rekisteröidyn suoja korkean riskin toiminnassa. Henkilötietojen käsittelyn riskeillä tarkoitetaan rekisteröidylle mahdollisesti aiheutuvia aineellisia/aineettomia tai fyysisiä vahinkoja kuten esim. identiteettivarkauksia, taloudellisia menetyksiä, petoksia tai sosiaalisia vahinkoja. Rekisterinpitäjä ja henkilötietojen käsittelijä on velvoitettu ryhtymään toimiin, jotka vastaavat henkilötietojen käsittelyyn kohdistuviin riskeihin. Rekisterinpitäjän tulee tehdä kattava arvio henkilötietojen käsittelyyn liittyvistä riskeistä. (Andreasson ym. 2019, 27–30.)

3.1.2 Tietosuojaperiaatteet ja rekisterinpitäjän osoitusvelvollisuus

Tietosuoja-asetus perustuu ns. tilivelvollisuusajatteluun. Edellytyksenä on riskilähtöisen tietosuojan suunnittelu ja todistuskyky tehdyistä toimenpiteistä. Asetuksessa on mainittu sisäänrakennettu ja oletusarvoinen tietosuoja. Niissä on mm. kyse siitä, että tietojen käsittelytavat ja prosessit määritellään ja kuvataan. Lisäksi tietojen käsittelyssä varmistetaan se, että käsitellään vain käsittelyn tarkoituksen mukaisesti tarpeelliset henkilötiedot niiden määrän, laajuuden, saatavilla olon ja säilytysajan suhteen. Rekisterinpitäjän on

määritellessään käsittelytapoja ja käsittelyn yhteydessä toteutettava asianmukaiset tekniset ja hallinnolliset toimenpiteet, joilla tarkoitetaan suojatoimenpiteitä kuten esim. henkilöstön koulutusta, henkilöstölle annettuja ohjeistuksia tai määräyksiä, tietojärjestelmien tietoturvaa, tietojen salausta, auditointeja, tilavalvontaa, käytönvalvontaa, tietojen salausta ja teknisiä rajoituksia. Pääsääntöisesti rekisterinpitäjän tulee itse määritellä asianmukaiset suojatoimet, joissa huomioidaan käytettävissä oleva tekniikka, käsittelyn luonne, laajuus, asiayhteys ja tarkoitus, toteuttamiskustannukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit. (Andreasson ym. 2019, 30.)

Tietosuoja-asetuksen henkilötietojen tietosuojaperiaatteet ovat seuraavat:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus. (Andreasson ym. 2019, 31.)

Rekisterinpitäjän tulee pystyä osoittamaan, että se noudattaa yllä olevia tietosuojaperiaatteita kaikissa henkilötietojen käsittelyvaiheissa. Rekisterinpitäjän tulee ymmärtää käytännössä, mitä periaatteet tarkoittavat ja miten ne toteutuvat omassa toiminnassa. Osoitusvelvollisuus edellyttää siis mm. henkilötietojen käsittelyn suunnittelua ja dokumentointia. (Andreasson ym. 2019, 31.)

Sisäänrakennetun ja oletusarvoisen tietosuojan lisäksi on asetuksessa eroteltu tietosuojan suunnitteleminen ennakkoon. Tietosuoja tulee huomioida suunnitteluvaiheessa ja henkilötietojen käsittelyyn liittyvät tekniset ja organisatoriset toimenpiteet tulee toteuttaa niin, että rekisteröityjen oikeudet toteutuvat ja asetusta noudatetaan. (Andreasson ym. 2019, 30.)

3.1.3 Rekisterinpitäjä ja henkilötietojen käsittelijä

Rekisterinpitäjä määrittää yksin tai yhdessä muiden kanssa henkilötietojen käsittelyn tarkoituksen ja keinot. Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta ja lukuun. Kummankin tulee varmistaa käsittelyn ja suojattavien henkilötietojen

asianmukainen turvallisuustaso. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee ylläpitää selostetta heidän kaikista vastuullaan olevista tietojenkäsittelytoimista. Tietoturvaloukkauksista on rekisterinpitäjällä velvollisuus ilmoittaa valvontaviranomaiselle ja rekisteröidyille, henkilötietojen käsittelijällä on velvollisuus ilmoittaa tietoturvaloukkauksista rekisterinpitäjälle. Rekisterinpitäjällä on myös velvollisuus luovuttaa rekisteröidylle tietoja tämän henkilötietojen käsittelystä. (Andreasson ym. 2019, 32.)

3.1.4 Rekisteröidyn oikeudet

Rekisteröidyn eli henkilötietojen käsittelyn kohteena olevan henkilön oikeudet riippuvat osittain tietojen käsittelyperusteesta ja niiden rekisterinpitäjästä. (Andreasson ym. 2019, 33).

Oikeudet ovat seuraavanlaiset:

- saada läpinäkyvää informaatiota, kun henkilötiedot kerätään suoraan rekisteröidyltä tai kun henkilötiedot kerätään muualta kuin rekisteröidyltä
- saada pääsy tietoihin (tarkastusoikeus)
- vaatia tietojen korjaamista (tiedon korjaaminen)
- tietojen poistaminen (tulla unohdetuksi)
- käsittelyn rajoittaminen
- luottaa siihen, että rekisterinpitäjä ilmoittaa henkilötietojen oikaisuista, poistoista ja käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu
- siirtää tiedot järjestelmästä toiseen
- vastustaa käsittelyä
- vastustaa automatisoituja yksittäispäätöksiä, ml. profilointi
- tulla informoiduksi henkilötietojen tietoturvaloukkauksista. (Andreasson ym. 2019, 33.)

Lisäksi tulee huomioida EU:n yleiseen tietosuoja-asetukseen ja kansalliseen tietosuojalakiin sisältyvä lasten erityisasema, rekisteröidyn oikeus saada valvontaviranomaiselta apua ja rekisteröidyn oikeus luottaa tietoturvaan. (Andreasson ym. 2019, 34).

3.1.5 Rekisteröidyn informointi

Rekisterinpitäjän tulee toteuttaa asianmukaiset toimenpiteet toimittaakseen rekisteröidylle kaikki käsittelyä koskevat tiedot tiiviisti, helposti ymmärrettävissä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Rekisteröityä tulee informoida mm. kuka on rekisterinpitäjä, henkilötietojen käsittelyn tarkoitus ja perusteet, henkilötietojen vastaanottajat ja säilytysaika ja miten rekisteröity voi käyttää oikeuksiaan. (Andreasson, ym. 2019, 165–166.)

Jos tiedot on kerätty rekisteröidyltä, tulee käsittelyä koskeva informaatio antaa tietojen keräämisen aikaan. Jos tietoja ei ole saatu suoraan rekisteröidyltä, niin tiedot on toimitettava viimeistään kuukauden kuluttua niiden saamisesta. Muutamissa tilanteissa ei ole tarvetta informoida henkilötietojen käsittelystä, kuten esim. silloin kun tiedot on saatu muualta kuin rekisteröidyltä ja tietojen hankinnasta tai luovuttamisesta säädetään nimenomaan rekisterinpitäjään sovellettavassa lainsäädännössä. (Andreasson, ym. 2019, 166.)

3.1.6 Henkilötietojen käsittelyn perusteet

Henkilötiedot tulee kerätä tiettyä, nimenomaista ja laillista tarkoitusta varten. Niitä ei saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Tietosuoja-asetuksessa on määritelty kuusi edellytystä, joiden perusteella saa laillisesti käsitellä henkilötietoja. Vähintään yhden seuraavista edellytyksistä tulee täyttyä: rekisteröidyn suostumus, oikeutettu etu, sopimus, lakisääteinen velvoite, elintärkeä tai yleinen etu tai julkinen tehtävä. (Yrittäjät 2019.)

Tietosuojalaissa on myös mainittu erityiset henkilötietoryhmät, joilla viitataan arkaluonteisten tietojen käsittelyyn. Näitä ovat mm. rotu tai etninen alkuperä, terveydentila, poliittinen mielipide, ammattiliiton jäsenyys ja uskonnollinen vakaumus. Arkaluonteisten tietojen käsittely on pääsääntöisesti kiellettyä. (Yrittäjät 2019.)

3.1.7 Sanktiot ja hallinnolliset sakot

Jos rekisteröidylle on aiheutunut tietosuoja-asetuksen rikkomisesta aineellista tai aineetonta vahinkoa niin hänellä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus. Kukin tietojenkäsittelyyn osallistunut rekisterinpitäjä on siis vastuussa vahingosta. (Yrittäjät 2019.)

Rekisterinpitäjä tai henkilötietojen käsittelijän tulee vapauttaa vastuusta, mikäli se pystyy osoittamaan, ettei se ole millään tavalla vastuussa vahingon aiheuttaneesta tapahtumasta. (Yrittäjät 2019).

Päätettäessä hallinnollisten sakkojen määräämisestä ja määrästä, tulee ottaa asianmukaisesti huomioon seuraavat seikat:

- velvollisuudet, joita on rikottu
- rekisteröityjen lukumäärä, joihin rikkominen vaikuttaa
- rekisteröidyille aiheutuneiden vahinkojen suuruus
- tapa, jolla teko tuli valvontaviranomaisen tietoon (ilmoittiko rekisterinpitäjä itse rikkomisesta vai joku muu)
- mahdolliset muut asiaan liittyvät raskauttavat tai lieventävät tekijät. (Yrittäjät 2019.)

Hallinnollinen sakko on enintään 20 miljoonaa euroa tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. (Yrittäjät 2019.)

3.2 Tietosuoja-asetuksen edellyttämiä keskeisiä toimenpiteitä

3.2.1 Yrityksen tietosuojan nykytilan kartoittaminen ja arviointi

Yrityksen tulee arvioida EU:n yleisen tietosuoja-asetuksen vaatimusten mukaisesti kokonaisvaltaisesti henkilötietojen käsittelykäytäntönsä mm. asiakasprosesseissa, työntekijöidensä henkilöstöhallinnossa ja alihankkijoiden sopimuksissa. Yritys voi kartoittaa ja arvioida henkilötietojensa käsittelykäytännöt ja tietosuojan nykytilan esim. kuvaamalla hallitsemansa henkilötietovarannot, henkilötietojen käsittelyssä sovellettavat lait, huomioonotetut tietosuojaperiaatteet, henkilötietojen käsittelyn oikeusperusteet ja tietoturvan

ja henkilötietojen käsittelyn riskienhallinnan toteuttaminen. Yrityksen tietojen käsittelyn keskeisten asioiden nykytilan kartoituksen ja arvioinnin lopputuloksena voi syntyä esim. tietotilinpäätös. (Andreasson ym. 2019, 41–42.)

3.2.2 Tietosuoja-asetuksen osoitusvelvollisuus

Tietosuoja-asetuksen mukaan ei enää riitä, että yritys noudattaa tietosuojakysymyksissä lakia, vaan sen on myös pystyttävä konkreettisesti osoittamaan, miten tietosuoja on otettu huomioon yrityksen toiminnan suunnittelussa ja toiminnassa. Kun vastuut ovat selkeästi kuvattu, henkilötietojen käsittelyn prosessit ennalta määritelty ja tietosuojatoiminnot kattavasti dokumentoitu, ollaan jo hyvällä tasolla.

Dokumentteja osoitusvelvollisuuden toteuttamiseksi ovat esimerkiksi:

- tietosuoja- ja tietoturvaprosessit
- tietojen käsittelyyn liittyvät käytännöt
- seloste käsittelytoimista (henkilötietojen käsittelyn yleinen kuvaus)
- ohjeistuksia ja selosteita koskevat informoinnit (informointikäytännöt)
- rekisteröityjen oikeuksien toteuttamisen prosessit
- henkilöstön ohjeistus
- henkilöstön koulutus
- henkilöstön salassapito- ja käyttäjäsitoumus
- riskiarvioinnit
- tietoturvaloukkauksen ilmoittamisen prosessi. (Andreasson ym. 2019, 43–44.)

Tietyt tietosuoja-asetuksen velvoitteet eivät kohdistu kaikkiin yrityksiin tai henkilötietojen käsittelytoimiin. Tällaisia velvollisuuksia ovat mm. tietosuojavastaavan nimittäminen, tietosuojaa koskevan vaikutustenarvioinnin tekeminen, ennakkokuuleminen ja velvollisuus laatia seloste käsittelytoimista. On kuitenkin suositeltavaa, että dokumentoidaan, millä tavalla on päädytty näiden velvoitteiden noudattamiseen tai noudattamatta jättämiseen. (Tietosuojavaltuutetun toimisto 2020.)

Tietosuojavastaava voidaan nimittää, vaikka asetus ei siihen velvoitakaan. Tilanteissa, joissa tietosuojaavastaavan nimittäminen ei ole velvollisuus, voidaan yrityksessä määri-

tellä henkilö, jonka tehtävänä on tietosuojaa koskevien asioiden huomioonottaminen yrityksen toiminnassa, joka voi toimia yhteyshenkilönä rekisteröidyn oikeuksiin ja viranomaisen valvontaan liittyvissä kysymyksissä. (Andreasson ym. 2019, 45.)

3.3 Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkauksessa yrityksen vastuulla olevien tietojen saatavuus, eheys ja salassapito ovat vaarassa. Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja häviää, muuttuu tai tuhoutuu, tietoja luovutetaan luvattomasti tai jollakin on luvatta pääsy tietoihin. Tietoturvaloukkauksesta voi seurata esim. identiteettivarkaus tai petos, maineen vahingoittuminen, salassapitovelvollisuuden alaisten henkilötietojen paljastuminen, taloudellinen tai sosiaalinen vahinko. (Andreasson ym. 2019, 172.)

3.3.1 Tietoturvaloukkausten dokumentointi

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee suojata henkilötiedot niin, että suojaustoimenpiteet vastaavat henkilötietojen käsittelyyn liittyvää riskiä. Rekisterinpitäjällä tulee olla toimintaohjeet tietoturvaloukkaustilanteita varten eli rekisterinpitäjän tulee varautua mahdollisiin tietoturvaloukkauksiin, jotta niihin pystytään reagoimaan viivytyksettä. (Andreasson ym. 2019, 175.)

Rekisterinpitäjän tulee arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu sen kohteena olleille henkilöille: ei aiheudu riskiä, aiheutuu riski tai aiheutuu korkea riski. Rekisterinpitäjän toimenpiteet määrittää riskin taso, toimenpiteitä ovat esim. dokumentti tietoturvaloukkauksesta, ilmoitus valvontaviranomaiselle ja ilmoitus rekisteröidylle. (Andreasson ym. 2019, 175–176.)

Yrityksen tulee dokumentoida kaikki henkilötietojen tietoturvaloukkaukset, niiden vaikutukset ja toteutetut korjaavat toimenpiteet riippumatta siitä, mitä toimenpiteitä tietoturvaloukkauksesta loppujen lopuksi seuraa. Mikäli yritys laiminlyö dokumentointivelvollisuuden tai ilmoituksen tekemisen, niin kyseessä on EU:n yleisen tietosuoja-asetuksen vastainen teko ja se voi mahdollisesti johtaa tietosuoja-asetuksessa määriteltyihin seuraamuksiin. (Andreasson ym. 2019, 176.)

3.3.2 Ilmoitus valvontaviranomaiselle

Henkilötietojen tietoturvaloukkauksesta tulee ilmoittaa valvontaviranomaiselle eli tietosuojavaltuutetun toimistolle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Kun rekisterinpitäjä on tullut tietoiseksi henkilötietojen tietoturvaloukkauksesta, tulee hänen ilmoittaa tietoturvaloukkauksesta tietosuojavaltuutetun toimistolle ilman viivytystä ja viimeistään 72 tunnin kuluessa. Henkilötietojen käsittelijän tulee ilmoittaa ensin rekisterinpitäjälle, jos ei ole sovittu, että käsittelijä voi ilmoittaa tietoturvaloukkauksesta suoraan valvontaviranomaiselle. Rekisterinpitäjällä säilyy kuitenkin vastuu ilmoituksen tekemisestä. Ilmoituksen voi laatia sähköisellä lomakkeella. Rekisterinpitäjän tulee toimittaa tietosuojavaltuutetun toimistolle perusteltu selitys, mikäli ilmoitusta ei ole tehty 72 tunnin kuluessa. (Tietosuojavaltuutetun toimisto 2020.)

3.3.3 Ilmoitus rekisteröidylle

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa rekisteröidylle, jos loukkauksesta voi todennäköisesti aiheutua korkea riski tämän oikeuksille ja vapauksille. Rekisterinpitäjän tulee ilmoittaa asiasta ilman viivytystä. (Tietosuojavaltuutetun toimisto 2020.)

Ilmoitukseen tulee sisällyttää seuraavat tiedot:

- henkilötietojen tietoturvaloukkauksesta selkeä kuvaus
- tietosuojavastaavan nimi ja yhteystiedot (tai lisätietoja muusta yhteyspisteestä)
- todennäköiset seuraukset henkilötietojen tietoturvaloukkauksesta
- rekisterinpitäjän ehdottamat tai jo toteuttamat toimenpiteet (tarvittaessa lisäksi toimenpiteet mahdollisten haittavaikutusten minimoimiseksi). (Tietosuojavaltuutetun toimisto 2020.)

Ilmoitusta rekisteröidylle ei edellytetä, jos

- rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja joita on sovellettu tietoturvaloukkauksen kohteena oleviin henkilötietoihin (erityisesti sellaisia, joiden avulla henkilötiedot muutetaan ulkopuoliselle mahdottomaksi tulkita, kuten salausta)

- rekisterinpitäjä on suorittanut jatkotoimenpiteet, joilla on varmistettu, että rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu
- se vaatii kohtuutonta vaivaa, jos ei esim. ole tiedossa, keitä rekisteröidyt ovat. Asiaa tulee arvioida riskiperusteisesti. Jos rekisteröityihin ei voi ottaa yhteyttä henkilökohtaisesti, tulee käyttää esim. julkista tiedonantoa tai jotakin vastaavaa toimenpidettä, jolla rekisteröityjä informoidaan yhtä tehokkaalla tavalla. (Tietosuojavaltuutetun toimisto 2020.)

4 TUTKIMUSHAVAINNOT TIETOTURVAN TOTEUTTAMISESTA JA TIETOSUOJA-ASETUKSEN NOUDATTAMISESTA

Tutkimuskohteena olivat yrityksen tietoturvan toteuttaminen ja EU:n yleisen tietosuoja-asetuksen noudattaminen. Tutkimus suoritettiin haastatteluilla ja tutustumalla yrityksen työtiloihin, laitteisiin ja dokumentteihin.

Tutkimushavainnot tietoturvan toteuttamisesta ovat seuraavat:

Fyysistä turvallisuutta on toteutettu työtilan, laitteiden ja henkilöiden osalta. Ulkopuolisilta pääsy on estetty, vesivahinkojen todennäköisyys on minimoitu ja tulipalovahinkoon on varauduttu alkusammuttimilla. Sähkövahinkoihin esim. sähkökatkoksiin tai virtapiikkeihin ei ole varauduttu.

Hallinnollista turvallisuutta ei ole kaikilta osin toteutettu. Tietoturvaa ei ole suunnitelmallisesti kehitetty ja johdettu, kirjallisia dokumentteja puuttuu kuten mm. riskienhallinta- ja jatkuvuussuunnitelma.

Henkilöturvallisuudessa on huolehdittu työntekijöiden käyttöoikeuksista tietoihin ja tietojärjestelmiin. Työntekijöiden tietoturvakoulutuksessa on parannettavaa, jotta tietoturvakäytännöt pysyvät ajan tasalla. Sijaisjärjestelyjä tulee myös kehittää.

Käyttöturvallisuudessa ei ole tunnistettu tietojärjestelmän käytöstä aiheutuvia riskejä ja varauduttu niihin.

Laitteistoturvallisuudessa on huomioitu laitteiden suojaaminen, mutta ei vanhentuneiden laitteiden poistoa.

Ohjelmistoturvallisuudessa ei ole kontrolloitu ohjelmistoversioita eikä lisenssejä. Useita ohjelmistoja ei voi enää pitää luotettavina.

Tietoaineistoturvallisuutta on toteutettu tietojen ja asiakirjojen säilyttämisessä, mutta niiden varmistamisessa, palauttamisessa ja tuhoamisessa on korjattavaa.

Tietoliikenneturvallisuus on toteutettu pääosin asianmukaisesti.

Yrityksen tietoturvan toteuttamisessa oli useita puutteita ja korjattavia asioita. Tietoturvallisuuden osa-alueista hallinnollisessa turvallisuudessa ja käyttö-, laitteisto-, ohjelmisto- ja tietoaineistoturvallisuudessa oli runsaasti toimenpiteitä vaativia havaintoja. Tietosuoja-asetuksen osalta toimenpiteet ja dokumentit osoitusvelvollisuuden toteuttamiseksi olivat osittain puutteelliset tai puuttuivat kokonaan. Henkilöstön tietoturvatietoisuudessa havaittiin puutteita.

Opinnäytetyöhön liittyy vain yrityksen käyttöön laadittu selvitys, jossa on yksityiskohtaiset tutkimushavainnot tietoturvan toteuttamisesta ja tietosuoja-asetuksen noudattamisesta.

5 VERKKOLASKUTUS 2020

5.1 Laki hankintayksiköiden ja elinkeinonharjoittajan sähköisestä laskutuksesta

Eduskunnassa hyväksyttiin helmikuussa 2019 laki hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta (241/2019). Laki on ollut voimassa 1.4.2019 alkaen, ja se koskee valtion keskushallintoviranomaisia ja yhteishankintayksiköitä. Lain tavoitteena on tehostaa julkishallinnon ja yritysten taloushallintoja luomalla puitteet laskujen automaattiseen käsittelyyn. (Valtiokonttori 2019.)

Laki hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta eli verkkolaskulain mukaan sähköisellä laskulla tarkoitetaan laskua, joka on tehty ja vastaanotettu rakenteisessa sähköisessä muodossa ja joka noudattaa sähköisen laskutuksen eurooppalaista standardia (EN 16931). Kotimaiset verkkolaskuformaatit (Finvoice 3.0 ja TEAPPSXML 3.0) vastaavat eurooppalaista standardia. (Valtiokonttori 2019.)

5.2 Verkkolaskutuksen muutokset yritykselle 1.4.2020 alkaen

Vuoden 2020 huhtikuusta alkaen elinkeinonharjoittajilla on ollut oikeus saada pyynnöstä toiselta yritykseltä lasku sähköisessä muodossa. Laskun sisältöön on tullut lisäyksenä tiettyjä pakollisia laskutustietoja, joita Suomen laki ei ole aikaisemmin vaatinut. Verkkolaskulaki ei koske alle 10 000 euron liikevaihdon yrityksiä tai yrityksiä, jotka tekevät pelkästään kuluttajakaupankäyntiä. (Visma 2020.)

Verkkolaskulaki tulee vaikuttamaan yrityksiin mm. siten, että jos toimittajayritys ei lähetä laskua sähköisessä muodossa (verkkolaskuna), niin yrityksellä on niin halutessaan oikeus jättää lasku maksamatta. Suuret yritykset edellyttävät toimittajiltaan laskuttamista sähköisessä muodossa ja Suomen valtio on 1.4.2020 lähtien vastaanottanut ainoastaan verkkolaskuja. (Rantalainen 2020.)

5.3 Laskun tietosisältö

Laskuun tulee merkitä riittävät ja oikeat tiedot, jotta lasku onnistutaan käsittelemään kerralla oikein ja verottajan vaatimusten mukaisesti. Laskun on täytettävä verohallinnon ohjeiden mukaiset pakolliset laskuvaatimukset arvonlisäverotuksessa (AVL 209 e §). Lisätietoa laskuvaatimuksista arvonlisäverotuksessa on verohallinnon internetsivustolla https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48090/laskutusvaatimukset-arvonlis%C3%A4verotuksessa/. (Verohallinto 2021.)

Uuden lain mukaan laskujen tulee sisältää tietoja, joita ei ole aikaisemmin vaadittu. Se tarkoittaa sitä, että laskuilla on hieman enemmän pakollisia tietoja ja että se antaa monipuolisempaa tietosisältöä. (Isolta 2021a.)

Laskun vastaanottaja voi edellyttää laskulle esim. sopimusnumeron, tiliöintiviitteen tai työmaatunnisteen. Verkkolaskulain mukaan laskulla pitää olla verokohtelukoodi. Esimerkki verkkolaskusta on liitteessä 1. (Isolta 2021e.)

Verkkolaskun pakollisia laskumerkintävaatimuksia ovat mm. vastaanottajan osoitetiedot (katuosoite, postinumero ja postitoimipaikka), omat pankkitilitiedot (IBAN ja BIC) ja verkkolaskuosoitteet. (Isolta 2021g.)

6 VERKKOLASKUTTAMISEEN SIIRTYMINEN

6.1 Verkkolaskutusohjelman valinta

Yrityksessä on hoidettu laskutus jo useita vuosia syöttämällä laskutustiedot Word-pohjaiselle dokumentille, minkä jälkeen lasku on tulostettu, kuoritettu ja lähetetty postitse asiakkaalle. Silloin tällöin lasku on lähetetty sähköpostitse asiakkaan pyynnöstä tai viety tulostettu lasku asiakkaalle. Yrityksellä ei ole käytössä taloushallinnon ohjelmistoa. Yrityksen työntekijä on vienyt sovittujen aikataulujen mukaisesti lähetettyjen paperilaskujen kopiot tilitoimiston kirjanpitäjälle. Yhdet kopiot paperilaskuista on arkistoitu yrityksen toimitilassa, ja laskut ovat myös sähköisessä muodossa tietokoneella.

Yritykselle parhaiten soveltuvaa verkkolaskutusohjelmaa oli alustavasti tiedusteltu asiakkailta, yhteistyökumppaneilta ja tilitoimistolta. Yritys päätti valita laskutusohjelmaksi kotimaisen Isolta Arkhimedes-laskutusohjelman, jolla voi lähettää verkkolaskuja, sähköpostilaskuja ja myös tarvittaessa paperilaskuja.

Verkkolaskujen lähettämiseksi tulee olla käytössä erillinen laskutusohjelma, jolla voidaan lähettää laskuja. Arkhimedes-laskutusohjelma on nettiselaimella käytettävä online-palvelu (pilvipalvelu) eli tietokoneelle ei ole tarvetta tallentaa mitään. Kun käytössä on internet-yhteys, niin voidaan kirjautua tietokoneella, puhelimella tai tabletilla laskutusohjelmaan, ja lähettää verkkolaskuja eteenpäin. Jotta laskut välittyvät eteenpäin vastaanottajille, tarvitaan verkkolaskuoperaattori. Isolta Arkhimedes-laskutusohjelmaa käyttävän yrityksen ei tarvitse tehdä erikseen sopimusta verkkolaskuoperaattorin kanssa, koska laskutusohjelmassa on jo valmis integraatio verkkolaskuoperaattoriin. (Isolta 2021c.)

6.2 Verkkolaskutuksen käyttöönotto, laskun lähettäminen ja vastaanotto

Isolta Arkhimedes-laskutusohjelman käyttöönotto vaatii muutamia minuutteja. Yrityksen tulee rekisteröityä (maksutta) Isolta Arkhimedes-palveluun, jonka jälkeen voi laskutusohjelmaa koekäyttää tai aloittaa laskuttamisen välittömästi. Sopimus syntyy, kun rekisteröitymisen yhteydessä käyttäjä eli Isoltan asiakas hyväksyy sopimusehdot, jonka jälkeen Isolta vahvistaa rekisteröinnin sähköpostitse ja lähettää asiakkaalle käyttäjätilin aktivointilinkin palvelun käyttöä varten. Asiakas voi sitten kirjautua rekisteröinnin yhteydessä luomallaan salasanalla laskutusohjelmaan (Kuva 1).

Kuva 1. Kirjautuminen laskutusohjelmaan (Isolta 2021d).

Laskutusohjelman avaamisen jälkeen laskuttaja voi esim. tallentaa laskutettavan asiakkaan yrityksen tiedot ohjelmaan ja syöttää sitten vaadittavat laskutustiedot laskupohjalle. Arkhimedes huolehtii automaattisesti, että lasku on verkkolaskustandardien mukainen ja että siinä on kaikki pakolliset laskumerkinnät. Jos laskuttaja on esim. jättänyt syöttämättä yleisesti vaadittavan tiedon (esim. osoitetieto) laskulle, niin Arkhimedes estää laskun lähettämisen. (Isolta 2021a.)

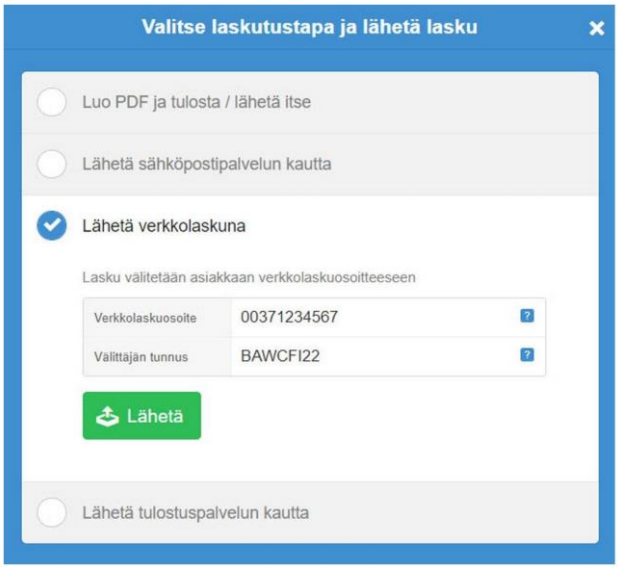
Kun verkkolasku on valmis, se lähetetään Arkhimedeksesta verkkolaskupalveluun. Jotta verkkolasku onnistutaan välittämään vastaanottajalle, verkkolaskulla tulee olla vastaanottajan verkkolaskuosoite ja välittäjän tunnus. Verkkolaskuosoite on yrityskohtainen tieto ja välittäjän tunnus informoi laskutettavan yrityksen käyttämää operaattoria laskujen vastaanottamiseen. (Isolta 2021a.)

Onnistuneesti lähetetty verkkolasku välittyy vastaanottajalle verkkolaskuoperaattorin kautta muutamissa minuuteissa. Asiakkaan taloushallinnonjärjestelmä vastaanottaa verkkolaskun, joka on heti tarkastettavissa, hyväksyttävissä ja maksettavissa. (Isolta 2021c.)

6.3 Sähköposti-, verkko- ja paperisen laskun matka asiakkaalle

Isolta Arkhimedes-laskutusohjelmalla voidaan lähettää lasku verkkolaskun lisäksi myös sähköpostitse ja paperilaskuna (Kuva 2, Kuva 3). Asiakkaalle lähetetyssä sähköpostilaskussa on linkki sivulle, josta asiakas näkee laskun. Arkhimedes seuraa sähköpostin perille menoa ja linkin avaamista, jolloin laskuttaja voi tarkistaa, koska vastaanottaja on

avannut sähköpostipalvelun kautta lähetetyn laskun. Paperilaskun osalta lähetettävä lasku avataan tulostuspalvelussa, kirje kuoritetaan ja postitetaan asiakkaalle. (Isolta 2021f.)



Kuva 2. Laskutustavan valinta ja laskun lähettäminen (Isolta 2021a).

Kuva 3. Sähköposti-, verkko- ja paperisen laskun matka asiakkaalle (Isolta 2021a).

6.4 Laskujen arkistointi

Kirjanpitoon liittyvä aineisto tulee säilyttää kuusi vuotta sen kalenterivuoden lopusta, jonka aikana tilikausi päättyy. Jos käytetään verkkolaskua tai paperilaskua, tulee huolehtia siitä, että niistä siirtyvät tositteet kirjanpitoon. Sähköisessä muodossa olevat tositteet mahdollistavat paperittoman kirjanpidon ja arkistoinnin. (Yrittäjät 2021.)

6.5 Verkkolaskutuksen kustannukset

Arkhimedes-laskutusohjelmassa on valittavissa kolme eri pakettia: Starter-paketti (0 €, 10 laskua vuodessa), Pro- ja Premium-paketit, joiden hinnoittelu määräytyy valitun laskutusjakson mukaan (1kk, 3kk tai 12kk). Pro- ja Premium-paketeissa ei ole laskurajaa. Laskutusohjelman ominaisuuksia ovat mm. asiakkuudenhallinta, hyvityslaskut, laskutus, maksumuistutukset, myynninraportointi, saatavien seuranta, sähköpostilaskut, tulostuspalvelu, tuoterekisteri ja verkkolaskut, jotka ovat käytössä kaikissa valittavissa paketeissa. Premium-paketissa on mahdollisuus hyödyntää maksuvalvontaa lähetettyjen laskujen osalta. Kaikissa paketeissa lähetetyn verkkolaskun hinta on 0,49 euroa kappaleelta. Jos lasku lähetetään tulostuspalveluun, jossa lasku tulostetaan ja postitetaan, hinta on 1,58 euroa kappaleelta kaikissa paketeissa. Sähköpostilaskuista ei veloiteta. (Isolta 2021b.)

Kuljetusyritys valitsi Pro-paketin ja kolmen kuukauden laskutusjakson, koska laskutus tulee olemaan enemmän kuin 10 laskua vuodessa. Kuukausitasolla yrityksen laskutus vaihtelee työtilausten mukaan.

6.6 Verkkolaskutukseen siirtymisessä havaittuja hyötyjä

Verkkolaskuttamiseen siirtymisestä oli välittömästi havaittavissa useita hyötyjä. Suurena yllätyksenä ei tullut se, että aikaisempaan paperiseen laskutusprosessiin (tietojen syöttö Word-laskupohjalle, tulostaminen, kuorittaminen ja postiin vienti) verrattuna verkkolaskuttaminen vie merkittävästi vähemmän työaikaa ja on vaivattomampaa, helpompaa, edullisempaa ja onnistuu todennäköisemmin kerralla oikein. Postitse lähetetty lasku on huomattavasti epävarmempi, hitaampi ja vastaanottavassa yrityksessä mm. laskutustiedot joudutaan syöttämään manuaalisesti taloushallintojärjestelmään ja laskun käsittely (tarkastus ja hyväksyntä) vie enemmän työaikaa. Verkkolaskun käsittely ja maksaminen ovat asiakkaalla siis helpompia, ja näin ollen laskuttava yritys saa maksunsa nopeammin.

Laskutusohjelma tukee käyttäjää laskujen tekemisessä, esim. laskutoimitukset on automatisoitu, jolloin laskuvirheitä ei tule. Pakolliset laskumerkinnät on myös huomioitu laskutusohjelmassa. Kun asiakastiedot on tallennettu laskutusohjelmaan, niistä muodostuu

asiakasrekisteri, jota on tarvittaessa helppo päivittää ja poimia tiedot laskulle. Aikaisemmin tehtyjä laskuja voi myös hyödyntää pohjana uusia laskuja laadittaessa eli kaikkia tietoja ei tarvitse hakea tai syöttää uudelleen. Saatavien seuranta on helppoa, kun käyttäjä pystyy seuraamaan erääntyviä laskuja yhdeltä näkymältä. Verkkolaskun ulkonäkö on selkeämpi kuin Wordilla laadittu lasku. Verkkolaskuttaminen on turvallista (lähettäjä ja vastaanottaja on tunnistettu), koska se eliminoi huijauslaskut, joita lähetetään postitse tai sähköpostitse.

6.7 Laskutusohjelman kirjautumiskäytännössä huomioitavaa

Arkhimedes-laskutusohjelmaan kirjaudutaan siis käyttäjän sähköpostiosoitteella ja käyttäjän luomalla salasanalla. Salasanan tulee olla vahva eli riittävän pitkä ja monimutkainen, vaihtoehtoisesti se voi olla myös pitkä ja monimutkainen salasanalause, kunhan se on helppo muistaa. Laskutusohjelmaan kirjauduttaessa ei ole monivaiheista tunnistautumista. Jos esim. käyttäjän sähköpostiosoite ja salasana päätyy vääriin käsiin, niin se mahdollistaa mm. pääsyn laskutusohjelmaan. On suositeltavaa, että laskutusohjelman käyttäjä suojaa sähköpostitilinsä ottamalla käyttöön monivaiheisen tunnistautumisen.

7 YHTEENVETO

Opinnäytetyön tavoitteena oli tutkia erään kuljetusyrityksen nykyisen tietoturvan toteutusta, EU:n yleisen tietosuoja-asetuksen noudattamista, varmistua työntekijöiden riittävästä tietoturvatietoisuudesta, ja varmistaa verkkolaskuttamiseen siirtyminen onnistuneesti.

Yrityksen tietoturvan toteuttamisessa oli monilta osin korjattavaa tai puutteita, ja tietosuoja-asetusta ei ole kaikilta osin noudatettu. Ei riitä, että rekisterinpitäjä noudattaa tietosuojakysymyksissä lakia, vaan sen on pystyttävä konkreettisesti osoittamaan, miten tietosuoja on otettu huomioon yrityksen toiminnan suunnittelussa ja toiminnassa, ja dokumentoida se. Henkilöstön tietoturvatietoisuus oli kohtalaisella tasolla, mutta säännöllinen tietoturvakoulutus ja tietoturvaa koskevien uutisten seuraaminen on suositeltavaa.

Verkkolaskutukseen siirtyminen ei ollut mahdollista välittömästi, koska edellytyksiä riittävän tietoturvalliseen siirtymiseen ei tutkimushavaintojen perusteella ollut. Tietoturvallisuudessa havaitut epäkohdat poistettiin, ja myös tietosuoja-asetuksen noudattamisessa havaitut puutteet korjattiin. Henkilöstö ymmärtää nyt tietoturvatietoisuuden merkityksen huomattavasti paremmin kuin mitä se oli ollut aikaisemmin.

Siirtymisprosessi manuaalisesti laskuttamisesta verkkolaskutukseen onnistui kuitenkin nopeasti, ja laskutusohjelman ja verkkolaskutuksen monet hyödyt olivat välittömästi havaittavissa. Verkkolaskuttamiseen siirtyminen on vähentänyt laskuttamiseen käytettävää aikaa, helpottanut laskuttamista ja saatavien seurantaa, poistanut mahdolliset laskuvirheet, ja nopeuttanut laskujen käsittelyä ja maksamista asiakkaalla.

Yrityksen laskutusprosessi on nyt verkkolaskutuksen myötä ryhdistynyt merkittävästi, valmiit työsuoritukset pyritään laskuttamaan jo samana päivänä, kun joskus aikaisemmin laskutus viivästyi pahimmillaan useita viikkoja.

Kuljetusyrityksen onnistunut laskutusohjelman käyttöönotto ja siirtyminen verkkolaskutukseen mahdollistavat tarvittaessa laskutusohjelman monipuolisten lisäominaisuuksien käyttöönoton.

LÄHTEET

Andreasson, A.; Riikonen, J. & Ylipartanen, A. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. 2019. Helsinki: Tietosanoma.

Elisa 2017. Mikä on pilvipalvelu? Viitattu 5.12.2021. https://elisa.fi/ideat/mika-on-pilvipalvelu/

Hakala, M.; Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Helsingin yliopisto 2020. Opiskelijan digitaidot. Tietoturvan edellytykset. Viitattu 22.7.2020. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/tietoturvan-edellytykset

Isolta 2021a. Vältä verkkolaskutuksen sudenkuopat. Viitattu 25.4.2021. https://www.isolta.fi/valta-verkkolaskutuksen-sudekuopat/

Isolta 2021b. Laskutusohjelma yrittäjälle. Viitattu 4.11.2021. https://www.isolta.fi/

Isolta 2021c. Verkkolaskutus tutuksi – 10 asiaa, jotka jokaisen yrittäjän on hyvä ymmärtää verkkolaskuista. Viitattu 25.4.2021. https://www.isolta.fi/verkkolaskulaskutus/

Isolta 2021d. Aloita laskuttaminen muutamassa minuutissa. Viitattu 25.4.2021. https://www.isolta.fi/ota-kayttoon/

Isolta 2021e. Mitä merkintöjä laskulle vaaditaan? Viitattu 20.4.2021. https://www.isolta.fi/mita-merkintoja-laskulle-vaaditaan/

Isolta 2021f. Miten sähköinen laskuttaminen toimii? Viitattu 27.4.2021. https://www.isolta.fi/ominaisuudet/sahkoinen-laskutus/

Isolta 2021g. Opas verkkolaskutukseen. Viitattu 3.11.2021. https://help.isolta.com/fi/articles/1596790-opas-verkkolaskutukseen#h_44a9fbe5b7

Laki hankintayksiköiden ja elinkeinonharjoittajien sähköisestä laskutuksesta 241/2019. Viitattu 5.12.2021. https://www.finlex.fi/fi/laki/alkup/2019/20190241

Järvinen, P. 2012. Arjen tietoturva – vinkit ja ratkaisut. Jyväskylä: Docendo.

Mikrobitti 2019. Mikä on nollapäivähaavoittuvuus? Viitattu 24.8.2020. https://www.mikrobitti.fi/uutiset/mika-on-nollapaivahaavoittuvuus-jarjestelmassa-piilevista-aukoista-maksetaan-jopa-miljoonia/ad7d6697-6be8-40d5-9912-d61e217bfba4

Pro Tietosuoja 2020. Tietoturvariskien arviointi. Viitattu 11.9.2020. https://www.tietoturvariskien-arviointi.fi/

Rantalainen 2020. Uusi verkkolaskulaki. Viitattu 12.8.2020. https://www.rantalainen.fi/uusi-verkkolaskulaki/

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

Suomen Riskienhallintayhdistys 2020. Riskienhallintaprosessi. Viitattu 11.9.2020. https://pk-rh.fi/riskienhallintaprosessi.html

Tietosuojavaltuutetun toimisto 2020. Tietoturvaloukkaukset. Viitattu 6.10.2020. https://tietosuoja.fi/tietoturvaloukkaukset

Traficom 2020a. Tietoturva. Viitattu 22.7.2020. https://www.kyberturvalsuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Traficom 2020b. Kybersää, heinäkuu 2020. Viitattu 26.8.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybers%C3%A4%C3%A4%20hein%C3%A4kuu%202020.pdf

Traficom 2020c. Haittaohjelmat ja haavoittuvuudet hallitsivat heinäkuun kybersäätä. Viitattu 26.8.2020. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haittaohjelmat-ja-haavoittuvuudet-hallitsivat-heinakuun-kybersaata

Traficom 2020d. Näin suojaudut tietomurroilta. Viitattu 28.8.2020. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta

Traficom 2020e. Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen. Viitattu 28.8.2020. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen

Turvallisuuskomitea 2018. Kyberturvallisuuden sanasto. Viitattu 26.8.2020. https://-www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Valtiokonttori 2019. Valtio vastaanottaa eurooppalaisen standardin mukaisia laskuja. Viitattu 12.8.2020. https://www.valtiokonttori.fi/uutinen/valtio-vastaanottaa-eurooppalaisen-standardin-mukaisia-laskuja/#9ba418be

Valtiovarainministeriö 2017. Ohje riskienhallintaan. Viitattu 11.9.2020. http://julkaisut-.valtioneuvosto.fi/bitstream/handle/10024/80013/Liitteet_VM22_2017.pdf?sequence-=2&isAllowed=y

Verohallinto 2021. Laskutusvaatimukset arvonlisäverotuksessa. Viitattu 20.4.2021. https://www.vero.fi/syventavat-vero-ohjeet/ohje-hakusivu/48090/laskutusvaatimukset-arvonlis%C3%A4verotuksessa/

Viestintävirasto 2016. Selviytymisopas kiristyshaittaohjelmia vastaan. Viitattu 26.8.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kiristyshaittaohjelmat__teemakooste_07_2016.pdf

Visma 2020. Laki sähköisestä laskutuksesta. Viitattu 12.8.2020. https://www.visma.fi/tietopankki/laki-sahkoisesta-laskutuksesta/?gclid=EAIaIQobChMIvtv4lbOd6wIVjKiyCh1JWQ93EAAYASAAEgJi-PD_BwE

Yrittäjät 2019. Yrittäjän tietosuojaopas. Viitattu 4.10.2020. https://www.yrittajat.fi/yrittajan-abc/yritystoiminnan-abc/yrittajan-tietosuojaopas-570864

Yrittäjät 2021. Yrityksen laskutus kuntoon. Viitattu 20.4.2021. https://www.yrittajat.fi/yrittajan-abc/perustietoa-yrittajyydesta/yrityksen-perustaminen/yrityksen-laskutus-kuntoon-566003

Esimerkki laskusta
(Isolta 2021e)

Mausteiden Maahantuonti Oy
Kaisaniemenkatu 6A
00100 Helsinki

Beringe Catering
Hans Jaakkola
Bulevardi 15
00180 Helsinki

LASKU 1(1)

Laskun numero	193
Viitenumero	1931
Laskun pvm	27.01.2016
Eräpäivä	**10.02.2016**
Toimituspvm	26.01.2016
Toimitustapa	DDP
Maksuehto	**14 pv netto**
Viitteemme	Mats Mikkola
Viitteenne	Hans Jaakkola
Ostajan tilausnumero	1234
Viivästyskorko	7,50 %
Huomautusaika	7 pv

Toimitettu Vantaan varastolle tilauksen 1234 mukaisesti 26.1.2016

	Kuvaus	Yksikköhinta €	Määrä	ALV %	Yhteensä €
1.	Katajanmarja 1 kg	60,55	2 kg	24	121,10
2.	Grillimauste 1 kg	12,18	5 kg	24	60,90
3.	Kanelitanko 1 kg	20,15	3 kg	24	60,45
4.	Korianteri kokonainen 1 kg	18,65	4 kg	24	74,60
5.	Pomeranssinkuori 1 kg	12,85	2 kg	24	25,70

Yhteensä ilman arvonlisäveroa €	342,75
Arvonlisävero yhteensä €	82,26
Maksettava yhteensä €	425,01

Puh: 0207181710 mikko@mausteidenmaahantuonti.fi www.mausteidenmaahantuonti.fi Y-tunnus: 1234567-8 ALV-numero: FI12345678

TILISIIRTO, GIRERING

Saajan tilinumero Mottagarens kontonummer	IBAN Nordea FI21 1234 5600 0007 85	BIC NDEAFIHH	
Saaja Mottagare	Mausteiden Maahantuonti Oy Kaisaniemenkatu 6A 00100 Helsinki		
Maksajan nimi ja osoite Betalarens namn och adress	Beringe Catering Bulevardi 15 00180 Helsinki		
Allekirjoitus Underskrift		Viitenumero Ref. nr	1931
Tilltä nro Från konto nr		Eräpäivä Förfallodag	10.02.2016
		Euro	425,01

Maksu välitetään saajalle maksujenvälityksen ehtojen mukaisesti ja vain maksajan ilmoittaman tilinumeron perusteella.
Betalningen förmedlas till mottagaren enligt villkoren för betalningsförmedling och endast till det kontonummer som betalaren angivit.