Opinnäytetyö (AMK)

Tietojenkäsittely

2018

Santeri Tuhkalainen

TIETOTURVAKARTOITUS MAINOSALAN YRITYKSESSÄ

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoverkot ja tietoturva

2018 | 37 sivua, 4 liitesivua

Santeri Tuhkalainen

TIETOTURVAKARTOITUS MAINOSALAN YRITYKSESSÄ

Mainosalan yritykset muodostavat erittäin mielenkiintoisen kohteen hakkereille. Tällaiset yritykset käsittelevät ja säilövät useiden eri tahojen arkaluonteisiakin tietoja esimerkiksi tulevista tuotteista, kampanjoista ja palveluista. Iskemällä yhteen mainostoimistoon hakkeri voi nopeasti saada käsiinsä suuren määrän useiden eri tahojen salassa pidettäviä tietoja. Näitä tietoja voivat hyödyntää niin kilpailevat yritykset, kuin tahot, jotka haluavat vain häiritä yritysten toimintaa. Vahvasti kilpailuhenkisessä liiketoimikulttuurissa uuden tuotteen tietojen vuotaminen kilpailijalle, tai medialle muutamakin päivä etukäteen saattaa aiheuttaa suurta vahinkoa. Tietovuodossa haltuun saatuja tietoja voidaan myös pyrkiä muokkaamaan yrityksen maineen pilaamiseksi. Mainostoimistoon kohdistuvan tietovuodon yhteydessä saattaa myös paljastua eri organisaatioiden ja näihin kuuluvien henkilöiden yhteystietoja, joita voidaan mahdollisesti käyttää myöhemmissä tietomurroissa hyödyksi.

Tässä case-tutkimuksessa tarkasteltiin turkulaista mainostoimistoa ja sen tietoturvan nykytilaa. Tutkimusmetodeina käytettiin henkilöstön ja asiantuntijan haastatteluja, tutkittaessa tehtyjä havaintoja sekä henkilöstölle osoitettuja kyselykaavakkeita ja kirjallisia tietolähteitä. Kerätyn tiedon pohjalta muodostettiin kuva yrityksen tietoturvan nykytilasta, jonka jälkeen tutkittiin mahdollisia parannusehdotuksia.

Opinnäytetyötä tehtäessä keskityttiin erityisesti tarkastelemaan sitä, kuinka eri tietoturvavaatimukset suhteutetaan juuri kohteena olleeseen yritykseen. Parannusehdotuksia kartoittaessa otettiin siis huomioon yrityksen koko, sen käsittelemän tiedon arvo sekä potentiaalinen hyökkäyksen kohteeksi joutumisen todennäköisyys.

Opinnäytetyön lopputuloksena saatiin aikaan kattava tieto yrityksen tietoturvan tilasta sekä kokoelma kehitysehdotuksia.

Johtopäätöksenä tutkimuksessa voitiin todeta, että tietoturva ei rakennu ainoastaan teknisistä ratkaisuista, vaan myös henkilöstön kouluttamisesta sekä varautumisesta inhimillisiin virheisiin.

ASIASANAT:

tietoturva, yrityssalaisuus, auditointi, luottamuksellisuus, kyberturva, ulkoistus, riskienhallinta

BACHELOR´S | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bussiness Information Technology | Networks and Information Security

2018 | 37 pages, 4 pages in appendices

Santeri Tuhkalainen

MAPPING INFORMATION SECURITY IN A MARKETING COMPANY

Marketing companies form a very lucrative target for hackers. These kinds of companies handle and store sensitive information from many sources. This information can for example be about upcoming products, campaings and services. By striking just one marketing company, a hacker can quickly get on their hands a large amount of secret information, from many different sources. This information can be used by competing companies and also instances that want to disturb the company. In a strongly competitive marketculture, information leakage of a new product to a competitor or to the media even a few days early, can be devastating. Information obtained in an attack can also be altered so that it ruins the company's reputation. Also a data leak at a marketing company can reveal contact information of their clients that can be used later for different attacks.

In this case-study, a marketing company in Turku was investigated in terms of their information security. Studymethods where interviews, own observations, fillable forms and written sources. From the collected information, a picture about the company's security situation was formed. After this, a list of suggestions for improvement was made.

While working on this thesis, special care was put into the fact, how different regulations and demands affect especially this kind of company. When suggesting improvements, the company's size, the value of their data, and their potential for attack was observed.

At the end of this thesis, a set of data about the company's security situation was produced, alongside with a list of improvements.

As a summary of this study it can be said that information security is not just the technical implementations, but also the human factor and employee knowledge.

KEYWORDS:

information security, corporate secret, auditing, confidentiality, cybersecurity, outsourcing, risk management

SISÄLTÖ

LIITTEET

KÄYTETTY SANASTO

Anonymisointi	Prosessi, jossa tiedon alkuperä poistetaan, tai muutetaan sellaiseen muotoon, ettei ulkopuolinen taho pysty enää päättelemään tiedon lähdettä.
Yleinen tietosuoja-asetus	EU jäsenvaltioita koskeva uusi asetus, joka yhtenäistää jäsenvaltioiden tietosuoja-asetukset keskenään. Englanniksi general data Protection regulation, eli GDPR (GDPR-info 2018.)
Kybervakuutus	Erityisesti tietojenkäsittelyyn liittyvien tapahtumien korvaamiseen tarkoitettu, yksityinen vakuutus.
Salassapitosopimus	Yksityisten tahojen kesken solmittu sopimus, olla paljastamatta määrättyjä asioita sopimuksessa määriteltyjen ehtojen mukaisesti. Englanniksi Non-disclosure agreement, eli NDA (Sopimustieto 2018.)

1 JOHDANTO

Ulkoistuksesta on tullut vahvasti 2010-luvun teema yrityselämässä. (Talouselämä 2018) Kävellessä millä tahansa rakennustyömaalla voi havaita, että yksittäiset yritykset erikoistuvat nykyään yhä kapeampiin osioihin projekteissa. Yksi yritys toimittaa sähkömiehet, toinen muurarit, kolmas siivoojat ja neljäs työnjohdon. Saman projektin piirissä työskentelee parhaimmillaan henkilöitä kymmenistä eri yrityksistä. Vaikka työmaan kyltissä lukisi tietyn pääurakoitsijan nimi, ei välttämättä alueella liiku ainuttakaan tuon urakoitsijan edustajaa missään projektin vaiheessa. Tätä tilannetta voidaan käyttää suoraan vertauskuvana melkeinpä millä tahansa alalla. Yhä harvenevissa määrin yksittäiset yritykset tuottavat kokonaisvaltaisia palveluja.

Ulkoistaminen johtaa väistämättä myös riskeihin, joita ei aikaisemmin ole välttämättä jouduttu ajattelemaan. Mitä useampi projektin omistajan hallinnasta ulkopuolinen taho käsittelee projektia, sitä useampia mahdollisia heikkoja lenkkejä projektiin muodostuu. Jokainen ulkoistettu taho tuo mukanaan projektinomistajalle lukuisia tahattomia ja valitettavasti tahallisiakin riskejä. Onko yrityksen henkilöstö riittävästi koulutettua? Noudattaako henkilöstö prosesseissaan hyviä käytäntöjä? Toimiiko yritys eettisesti? Näitä ja monia muita kysymyksiä jokainen ulkoistusta harkitseva joutuu ottamaan huomioon harkitessaan potentiaalista yhteistyökumppania. Tästä syystä mahdollisten ulkoistuskumppanien on itse tärkeää antaa itsestään mahdollisimman hyvä kuva ulospäin. Etenkin tuote- ja ohjelmistokehitykseen liittyvissä projekteissa yksi parhaimpia tapoja erottua joukosta on esittää, että yrityksessä otetaan tietoturva vakavasti. (Talouselämä 2018)

Tahallaan ja tahattomasti, huvin vuoksi ja vahingoittaakseen suoritetut tietovuodot ovat yksi suurimpia ja yleisimpiä riskejä, joita yritykset kohtaavat tänä päivänä. Yhä useampien yritysten herättyä tähän, on ulkoistuskumppaneilta osattu alkaa vaatia toimenpiteitä uhkien minimoimiseksi.

Tämä opinnäytetyö on tehty turkulaiselle asiakkaalle, joka on markkinointimateriaalia tuottava yritys. Yritys suorittaa toimeksiantoina markkinointimateriaalin suunnittelua, käytännön toteutusta sekä kuluttajille katsottavaksi saattamista verkossa ja televisiossa. Työssään yritys näkee, käsittelee ja pitää hallussaan sellaisia tietoja asiakkaiden projekteista, jotka tekevät yrityksestä kiinnostavan kohteen yritysvakoilulle ja kiusanteolle. Tällaisia tietoja ovat esimerkiksi tuotejulkaisut, uusien tuotteiden tiedot, arpajaisten ja muiden kampanjoiden rakenteet sekä asiakasyritysten henkilöstön yhteystietoja. Kaikki

tämä on potentiaalisesti tietoa, jota jokin taho voisi tahtoa päästä näkemään tai hävittämään. Tästä syystä tietoturva-asiat ovat yritykselle erittäin tärkeitä.

Kilpailtaessa tällaisista projekteista suureksi valttikortiksi voi muodostua osoitus asiakkaalle siitä, että yrityksen tietoturva on kunnossa. Tässä tutkimuksessa kartoitetaan yrityksen tietoturvan nykytila. Nykytilan pohjalta laaditaan lista mahdollisista parannusehdotuksista yrityksen tietoturvaan.

Teoriaosuudessa käsitellään yleisesti tietoturvan merkitystä sekä sitä, mitä siltä osin tällaisessa yrityksessä vaaditaan. Vaatimuksia tutkittaessa otetaan huomioon yrityksen koko ja toiminta, sillä tämä vaikuttaa siihen, mitkä säädökset sitä koskevat. Teoriaosassa myös käsitellään mainosalan ammattilaiselle esitettyä haastattelua, jossa hän on vastannut alansa tietoturvaan liittyviin kysymyksiin.

Empiriaosassa toteutettiin kyselytutkimus, jossa kartoitettiin yrityksen nykyinen tietoturvan taso. Kyselytutkimus toteutettiin kaksiosaisena. Ensimmäisessä osuudessa henkilöstön edustajille annettiin täytettäväksi pk-yritysten riskienhallinta kyselykaavakkeet. Tämän jälkeen toteutettiin suullinen haastattelu. Suullisessa haastattelussa kirjattiin henkilöstön omia tuntemuksia ja kokemuksia tietoturvasta.

2 TIETOTURVA KÄSITTEENÄ

Tietoturvalla käsitteenä tarkoitetaan laaja-alaisesti kaikkia toimia, joilla pyritään ylläpitämään säilötyn informaation saatavuutta, eheyttä sekä luottamuksellisuutta (TEPA-termipankki 2018.) Suojaustoimet voivat kohdistua sekä tiedon säilytysmetodiin, sitä kuljettavaan mediaan, että tiedon käsittelytapoihin. Vielä muutama kymmentä vuotta sitten tämä tarkoitti lähinnä lukittavia arkistokaappeja, avaimien seuraamista, tiedonkäsittelijöiden kirjaamista, sekä kuriirien auditointia. 2010-luvulla enää hyvin vähän tietoa säilötään tai kuljetetaan fyysisen median välityksellä. Myös käsittely on siirtynyt pitkälti digitaaliseksi. Sekä tavalliset ihmiset, että yritykset luottavat nykyisin intiimeimmätkin tietonsa sähköiselle medialle, joka useasti ei edes ole heidän itsensä omistuksessa tai hallinnassaan. Tällaisia tallennusmedioita kutsutaan yleisnimityksellä pilvipalveluiksi.

Tietoturvan tarpeisiin herätään useasti vasta sitten, kun jotain on jo tapahtunut. Tässä vaiheessa kuitenkin mahdollinen vahinko on jo sattunut, asiakkaiden luottamus menetetty sekä mahdollisesti pahimmassa tapauksessa jouduttu rikosoikeudelliseen vastuuseen.

Eräs suurista ongelmista suunniteltaessa tietoturvaa, on tekniikoiden erittäin nopea kehittyminen. Tämä johtaa siihen, että myös suojausta käsittelevät ohjeistukset vanhenevat erittäin nopeasti. Jotain mistä ei tänään tarvitse murehtia tai tietää, saattaa ollakin huomisen pahin uhka. (FLOSS Manuals 2018.)

Tietoturvallisen ajattelun kolme peruspilaria ovat käsitteet luottamuksellisuudesta, eheydestä sekä saatavuudesta. Turvatoimenpiteitä suunniteltaessa nämä kolme termiä toimivat peukalosääntöinä, joiden varmistamista tulee harkita aina uusiin tiedonsäilytykseen ja -kuljetukseen liittyviin toimenpiteisiin ryhtyessä.

2.1 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että kyseessä oleva tieto on saatavilla vain siihen valtuutetuille henkilöille (TEPA-termipankki 2018.) Tietojen luottamuksellisuudelle asetetaan erilaisia vaatimuksia riippuen tiedon laadusta. Nämä vaatimukset voivat tulla niin lainsäädännöstä, yritysten ja yhteisöjen omista ohjeistuksista, kuin yksittäisten hen-

kilöidenkin toiveesta. Luottamuksellisuuteen tähtääviä suojatoimia ovat esimerkiksi kiinteistön kulunvalvonta, sähköisten käyttäjätilien valvonta sekä tietojen tarkastelusta kerättävät lokitiedot.

2.2 Saatavuus

Saatavuudella tarkoitetaan tietoturvan suhteen sitä, että säilötty informaatio on oikeiden tahojen käytettävissä silloin, kun sitä tarvitaan (TEPA-termipankki 2018.) Aina hyökkääjän ei ole tarvetta päästä näkemään säilöttyä informaatiota. Häirinnän tarkoituksena voi olla myös vain estää tiedon oikean käsittelijän pääsy siihen. Tiedon saatavuutta uhkaaviin tekijöihin lukeutuvat hyökkäysten lisäksi laitteistorikot sekä muut vastaavat tapahtumat, joissa ei ole kyseessä suunnitelmallisuutta tai päämäärää. Saatavuus on tietoturvaa ajatellessa seikka, joka useasti unohdetaan, ajatellessa mahdollisia uhkakuvia. Oikeassa tilanteessa kuitenkin se, ettei tietoon päästä oikeaan aikaan käsiksi, saattaa olla aivan yhtä tuhoisaa, kuin tiedon urkintakin. Tällaisia tilanteita ovat esimerkiksi, kun lääkäri ei pääse tarkastelemaan potilastietokantaa tai yrittäjä ei pääse sisään tuotesuunnitelmakansioonsa. Tahallinen hyökkäys saatavuutta kohtaan suoritetaan useimmiten kiristysohjelmalla. Kiristysohjelma on järjestelmään asentuva haittaohjelma, joka sulkee käyttäjän ulos tiedostoista. Tämän jälkeen ohjelma vaatii käyttäjää suorittamaan maksun, jota vastaan tiedostot luvataan jälleen avata. Useasti tällaiset kiristysohjelmat yrittävät esiintyä jonkin viranomaistahon toimenpiteinä, luodakseen itsestään uskottavamman kuvan. (ransomware.fi 2018.)

2.3 Eheys

Informaation eheydellä tarkoitetaan sitä, että säilytyksen tai kuljetuksen aikana informaation sisältö, taikka luonne eivät ole muuttuneet (TEPA-termipankki 2018.) Tiedon eheys saattaa kärsiä säilössä ollessa, käsiteltäessä sekä kuljetuksessa, mikäli sitä ei ole suojattu riittävin toimenpitein. Uhat tiedon eheydelle voivat tulla organisaation sisältä tai ulkoa, jonkun tietoihin käsiksi pääsevän muuttaessa niitä. Ulkopuolelta tulevia uhkaskenaarioita ovat muun muassa järjestelmiin ja verkkoihin tunkeutuminen sekä tiedon muuntaminen sen ollessa matkalla.

3 TIETOTURVAVAATIMUKSET MAINOSALALLA

Media- ja mainosalan yritys käsittelee työssään useiden eri tahojen hyvinkin arvokasta tietoa. Tällaista tietoa voivat olla esimerkiksi uudet tuotejulkistukset. Mainosalan yritys voi joutua käsittelemään työssään myös henkilötietoja. Tällainen tilanne tulee kyseeseen esimerkiksi yrityksen säilöessä asiakkaiden ja kumppanien yhteystietoja. (Liite 1)

Mainosalanyritys toimii sellaisessa asemassa, että se saa haltuunsa useiden eri tahojen tietoja (Marskidata 2018). Vaikka hallussa oleva tieto olisikin tarkoitettu julkistettavaksi, tärkeäksi tekijäksi nousee aiottu julkaisuajankohta sekä julkaistavan tiedon eheys. Kilpailevalle yritykselle muutaman kuukaudenkin ennakkotieto tuotejulkistuksista tai tarjouskampanjoista tarjoaa arvokkaan tilaisuuden vastata omilla kampanjoillaan. Toiseksi mahdolliseksi uhaksi nousee mustamaalaaminen ja maineen tuhoaminen. Tiedon ollessa käsiteltävänä alihankkijalla, tässä tapauksessa mainosmateriaalin tuottajalla, tieto on niin sanotusti liikkeessä ja tällöin potentiaalinen kohde haitanteolle. Tällainen haitanteko voi olla niin kilpailevan yrityksen, kuin yksityisenkin tahon suorittamaa. Kilpailevan yrityksen ollessa kyseessä motiivit toiminnalle ovat kaupalliset. Yksityisen henkilön ollessa kyseessä, motiivina voi toimia pahansuopaisuus yritystä kohtaan, poliittinen agenda tai vain puhdas hupi (Peda.net 2018.)

Molemmissa tapauksissa riski yrityksen liiketoiminnan häiriintymiselle ja maineen menetykselle on suuri. (Peda.net 2018) Hyökkäys tietoja kohtaan saattaa muuttaa koko mainoskampanjan sisällön virheelliseksi tai loukkaavaksi, pettäen asiakkaiden luottamuksen. Kohteena olevan yrityksen on myös erittäin vaikea todistaa tällainen tilanne tyhjentävästi asiakkailleen, joten jonkin asteinen vahinko tapahtuu aina, vaikka tilanteeseen puututtaisiinkin. Oman riskinsä luovat myös mainoskuvauksissa usein käytettävät ekstratyöntekijät. Nämä henkilöt eivät välttämättä ole valveutuneita tietoturvallisuuden suhteen. Julkisilla ilmoituksilla etsityillä näyttelijöillä ja ekstroilla voi olla myös kova halu kertoa lähipiirilleen osallistumisestaan kuvaustoimintaan.

Näistä syistä media-alan yritykseen kohdistuu vaatimuksia tietoturvan suhteen niin lainsäädännön kuin asiakasyritystenkin suunnalta. Asiakasyrityksen koosta ja tilanteesta riippuen vaatimukset saattavat olla erittäinkin kovia. Vastaavasti tietovuototilanteissa myös seuraamukset voivat olla erittäin rajuja ja tuhoisia mainosyritykselle. Yksikin julkinen tietovuoto, sabotoitu kampanja tai tyytymätön asiakas on kykenevä pilaamaan yrityksen maineen pysyvästi.

3.1 Asiakasyritysten vaatimukset

Yksi yleisimmistä vaatimuksista, jota asiakasyritykset odottavat yhteistyössä, on salassapitosopimus. Salassapitosopimukset ovat sopimuksia, joissa osapuolet sopivat siitä mitä tietoja saa jakaa ja mille tahoille saa jakaa sekä millä aikavälillä tiedot tulee pitää luottamuksellisina. Salassapitosopimuksissa myös yleisesti kuvataan mahdolliset vaateet, joita sopimuksen ehdot rikkova osapuoli saa osakseen mahdollisessa ongelmatilanteessa. Useimmiten nämä vaateet ovat rahallisia. Salassapitosopimukset saattavat kuitenkin sisältää myös muita oikeudellisia vaateita. Asiakasyritys voi myös vaatia yhteistyön edellytyksenä, että heille esitellään projektiin käytettävät laitteistot sekä teetetään projektiin osallistuville työntekijöille taustatarkistukset. Asiakas voi myös esittää vaateita siitä, miten tietoja säilötään ja myöhemmin tuhotaan. Nämä vaatimukset eivät ole sellaisia, jotka perustuisivat lainsäädäntöön tai standardeihin. Tällaiset vaatimukset ovat tahojen keskenään sopimia ja niiden noudattamisen motivaationa toimii mahdollinen yhteistyön ja taloudellisen edun kariutuminen. (Minilex 2018)

Vaikka asiakas ei erityisesti esittäisi vaateita tietoturvan suhteen, tulee silti hyvän ammattietiikan nimissä tarjota näillekin asiakkaille sama tietoturva kuin niille, jotka sitä erikseen osaavat vaatia (Liite 1.) Asiakkaiden vaatimuksista puhuttaessa, suurin osa vaatimuksista ovatkin sopimusasioita, eivätkä niinkään lain vaatimia. Hyvä tapa osoittaa yrityksen sitoutumista tähän, on esittää potentiaalisille yhteistyökumppaneille ja asiakkaille luettavaksi yrityksen tietoturvapolitiikka. Tietoturva on yleisesti käsitteenä sellainen, jota suurin osa, joka ei erikseen sen parissa työskentele, ei tule edes ajatelleeksi. Tästä syystä yritys saattaa erottua asiakkaan silmissä edukseen ottaessaan tietoturva-asiat puheeksi kysymättä, verrattuna muihin asiakkaan harkitsemiin yrityksiin, joissa ei asiaa ole erikseen otettu puheeksi.

3.2 Lainsäädännön vaatimukset

Lainsäädännöllisiä vaatimuksia yritykselle tulee kahdesta lähteestä. Ensinnäkin Suomen lainsäädännöstä, toisaalta 25.5.2018 täytäntöönpanokelpoiseksi tulleesta EU:n GDPR-asetuksesta. Lyhenne muodostuu sanoista General Data Protection Regulation. Suomenkieliseltä nimeltään asetusta kutsutaan nimellä Yleinen tietosuoja-asetus. Lainsäädännöllisiä vaatimuksia yritys kohtaa useimmiten luonnollisten henkilöiden tietojenkäsit-

telyssä sekä tiettyjen taloudellisten tietojen säilömiseen liittyen. Yritysten ja organisaatioiden välisiin tietoturvaseikkoihin laki puuttuu yleensä vasta sitten kun on rikottu solmittuja salassapitosopimuksia.

Suomen laki asettaa yrityksille ja organisaatioille vaatimuksia koskien luonnollisten henkilöiden tietojenkäsittelyä. Luonnollisella henkilöllä tarkoitetaan kansankielellä sanottuna normaalia yksityishenkilöä. (Tilastokeskus 2018) Yrityksiä ja muita organisaatioita taas kuvataan oikeustieteessä oikeushenkilöiksi. (Minilex 2018) Vaatimuksia tietoturvalle esitetään pääsääntöisesti henkilötietolaissa. Henkilötietolaki asettaa vaatimuksia sille, milloin luonnollisten henkilöiden tietoja saa kerätä ja mihin tarkoituksiin sekä miten tietoja tulee säilöä. Henkilötietolaki myös selvittää luonnollisen henkilön oikeudet omien tietojensa suhteen sekä ohjeet tietojen tuhoamisesta. Tilanne, jossa media- ja mainosalan yritys voi joutua ottamaan tämän huomioon on esimerkiksi yritykselle ulkoistettu tuotearpajaisten järjestäminen tai ekstrana kuvauksissa toimivien henkilöiden hakemukset. Näiden lisäksi yritys käsittelee myös oman henkilöstönsä henkilötietoja sekä mahdollisesti asiakkaidensa ja kumppaniensa yhteystietoja.

Suomen henkilötietolaki määrittelee luottamukselliseksi henkilötiedoksi kaikki sellaiset elinolosuhteet, joista henkilön voi tunnistaa. Henkilötietolaki määrää säilytys-, käyttö-, sekä hävitystapoja tällaisille tiedoille silloin, kun niitä kerätään muodostamaan henkilörekisteri. Henkilörekisterejä ovat edellä mainittuja ominaisuuksia luonnollisista henkilöistä kirjaava järjestelmä, jota käytetään kaupallisiin, taikka muihin organisaatiollisiin tarkoituksiin. Laki ei näin koske yksityisten henkilöiden suorittamaa henkilöiden listausta omaan käyttöön. Lain määrittelemiä henkilörekistereitä mainos- ja medianalan yrityksissä muodostuu muun muassa henkilöstörekisteristä, asiakasrekisteristä, yhteistyökumppanirekisteristä sekä mahdollisista luonnollisten henkilöiden tiedoista. Henkilötietolaki määrittää erityisen arkaluonteisiksi tiedoiksi luonnollisen henkilön uskontoa, terveyttä, seksuaalisuutta sekä taloudellista tilannetta kuvaavat tiedot. Tällaisten tietojen keräämiseen pitää rekisterinpitäjällä olla erityiset perusteet. Laki velvoittaa rekisterinpitäjää toteuttamaan tarvittavat tekniset sekä käytännölliset suojatoimenpiteet tietoturvallisuuden säilyttämiseksi. Koko rekisteriä koskee myös vaitiolovelvollisuus. Henkilörekisterin vaitiolovelvollisuudesta saa poiketa ainoastaan määriteltyyn tarkoitukseen rekisteröidyn henkilön suoralla luvalla sekä viranomaisen määräyksestä. Laki myös sanelee, että rekisteri, joka ei enää palvele tarkoitustaan, on hävitettävä ensi tilassa. Suomen henkilötietolaki määrää rekisterinpitäjän korvausvelvolliseksi, mikäli rekisterin väärin-

käyttö aiheuttaa rekisteröidylle haittaa. Luonnolliselle henkilölle on myös jo ennen rekisteriin kirjaamista tehtävä selkeästi selväksi, mitä hänestä rekisteröidään, miksi tiedot kerätään sekä miten tietoja säilötään ja hävitetään. Henkilötietolaki määrittelee rekisteröidylle henkilölle oikeuden saada tietää mitä hänestä on rekisteröity sekä tarvittaessa kieltää hänen tietojensa käyttö tiettyihin tarkoituksiin. (Henkilötietolaki 2018) Tällainen kieltäminen voi kuitenkin johtaa siihen, että henkilölle ei pystytä tarjoamaan jotain tiettyä palvelua, mikäli henkilö kieltää jonkin tietonsa käsittelyn. Henkilötietolaki ei erikseen määrittele mitä riittävät suoja- sekä hävitystoimet ovat, vaan näitä käsitellään aina tapauskohtaisesti.

Yleinen tietosuoja-asetus on uusi, 2018 täytäntöönpanokelpoiseksi tullut, Euroopan unionin säätämä asetus. Yleisen tietosuoja-asetuksen on tarkoitus yhtenäistää unionin jäsenmaiden luonnollistenhenkilöiden tietojenkäsittelemistä sekä luoda koko unionille yhtenäinen politiikka sille, kuinka tietoja siirretään union ulkopuolelle. Asetus koskettaa nimenomaan luonnollisten henkilöiden tietojenkäsittelyä. Säädös toi mukanaan uusia rajoituksia sille miksi ja miten luonnollistenhenkilöiden tietoja saa kerätä. Säädös tarkentaa myös henkilörekisteriin kirjatun luonnollisen henkilön omia oikeuksia sekä puuttuu siihen, miten hänen tietojaan käsitellään. Samalla myös tietoja keräävien organisaatioiden kohtaamia sanktioita kovennettiin tietovuotojen tapahtuessa. Asetus toi mukanaan vaatimuksen jäsenmaille miten viranomaistoiminta tietojenkäsittelyn valvonnassa tulee toteuttaa. Yleinen tietosuoja-asetus laajensi rekisteröidyn henkilön oikeuksia entisestään niin, että rekisteröidyllä on entistä vahvempi oikeus määrätä omien tietojensa säilyttämisestä, käytöstä sekä hävittämisestä. Rekisteröity saa tarkemmin määritellä ne tavat, joilla hänen tietojaan säilötään ja mihin käyttöön niitä käytetään. Lainsäädäntö helpottaa rekisteröidyn tietojenhallintaa, sillä nyt rekisteröity henkilö voi hoitaa myös ulkomaille rekisteröityjä tietojaan vain yhden säännöksen puitteissa. (GDPR-info 2018)

Yleinen tietosuoja-asetus helpottaa myös rekisteröityjen mahdollisuuksia ottaa yhteyttä viranomaisiin, tahtoessaan puuttua tietojensa käsittelyyn virallisia kanavia pitkin. Kun ennen henkilön oli otettava yhteyttä sen valtion viranomaisiin, jossa palvelun toiminta päätoimisesti sijaitsi, uuden asetuksen myötä henkilö voi kääntyä oman kotivaltionsa viranomaisen puoleen. (GDPR-info 2018)

Uuden säädöksen myötä rekisterinpitäjille määrättiin tarkemmat puitteet sen suhteen, kuinka toimia tietovuodon sattuessa sekä se, millaiset sanktiot rekisterinpitäjä voi saada tietovuodon sattuessa. Rekisterinpitäjän on ilmoitettava tietosuojaviranomaiselle mahdollisesta tietovuodosta 72 tunnin kuluessa siitä, kun vuoto on huomattu rekisterinpitäjän

toimesta. Julkista ilmoitusta ei tarvitse tehdä silloin, mikäli vuotanut tieto voidaan luotettavasti todeta sellaiseksi, ettei se pysty aiheuttamaan vahinkoa rekisteröidyille. Tällaisia tapauksia ovat esimerkiksi ne, milloin tiedon sisältö on salattu tai alkuperä anonymisoitu niin, että siitä ei pysty tunnistamaan rekisteröityä. Mikäli rekisterinpitäjä ei noudata määräyksiä, tälle voidaan asettaa rahallinen sanktio, joka on suuruudeltaan korkeintaan 10-20 miljoonaa euroa tai 2- 4% rekisterinpitäjän vuotuisista ansioista. Rahallisen sanktion lisäksi viranomainen voi määrätä rekisterinpitäjälle tulevaisuuden varalta tiukempia raportointivaatimuksia sekä rekisterinpitorajoituksia. (GDPR-info 2018)

Muita mahdollisesti mainosalan yritystä koskevia laillisia haasteita tarjoavat sopimusoikeudelliset salassapitosopimukset. Suomen lain mukaan työnantaja voi työsopimuksessa määrätä siitä, mitä organisaation sisäisiä asioita työntekijä saa ilmaista organisaation ulkopuolisille. Nämä vaatimukset kuitenkin pätevät vain työsopimuksen voimassaolon ajan. Erillisellä salassapitosopimuksella työnantaja voi laajentaa vaitiolovelvollisuuden koskemaan henkilöä myös tämän työsuhteen päätyttyä. Laki ei erikseen määrää mitä ovat sellaiset tiedot, joita voidaan määrätä sopimuksella salassapidon piiriin. Tämä jää sopimuksen laatijan vastuulle. Salassapitosopimuksen rikkomisen mahdollisia sanktioita ovat yleisesti rahalliset korvaukset sekä työsuhteen purku, riippuen paljastetun tiedon arvosta sekä siitä, onko paljastus tapahtunut tahallisesti vaiko tahattomasti. (Minilex 2018)

Mikäli henkilö paljastaa liikesalaisuuksia saadakseen suoraan itselleen hyötyä, esimerkiksi siirtyessään kilpailijan toimeen tai tehdessään osakekauppaa, on kyseessä rikoslainmukainen rikos. Tästä voi seurata tietojen vuotajalle jopa vankeutta (TEK tekniikan akateemiset 2018.) Käsiteltäessä mainosalan yritystä salassapitosopimukset tulevat ajankohtaisiksi uuden henkilöstön tullessa yritykseen, vanhan henkilöstön lähtiessä yrityksestä sekä solmittaessa uusia yhteistyökumppanuuksia ja asiakassuhteita. Mainosalan yritykset saavat hallintaansa asiakasyritysten tuotetietoa sekä mahdollisesti yrityksen henkilöstön yhteystietoja, jotka saattavat olla kiinnostavia kilpailevalle yritykselle tai hakkerille.

Myös näiden tietojen tahaton paljastuminen ulkomaailmalle voi aiheuttaa asiakasyritykselle haittaa niin rahallisesti, kuin maineellisestikin. Tästä syystä on suosittavaa, että yritys solmii kaikkien työntekijöidensä kanssa salassapitosopimukset. Vaikka salassapitosopimus ei itsessään estä tietojen tahatonta vuotamista, sellaisen allekirjoittaminen voi saada henkilön kiinnittämään enemmän huomiota käytökseensä liittyen tietojen jakamiseen. Henkilö, joka ei ole aikaisemmin miettinyt lainkaan tietoturvaa, saattaa sopimusta

allekirjoittaessa herätä asian vakavuuteen ja ymmärtää paremmin mitä saa ja ei saa levittää. Näin vältetään paremmin tilanteita, joissa henkilö ei ole ymmärtänyt sitä, miten tietoja saa jakaa ja kenelle. Sopimus on siis helppo tapa luoda yhteiset pelisäännöt organisaation sisällä. Myös useimmat asiakkaat vaativat omat sopimuksensa, jolloin saavat itse määritellä vielä erikseen, miten tietoja saa käsitellä ja mitkä ovat mahdolliset sanktiot.

4 MAINOSALAN AMMATTILAISEN HAASTATTELU

Tätä opinnäytetyötä varten toteutettiin haastattelu, johon vastasi mainosalalla toimiva henkilö. Kyseinen henkilö ei kuulunut case-tutkimuksen kohdeorganisaatioon. Henkilöä haastateltiin, jotta saataisiin selkeämpi kuva tietoturvan tasosta sekä asenteista alalla yleisemmin. Haastateltava vastasi kysymyksiin nimettömänä. Haastattelu löytyy kokonaisuudessaan liitteenä. (Liite 1)

Haastateltava henkilö toimii pääsääntöisesti graafisena suunnittelijana niin paino-, kuin digituotannossa. Suunnittelutyön lisäksi hän on toiminut myös käytännön toteutuspuolella, käyttäen painokoneita sekä osallistuen esimerkiksi verkkosivustojen ohjelmointiin. Haastateltava on toiminut sekä freelancerina, että työntekijänä useassa alansa yrityksessä.

Haastattelussa kävi ilmi, että käytännössä ainut tietoturvatoimi, johon haastateltava on itse törmännyt urallaan, ovat olleet satunnaiset salassapitosopimukset. Nämä sopimukset ovat olleet paikoin niin tiukkoja, ettei ole voinut edes seuraava työpaikkaa hakiessaan mainita työskennelleensä tietyille tahoille tai näiden kanssa. Omassa freelance toiminnassaan hän ei ole vielä kertomansa mukaan kohdannut tilannetta, jossa olisi omasta tai asiakkaan tahdosta allekirjoittanut salassapitosopimusta. Haastateltava kertoo kuitenkin itse pyrkivänsä aina tarjoamaan joka asiakkaalleen ja työkumppanilleen saman luottamuksellisuuden.

Luottamuksellisiin tietoihin haastateltava on törmännyt työssään useaan otteeseen. Hän on käsitellyt sekä yritysten luottamuksellisia tietoja, että henkilöiden yhteystietoja. Näiden lisäksi hänellä on ollut pääsy joihinkin sopimustietoihin, jotka ovat sisältäneet yritysten arkaluontoista tietoa.

Haasteltava totesi vastauksissaan, että työympäristössä erillinen koulutus tai perehdytys tietoturvaan on ollut käytännössä olematonta, eikä näistä asioista ole muutenkaan puhuttu työpaikalla. Hänen mukaansa yleinen käsitys työympäristössä on, että jokainen niin sanotusti maalaisjärjellä ymmärtää olla puhumatta asioista työpaikan ulkopuolella. Tällaisessa järjestelyssä on ongelmansa sillä jokaisen käsitys siitä, mitä saa ja ei saa puhua, voi olla radikaalistikin erilainen. Tämän lisäksi, vaikka jokainen ymmärtäisikin olla puhumatta asioista suullisesti, sähköinen tietojen käsittely ja säilöminen jäävät kokonaan yhteisten pelisääntöjen ulkopuolelle.

Henkilö toteaa pyrkivänsä itse pysymään mahdollisimman hyvin perillä tietoturvallisuusasioista omatoimisesti. Hän onkin perehtynyt tärkeimpiin lainsäädännön vaatimuksiin omatoimisesti jo opiskeluaikoinaan. Ammattinsa byrokraattisiin tai laillisiin puoliin ei hänen mukaansa opiskelujen aikana paneuduttu lainkaan ja opiskelijat olivat täysin oman viitseliäisyytensä varassa oman alansa byrokraattisen puolen opiskelussa. Haastateltava kertoi ottaneensa asian puheeksi omassa oppilaitoksessaan, jotta tätäkin puolta otettaisiin tuleviin vuosikursseihin mukaan.

Haastattelussa henkilö totesi, ettei ole havainnut työympäristöissään käytännössä minkäänlaista valvontaa organisaatioiden sisällä liittyen tietoturvallisuuteen. Tämän lisäksi tietämys ja välittäminen asioista ovat olleet huolestuttavan vähäisiä. Tietoa ei ole edes pyritty hakemaan ja asian puheeksi ottaessa kohtaa vähätteleviä asenteita. Asioihin useimmiten herätään vasta, kun vahinko on jo tapahtunut peruuttamattomasti. Hänen mukaansa joissakin organisaatioissa on ollut käytössä erillinen tietoturvajäteastia. Tämä astia on kuitenkin ollut sijoitettu sellaiseen paikkaan, jossa siihen on ulkopuolisilla vapaa pääsy eikä sen käyttäjiä ole pystytty valvomaan.

Koskien oman alansa tietomurtoja, haastateltava toteaa, että ne harvemmin päätyvät valtamedian uutisointiin. Alan sisällä kuitenkin kiertää puheita useista erinäisistä tapahtumista. Yhdeksi suurimmista tietoturvatapauksista alallaan haastateltava nostaa tilanteen, jossa alalla yleisesti käytetty pilvipalvelu antoi tiedostojen katseluoikeuden väärille käyttäjille. Haastateltavan kokemuksen mukaan hänen alansa tietoturvaongelmat johtuvat useimmiten puhtaasti vahingoista ja virheistä, kuin tahallisista hyökkäyksistä tai rikoksista.

Haastateltava myöntää, että vaikka pyrkiikin pysymään perässä kaikista vaatimuksista ja suosituksista, ei itsekkään ole tietoinen aivan kaikista tietoturvaan liittyvistä seikoista. Hän ei esimerkiksi ollut lainkaan kuullut vakuutusyhtiöiden tarjoamista kybervakuutuksista tai tiennyt mitään tahoa, joka olisi tällaisen palvelun ostanut.

Haastateltava toteaa, että asioille pitäisi hänen alallaan ehdottomasti tehdä jotain. Lääkkeeksi hän nostaakin lisäkoulutuksen, joka aloitettaisiin jo ammattiin opiskellessa. Graafisen suunnittelijan, kuten muidenkin media-alan työskentelijöiden työ, sisältää kuitenkin paljon muutakin, kuin vain itse luovan osuuden. Monelle alalle tuleville saattaakin tulla yllätyksenä, kuinka paljon toimistotyötä ala sisältää. Oppilaitoksissa tapahtuvan koulutuksen lisäksi hän kokee yritysten oman koulutuksen erittäin tärkeäksi ja toivoisikin kai-

kenlaisia kursseja lisää. Hänen mukaansa tällä hetkellä tietoturvatietämyksessä mennään pitkälti ”musta tuntuu” asenteella ja luotetaan siihen, että ei ennenkään ole mitään tapahtunut. Uuden Yleisen tietosuoja-asetuksen haastateltava kokee hyväksi aluksi asioiden kehittymiselle ja toivookin, että suuret sanktiot herättäisivät alan toimijat vihdoinkin asiaan. Hän pelkää kuitenkin vaikutuksen jäävän käytännön tasolla vähäiseksi.

Haastattelun lopuksi henkilö nostaa esiin kaksi tärkeäksi kokemaansa asiaa. Hän toteaa, että niissäkin yrityksissä, joissa ollaan tarkempia ulkoisista uhista, kuitenkin luotetaan sokeasti kaikkeen, mitä asiakkailta tai yhteistyökumppaneilta saadaan haltuun. Tällä hän tarkoittaa sitä, että vaikka ulkoisista lähteistä tulevia linkkejä ja liitteitä varotaan, asiakkaan antamia tiedostoja avataan ja käsitellään ilman mitään varotoimia. Hän nostaakin esille mahdollisuuden, että asiakkaan tai kumppanin järjestelmä saattaa olla saastunut, jolloin mahdollinen tietoturvariski leviää tiedostojen mukana myös muiden tahojen järjestelmiin. Hän toteaakin, että tietoturvaongelmat monesti mielletään aina vain pahantahtoisen hakkerin tahallisiksi teoiksi. Ideaaliksi tilanteeksi hän kuvaa järjestelmän, jossa kaikki yrityksen kautta kulkevat tiedostot avattaisiin ensin erillisellä laitteella.

Tähän liittyen hän toteaa toiseksi asiaksi tietoturvaseikoista puhumisen vaikeuden asiakkaiden kanssa. Mikäli asiakkaan kanssa yrittää ottaa puheeksi millä tolalla tämän oma tietoturva on, tämä tulkitaan nopeasti negatiiviseksi arvosteluksi ja johtaa helposti asiakkuuden kariutumiseen.

Haastattelussa tuli ilmi erittäin selvästi haastateltavan kokemus siitä, että tietoturva mainos- ja media-alalla on riittämätöntä. Haastattelun mukaan tietoturvaan, kuten muuhunkin alan byrokratiaan kiinnitetään erittäin vähäistä, käytännössä olematonta huomiota niin alan koulutuksessa, kuin käytännön työssäkin. Haastattelun perusteella alan tietoturvatapahtumiin reagoiminen on lähinnä vasta jälkikäteen tapahtuvaa vahinkojen minimoimista. Ennaltaehkäisy on jätetty pitkälti salassapitosopimusten varaan. Salassapitosopimuskaan ei kuitenkaan itsessään estä työntekijän virhettä, jos tämä ei ymmärrä sopimuksen sisältöä, eikä ole koulutettu toimimaan sopimuksen edellyttämillä tavoilla. Lisäkoulutus olisi siis kipeästi tarpeen. Salassapitosopimus ei myös itsessään suojaa ulkoapäin organisaatioon kohdistuvilta hyökkäyksiltä. Mahdollisen hyökkäyksen riskiä nostaa henkilöstön ilmeinen tiedon sekä osaamisen puute teknisten tietoturvallisuusratkaisujen, lainsäädännön ja hyvien standardien suhteen. Mikäli nämä perusasiat eivät ole kunnossa, mahdollisen hyökkääjän on erittäin helppo tunkeutua järjestelmiin ja tarkastella luottamuksellisia tietoja. Myöskin fyysisissä ratkaisuissa ilmenee puutteita kuten

haastattelussa mainittu tietoturvajäteastia, joka oli samanaikaisesti useamman ulkopuolisen tahon käytettävissä. Tällaiset itsessään pienet seikat yhdessä aiheuttavat organisaation toiminnan ketjussa useamman heikon lenkin, jotka ovat omiaan aiheuttamaan tietovuodon. Erityisen mielenkiintoisena asiana haastateltava esitti näkemyksensä siitä, että myös luotetuilta tahoilta tulevalta materiaalilta voi olla tarve suojautua. Vaikka pahantahtoinen taho ei kohdistaisikaan hyökkäystään mainostoimistoon, saattaa asiakkaan taikka kumppanin järjestelmien saastuminen päästä tahattomasti leviämään myös mainostoimistoon.

5 TIETOTURVANKARTOITUS PROSESSI YRITYKSESSÄ

Tietoturvallisuuden tarkastelu on jaettu kolmeen kategoriaan. Nämä ovat henkilöstö, hallinto sekä tekninen ja fyysinen osa (Viestintävirasto 2017.)

Tarkasteltaessa yrityksen tietoturvaa on näiden kaikkien kolmen osa-alueen oltava kunnossa. Yritys voi toteuttaa parhaimman ja kalleimman mahdollisen teknisen tietoturvaratkaisun. Kuitenkin mikäli henkilöstöä ei ole ohjeistettu sen oikeaoppiseen käyttöön, ratkaisu on aivan tyhjän kanssa (Professio 2016.) Samoin mikäli hallinto ei valvo ratkaisun käyttöä ja ylläpitoa, sen teho laskee huomattavasti. Vastaavasti yritys saattaa olla tilanteessa, jossa hallinto toteuttaa vahvaakin valvontaa ja organisointia. Mikäli näitä keinoja ei kuitenkaan ole mietitty kunnolla läpi, näistä muodostuu vain pinnallista turvallisuusteatteria. Turvallisuusteatterilla tarkoitetaan tilannetta, jossa ulkoisesti luodaan sellainen kuva, että turvallisuus otetaan vakavasti. Kuitenkin mikäli turvatoimia tarkastelee vähänkään tarkemmin ne osoittautuvat vain pinnallisiksi toimiksi, jotka on helppo ohittaa (Privacy SOS 2018.) Tietoturvallisuus ei ole koskaan vain yksittäinen asia, vaan kokonaisuus, joka on juuri niin vahva, kuin sen heikoin lenkki.

Yrityksen henkilöstöä tarkastellessa tulee ottaa huomioon henkilöstön tämän hetkinen tietämyksen taso, toimintakäytännöt sekä henkilökohtaiset asenteet. Etenkin henkilöstön omiin asenteisiin tulee kiinnittää erityishuomiota (Liite 1.) Henkilöstön asenteet tietoturvan suhteen vaihtelevat aivan laidasta laitaan täysin välinpitämättömän ja erittäinkin tiukan välillä. Näiden ääripäiden välillä tulisi pyrkiä löytämään tasapaino. Liian heppoinen asennoituminen tietoturvaan aiheuttaa hienoimmankin hallinnon ja järjestelmän romuttumisen. Vastaavasti liian tiukka asenne taas aiheuttaa jo yritykselle haittaa, hidastaen työntekoa, tehden työstä jähmeää ja joustamatonta. Asenteissa tulee ottaa huomioon myös niiden sosiaalinen aspekti. Yhdenkin työntekijän liian jähmeä tai välinpitämätön asenne voi levitä muihin. Yhden henkilön liian tiukka asenne saattaa aiheuttaa närkästystä muissa ja saada heidät asennoitumaan tietoturvaan negatiivisena taakkana. Vastaavasti yhdenkin henkilön liian löysä asenne voi saada muutkin ajattelemaan, ettei tietoturvasta tarvitse välittää. Henkilöstön kohdalla on myös tärkeää, että heidät koulutetaan mahdollisiin teknisiin ratkaisuihin. Riittämätön koulutus sekä teknisen osaamisen puute voivat aiheuttaa teknisten järjestelmien väärin konfiguroimista, joka taas johtaa nopeasti koko järjestelmän hyödyttömäksi muuttumiseen. Henkilöstön tulee myös ym-

märtää omaa alaansa koskettava lainsäädäntö sekä alan sisäiset standardit. Henkilöstön tulee myös ymmärtää, että tietoturva ei ole vain teknisiä ratkaisuja, vaan myös omaa käyttäytymistä ja tietämystä, varsinkin organisaation asioista puhumisen ja kirjoittamisen suhteen (Professio 2018.) Eräs usein unohdettu huomio työntekijöitä tarkastellessa käsittelee sitä, onko organisaatiosta poistuvan henkilön kohdalle olemassa käytännöt, kuinka hänen jälkeensä jättämiä tietoja sekä käyttäjätunnuksia käsitellään. Pahimmassa tapauksessa poistuneen henkilön tunnukset järjestelmissä saattavat jäädä vuosiksi elämään avaten näin mahdollisen turvallisuusriskin organisaation järjestelmiin.

Hallintoa tarkastellessa tulee ottaa huomioon hallinnon ymmärrys henkilöstön nykytilasta, tietämys lainsäädännöstä ja standardeista. Hallinnon tulee myös olla perillä yrityksen teknisen turvallisuuden tarpeista, osatakseen valita tähän oikeat ratkaisut, jotka täyttävät sekä lain, että yrityksen omat tarpeet. Ei riitä, että hallinto vain kirjoittaa paperille säännöt ja kustantaa järjestelmät, ellei se myös kouluta ja valvo henkilöstöä. Pahimmassa tapauksessa hallinto saattaa elää käsityksessä, että organisaation tietoturvan taso on riittävä, samalla kun henkilöstö jättää käytännöt noteeraamatta. Vaikka tietoturva on organisaatiossa jokaisen asia, on kuitenkin viime kädessä hallinnon vastuu seurata järjestelmien ajantasaisuutta, henkilöstön osaamista sekä järjestää lisäkoulutusta. (Viestintävirasto 2017)

Teknisiä ratkaisuja tarkasteltaessa ei tule keskittyä vain tietokoneiden virusturvaohjelmistoihin. Tulee tarkastella myös mitä ohjelmistoja näihin järjestelmiin on asennettu, käyttöjärjestelmien ajantasaisuutta sekä kuinka mikäkin laite on liitetty verkkoon. Lisäksi tulee tarkastella yrityksen muita fyysisiä turvallisuusratkaisuja, kuten lukittavia kaappeja, toimitiloissa tapahtuvaa liikkumista ja sen seurantaa. Vaikka yrityksen verkko sekä laitteet olisivat täydellisesti suojatut, altistuu se kuitenkin tietoturvaongelmille, mikäli toimitiloissa pystyy kulkemaan valvomatta ja tarkastelemaan esimerkiksi esille jääneitä papereita tai lukitsemattomia tietokoneita. Fyysinen turvallisuus tulee ottaa myös erityisesti huomioon silloin, kun järjestelmien ja paperien kanssa liikutaan yrityksen toimitilojen ulkopuolella. (Viestintävirasto 2017)

Kaikki kolme edellä mainittua osa-aluetta toteutuksineen kannattaa organisaation kirjata ylös tietoturvapolitiikaksi. Tämä politiikka on hyvä pitää aina henkilöstön saatavilla, päivitettävä säännöllisesti sekä esiteltävä tarvittaessa myös asiakkaille ja yhteistyökumppaneille. Kirjallinen tietoturvaohjeistus takaa sen, ettei henkilöstön keskuudessa synny väärin ymmärryksiä käytännöistä tai tilannetta, jossa jokin ohje ei ole saavuttanut kaikkia.

Näin myös vältetään tilanne, jossa henkilö voisi vedota tietämättömyyteen jotain mennessä vikaan. Kirjallisen ohjeistuksen esitteleminen myös muille tahoille osoittaa, että organisaatiossa otetaan tietoturva-asiat vakavasti, joka selvästi nostaa organisaation arvoa esimerkiksi asiakkaiden silmissä. Asiakkaat luovuttavat kuitenkin mainosalan yrityksen haltuun erittäinkin arkaluentoisia tietojaan, joiden haavoittuminen saattaa pahimmassa tapauksessa romuttaa koko asiakasorganisaation toiminnan. Kirjallisen ohjeistuksen olemassaolo ja noudattaminen takaavat myös sen, että mahdollisissa oikeustapauksissa organisaatio pystyy paremmin todistamaan, missä mahdollinen haavoittuvuus on sijainnut, kun tarkastellaan asetettua käytäntöä ja todellista toimintaa keskenään.

6 CASE-YRITYKSEN TARKASTELU

Kyseessä on suomalainen, turkulainen mainostoimisto. Organisaatio työllistää täysipäiväisesti alle kymmenen henkilöä. Tämän lisäksi yritys hankkii lisäpalveluja, kuten IT-konsultointia sekä mainosnäyttelijöitä alihankintana. Alihankinta tapahtuu sekä toimimalla toisten yritysten kanssa, että suoraan yksittäisten henkilöiden kanssa. Yritys tuottaa asiakkailleen markkinointimateriaalia, erikoistuen erityisesti videomateriaaliin. Yritys pyrkii myös laajentamaan toimintaansa verkkomarkkinoinnin tarjoamiseen. Tähän pyritään erityisesti tuottamalla oma, tarkoitukseen sopiva ohjelmistopohja, jonka lisensointia, käyttöopastusta sekä kustomointia voidaan myydä eteenpäin. Yritys toimii vuokratussa toimistotilassa kiinteistössä, jossa sijaitsee myös muita yrityksiä. Työtehtäviä henkilöstö suorittaa toimistolla, etänä kotoaan käsin sekä paikan päällä esimerkiksi kuvauspaikoilla. Yrityksellä ei ole varsinaisia aukioloaikoja, vaan asiakkaisiin ollaan kontaktissa lähinnä sopimuksen mukaan. Myös työtehtävien hoidossa ovat päivämäärät tärkeämpiä, kuin tietyt kellonajat.

6.1 Hallinnon tarkastelu

Hallinnon tarkastelu tulee aloittaa hallinnon kartoittamisesta. Tässä case-tapauksessa hallinnon laajuuden kartoitus suoritettiin tutustumalla yrityksen henkilöstöön ja haastattelemalla heitä aiheesta. Keskustelun tukena käytettiin Pk-yritysten riskienhallintaan luotuja kyselykaavakkeita (PK-RH 2018.) Kyselykaavakkeiden kysymykset käytiin läpi yhdessä ja niiden sisältöä käytettiin keskustelun kulun rankana.

Henkilöstön haastattelun perusteella organisaation hallinnosta muodostui kuva modernista, hajautetusta hallinnosta. Yrityksellä on virallisesti toimitusjohtaja ja esimies, jotka ovat sama henkilö. Vaikka yrityksellä on nimetty esimiesasemassa oleva henkilö, on yrityksessä päätöksenteko silti hyvin hajautettua. Jokainen organisaation jäsen on osaltaan vastuussa omista työtehtävistään, eikä näiden suorittamista varsinaisesti perinteiseen tapaan seurata esimiestasolla, ellei itsenäisessä työskentelyssä ilmene ongelmia. Suurimmat päätökset, jotka koskevat organisaatiota, kuten esimerkiksi projektien vastaanottaminen, työtapojen suunnittelu sekä taloudelliset asiat, keskustellaan yhdessä koko henkilöstön keskuudessa. Yrityksessä hallinnolla ei ole hallussaan sellaista tietoa, jota

vakituinen henkilöstö ei pääsisi tarkastelemaan. Tunnettujen vakituisten henkilöiden kesken kaikki yrityksen hallussa oleva tieto on avoimesti saatavilla. Tietojen tarkastelua ei valvota erikseen, sillä yrityksessä vakituisesti toimivat henkilöt ovat entuudestaan toisilleen tuttuja, tietävät toistensa työskentelytavat sekä luottavat toisiinsa. Yrityksen henkilöstöltä ei tarkasteluhetkellä hallinnon suunnalta ole vaatimuksia erityisesti tietoturvallisuuteen liittyvän tietämyksen suhteen. Hallinto ei myöskään järjestä erillisiä koulutuksia aiheesta tai oleta sellaisiin osallistumista oma-aloitteisesti. Tämän kokoisessa ja laatuisessa organisaatiossa hallinto luottaa omalta osaltaan tietoturvallisuusasiat pitkälti yleisen maalaisjärjen varaan henkilöstöllä. Oletus on, että jokainen ymmärtää erikseen käskemättäkin olla puhumatta yrityksen asioita ulkopuolisille.

Tällainen hallintotapa on toiminut keskustelun perusteella hyvin organisaatiossa. Syiksi toimimiselle annetaan organisaation pieni koko sekä tehtävissä toimivien henkilöiden pitkäaikainen suhde keskenään. Näin ollen sellaisiakin asioita, joita muissa yrityksissä ei välttämättä jaettaisi hallinnon ja henkilöstön välillä, ovat kaikkien tiedossa. Hallinto ei koe, että tällainen toimintatapa olisi tähän asti aiheuttanut ongelmia.

Tarkempaa varovaisuutta tiedonjaossa harjoitetaan keskusteltaessa ulkopuolisten toimijoiden sekä väliaikaisten osallistujien kanssa. Näistä henkilöistä ei voida aina mennä takuuseen, sillä heitä ei tunneta välttämättä yhtä läheisesti. Tämän lisäksi ulkopuolisten henkilöiden ei ole muutenkaan tarvetta tietää esimerkiksi kaikkia asiakkaan yritykselle luovuttamia tietoja tai yrityksen omia sisäisiä tietoja. Ulkopuolisten henkilöiden kanssa toimiessa yrityksen hallinto ei järjestelmällisesti vaadi salassapitosopimuksia. Tällöinkin luotetaan pitkälti ihmisten omaan järkeen ja hyväntahtoisuuteen. Ulkopuolisia tekijöitä ei myöskään erikseen tarkasteta juuri tietoturvan kannalta ennen yhteistyön aloittamista, ellei ulkopuolisella tekijällä ole ennalta tiedettyä, räikeää historiaa tämän tyyppisistä ongelmista. Hallinto tarkastelee ulkopuoliset tahot muilla tavoin varmistuakseen kuitenkin siitä, että nämä omaavat yhteistyöhön mahdollisesti tarvitut resurssit sekä taidot.

Tällaisessa hallintotavassa on sekä hyvät että huonot puolensa. Avoin ja hajautettu hallinto vapauttaa henkilöstön toteuttamaan työtehtäviään itselleen mielekkäillä tavoilla ja itselleen mielekkäisiin aikoihin. Tämä on etenkin luovilla aloilla yleistä, sillä luovaa työtä tekevä henkilö ei välttämättä saa inspiraatiota aina juuri toimistoaikaan. Kevyt hallinto toimii myös yleisesti parhaiten pienissä yrityksissä, joissa henkilöstö on jo hitsautunut yhteen pidemmän ajan sisällä.

Mahdollisia huonoja puolia tällaisessa hallintotavassa ovat vastaavasti vastuun sekä työnorganisoinnin hajautuminen niin, että saattaa syntyä tilanteita, joissa kaikki tarvittavat henkilöt eivät ole täysin perillä toistensa tekemisistä. Tällainen ongelma voi syntyä esimerkiksi useamman henkilön aikataulujen mennessä ristiin, koska he eivät ole olleet täysin tietoisia toistensa työajoista. Toisena ongelmana voidaan kohdata ongelmien sattuessa vaikeuksia määrittää, kuka on loppukädessä vastuussa tapahtuneesta. Teknisesti esimies on aina vastuussa alaisistaan. Hallinnon kuitenkin ollessa hajautettua, voi syntyä ongelma määrittää, missä menee henkilöstön sekä hallinnon vastuualueiden raja. Tarkasteltaessa erityisesti tietoturvaa, tällainen tilanne on hyvinkin mahdollinen. Mahdollisen tietoturvaongelman ilmaantuessa saattaa syntyä ongelma määrittää johtuiko ongelma esimerkiksi siitä, ettei hallinto kouluttanut henkilöstöään tarpeeksi, vaiko siitä, ettei henkilöstön jäsen itse ymmärtänyt toimiensa vääryyttä. Tällaisista tilanteista johtuen myös hajautetun hallinnon organisaatioissa tulisi silti luoda selvät, yhteiset pelisäännöt tietyille toimille, kuten esimerkiksi tietoturva-asioille.

6.2 Henkilöstön tarkastelu

Henkilöstöä lähdettiin tarkastelemaan hallintoon perehtyessä esille tulleiden kohtien kautta. Havainnointia suoritettiin keskustelemalla henkilöstön kanssa, sekä seuraamalla henkilöstön päivittäistä toimintaa.

Kuten edellisessä osiossa mainittiin, henkilöstön työskentelytavat yrityksessä ovat melko vapaita. Sovittuja tapaamisia sekä määräaikoja lukuun ottamatta henkilöstön liikkeitä tai työaikoja, ei seurata millään erityisellä tavalla. Työtehtävien ajallaan suorittaminen haluttujen vaatimusten mukaisesti koetaan tärkeämmäksi, kuin virallisten työaikojen tai vastaavien noudattaminen.

Henkilöstöllä on oikeus kuljettaa työpaikan sekä projektien materiaaleja ja välineitä organisaation toimitilojen ulkopuolelle vapaasti ilman eri valvontaa. Yrityksellä ei myöskään näytä olevan valmiina erillistä protokollaa tai ohjeistusta siihen, kuinka materiaaleja säilötään näiden ollessa toimitilojen ulkopuolella. Toiminnassa luotetaan henkilöstön maalaisjärkeen materiaalin säilytyksen suhteen. Oletus siis on, että jokainen ymmärtää erikseen kertomattakin, ettei materiaaleja ja välineitä jätetä lojumaan avoimesti valvomatta. Henkilöstöä haastatellessa asiasta ei tullut ilmi, että henkilöstö kokisi tätä nykyistä menettelyä ongelmaksi. Esiin ei noussut esimerkkejä tapauksista, joissa yrityksen materiaalia olisi päätynyt vääriin käsiin sen ollessa liikkeessä tilojen ulkopuolella.

Henkilöstön käyttämät työkalut sekä ohjelmistot ovat yrityksen omaisuutta. Henkilöstölle on kuitenkin sallittua käyttää työssään myös omia välineitään. Tietoturvan kannalta tarkasteltuna tämä ei synnytä ongelmaa, kun puhutaan esimerkiksi kameranjalasta tai vastaavista välineistä. Ongelmalliseksi tämä saattaa muodostua kuitenkin siinä tapauksessa, kun henkilöstö käyttää työssään esimerkiksi omaa puhelintaan, siirrettävää mediaansa tai ohjelmistojaan. Näiden ulkopuolisten välineiden ja ohjelmistojen sisältö ei ole yrityksen hallinnassa ja valvomaa, jolloin syntyy riski, että ne saattavat levittää haavoittuvuuksia yrityksen järjestelmiin.

Yrityksen henkilöstön jäsenet eivät ole suorittaneet nykyisessä tai edellisissäkään toimissaan minkäänlaisia tietoturvaan liittyviä koulutuksia. Myöskin heidän oma perehtyneisyytensä asiaan on erittäin pintapuolista. Selkeimmät käsitteet, kuten salassapitosopimus olivat heille tuttuja. Kuitenkin lainsäädännön tarkemmat piirteet, esimerkiksi vaatimukset tavoista henkilötietojen säilyttämiseen tai luottamuksellisten tietojen oikeaoppiseen hävitykseen olivat joko erittäin pintapuolisessa tiedossa tai kokonaan tuntemattomia. Henkilöstö ei haastatellessa kokenut itse tällaisia koulutuksia tai kurssituksia tarpeellisiksi.

Yrityksessä ei ole henkilöstölle olemassa erillistä luettavaa tietoturvaohjeistusta, eikä yritys ole vaatinut henkilöstöään allekirjoittamaan yleistä salassapitosopimusta. Koska yrityksen henkilöstö on pääsääntöisesti keskenään vanhoja tuttuja, vallitsee työpaikalla yhteinen ymmärrys siitä, miten eri asioita hoidetaan. Yritys tekee kuitenkin yhteistyötä myös ulkopuolisten konsulttien sekä toimijoiden kanssa. Myöskään tälle ulkopuoliselle henkilöstölle ei ole tarjolla luettavaksi tietoturvaan liittyvää dokumentaatiota, eikä heiltä vaadita salassapitosopimuksia. Ulkopuolista henkilöstöä ei myöskään ennalta tarkastella tietoturvan kannalta, ellei kyseessä ole jokin tunnetusti virheitä tehnyt taho. Tämä voi synnyttää helpostikin ongelmia tietoturvan suhteen. Mikäli ulkopuolista henkilöstä ei perehdytetä yrityksen tietoturvan vaatimuksiin, voi syntyä helposti tahattomia tietovuotoja, henkilöiden puhuessa työstään ulkopuolisille keskusteluissaan. Huomion arvoista on myös mietintä vastuunjaosta mahdollisten virheiden tapahtuessa. Mikäli ulkopuoliselle henkilöstölle ei ole esitetty mitään vaatimuksia tietoturvasta, eikä teetetty salassapitoisuuksia, voi syntyä tilanne, jossa mahdollisen tietovuodon tapahtuessa on erittäin vaikea määritellä, kuka on viime kädessä vastuussa tapahtuneesta. Kaikkien osapuolten välillä vallitessa voimassa oleva salassapitosopimus, on helppo ulkopuoliseen henkilöstöön kuuluvan henkilön tehdessä virheen tietoturvassa ja ohjata vastuu tapahtuneesta koh-

distumaan häneen. Ilman sopimuksia on organisaatio itse aina suoraan vastuussa tapahtuneesta, vaikka ei olisi itse suoraan osallinen tapahtuneeseen tietovuotoon. Tällöin yritys kohtaa itse suoraan kaikki mahdolliset lailliset, maineelliset sekä sopimusehdolliset sanktiot. Tällöin yrityksen on itsekin lähes mahdotonta lähteä vaatimaan korvauksia esimerkiksi omista lakikuluistaan tai sakkomaksuistaan ulkopuoliselta taholta.

Työtehtävissään henkilöstöllä on käytännössä pääsy kaikkeen yrityksen omistamaan tietoon ja aineistoon, ilman erillisiä rajauksia tehtävien mukaan. Yrityksessä ei myöskään seurata tai dokumentoida erillisesti, kuka milloinkin ja mihin tarkoitukseen jotain tietoa on käytetty. Pienessä yrityksessä, jossa kaikki henkilöstön jäsenet tuntevat toisensa, tämä ei muodosta sinänsä ongelmaa. Pienen yrityksen henkilöstö tuntee toisensa jo täysin muutenkin, joten henkilöstörekisterin salassapito firman sisällä ei ole tarpeellista. Samaten myöskin asiakkaiden ja yhteistyökumppanien tietojen piilottelu sisäisesti ei ole tarpeen. Tämän kokoisessa ja kulttuurisessa yrityksessä kuitenkin päätökset jokaisen asiakkaan ja yhteistyökumppanin ottamisesta mukaan on tehty yhdessä jo alusta alkaen, joten jokainen henkilöstön jäsen tuntee näistä jokaisen jo suoraan. Lisäksi pienessä yrityksessä, jossa ei ole työtehtäviä tarkalleen jaettu henkilöittäin, on jokaisella oltava pääsy samoihin materiaaleihin. Vaikka tällaisessa organisaatiossa ei synnykään ongelmia henkilöstön tiedonjaosta ristiin organisaation sisällä, tulisi tiedon säilömiseen silti kiinnittää huomiota lainopillisesta näkökulmasta. Esimerkiksi tässä tapauksessa henkilöstörekisterin sisältöä ei tarvitse salata organisaation sisällä siksi, että kaikki henkilöstössä ovat vanhoja ystäviä ja tuntevat toisensa henkilökohtaisella tasolla. Kuitenkin henkilöstörekisterin sisällöstä sekä säilyttämisestä on olemassa säännöksiä, jotka määräävät, kuinka rekisteriä tulee säilyttää ja suojata, huolimatta henkilöstön välisistä omista suhteista.

Tarkastelun aikana huomattiin, että henkilöstö ei erityisesti poista näkyviltä muihin asiakkaisiin liittyvää aineistoa tai mieti sanomisiaan, kun tiloissa oleskelee ulkopuolisia henkilöitä. Tällainen käytös on itsessään suoraan riski kahdella tapaa. Ensinnäkin tämä voi aiheuttaa tahattoman tietovuodon, jossa yritykseen tai sen yhteistyökumppaneihin ja asiakkaisiin liittyvää tietoa voi vuotaa yrityksen ulkopuolelle. Vaikka tiedon näkevä tai kuuleva ei olisikaan pahantahtoinen, saattaa hän keskustella kuulemastaan ja näkemästään ulkopuolisille tahoille tietämättä, että tätä tietoa ei saisi levittää. Toisena riskitekijänä voidaan nähdä se yleinen luotettavuuden kuva, jota yritys heijastaa tällä toiminnallaan. Potentiaalisen asiakkaan saapuessa tiloihin tutustumaan ja tekemään päätöstä yrityksen palkkaamisesta, voi tälle taholle syntyä yrityksestä negatiivinen kuva huomatessaan,

että hänen mahdollisesti yritykselle luovuttamansa tiedot eivät ole tarpeeksi hyvin suojattuja. Tarkempi asiakas saattaa huomioida tällaisen piirteen erittäinkin tarkasti ja päättää vetäytyä yhteistyöstä jo pelkästään tämän takia pelätessään, että hänen jakamiaan tietojaan käsitellään samalla tavalla ja ovat näin riskissä vuotaa.

Yrityksellä ei ole olemassa mahdolliselle uudelle henkilöstölle esitettävää perehdytysdokumentaatiota yrityksen toimintatapoihin. Tässäkin tilanteessa voidaan pohtia tällaisen tarpeellisuutta ottaen huomioon, että yritys toimii pitkälti keskenään tuttujen henkilöiden voimin, eikä ole ainakaan lähitulevaisuudessa palkkaamassa uutta henkilöstöä. Yritykseltä puuttuu myöskin valmis menettelyprosessi sille tilanteelle, jossa yrityksestä poistuu henkilö. Tällöin on tarpeen olla tietoinen kaikista hänelle kuuluvista tunnuksista, tileistä sekä muuta yrityksen immateriaalioikeudesta. Muussa tapauksessa vanhan työntekijän käyttäjätilit yrityksen järjestelmiin saattavat jäädä tahattomasti elämään, jolloin näitä voi käyttää hyväkseen niin ulkopuolinen taho, kuin mahdollisesti yrityksen kanssa riitoihin joutunut entinen työntekijä. Henkilön poistuessa tulee myös olla tietoinen siitä, mitä hän mahdollisesti tietää yrityksen toiminnasta sellaista, josta pitäisi vielä solmia salassapitosopimus. Vaikka jälleen voidaan todeta kaikkien yrityksen henkilöstöön kuuluvien olevan vanhoja tuttuja, tällaisen työntekijän poistumissuunnitelman luominen saattaa silti olla aiheellista. Ensinnäkin siksi, että yritys voi tulevaisuudessa käyttää enemmän ulkopuolisia apulaisia ja työntekijöitä palveluksessaan, jolloin pitää olla tietoinen, mitä tietoja näistä kullakin on hallussaan ja mihin järjestelmiin heillä on pääsy. Toisena huomiona voidaan todeta, että vaikka yrityksessä työskentelevät ovatkin keskenään ystäviä, myös ystävyyssuhteet voivat kariutua. Tällöin saattaa olla riski tiedon vuotamisesta, sillä yrityksestä poistuvalla henkilöllä voi olla erosuuttumuksen lisäksi mielessään myös henkilökohtaisempia kaunoja, jotka saattavat ajaa henkilön herkemmin toimimaan entistä työpaikkaansa vastaan.

6.3 Teknisten ratkaisujen tarkastelu

Yrityksen teknisiä ratkaisuja tietoturvan suhteen tarkasteltiin keskustelemalla sekä kartoittamalla yrityksen kalustoa ja kiinteistöä.

Yrityksen pääasialliset työkalut ovat puhelimet, tietokoneet sekä erinäiset kuvaus- ja mediakalustot. Älypuhelimista yrityksellä on käytössään sekä Android- ja iOS-käyttöjärjestelmillä toimivia älypuhelimia. Android-pohjaiset älypuhelimet vaihtelivat käyttöjärjestel-

mänsä päivitystilanteen mukaan laidasta laitaan. Tähän valitettavasti käyttäjä ei voi vaikuttaa, muuta kuin ostamalla kokonaan uuden laitteen, sillä valmistajat päivittävät laitteitaan hyvin lyhyen aikaa. Älypuhelimissa ei ollut asennettuna erillisiä tietoturvaohjelmistoja. Henkilöstö ei myöskään vaikuttanut täysin tietoiselta siitä, että älypuhelimet kohtaavat tänä päivänä aivan samoja tietoturvariskejä, kuin tietokoneetkin.

Tietokoneita yrityksessä käytetään Windows-, macOS-, sekä ChromeOS-käyttöjärjestelmillä varustettuina. Näidenkin laitteiden iät vaihtelivat hyvin suurella skaalalla. Päätelaitteissa ei ollut asennettuna erillisiä tietoturvaohjelmistoja tai näissä käytetään tietoturvaohjelmien rajallisia, ilmaisia kokeiluversioita. Henkilöstö vaikutti olevan päällisin puolin tietoinen päätelaitteita uhkaavista yleisimmistä riskeistä, kuten sähköpostiliitteistä sekä internetin mainostauluista. Päätelaitteiden tietoturvan tasoon henkilöstö suhtautui pitkälti sillä ajatuksella, että kun tähänkään asti ei ole mitään tapahtunut, niin ohjelmistoja ei tarvita. Vaikka käytännössä välttämättä mitään ei ikinä tapahtuisikaan, tällainen asenne voi tuottaa yritykselle juridisia ongelmia. Yleinen tietosuoja-asetus, henkilötietolaki sekä alan omat standardit määräävät tapoja sille, millä tavalla yritysten arkaluentoisia tietoja sisältäviä järjestelmiä on suojattava. Vaikka yritys välttyisikin kaikilta tietovuodoilta ja hyökkäyksiltä, voi järjestelmien suojaamattomuuden tullessa ilmi yritys kohdata juridisia sanktioita riittämättömistä suojauksista.

Yrityksen verkkona toimii vuokrakiinteistön oma verkko, johon henkilöstö ei pääse vaikuttamaan. Verkkoon liittyäkseen yrityksellä on käytössään oma hankkimansa reititin. Reititin sisältää sisäänrakennettuja tunkeutumisen esto mekanismeja, kuten käyttäjienhallinta- sekä palomuuriominaisuuksia. Ominaisuuksista mikään ei ollut tarkasteluhetkellä aktivoitu. Reititin onkin keskustelun perusteella vain liitetty suoraan verkkoon. Reitittimeen on asetettu oma salasanansa, joka estää suoran liittymisen yrityksen langattomaan verkkoon.

Tarkastellessa mitkään edellä mainituista yrityksen välineistä eivät ole erillisiä yrittäjämalleja, vaan normaaleja kuluttajille myytäviä versioita.

Tarkastellessa yrityksen muuta tietoturvaan liittyvää välineistöä, kiinnittyy huomio fyysisen materiaalin säilyttämiseen sekä hävittämiseen. Yritys ei käsittele suuria määriä fyysistä paperia, suurimman osan tiedoista ollessa pilvipalveluissa. Kuitenkin ne fyysiset mediat, joita yritys käsittelee, ovat säilöttyinä kiinteistössä avoimesti pöydille tai lukitse-

mattomiin laatikkoihin. Yrityksellä ei näytä olevan hallussaan silppuria tai muuta soveltuvaa välineistöä fyysisen median oikeaoppiseen tuhoamiseen, eikä yrityksellä ole sopimusta materiaalin hävittämisestä ulkoisen yrityksen kanssa.

Käsitellessään digitaalista dataa yritys hyödyntää enimmäkseen Googlen tarjoamia yrityspalveluita sekä Google Drive pilvitallennustilaa. Googlen palveluiden lisäksi henkilöstö käyttää työssään muun muassa Adoben tarjoamia pilvipalveluita. Myös yrityksen talous- ja henkilöstöhallinto sijaitsee ulkopuolisen tilitoimiston pilvipalvelussa. Google sekä Adobe julkaisevat palveluistaan avoimesti tietoja liittyen siihen, kuinka näiden palveluiden yritysasiakkaiden turvallisuus pyritään takaamaan. Näiden palveluiden selonteot tietoturvansa tasoista ovat kattavia ja vakuuttavia, vaikka eivät tietenkään voi avoimesti kertoa aivan kaikkea, esimerkiksi esittää lähdekoodiaan. Kun Googlen sekä Adoben pilvipalveluiden turvallisuuden tilaa tarkastellaan etsimällä mediasta esimerkkejä näiden palveluiden tiedetyistä tietoturvauhista, yritysten omat selonteot vaikuttavat pitävän paikkansa. Kuten aikaisemmin tässä opinnäytetyössä haastateltu mainosalan ammattilainen totesi, on Adoben palveluissa lanseerausvaiheessa sattunut jonkin verran tietoturvaongelmia, jotka ovat johtuneet palvelussa esiintyneistä tuotantovirheistä (Liite 1.) Tällaisia ongelmia ovat esimerkiksi olleet tietojen häviäminen palvelimilta tai virheellisesti tietojen näkyminen toisille käyttäjille. Nämä ongelmat vaikuttavat kuitenkin tulleen korjatuksi melko pikaisesti Adoben suunnalta eikä tuoreempia, vakavimpia tietoturvauhkia löydy mediasta normaalilla etsimisellä. Googlen pilvipalveluita tarkastellessa median näkökulmasta, ei löydy viitteitä mistään suoraan Googlesta tai sen pilvipalveluista johtuvasta tietoturvauhasta. Google Drive palveluun liittyvät vähäiset tietoturvatapauksetkin ovat olleen lähinnä käyttäjien omia virheitä, esimerkiksi käyttöoikeuksien jakamisen kanssa.

Yrityksen tiloihin johtaa kaksi kulkuovea, jotka ovat lukittuina silloin, kun paikalla ei ole ketään. Tilan ikkunat sijaitsevat niin korkealla, ettei näistä tarkastelu sisään ole kovinkaan realistinen uhka. Yrityksen toimitila sijaitsee rakennuksessa, jossa toimii muitakin yrityksiä, joten kiinteistössä liikkuu päiväsaikaan ulkopuolisia henkilöitä. Kiinteistön ulkoovet ovat yöaikaan lukittuja. Kiinteistöä kokonaisuutena suojaa myös kiinteistön omistajan ottama vartiointi- ja hälytyspalvelu. Miettiessä muutoksia kiinteistöön, koskien tietoturvaa, yrityksellä on melko tiukat rajat, mitä muutoksia he voivat itse tehdä. Esimerkiksi toimitilan ovea tai lukitusjärjestelmää yritys ei pysty itse lähteä vaihtamaan parempaan.

7 EHDOTETUT PARANNUKSET YRITYKSEN TIETOTURVAAN

Edellä esitettyjenhavaintojen pohjalta voidaan esittää joukko parannuksia organisaation tietoturvan tasoon. Tällaisia parannuksia ja ratkaisuja mietittäessä tulee ottaa huomioon yrityksen koko sekä luonne. Esimerkiksi kuten aikaisemmin luvussa 6.1 todettiin, henkilöstörekisterin salaamiseen firman sisällä resurssien runsas kuluttaminen ei ole perusteltua yrityksessä, jossa kaikki osalliset ovat jo entuudestaan tuttuja. Toisaalta yrityksen tulee lainsäädännön perusteella ottaa tiettyjä askeleita suojatakseen henkilöstötietonsa ulkopuolisilta tahoilta.

7.1 Parannukset hallintoon tietoturvan kannalta

Hallinnon tulisi laatia yritykselle kirjallinen tietoturvapolitiikka, joka olisi henkilöstön, ulkopuolisten henkilöstöjen sekä mahdollisesti myös asiakkaiden saatavilla luettavaksi. Hallinnon tulisi myös valvoa, että henkilöstön jäsenet ovat oikeasti lukeneet tämän politiikan. Hallinnon suositellaan myös itse kouluttautuvan sekä hoitavan henkilöstölle kurssituksen koskien alaan liittyviä tietoturvaa koskettavia lakeja ja standardeja. Näin varmistettaisiin, että henkilöstö on myös ymmärtänyt lukemansa tietoturvapolitiikan. Mahdollisen tietovuodon tapahtuessa ja vastuullista etsittäessä yrityksen on huomattavasti helpompi puolustaa asiassa omaa kantaansa, voidessaan esittää sen henkilöstön olleen koulutettua ja toimineen ajantasaisten normien mukaan. Erillisen tietoturvapolitiikan ja koulutuksen omaaminen, sen lisäksi, että se vahvistaa yrityksen omaa osaamista, voi myös toimia valttina asiakkaan harkitessa toimiston palkkaamista. Asiakkaalle sen näyttäminen, että organisaatio ottaa tietoturvan vakavasti, luo jo heti suhteen alussa hyvän vaikutuksen yrityksen toiminnasta.

Hallinnon tulisi myös harkita taktiikkaa sille, kuinka uutta henkilöstöä otetaan töihin ja vanhaa henkilöstöä poistuu organisaatiosta. Näin pyritään varmistamaan, että henkilön saapuessa työskentelemään, hän ymmärtää heti tietoturvan tärkeimmät periaatteet sekä vastaavasti henkilön poistuessa voidaan varmistua, ettei hän poistumisellaan aiheuta tietoturvariskiä.

Hallinnon tulisi laatia pohja salassapitosopimukselle ja myös vaatia tämän sopimuksen solmimista ulkopuolisten kanssa sekä henkilöstön kanssa. Vaikka henkilöstössä kaikki luottaisivatkin toisiinsa, mahdollisen ongelmatilanteen sattuessa sopimusten olemassaolo voi helpottaa yrityksen asemaa laillisten seurausten edessä. Hallinnon tulisi myös tarjota uusille asiakkaille mahdollisuutta tällaisen sopimuksen solmimiseen. Vaikka asiakas ei lopulta kokisikaan sopimusta tarpeelliseksi, sopimusmahdollisuuden esittäminen luo kuvan asiakkaalle, että hänen tietonsa ovat yrityksessä hyvissä käsissä.

Hallinnon tulisi nimetä yrityksen keskuudesta erillinen tietoturvavastaava. Tämän henkilön vastuulla olisi esimerkiksi huolehtia ohjelmistojen lisensseistä ja päivityksistä sekä tietoturvan noudattamisen valvonnasta. Kun tietoturvaa hoitamaan on nimetty tietty henkilö, vältytään tilanteilta, joissa ongelman syntyessä ei tiedetä, kuka on vastuussa tai kuinka tulisi toimia. On tärkeää, että henkilöstön jäsen tietää, kenen puoleen kääntyä epäillessään ongelmaa. Näin myös saadaan koko organisaation tietoturva yhtenäiselle tasolle ja vältetään yksittäisten henkilöiden väärin toimiminen.

7.2 Parannukset henkilöstöön tietoturvan kannalta

Henkilöstön tulisi kouluttautua tietoturvan suhteen, kuten kappaleessa 7.1 mainittiin. Kuitenkin kouluttautuminen on vasta ensimmäinen askel. Tämän jälkeen henkilöstön tulisi vielä työskennellä niin, että myös oikeasti toteuttavat oppimiaan periaatteita. Henkilöstön tulisi pyrkiä esimerkiksi pitämään muihin toimiinsa liittyvä materiaali poissa esiltä sekä pidättäytyä puhumasta muista asiakkaistaan silloin, kun yrityksen tiloissa oleskelee ulkopuolisia tai itse ovat liikkeellä toimitilan ulkopuolella. Henkilöstön tulee myös noudattaa yleistä huolellisuutta ja varovaisuutta aina käsitellessään yrityksen dataa. Henkilöstön tulisi myös itse perehtyä esimerkiksi omiin ohjelmistoihinsa ja työvälineisiinsä niin, että ovat tietoisia näissä mahdollisesti esiintyvistä tietoturvaongelmista ja osaavat suhteuttaa näiden ohjelmistojen käytön niihin liittyvään riskiin. Ottaessaan käyttöön uusia työkaluja, henkilöstön tulisi ennen käyttöönottoa pyrkiä perehtymään näihin tarkistaakseen, onko näissä työkaluissa tunnettuja tietoturvaongelmia. Käsitellessään tietoja ja materiaaleja työntekijän tulisi käsitellä aina kerrallaan vain niitä tietoja, joita tarvitsee kulloinkin ja aina käsittelyn loputtua, siirtää tiedot takaisin säilöön.

7.3 Parannukset teknisiin ratkaisuihin tietoturvan kannalta

Yrityksen tulisi pitää tietolaitteidensa käyttöjärjestelmät sekä kaikki käyttämänsä ohjelmistot aina ajan tasalla. Jokaiseen laitteeseen tulisi myös asentaa erillinen, maksullinen versio tietoturvaohjelmistosta. Tietoturvaohjelmistojen ilmaisversiot sisältävät useasti vain erittäin karsittuja ominaisuuksia, jotka eivät riitä suojaukseksi yritys tasolla. Tämä koskee myös älypuhelimia. Tietoturvaohjelmiston tulisi olla yhtenäinen kaikissa laitteissa, jotta ohjelmistoa olisi mahdollisimman helppo hallinnoida sekä että kaikki laitteet olisivat turvallisuudessa samalla tasolla.

Yrityksen tärkeät tiedot olisi hyvä varmuuskopioida fyysiselle medialle. Näitä varmuuskopioita sekä yrityksen muutakin fyysistä mediaa varten tulisi hankkia lukittava, palon kestävä laatikosto, jossa tärkeitä tietoja ja medioita säilytettäisiin. Tästä laatikostosta mediat otettaisiin ulos vain käyttöä varten ja myös palautettaisiin takaisin käytön loputtua. Yrityksellä tulisi olla myös standardisoitu silppuri, fyysisten medioiden hävittämiseen. Silppureiden turvallisuusstandardeja määrittelevät muun muassa saksalainen Deutsches Institut für Normung sekä yhdysvaltalainen National Security Agency (Din-66399 2018 ; NSA 2015.)

Uusia ohjelmistoja ja palveluita käyttöön otettaessa tulee ensin tutustua, onko kyseisissä palveluissa tunnettuja tietoturvauhkia. Tämän lisäksi jo käytössä olevien palveluiden tietoturvatilannetta tulisi seurata mediasta sekä yritysten omista viestintäkanavista. Ohjelmistot ja palvelut, jotka eivät enää ole yritykselle tarpeellisia, ei tulisi jättää lojumaan järjestelmiin, vaan poistaa käytön loputtua. Myöskin työssä käytetyt tiedostot ja tiedot tulisi säilyttää päätelaitteilla vain niin kauan, kuin niiden käyttö on ajankohtaista. Projektien loputtua tulisi ylimääräiseksi jäänyt data joko poistaa tai siirtää sille tarkoitettuun säilöön, riippuen tilanteesta.

Yrityksen verkkolaitteessa tulisi aktivoida sen sisältämät turvallisuusominaisuudet. Tämän lisäksi yrityksen kannattaa harkita tulevaisuudessa siirtymistä erikseen yrityskäyttöön tarkoitettuun verkkolaitteeseen, joka sisältää vahvemman suojauksen sisäisesti.

8 YHTEENVETO

Tämän tutkimuksen tavoite oli kartoittaa tutkimuksen kohteena olleen yrityksen tietoturvan nykyinen tila sekä ehdottaa sen pohjalta parannuksia. Lopputuloksena saatiin aikaan kartoitus kohdeyrityksen tietoturvan nykytilasta sekä määritelmä lainsäädännöistä, jotka yrityksen tulisi ottaa huomioon toiminnassaan. Tämän lisäksi laadittiin lista ehdotuksia, joilla yritys voisi kehittää tietoturvansa tasoa.

Tiedonhankintaan käytettiin sekä kirjallisia lähteitä, että haastatteluja. Nämä tiedonhankintamenetelmät sopivat tällaiseen tutkimukseen, sillä kyseessä oli nimenomaan yhden tietyn asiakkaan tilanteen tarkastelu. Haastattelussa saadun tiedon avulla osattiin kirjallisen tiedon haku kohdentaa tarkemmin ja näin säästettiin aikaa. Keskusteluissa oli erittäin arvokasta se, että keskusteluun saatiin osallistumaan yrityksen koko henkilöstö ja pystyttiin keräämään tietoa useasta eri näkökulmasta. Tämän lisäksi yleistä tietoa alan tietoturvan tilanteesta saatiin kohdeyrityksen henkilöstön lisäksi haastattelemalla ulkopuolista, samalla alalla toimivaa henkilöä. Hänen haastattelunsa antoi yleistä kuvaa siitä, miten media-alalla suhtaudutaan tietoturvaan. Tämä auttoi laittamaan case yrityksen tilanteen parempaan viitekehykseen. Henkilöstön haastattelut toteutettiin yrityksessä paikan päällä. Haastattelussa käytettiin valmista kyselykaavakkeiden sarjaa, jonka kysymykset käsittelivät pienyritysten tietoturvaa. Ulkopuolisen henkilön haastattelussa käytettiin omia kysymyksiä. Haastattelut olivat hyvin vapaamuotoisia ja saivat rönsyillä rauhassa keskusteluiksi aiheesta syvemminkin. Kirjallisten lähteiden haku kohdennettiin tarkemmin haastatteluissa ja keskusteluissa ilmi tulleiden seikkojen avulla.

Edellä mainitut tiedonhakumenetelmät olivat päteviä tähän kyseiseen tutkimukseen. Koska kyseessä oli case-tutkimus, tuli tiedonhaku keskittää vastaamaan juuri kohdeyrityksen tarpeita. Vaikka tässäkin tapauksessa tulee tutustua paljon yleiseen materiaaliin, voidaan case-tutkimuksessa rajata tiedonhaku paljon tarkemmalle skaalalle. Haastattelut olivat myös hyvä keino määrittää yrityksen nykyinen tilanne, sillä henkilöstöhän parhaiten tietää oman yrityksensä tilanteen. Haastatteluissa myös annettiin kysymysten rönsyillä vapaasti, sillä liian tiukkaan määritelty kysymys saattaa jättää paljastamatta jotain tietoa, joka haastateltavalla tulee mieleen kysymyksen avulla.

Tutkimus on validi, sillä se käsittelee tarkasti yhtä tiettyä tapausta ja esittää väittämiä niissä rajoissa, joita kyseinen case sallii. Esimerkiksi tutkimus ei esitä yritykselle sellaisia muutoksia kiinteistöön, jollaisia yritys ei vuokralaisena voi missään nimessä toteuttaa.

Ehdotuksissa on otettu huomioon myös yrityksen koko ja profiili, joka vaikuttavat siihen, kuinka suuri kohde kyseinen yritys olisi mahdollisille tahallisille tietoturvahyökkäyksille.

Kehittämisehdotuksena toimeksiantajalle esitetään lainsäädäntöön tutustumista, välineistön uusimista sekä henkilöstön kouluttamista.

Jatkokehityksenä ja tulevaisuuden opinnäytetöitä silmällä pitäen voitaisiin seuraavaksi suorittaa vastaava tutkimus, jossa otettaisiin saman tutkimuksen piiriin useampia saman alan yrityksiä sekä mahdollisesti myös heidän asiakkaitaan. Näin saataisiin muodostettua suurempi kuva siitä, mikä on tietoturvan taso media-alalla sekä kuinka paljon nämä yrityksen oikeasti kohtaavat konkreettisia hyökkäyksiä tai vuotoja. Asiakkaan näkökulman saaminen olisi myös arvokasta, koska tällöin saataisiin selville, mitä media-alan yrityksiltä toivottaisiin ja kuinka nämä voisivat nostaa arvoaan asiakkaiden silmissä.

LÄHTEET

Din-66399.com 2018. Security levels. Viitattu 21.11.2018. Saatavilla sähköisesti osoitteessa http://www.din-66399.com/index.php/en/securitylevels

Floss Manuals 2018. Tietoturvan perusteet. Viitattu: 14.3.2018. Saatavilla sähköisesti osoitteessa http://write.flossmanuals.net/tietoturvan-perusteet/johdanto/.

GDPR-info 2018. General data protection regulation. Viitattu 25.8.2018. Saatavilla sähköisesti osoitteessa https://gdpr-info.eu/

Henkilötietolaki 1999. Viitattu 24.8.2018. Saatavilla sähköisesti osoitteessa https://www.finlex.fi/fi/laki/ajantasa/1999/19990523#L10P47

Marskidata 2018. Mainostoimisto Fabrik halusi lisätä palveluidensa tietoturvaa. Viitattu 12.11.2018. Saatavilla sähköisesti https://www.marskidata.fi/ajankohtaista/mainostoimisto-fabrik-halusi-lisata-palveluidensa-tietoturvaa/

Minilex 2018. Työntekijän salassapitosopimus. Viitattu 17.10.2018. Saatavilla sähköisesti osoitteessa https://www.minilex.fi/a/ty%C3%B6ntekij%C3%A4n-salassapitosopimus

Minilex 2018. Salassapitosopimus liikesuhteissa. Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://www.minilex.fi/a/salassapitosopimus-liikesuhteissa

Minilex 2018. Mikä on oikeushenkilö? Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://www.minilex.fi/a/mik%C3%A4-on-oikeushenkil%C3%B6

NSA 2015. Media destruction guidance. Viitattu 21.11.2018. Saatavilla sähköisesti osoitteessa https://www.nsa.gov/resources/everyone/media-destruction/

Peda.net 2018. Kyberuhat ja niiden aiheuttajat. Viitattu 12.11.2018. Saatavilla sähköisesti osoittessa https://peda.net/jyu/it/do/kkv/4kjna

Privacy SOS 2018. What is " security theater"? Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://privacysos.org/security_theater/

PK-RH 2018. Tietoriskit. Viitattu 18.10.2018. Saatavilla sähköisesti osoitteessa http://virtual.vtt.fi/virtual/pkrh/riskilajit/tietoriskit/tietoriskit.html

Professio 2016. Miksi henkilöstön rooli on merkittävin tietoturvallisuustekijä? Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://www.professio.fi/blogi/henkiloston-rooli-merkittavin-tietoturvallisuustekija/

ransomware.fi 2018. Mitä on ransomware. Viitattu 14.3.2018 Saatavilla sähköisesti osoitteessa http://www.ransomware.fi/

Sanastokeskus TSK. TEPA-termipankki. Viitattu 14.3.2018. Saatavilla sähköisesti osoitteessa http://www.tsk.fi/tepa/fi/haku/tietoturva

Talouselämä 2018. Kumppanin tietoturvasähläily on sinunkin murheesi. Viitattu 19.10.2018. Saatavilla sähköisesti https://www.talouselama.fi/kumppaniblogit/f-secure-oyj/kumppanin-tietoturvasahlaily-on-sinunkin-murheesi/c91659cd-a6c5-377f-9bf9-d3da97f4699a

Talouselämä 2004. Ulkoistus on luottamusta. Viitattu 19.10.2018. Saatavilla sähköisesti osoitteessa https://www.talouselama.fi/uutiset/ulkoistus-on-luottamusta/a993d08b-ff04-321f-8ec5-e7e42dcb5807

TEK tekniikan akateemiset 2018. Liikesalaisuudet sekä salassapitosopimus. Viitattu 25.8.2018. Saatavilla sähköisesti osoitteessa https://www.tek.fi/fi/tyoelama/lakipalvelut/lakitieto/liike-ja-ammattisalaisuudet-seka-salassapitosopimus

Tilastokeskus 2018. Luonnollinen henkilö. Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://www.stat.fi/meta/kas/luonnollinen_he.html

Tietoturvakartoitus mainosalan yrityksessä: Opinnäytetyön haastattelu. Viitattu 12.11.2018. Liite 1.

Sopimustieto 2018. Salassapitosopimus (NDA), molemmin puolin velvoittava. Viitattu 8.11.2018. Saatavilla sähköisesti osoitteessa https://sopimustieto.fi/yrityksille/sopimus/BZVlkO-salassapitosopimus_nda_molemmin_puolin_velvoittava

Viestintävirasto 2017. Tietoturva käytännössä. Viitattu 12.11.2018. Saatavilla sähköisesti osoitteessa https://www.viestintavirasto.fi/fiverkkotunnus/tietoavalittajalle/valitystoiminnantietoturva/tietoturvakaytannossa.html

Tietoturvakartoitus mainosalan yrityksessä: Opinnäytetyön haastattelu

Haastateltava:Freelance graafinen suunnittelija.

1. Kuvailisitko lyhyesti toimenkuvasi?
   - Digi- ja painograafikko

2. Oletko työssäsi itse vaatinut, taikka laatinut NDA'ta?
   - Minua on joskus vaadittu kirjoittamaan NDA sopimuksia, mutta itse en ole niitä toistaiseksi laatinut tai kirjoittanut. Kuitenkin edellytän itseltäni tarkaavaisuutta tallentaessani asiakkaitteni tietoja.

3. Oletko työssäsi allekirjoittanut NDA'ta toisen osapuolen vaatimuksesta?
   - Kyllä. Tiukin NDA sopimus, jonka olen allekirjoittanut kielsi minua jopa laittamasta mitään esimerkki näytteitä tai tietoja portfoliooni.

4. Oletko työssäsi käsitellyt tietoja, jotka ovat osapuolen vaatimuksesta luottamuksellisia?
   -Kyllä. mm. työskennellessäni mainostoimistojen kanssa.

5. Oletko työssäsi käsitellyt tietoja, jotka ovat lain vaatimuksesta luottamuksellisia?
   -Kyllä, asiakkaiden yhteystietoja ja sopimuksia

6. Miten työpaikallasi, taikka organisaatiossasi on huolehdittu työntekijöiden perehdyttämisestä tietoturvaan?
   -Yleisesti ottaen niistä ei yleensä puhuta kovin paljon vaan oletetaan ihmisten ymmärtävän itse niin hyvässä kuin huonossa.

7. Miten työpaikallasi, taikka organisaatiossasi on valvottu tietoturvan noudattamista? -Ei varsinaisesti mitenkään. Asia tulee ilmi vain jos jotakin pahaa tapahtuu, jolloin asia on jo myöhäistä korjata.

8. Oletko tutustunut alasi tietoturvavaatimuksiin, -käytäntöihin, sekä lainsäädäntöön omasta aloitteestasi?

-Kyllä, koska mielestäni ne ovat asioita mitä olisi hyvä ymmärtää mahdollisimman hyvin aivan kuten esim. elvytyksen alkeet.

9. Käsiteltiinkö tietoturvallisuuteen liittyviä seikkoja kouluttautuessasi ammattiisi? MIllä tavoin?
   -Ei, Koulutukseeni ei kuulunut niitä vaikka olisi hyvä ollut. Opiskellessani esitin oppilaitokselle tällaisia ja muita byrokraattisia ja lainopillisia asioita käsittelevän kurssin lanseeraamista koulussani.

10. Oletko itse, taikka organisaatiosi tietoinen luottamuksellisten tietojen säilytysaikoja, sekä hävittämistä koskevasta lainsäädännöstä, sekä alasi omista standardeista(esimerkiksi vaatimuksia siitä, millaisella paperisilppurilla mitäkin tietoa sisältävä paperi tulee silppua)?
    -Koulutuksessani niin koulussa tai töissä sitä ei ole huomioitu. Välillä jotkin tärkeämmät paperit piti laittaa lukolliseen roskikseen (joka oli muidenkin yritysten käytössä), mutta niitä ei kuitenkaan silputtu millään tavalla. Pyrin itse aina pysymään lainsäädännöissä perillä niin paljon kuin mahdollista.

11. Koetko, että yleisesti alallasi toimivat henkilöt ottavat tietoturvallisuuden vakavasti? Millaisia asenteita olet kohdannut?
    -Asenteet ovat olleet suurimmaksi osaksi väliinpitämättömiä tai vähätteleviä. Joskus kuitenkin asiat on otettu hieman vakavammin, mutta tämä on toistaiseksi ikävä kyllä valitettavan harvinaista. Myös tieto turvallisuudesta on todella alkeellista.

12. Oletko tietoinen omalla alallasi mahdollisesti tapahtuneista tietoturva hyökkäyksistä, vuodoista tms?
    -Uutisointia ei aina tapahdu julkisesti vaan ihmisten kautta, mutta olen kuullut useasta tapahtumasta. Pahin mitä olen kuullut ovat olleet pilvipalvelimien tiedostojen tarkoittamaton näyttäminen väärille ihmisille niin että syyllisiä eivät ole olleet käyttäjät vaan esim. Adoben pilvipalvelin ja Google drive.

13. Mitä muuttaisit itse toiminnassasi, organisaatiossasi, taikka alallasi yleisesti, liittyen tietoturvallisuuteen?
    -Tietoturva tietoutta pitäisi aloittaa opettamaan ja valistamaan jo kouluissa ja erityisesti viimeistään työpaikoilla. Asia pitäisi myös alkaa ottamaan vakavasti ja

tarkistamaan jokaisen tiedot asiasta, koska aiheesta on paljon mututuntuma tietoa myös liikkeellä.

14. Koetko, että oma ymmäryksesi alasi tietoturvavaatimuksista, taikka tietoturvavsta yleensäkin on riittävä?
    -Koen että tietoni ovat keskiverto ihmistä parempia työni puolesta, mutta toisinaan tuntuu että oman alanikin sisällä tietotaito on matalaa.

15. Koetko, että alallasi toimivien henkilöiden ymmärrys tietoturvasta on riittävä? -Ei lähelläkään

16. Oletko itse, taikka osana organisaatiota ollut osallisena tietoturvallisuuteen liittyvässä koulutuksessa?
    -En

17. Koetko alallasi tällaisen koulutuksen tarpeelliseksi?
    -Ehdottomasti kyllä

18. Koetko, että alallasi ollaan turvallisuudessa ajan hermolla, vai reagoidaanko asioihin vasta, kun lehdistö raportoi jostain tapahtumasta?
    -Vasta kun asiat menevät vikaan

19. Oletko sinä, taikka organisaatiosi käyttäneet vakuutusyhtiöiden kybervakuutuksia? -Ei, enkä usko että suurinosa ihmisistä edes tietää moisen olemassaoloa.

20. Mikäli olet työskennellyt muissakin, kuin media/mainosalan yrityksissä, oletko huomannut tietoturvallisuudessa, taikka asenteissa tietoturvaan eroja media/mainosalan, sekä näiden muiden alojen yritysten välillä?
    -Eroja ei oikeastaan ole juurikaan. Kaikkialla asenteet tuntuvat olevan samanlaiset.

21. Oletko itse tietoinen voimaantulleesta EU’n GDRP-säädöksestä ja sen määräämistä velvoitteista, sekä rangaistuksista?
    -Kyllä, mutta kuulin kylläkin tiedon muualta kuin mediasta tai työpaikoilta.

22. Koetko, että voimaan tulleella EU’n uudella GDPR-säädöksellä, sekä sen määräämillä suurilla sakkorangaistuksilla on ollut vaikutusta siihen, miten alallasi on muutettu suhtautumista tietoturvaan?
    - Vaikea sanoa vielä tässä kohtaa. Pahoin kylläkin luulen että vaikutus ei ole vielä tarpeeksi.
23. Muita huomioita asiasta?
    - Uusi lainsäädäntö on hyvä alku, mutta koen että suurin hyöty asenteiden ja tietojen jakamisessa auttaisi kunnon koulutukset asiaa koskien niin kouluissa kuin työpaikoilla. Lisäksi turvallisuutta miettiessä aina unohdetaan riskit, joita voivat tulla esim. alihankinta yritysten ja asiakkaiden kautta. Esimerkiksi asiakas voi toimittaa korruptoituneita tiedostoja joista ei ole tietoinen tai yksityisiä tietoja joita he eivät saisi luovuttaa. Hyvin usein asiakkaat eivät ole myöskään tietoisia mistä heidän toimittamansa tiedot ovat alunperin peräisin tai missä kaikkialla mahdolliset salasanat kulkevat. Erittäin yleistä alalla on se, että yritys voi ostaa graafikon palveluita useilta eri tahoilta ja näin heidän tiedot ja tiedostot voivat olla usealla taholla. Salasanat tulisivat olla aina asiakkaan vastuulla vaihtaa uusiin projektin päätyttyä ja tallentaa ne, mutta usein he hukkaavat ne, jolloin graafikot kokevat paremmaksi säilyttää niitä itsellään tulevaisuuden projekteja varten.

¶ Osan vaihto (seuraava sivu)