Turun yliopisto
University of Turku

# TIIVISTELMÄ

| | |
|---|---|
| X | Pro gradu -tutkielma |
| | Lisensiaatintutkielma |
| | Väitöskirja |

| | | | |
|---|---|---|---|
| Oppiaine | Tietojärjestelmätiede | Päivämäärä | 31.5.2018 |
| Tekijä(t) | LuK Joona Lehikoinen | Matrikkelinumero | 77414 |
| | | Sivumäärä | 53 + liitteet |
| Otsikko | Seuraavan sukupolven tietoturvauhat pk-yrityksille | | |
| Ohjaaja(t) | FT Jani Koskinen,<br>FL Antti Tuomisto | | |


Tiivistelmä

Tietohierarkian teorian mukaan ennen kuin voi olla viisautta, tulee olla dataa, dataa joka koostuu numeroista – numeroista, joille me annamme merkityksen ja tarkoituksen; tehden niistä näin ollen opetettavaa tietoa muille, joka on vielä jalostettavissa viisaudeksi. Suomessa pienten ja keskisuurten yritysten toimintaprosessit ovat murroksessa. Myös halu kasvaa ja kansainvälistyä on varmasti monen pk-yrityksen tähtäimessä. Erilaiset pilvipalvelut ja muuttuneet hankintamallit mahdollistavat pienemmällekin yrittäjälle suurempien yritysten työkalu- ja toimintamallit. Myös julkishallinto on alkanut huomata pilvipalveluiden kiistattomat hintaedut. Entisestään mobilisoituvat työtavat voidaan nähdä muutokselle ominaisena tekijänä. Tutkimusten perusteella vaikuttaa siltä, että nämä ovat muuttaneet yritysten tietoturvan tarvetta ja laatua merkittävästi. Vanhoja uhkia ei voi yksinkertaisesti sivuuttaa ja uusia ilmestyy lisää tasaiseen tahtiin. Tietoturva on entistä enemmän sekä poliittinen että liiketoiminnallinen uhka ja samanaikaisesti mahdollisuus.

Tutkimusmenetelmänä käytettiin puolistrukturoitua teemahaastattelua ja haastattelukohteina toimi kuusi suomalaista pk-yritystä. Toisilla niistä oli enemmän teknistä taustaa kuin toisilla. Yritykset olivat entuudestaan tuntemattomia ja haastattelut suoritettiin salassapitovelvollisuuden alaisina. Tutkimustulokset ovat myös anonymisoituja eikä haastateltuja yrityksiä voi tunnistaa niistä.

Loppupäätelmänä voidaan todeta, että pk-yrityksillä on tarve huomioida tietoturva kriittisenä osana liiketoimintaansa. Uusi tietosuojalaki aiheuttaa toimia myös pienimmille yrityksille. Tutkimukseni mukaan yrityksen koolla on merkitystä sen käsitykseen omasta tietoturvastaan. Yrityksen tietoturvakäsitykselle on tunnistettavissa myös erilaisia tasoja ja vaiheita. Näitä on käsitelty osana pro gradu -työtä.



| | |
|---|---|
| Asiasanat | tietoturva, tietosuoja, pk-yritys, APT, pilvipalvelu |
| Muita tietoja | |

Turun yliopisto
University of Turku

# SEURAAVAN SUKUPOLVEN TIETOTURVAUHAT PK-YRITYKSILLE

## Kohdennetut hyökkäykset, pilvipalvelujen kasvava rooli ja muuttuva tietosuoja

Master's Thesis
in Information Systems Science
Tietojärjestelmätieteen
pro gradu -tutkielma

Author(s)/Laatija(t):
B.Sc. Joona Lehikoinen

Supervisor(s)/Ohjaaja(t):
Ph.D. Jani Koskinen
Ph.Lic. Antti Tuomisto

31.5.2018
Turku

## Sisällysluettelo

## Lista kaavioista

# 1 JOHDANTO: TIETOTURVA YLEISESTI

Tietohierarkian teorian mukaan ennen kuin voi olla viisautta, tulee olla dataa, dataa joka koostuu numeroista – numeroista, joille me annamme merkityksen ja tarkoituksen; tehden niistä näin ollen opetettavaa tietoa muille, joka on vielä jalostettavissa viisaudeksi (Rowley 2007). Suomessa pienten ja keskisuurten yritysten (pk-yritysten) toimintaprosessit ovat murroksessa. Myös halu kasvaa ja kansainvälistyä on varmasti monen pk-yrityksen tähtäimessä. Erilaiset pilvipalvelut ja muuttuneet hankintamallit mahdollistavat pienemmällekin yrittäjälle suurempien yritysten työkalu- ja toimintamallit. Myös julkishallinto on alkanut huomata pilvipalveluiden kiistattomat hintaedut. Entisestään mobilisoituvat työtavat voidaan myös nähdä muutokselle ominaisena tekijänä. Tutkimusten perusteella vaikuttaa siltä, että nämä ovat muuttaneet yritysten tietoturvan tarvetta ja laatua merkittävästi. Vanhoja uhkia ei voi yksinkertaisesti sivuuttaa ja uusia ilmestyy jatkuvasti lisää. Tietoturva on entistä enemmän sekä poliittinen että liiketoiminnallinen uhka ja samanaikaisesti mahdollisuus.

Aiemmin selkeästi toisistaan erottuneet tietoturvauhat ovat nyt vahvemmassa symbioosissa keskenään. Hyökkäykset ovat moninkertaistuneet ja samalla myös monimutkaistuneet huomattavasti. Niiden havaitseminen on myös vaikeutunut. Käyttäjien lisääntynyt ja muuttunut tietosuoja sekä alati laajeneva sosiaalisen median verkosto luovat ennennäkemättömiä tilanteita sekä yritysten johdolle että työntekijöille. Automatisoitu tietoturva voidaan ylätasolla katsoa jakaantuvan kahteen eri pääkategoriaan: ihmisläheisempään ja täysin konepohjaiseen. Esimerkki ihmisläheisemmästä automatisoidusta tietoturvasta olisi työkseen yrityksen tietoturvaa tutkiva ja tarkastava henkilö, joka yrittää etsiä poikkeamia automaattisesti (koneellisesti) kerätystä datasta ja jalostaa siitä tietoa. Automatisoitua tietoturvaa eli toimintoja, jotka ovat itsevalvovia sekä itsekorjaavia ja tulevaisuudessa tulevat tukeutumaan varmasti myös tekoälyyn nykyisen adaptiivisen logiikan lisäksi. Yleensä tähän automatiikkaan liittyy myös eri tason suojauksia ja nimenomaan suojausmekanismeja. Tätä aihetta ei kuitenkaan käsitellä tässä työssä tämän laajemmin vaan keskitytään perinteisempään tietoturvaan ja sen ilmiöihin.

Viime vuosina on alettu puhua paljon siitä, kuinka tietoturvaan liittyvät hyökkäykset tulisivat olemaan syy seuraavaan suureen maailmanlaajuiseen konfliktiin. On puhuttu myös mahdollisuudesta maailman sodan syttymiseen paikallisten konfliktien lisäksi ja kaikkeen siltä väliltä. Muun muassa Yhdysvallat, Etelä-Korea, Venäjä sekä Kiina ovat kaikki toistuvasti liitetty erilaisiin hyökkäyksiin eri puolilla maailmaa. Valtioiden välisiin sekä yksityisiin yrityksiin kohdistuviin hyökkäyksiin. Vaikuttaakin siltä, että osaksi tiedustelua on muodostunut murtautuminen vieraan vallan tietojärjestelmiin ja niiden ”vakoilu”, tai vähintään vahtiminen, tapahtuu sisältäpäin.

Kybersodankäynti on uusi ulottuvuus maa-, ilma-, meri- ja avaruusvoimien rinnalle eli täysin uusi rintama sodankäynnille. Kybersodankäynti määritellään hyökkäysmuodoksi, jossa asetetut tavoitteet saavutetaan ilman fyysisen konfliktin tarvetta. Kohdennetut hyökkäykset ovat arkipäivää kybersodankäynnissä ja ne lisääntyvät koko ajan. Tämän ansiosta siviilien erottaminen sotilaista on entistä vaikeampaa. Jo pienellä ihmismäärällä voidaan saada todella suuri vaikutus, hyökkäysvoima on täten asymmetrinen hyökkäyksiin nähden. Vaikka kyseessä ei olekaan perinteinen sotilaallinen voima ja konkreettiset ihmiset ei se silti vähennä hyökkäyksen symboliikkaa ja merkitystä. (Eom, Kim, Kim & Chung 2012.)

Rid (2012) esittää mielenkiintoisen näkemyksen siitä, kuinka kybersotaa ei ole koskaan ollut eikä tule koskaan myöskään olemaan. Hänen mukaansa nykyiset ”taistelut” sekä tulevaisuudessa ilmenevät uudet taktiikat perustuvat kaikki kolmeen vanhaan ja perinteiseen sodankäynnin piirteeseen: käännytykseen, salaliittoihin sekä sabotointiin. Tunnettu sodan määritelmä Clausewitzin (Rid 2012.) mukaan jakautuu kolmeen osaan:

1. Sodan väkivaltainen puoli
2. Sodan välineellinen puoli
3. Sodan poliittinen puoli

Sodan väkivaltaisella puolella tarkoitetaan sitä, että sodanjulistuksen on oltava väkivaltainen pakotus, jolloin toinen osapuoli alistetaan haluttuun tahtotilaan vastustuksesta huolimatta. Välineellisellä puolella taas tarkoitetaan fyysistä väkivaltaa tai sellaisen uhan esittämistä voimannäyttönä, jota ilman ei ole mahdollista pakottaa toista osapuolta täysin puolustuskyvyttömään tilaan. Kolmas ja viimeinen kohta eli sodan poliittinen puoli muistuttaa siitä, kuinka sodankäynti on aina poliittista ja sillä on suurempi tarkoitus. Ilman näiden kolmen tekijän täyttymistä ei klassisestikaan voida puhua sodasta. Kaikki kybersodankäyntiin liittyvät asiat, joita toistaiseksi on nähty tai tullaan näkemään, eivät täytä sille asetettuja ehtoja. Voidaankin todeta termin ”kybersodankäynti” olevan epävalidi ja laajalti väärin käytetty.

WikiLeaks-palvelusta julkisuuteen noussut käsite ”haktivisti” on tullut jäädäkseen. Haktivisti-termillä tarkoitetaan henkilöä, joka osallistuu lähtökohtaisesti pahantekoon hakkeroinnin muodossa ja jonkin liikkeen tai aatteen puolesta. Sen osalta voidaan puhua myös eräänlaisesta ”piraattikulttuurista”. WikiLeaksin tapauksessa se tarkoitti esiin tulleen informaation muokkausta, levitystä ja sitä kautta hyväksikäyttöä. Voidaan myös puhua tietynasteisesta fanaattisuudesta ja omistautumisesta yhteisen hyvän eteen. Vaikutuksen päämääränä on maailmanlaajuinen näkyvyys. (Lindgren & Lundström 2015.)

Internet on luonut aivan uudenlaisen pohjan protestoinnille. Jo pienellä vaivalla on mahdollista saada erittäin suuri ja laaja näkyvyys ajamalleen asialle. Voisi puhua

puskaradion ja hakkeroinnin yhdistämisestä yhdeksi kokonaisuudeksi tietyn päämäärän saavuttamiseksi. Se toimii yleisesti hyväksyttynä määritelmänä tällä hetkellä haktivismille. Voisi todeta kyseessä olevan siis sosiaalinen ja yhtä lailla kulttuurinen ilmiö. (Jordan & Taylor 2004.) Yleisiä hyökkäysmuotoja ovat palvelunestohyökkäykset (DoS/DDoS), verkkosivustojen töhriminen, verkkosivujen parodiointi, tiedon varastaminen ja verkkosivustojen uudelleenohjaus. Jos vertaillaan haktivismia perinteisempään protestointiin, on niissä helppo huomata yhtäläisyyksiä. Hyökkäykset toimivat yleensä vastineina erilaisille poliittisille tai sosiaalisille tapahtumille. Ajoitus sijoitetaan mahdollisimman suuren näkyvyyden takaamiseksi ja julkisuus onkin yksi yleisimpiä tavoitteita. Poikkeuksellisesti näihin hyökkäyksiin on yleensä mahdollista osallistua myös teknisesti osaamattomien henkilöiden heitä varten luotujen erityistyökalujen avulla. Haktivismin ympärille on muodostunut myös sille omistautuneita yhteisöjä, joista mahdollisesti tunnetuin (ja eniten uutisoitu) on ryhmä nimeltä ”Anonymous”. He luottavat yhteisön voimaan tehdä vaikutusta yhteiskuntaan, vaikka ryhmän toimivuudesta vastaisikin vain muutama avainhenkilö, jotka eivät välttämättä tunne edes toisiaan. Osa näistä ryhmistä puhuu itsestään enemmän ideologiana kuin ryhmänä. Näille yhteisöille on tyypillistä toimia anonyyminä, turvaten sillä oikeudellista selustaansa. Tämän tyyppisiin hyökkäyksiin liittyy kuitenkin yleensä rikollista toimintaa. (Xiang 2013.) Tämä työ ei tule syventymään tämän enempää aiemmissa kappaleissa kuvattuun poliittiseen tietoturvaan.

Tässä tutkimuksessa haastateltiin useita pk-yritysten johtohenkilöitä ja kysyttiin heidän käsityksiään yleisesti tietoturvan tilanteesta. Heiltä pyydettiin myös näkemystä heidän oman yrityksensä tietoturvan tasosta sekä arvioita mahdollisista tulevaisuuden uhista. Haastattelujen lopputuloksena huomattiin yrittäjien arvioivan oman yrityksensä tietoturvatason selkeästi paremmaksi kuin mitä se todellisuudessa vaikutti olevan. Toisaalta sen parantamiseen oltiin myös valmiita. Ei ole erityisten poikkeuksellista, että myös yritysten johto tahtoo päästä helpolla ja siksi suositaankin yksinkertaisia ja kattavia ratkaisuja, vaikka niiden kustannukset olisivatkin hieman korkeammat. Tietoturvaa ei nähdä yhtenä ehtona yrityksen vakaalle kasvulle, vaikka se ehdottomasti sitä on.

Tutkimuskysymys työssä on seuraava:

**Kysymys 1: Miten monipuolistuneet verkkohyökkäykset vaikuttavat pk-yritysten tietoturvatarpeisiin?**

**Kysymys 1.1: Onko pk-yritysten tietoturvalle tunnistettavissa erilaisia vaiheita ja tasoja näiden avulla?**

Tutkielma koostuu kuudesta eri pääluvusta ja niiden aliluvuista. Luvussa 2 esitellään kirjallisuuteen perustuen sekä pk-yrityksen määritelmää että niiden tietoturvan nykytilannetta. Luvussa sivutaan myös hieman tietoturvastrategiaa ja tietosuojan

kasvavaa merkitystä. Luvussa 3 mietitään kirjallisuuden kautta pääasiassa kohdennettuja pitkäkestoisia hyökkäyksiä (APT), pilvipalveluita sekä lyhyesti katsastetaan toimialan tai yrityksen koon vaikutusta sen tietoturvaan. Nykytutkimukset antavat myös näyttöä sille, että tietämyksen lisääminen tietoturvasta on edelleen hyödyllistä. Tietoturvasta kouluttaminen on tarpeellista. Myös seuraavan sukupolven tietoturvauhista on löydettävissä yhtenäisiä piirteitä, joita vastaan voi suojautua, kunhan ne tiedostetaan ja ymmärretään. Luvussa 4 esitellään tutkimuksessa käytetty tutkimusmenetelmä sekä itse tutkimuksen suorittaminen. Tässä tutkimuksessa on keskitytty nimenomaan pk-yrityksiin eikä vastaavia tutkimuksia ole juuri tehty. Tutkimuksessa on yhdistetty useamman tietoturvan osa-alueen pääkohtia uudella tavalla ja pystytty näin johtamaan uusia kattavampia tuloksia. Haastateltujen kohdeyritysten toimialat ovat toisistaan poikkeavat ja näin tuloksiin saadaan paljon tarvittavaa moniulotteisuutta. Luku 5 sisältää suoritetun tutkimuksen empirian tulosten läpikäynnin. Luvussa 6 on tutkielman loppupäätelmät ennen lähteitä ja liitteitä. Tutkimuksen lopputulos tukee ajatusta pk-yrityksen tarpeesta yhdelle kattavalle tietoturvaratkaisulle. Tämän tietoturvaratkaisun tulisi olla mahdollisimman kevyt, moniulotteinen ja automatisoitu. Ymmärrys omasta haavoittuvaisuudesta hyökkääjille aliarvioidaan eikä varsinaisia riskikohtia omassa yrityksessä edes täysin ymmärretä, tai niitä ei tahdota hyväksyä sellaisenaan. Uhat nähdään olevan ulkomaailmassa, mutta ei omassa yrityksessä. Juuri tämä, hieman jopa piittaamaton ajattelutapa, tekee tästä tutkimuksesta ajankohtaisen ja relevantin. Jatkotutkimuksia varten olisi hyödyllistä tutkia kustannuksia, joissa tulevaisuuden tuotteet voisivat tehokkaimmin toimia juuri pk-yrityksille. Mielestäni olisi myös hyödyllistä selvittää konkreettisia määriä panostuksesta tietoturvakoulutukseen yrityksissä ennen ja jälkeen hyökkäystä (eli sen huomaamista).

# 2 PK-YRITYSTEN TIETOTURVAN TILANNE

## 2.1 Pk-yritykset ja (niiden) mobiilityön yleistyminen

Yleisesti kun puhutaan pk-yrityksistä, eli pienistä ja keskisuurista yrityksistä, tarkoitetaan sillä melko laajaa joukkoa yrityksiä. Euroopan komission julkaiseman raportin (2017) mukaan se sisältää yritykset joiden työntekijämäärä on alle 250 henkilöä (vuosityöyksikköä). Toinen vaihtoehto määritellä pk-yritys on liikevaihto. Pk-yrityksen vuotuinen liikevaihto tulisi olla alle 50 M€ tai tilikauden taseen loppusumman alle 43 M€. Lisäksi usein puhutaan yrityksen riippumattomuudesta. Pk-yrityksen on oltava riippumaton muista yrityksistä eli sen liiketoiminta ei voi tukeutua esimerkiksi toisen yrityksen alaisuuteen. Pk-yritykset voidaan jakaa myös tarkemmin alalajeihin: keskisuuri yritys (henkilöstö < 250, vuotuinen liikevaihto ≤ 50 M€ tai tilikauden taseen loppusumma ≤ 43 M€), pieni yritys (henkilöstö < 50, vuotuinen liikevaihto ≤ 10 M€ tai tilikauden taseen loppusumma ≤ 10 M€) sekä mikroyritys (henkilöstö < 10, vuotuinen liikevaihto ≤ 2 M€ tai tilikauden taseen loppusumma ≤ 2 M€). (Euroopan komissio 2017.)

Erääseen tutkimukseen osallistuneista 400 pk-yrityksestä 60 % arvioi käynnistävänsä työn mobiiliuteen liittyvän projektin (Arbab, Korelin & Tuomisto, 2012). Tarkemmin tarkasteltuna näistä yrityksistä 66 % arvioi toteutuksen olevan helppo tai erittäin helppo. Yleisesti suhtautuminen mobiiliteknologiaan on enimmäkseen positiivinen ja useimpien yritysten tärkeimmät järjestelmät sisältävätkin mobiileja toimintoja jo nyt. Tämän voidaan katsoa kattavan myös liiketoiminnalle kriittisen datan käsittelyä mobiilisti. (Arbab, Korelin & Tuomisto 2012).

Mobiilityö määritellään työnä, jossa pääasiassa hyödynnetään mobiiliteknologioita työtehtävien suorituksessa ja niiden suunnittelussa, eli rajoittavana tekijänä työskentelylle ei enää toimi perinteinen ja paikkasidonnainen työpiste. Yleisesti ottaen mobiilityö korostuu tietotyössä. Mobiilityötä voidaan harkita, jos työssä tietotyön määrä on riittävä ja työ on riippumatonta ajasta ja paikasta. Toisaalta mobiilityöhön ryhtyminen on nykyään yrityksille helppoa ja myös suhteellisen halpaa. Nämä syyt tekevät siitä myös houkuttelevan työkulttuurimallin monelle kasvuvaiheessa olevalle yritykselle. (Raguseo, Neirotti & Paolucci 2015.)

Mobiilityötä myös kritisoidaan. Sen sanotaan luovan jännitettä työntekijän ja yrityksen välille. Investoinnit mobiilityöhön voivat aiheuttaa paineita henkilöstön osaamiselle ja resursoinnille, yrityksen strategisen näkemyksen noudattamiseen ja yleiseen työilmapiiriin. Yrityksen olisi tärkeintä ymmärtää tähän työskentelytavan muutokseen tarvittava kulttuurimuutos. Apuna voidaan tarvita esimerkiksi koulutusta. Myös läpinäkyvyyden merkitys yrityksen sisällä unohtuu helposti. Yrityksen sisällä voidaan luottosuhteiden todeta eroavan normaalista vanhemmanmallisesta työskentelystä.

Luottamista vaaditaan enemmän työnantajan puolelta. (Raguseo, Neirotti & Paolucci 2015.)

## 2.2 Liiketoiminnalle kriittinen data

Yrityksen toiminnan keskeisin tieto (eli data) on sen liiketoiminnalle arvokkainta. Osalle yrityksistä tämän tiedon tunnistaminen on haastavaa eikä siihen siksi paneuduta riittävästi. Tästä syystä tämä tieto jää usein suojaamatta ja varmuuskopioimatta. Kriittisen tiedon tunnistus on osa yrityksen tietoturvan kehityskaarta. Ilman systemaattista tiedon tunnistamista ei tehokas tietojen suojelu ole mahdollista. Myös riskien kartoitus on välttämätöntä niiden ennaltaehkäisyn kannalta. Erään näkemyksen mukaan jopa 60 % tärkeästä datasta on huonosti, jos lainkaan, suojattuna. Tähän liittyy vahvasti tämän kriittisen datan tunnistus – se mitä ei tunnisteta, ei ole mahdollista erikseen suojata tarvittavalla tasolla. (Schwartzel & Mnkandla 2011.)

Kriittisen tiedon tunnistaminen on haastavaa. Miten tunnistaa kaikesta tiedon kohinasta tarpeellinen tieto? Duff (1996) määrittelee kriittisen tiedon seuraavasti: ”— Tämän (kriittisen) tiedon hävittäminen tai väärinkäyttö aiheuttaisi peruuttamattomia seurauksia yritykselle: menetettyä tuottoa, oikeustoimia, uskottavuusongelmia, sakkoja sekä jopa mahdollisia henkilövahinkoja ääritapauksissa.” Toisaalta liiketoimintakriittisen tiedon jakaminen on yrityksille hyödyllistä: se nostaa tehokkuutta ja yleisesti parantaa asiakaspalvelua sekä vähentää valmistuskustannuksia. (Soliman & Yousser 2003.)

Mikä taas sitten on määritelmä liiketoiminnalle kriittiselle dokumentille eli tiedon koherentille kokonaisuudelle jolla on liiketoiminnallista merkitystä yrityksen näkökulmasta. Yleisesti se määritellään seuraavanlaisena: sen sisältö on myytävissä asiakkaille rahasta, sen avulla voidaan luoda tuote tai palvelu; jota voidaan myydä asiakkaille rahasta tai sillä voidaan vastata ulkopuolisille tekijöille (esimerkiksi valtiollisiin säädöksiin ja määräyksiin, kilpailupaineisiin, asetettuihin standardeihin, jne.). Chaleff (1995) muistuttaa tekstissään kriittisen tiedon löytämisen vaikeudesta tiedon kohinasta. 200 sähköpostin joukosta on vaikeaa löytää kolme kriittistä sähköpostia, jotka vaativat toimia. Sellaisia sähköposteja, jotka eivät ole vain tarkoitettu lisätiedoksi. Mitchell (1997) muistuttaa siitä, kuinka yksinkertaista tärkeän tiedon löytäminen yrityksen sisällä voi olla. Hän antaa esimerkkinä tilanteen markkinoinnin ammattilaisista, jotka unohtavat, että eniten tietoa asiakkaista ja asiakkuuksista on talousosastolla. Siellä tiedetään mihin rahat menevät, mistä rahat tulevat ja missä määrin. (Soliman & Yousser 2003.)

## 2.3 Tietosuojan kasvanut merkitys (GDPR)

General Data Protection Regulation eli GDPR on EU:n uusi tietosuoja-asetus, joka astui voimaan kesäkuussa 2016. Siihen varattu siirtymäaika on lopuillaan (loppuu toukokuussa 2018), Se tarkoittaa mahdollisten sanktioiden astumista voimaan. Lyhykäisyydessään tämä tarkoittaa, että EU tahtoo tämän asetuksen myötä varmistaa kaiken sen kansalaisia koskettavan sensitiivisen datan käsittelyn vastuullisuuden korkean tason sekä geopoliittisesti pitämään kyseisen datan valtioliiton rajojen sisäpuolella. Tämän uuden asetuksen keskiössä ovat kuluttajat tai yksityishenkilöt. Yritykset asetetaan oikeudelliseen vastuuseen henkilötietojen oikeaoppisesta ja sitä kautta vastuullisesta käsittelystä. Myös yksittäiset ihmiset saavat lisätietoja siitä taustasta, miten suuryritykset toimivat henkilötietojen osalta, esimerkiksi siitä, mitä palveluja ne hyödyntävät osana liiketoimintaansa. (Wright 2016.)

Yritykselle voidaan asetuksen valossa asettaa sanktio, joka on maksimissaan kaksikymmentä miljoonaa euroa tai vaihtoehtoisesti neljä prosenttia kyseisen yrityksen kansainvälisestä liikevaihdosta (kumpi tahansa näistä on isompi). Sanktio on tarkoituksella merkityksellinen, koska toistaiseksi yritykset ovat päässeet helpolla mahdollisissa tietomurtotapauksissa. Tietomurtojen osalta astuu myös voimaan 72 tunnin sääntö, jonka sisällä tietosuojaloukkauksista tulee ilmoittaa viranomaisille. Yrityksellä on myös velvollisuus ilmoittaa tapahtuneesta asianosaisille ilman tarpeetonta viivyttelyä. Yritysten olisikin tärkeintä ymmärtää, ettei tämän asetuksen tarkoitus ole tehdä kertaluontoista korjausliikettä vaan muuttaa toimintatapoja ja pakottaa yritykset miettimään, miten tietosuoja heillä toteutuu. Tämä on myös tarpeellista kuvata prosessiksi yrityksen omiin toimintatapoihin. Tiedonkäsittelyn tahdotaankin muuttuvan proaktiiviseksi aiemmasta usein käytössä olleesta reaktiivisesta mallista. (Wright 2016.)

Tietosuojavastaava (Data Protection Officer eli DPO) ja sen rooli muuttuu myös tämän uuden asetuksen myötä. Kyseinen toimenkuva tulee olla erikseen nimettynä yritykselle, jonka ydintoiminnot (eli asiat jotka sisältyvät yrityksen liiketoimintasuunnitelmaan) sisältävät järjestelmällistä tai säännöllistä henkilötietojen käsittelyä suuressa määrin. On yrityksensä itsensä vastuulla kouluttaa kyseisen toimenkuvan työntekijä tehtävän vaatimalle tasolle eli valvomaan GDPR:n toteutusta ja yrityksen toiminnan lainvoimaisuutta sen vaatimin osa-aluein. (Voigt & von dem Bussche 2017.)

Yksilön tärkeimmät oikeudet ovatkin oikeus saada yritykseltä kaikki tieto, jota kyseisestä henkilöstä on olemassa, sekä oikeus tulla unohdetuksi, jolloin kaikki tiedot järjestelmistä kyseisestä yksilöstä, tulisi pyyhkiä pois (tarkoittaa myös palvelun/palvelujen käytön lopettamisen). Uusi laki erottelee selkeämmin myös tietojenkäsittelijän tietojenkerääjästä verrattuna perinteiseen rekisteriselosteeseen. Tämä tarkoittaa, että myös ohjelmistoyritykset, jotka esimerkiksi verkkosivustoissaan

käsittelevät tietosuojan alaista materiaalia, ovat vastuullisia tiettyyn pisteeseen asti. (Wright 2016.)

Asetuksella uskotaan olevan vaikutusta myös EU-alueen ulkopuolella, koska se on samalla koonti hyvistä käytännöistä. Se on pohja, johon on mahdollista rakentaa oman maan vaatimat erityispiirteet. Tämän oletuksen perusteella, EU on laskenut suuryrityksille syntyvän mittavia säästöjä, koska eri maiden eriäviä käytäntöjä ei käytännössä enää ole ja niiden noudattaminen sitä kautta helpottuu. Ulkoistaminen voi olla hyvä tapa yritykselle hoitaa toimintatasonsa vaaditulle tasolle ja helpottaa hämmennystä, jota laaja asetus voi synnyttää. Useat eri yritykset ovat alkaneet tarjota GDPR-palveluita, mutta lopullinen vastuu on aina loppuasiakkaalla, vaikka hän siitä apua saisikin. On tärkeää kyetä erottelemaan esimerkiksi tiedon käsittelijän ja sen omistajan vastuiden selkeät erot ja mitä erikoispiirteitä niiden roolitukset tuovat mukanaan. (O'Brien 2016.)

## 2.4 Tietohallinnon roolin muuttuminen yrityksissä

Tietoturvan jokapäiväisen tarpeellisuuden ja kasvaneen roolin ansiosta yrityksen perinteinen IT-osasto ei lähtökohtaisesti ole enää toimiva (eikä riittävä) elin vastaamaan tietoturvasta yrityksessä. Tämän johdosta tietohallintojohtajan (Chief Information Office, CIO) rinnalle on noussut merkittävään rooliin tietoturvajohtaja (Chief Information Security Officer, CISO) sekä nykyään eroteltuna vieläpä erillinen digijohtaja (Chief Digital Officer, CDO), jonka vastuulla on esimerkiksi sosiaalinen media. Ajatus on pohjimmiltaan tiimityö eri johtajien välillä, eikä selkeiden rajojen vetäminen eri vastuista. Jos jotain mahdollisesti jotain tapahtuu, asia selvitetään yhdessä, jotta voidaan varmistua, ettei se toistu. Tämän ajatusmuutoksen haasteena voidaan nähdä IT-osaston jatkuva vastuu, vaikka tietoturvaa johdetaan muualta, voidaan syy silti sysätä IT-osastolle, koska se on ”loogista” ja siihen on totuttu. Tässä vaikuttavana tekijä toimii yrityksen koko. On myös liian helppoa jäädä ajattelemaan, kuinka nykyinen ”toimiva” tilanne on samalla riittävä. Tietoturvaosaaminen tulisi nähdä etuna ja parhaimmillaan jopa kilpailuetuna. (Koch 2004.)

Organisaatiokaaviossa tietoturvajohtajan (CISO) paikka ei ole yksiselitteinen. Sen yleisin sijoituspaikka on suoraa tietohallintojohtajan alla. Tämän sijoituksen heikkouksiin kuuluvat voimattomuus saada muutoksia aikaan, jäädä alibudjetoiduksi sekä kyvyttömyys toimia aidosti itsenäisesti. Hyviin puoliin lukeutuvat taas heikompi muutosvastarinta, konkreettisten (tekniset) toimien nopeampi hyödyntäminen käytössä sekä synergiaedut. Toinen, vähemmän ideaali vaihtoehto olisi toimia sisäisen auditoinnin alla (jos sellainen yrityksestä löytyy). Tämän hyviin puoliin kuuluvat erottautuminen IT-osastosta, kokonaisvaltaisempi asema yrityksessä, joka mahdollistaa poikkileikkaavan

toiminnan sekä sen, että tietosuojaa käsitellään myös tietoturvan ohessa tärkeänä osana. Heikkouksia tässä mallissa ovat, että sisäinen auditointi harvoin herättää positiivisia tunteita kollegoissa sekä osaaminen saatetaan nähdä vain pintapuolisena, koska auditointi on moniulotteista toimintaa ja vaatii paljon yleispätevää tietämystä (ei niinkään toimialakohtaista). Kolmas vaihtoehto, joka on paras perusmalleista, olisi taas toimia suoraa ylimmän johdon alaisuudessa. Sen positiivisia seikkoja olisivat, että tiimillä on suora yhteys päättäjiin, joka tuo mukanaan vaikutusvaltaa, toiminta on itsenäistä, koska raportoidaan vain suoraa ylimmälle taholle ja mahdollisuus nähdä ”kaikkialle” yrityksessä, koska raportoitavalla taholla on pääsy kaikkeen sekä se näyttäytyy työntekijöille tärkeänä toimintoja yrityksessä (eli kuinka turvallisuus otetaan vakavasti). Sen heikkouksiin taas kuuluu, että tiimi voidaan nähdä toimivan ”norsunluutornissaan” eli ilman kunnollista kosketusta arkeen, jolloin tehdään vain päätöksiä (tutkimatta niiden todellista vaikutusta) sekä IT-osaston toiminnan kartoittaminen voi olla hankalaa valta-asetelman ansiosta. (Osborne & Summitt 2006.)

Tietoturvaosaston tärkeimpiin tehtäviin kuuluu paneutua erinäisiin organisaatiota koskeviin tietoturvatapauksiin. Näihin lukeutuvat: tietovarkaudet, tietoturvaloukkaukset, tietoturvauhat sekä kaikki erinäiset muut tietotekniset väärinkäytökset organisaatiossa. Tietoturvaosaston vastuista ei sovi unohtaa erinäisten säännösten ja lakien noudattamisen valvomista ja niiden toteuttamisessa auttamista. Tietoturvajohtajan tärkeimpiin ominaisuuksiin voidaan lukea turvallisuuden lähettinä toiminen, johtajana toiminen, ongelmanratkaisukyvyn kautta uusien ideoiden luominen ja luova ajattelu, ajanhermolla pysyminen ja alan trendien seuraamiskyky, luotettavuus ja sitä kautta myös johdonmukaisuus. Jokainen johtaja toimii organisaatiolle parhaalla mahdollisella tavalla luoden mahdollisimman hyvän synergian ja koheesion eri osastojen välille edistäen liiketoimintaa. (Osborne & Summitt 2006.)

Järjestelmien testaus, tarkemmin sanottuna auditointi ja erityisesti ulkopuolinen auditointi, nähdään tärkeänä osana niiden elinkaarta, koska organisaation turvallisuuden ohelle on noussut kasvava tarve liiketoiminnallisuuden jatkuvuudesta. Jokaiselle järjestelmälle tulisi olla jatkuvuussuunnitelma sen varalta, jos jotain menee pieleen ja toiminnon jatkuvuus vaarantuu. Oli kyse sitten kriittisestä järjestelmästä tai jostakin vähemmän tärkeästä sivujärjestelmästä. Yleensä juuri jatkuvuussuunnittelu on johdolle tärkein yksittäinen asia mitä turvallisuuteen tulee, mutta silti se usein pyritään siirtämään toisten vastuulle tai pahimmassa tapauksessa jopa ulkoistamaan koko yrityksestä. Tämä korostaa tarvetta henkilöstön kouluttamiselle eli kuinka tulisi toimia häiriötilanteessa. Näitä luotuja käytäntöjä ja toimintatapoja olisi hyvä tarkastella organisaationa säännöllisesti, tarkistaen ovatko ne edelleen ajankohtaisia ja vastaavat vieläkin kaikkia yrityksen tarpeita. Käytäntöjä tulisi myös säännöllisesti testata, jotta niiden toimintavarmuuteen voidaan luottaa ja eri tahot tietävät myös käytännössä (teorian lisäksi) kuinka toimia sekä mitä heiltä odotetaan. Nämä koskevat yleensä työntekijöiden

lisäksi myös organisaatioiden johtohenkilöitä. Auditointeja tulisi hyödyntää myös näissä tapauksissa tasaisin väliajoin. (Järveläinen 2012.)

Tietoturvaa ei ole mahdollista aktivoida osaksi yritystä onnistuneesti ilman henkilöstön osaamisen lisäämistä kouluttamalla. Muutoksen on tultava mielellään henkilöistä itsestään. Täydellisinkään kokoelma toimintaprotokollia ja käytäntöjä ei ole mitään ilman oikeanlaista implementointia osaksi vallitsevaa yrityskulttuuria. Kuten kaikki muutokset, myös tietoturvakäytännöt on ensin ”myytävä” työntekijöille, jotta ne voidaan panna tehokkaimmin käytäntöön. Silloin voidaan luottaa niiden toimivan, kuten on tarkoitettu. Ne eivät siis voi tulla vain käskyinä ylhäältä alaspäin. Peltier (2005) esittää tämän oppimisen koostuvan kolmesta avaintekijästä:

1. Tietoisuus, stimulointi ja motivointi, muistutus siitä mitä yleisöltä vaaditaan
2. Harjoittelu, prosessi jossa opetetaan tietty taito tai jonkin työkalun oikeaoppinen käyttö
3. Koulutus, erikoistunut, syvällinen opetus joka vaaditaan kaikkien työkalujen hallintaan

Nämä tekijät huomioiden on mahdollista luoda yrityksille sopiva ohjelma, joka johtaa onnistuneeseen tietoturvaosaamisen lisäämiseen. On myös hyvä muistaa, kuinka tärkeää on itse uskoa muutosprosessiin eli uskoa tehtyyn suunnitelmaan ja sitoutua noudattamaan sitä. Suunnitelmaa esitellessä tulisi käyttää selkeitä ja yleiskielisiä ilmaisuja, jotta kaikki ymmärtävät mistä on kyse. Yrityksen työntekijöitä kiinnostaa lähtökohtaisesti eniten tietää, miten asiat vaikuttavat heidän työskentelyynsä ja mitä juuri heidän tulisi konkreettisesti tehdä. Kyse on samalla yrityksen arvon lisäämisestä. Oikeaoppisessa tietoruvaohjelmassa on viisi pääelementtiä, jotka tulee huomioida:

1. Prosessi, jolla saadaan viesti yrityksen tietoturvan merkityksen tärkeydestä koko käyttäjäkunnalle
2. Ohjelman implementoinnin avainhenkilöiden tunnistaminen
3. Tärkeän informaation ja kriittisten järjestelmien ja toimintojen päättely
4. Liiketaloudelliset syyt, miksi perustietoturvaosaaminen on merkityksellistä yritystoiminnassa
5. Ylemmän johdon täysi tuki ohjelman toteutukselle ja onnistumiselle

On tärkeää huomata, ettei mikään ohjelma ole suoraa sopiva yritykselle. Näiden tietoturvaohjelmien on tarkoitus olla räätälöityjä ja pitkälle harkittuja juuri kohdeyritykselle sopiviksi. Mitään täysin yleispäteviä ratkaisuja ei lähtökohtaisesti ole olemassa. Tarkoitus on toimia vahvassa yhteistyössä kaikkien yrityksen osien kanssa yhdessä kohti yhteistä päämäärää. Tietoturvaohjelman tekeminen ei vaadi suuri rahallisia

varauksia, enemmänkin aikaa ja oikeita avainhenkilöitä osaksi sen toteutusta. Joskus on helpompaa aloittaa pienestä muutoksesta ja pyrkiä sen jälkeen levittämään sitä laajemmalle suunnitellusti. (Peltier 2005.)

Pk-yritysten näkökulmasta aiemmin mainitut Peltierin (2005) opit ovat sovellettavissa myös pienempiin yrityskokoihin. Oppeja lähinnä suoraviivaistetaan pienemmän ihmismäärän myötä. Erityisesti avainhenkilöiden tunnistaminen ja tietoisuuden levittäminen yksinkertaistuvat merkittävästi. Pahimpaan varautuminen tulee silti olla osa tätä suunnittelua. Tärkeintä yritykselle olisi löytää kultainen keskitie, jossa tietoturvan taso on linjassa toimimiskyvyn säilyttämisen kanssa.

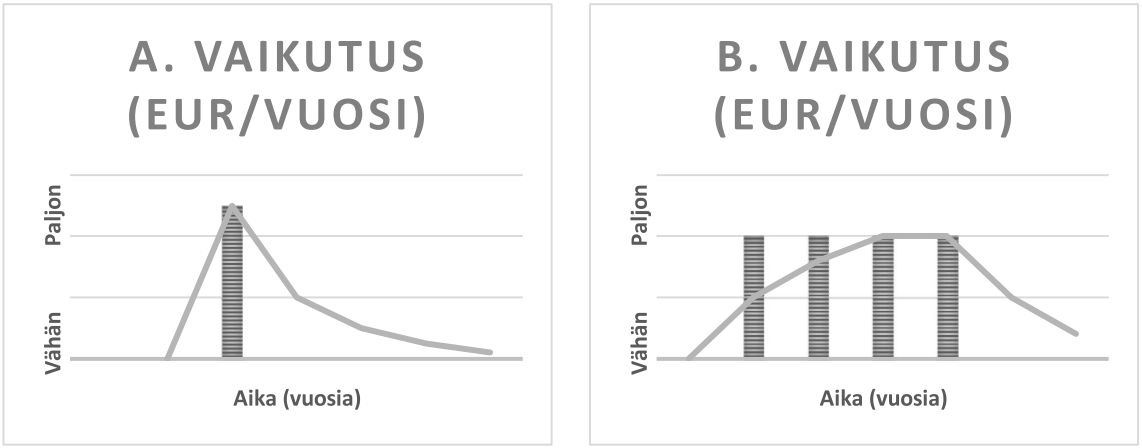
## 2.5 Organisaation tietoturvastrategia

Organisaation on mahdollista luoda itselleen strategia, jossa lähdetään rakentamaan hyviä käytäntöjä ja sovittuja toimintatapoja. Strategian tulisi sisältää kaikki pääasialliset tietojärjestelmille asetetut tietoturvalliset tavoitteet sekä kuinka niihin päästään. Strategian luonti voidaan nähdä joko suunnitelmana tai prosessina, joista jälkimmäinen on dynaamisempi muutoksien kannalta. Koko konseptin luonti ja määrittely ovat hieman kiistanalaisia, mitä luettuun kirjallisuuteen tulee eli mitään yksittäistä opasta tai prosessia tähän ei vaikuttaisi kirjallisuuden perusteella olevan. Kirjallisuudesta on löydettävissä epäselvyyttä myös muun organisaation linjaamisessa osaksi tätä strategista suunnitelmaa. Mielestäni se on tietoturvastrategian tavoitteiden onnistumisen kannalta välttämätöntä. Osan käytännöistä voidaan todeta olevan virallisempia kuin toiset, jolloin voidaan puhua myös hiljaisista säännöistä. Onnistumisen kannalta on tärkeää valvoa ja kouluttaa henkilöstöä luodun strategian mukaisesti. Strategian käyttöönottamisen onnistuminen tulee olla määrätietoista ja hallittua. Yrityksen johdon tulisi ottaa kantaa myös tietoturvaan liittyvään budjetointiin, koska kyse on ylemmän tason strategisista valinnoista. Näiden kautta yleensä päästään myös roolijakoon, joka selkeyttää vastuita ja oikeuksia riippuen asioiden luonteesta tai suuruudesta. (Horne, Maynard & Ahmad 2017.)

Joissakin suuremmissa organisaatioissa asiat on viety astetta pidemmälle. On mahdollista noudattaa standardeja, joissa myös tietoturva on joko keskipisteenä tai osana huomioitavia asioita. Tämän tutkimuksen mukaan yli puolet otantayrityksistä tukeutui standardeihin. Siitä huolimatta valtaosa tutkimuksessa olleista yrityksistä ei varsinaisesti seurannut tietoturvansa tasoa millään tavalla. Vain muutamat yritykset olivat onnistuneesti testanneet käytäntöjensä tai suunnitelmiensa toimivuuden käytännössä. Tämä päti esimerkiksi tietojen palautukseen liittyviä toimintoja ja tiedonjatkuvuutta. Toimintatavat pysyivät strategioista huolimatta hyvin reaktiivisina, eivätkä ne olleet muuttuneet proaktiivisiksi, kuten voisi kuvitella. Organisaatioiden turvallisuus oli myös

poikkeuksetta asetettu tavalla tai toisella osaksi vallitsevaa IT-osastoa ja sen sisältämiä toimintoja. (Sveen, Torres & Sarriegi 2009.)

Sveen, Torres & Sarriegi:n artikkeli (2009) esittelee kehämäisen mallin, jolla reaktiivisesta toimintatavasta turvallisuuden suhteen pystytään lopulta johtamaan turvallisuuden haluttu taso. Tämä onnistuu hakemalla sopivan, hyväksytyn, riskin raja-arvo ja johtamalla siitä vaaditun turvallisuuden taso. Mitä vähemmän riskejä halutaan hyväksyä, sitä korkeampi turvallisuuden tasosta tulee. Tämä tarkoittaa myös sitä, että turvallisuuteen sijoitetaan resursseja, kunnes se on saatu hyväksytylle tasolle. Sijoittaminen turvallisuuteen voidaan kuvata kahtena erilaisena kuvaajana, jotka on esitelty seuraavalla sivulla. Vasemmanpuoleisessa kuvaajassa (A.) yrityksessä on tapahtunut jokin akuutti tapaus, esimerkiksi tulva palvelinhuoneessa, joka on lisännyt äkillisesti turvallisuuteen kuluvia varoja ja samalla nostanut käsitystä yrityksen turvallisuuden tasosta hetkellisesti (kuvaaja on laskeva). Oikeanpuoleisessa kuvaajassa (B.) voidaan nähdä tilanne, jossa on käynyt useita pieniä tapauksia, jotka ovat tasaisesti lisänneet investointien avulla yrityksen käsitystä sen turvallisuuden yleisestä tasosta.




**Kuva 1: Yritys kokee oman turvallisuuden tasonsa johdon näkökulmasta. (Lähde: Sveen, Torres & Sarriegi 2009.)**

Yleensä muutoksen syntyminen organisaation tietoturvakäsitykseen vaatii jommankumman näistä toteutumisen (Kuva 1. kaavio A. tai B.). Tämä johtuu siitä, että tapaukset toimivat jopa hieman kipeinä muistutuksina siitä, missä organisaation heikkoja kohtia esiintyy ja mistä parannettavaa löytyisi. Kun oikeantyyppiset turvamekanismit ovat paikoillaan, ne ennaltaehkäisevät negatiivisia tapauksia syntymästä tai vähentävät niiden vaikutusta. Jos tietoturvastrategia on vain puhtaasti reaktiivinen sekä tapausten määrä epäsäännöllinen ja vähäinen, johtaa se vain välttävän tietoturvatason

säilyttämiseen organisaatiossa. Tämä ei ole optimaalista eikä haluttua yrityksen liiketoiminnan ja sen jatkuvuuden kannalta. (Sveen, Torres & Sarriegi 2009.)

Tälle vaihtoehtoinen, suositellumpi, toimintatapa on proaktiivisen tietoturvastrategian synnyttäminen ja sen toteuttaminen. Tietoturva-aukkoihin ja uusiin hyökkäysmalleihin valmistaudutaan jo etukäteen, ennen kuin ne ovat yleistyneet ja hyvin tunnetusti käytössä (eli suora, konkreettinen uhka organisaatiolle). Tämä vaatii lähtökohtaisesti myös riskien tunnistamista ja johtamistaitoa. Teknisten taitojen lisäämisestä ei ole myöskään haittaa. Eteenpäin katsova, tulevaisuuteen varautuva, yritys toimii itsekriittisesti omaa toimintaansa säännöllisesti arvioiden ja riskeihin varautuen. Organisaatioissa hyödynnetään yleensä, usein tiedostomatta, näitä kumpaakin toimintamallia. Useimmiten juuri proaktiivinen malli täydentää ja parantaa reaktiivista mallia entisestään. Toisinaan organisaatiolle suurin hyöty syntyisi nykyisiä toimintoja kehittämällä (usein näin jää tekemättä) eikä juurikaan uusia toimintamalleja oteta käyttöön. Usein yrityksessä ei huomata, mitä voimavaroja sen sisältä löytyisi jo valmiina. Ratkaisuja lähdetään herkästi hakemaan ulkopuolelta, esimerkiksi palkkaamalla lisää kyseistä työvoimaa. (Sveen, Torres & Sarriegi 2009.)

## 2.6 Pk-yritysten nykytila

Pk-yrityksillä on useita erilaisia tiedonlähteitä saatavilla tietoturvaan liittyen. Vaikuttaa kuitenkin siltä, etteivät yritykset osaa hyödyntää niitä edukseen, jolloin ne osaisivat luoda kokonaisvaltaisen tietoturvajärjestelmän ja se hallinnan. Pohdittuja syitä tälle ovat ainakin puutteellinen tietoisuus ja siltä osin koulutus asiasta, mutta samalla on myös pohdittu olemassa olevien ratkaisujen turhaa monimutkaisuutta, joka ajaa niistä poispäin. Asiaa useimmiten on myös haittaamassa taloudellisten varojen puutteellisuus tarpeeseen nähden. Investointia tietoturvaan saattaa olla vaikea perustella muulle yritysjohdolle, varsinkin jos se he eivät jaa samaa näkemystä ja vastuuntuntoa asiaan liittyen. (Groner & Brune 2012.)

On hyvä myös huomioida, kuinka tärkeää tietoturvastrategian päivittäminen on turvallisuuden kannalta ja sen tulisi tapahtua yrityksessä tehtävien säännöllisten riskianalyysien avulla. Yrityksen tulisikin itse arvioida omaa toimintaansa ja tehdä sen pohjalta mahdollisia muutoksia ja uusia päätöksiä. Jos katsotaan puhtaasti tekijöitä, jotka vaikuttavat tietojärjestelmien tietoturvariskeihin, voidaan ne karkeasti jaotella sisäisiin ja ulkoisiin tekijöihin. Löydät näistä tekijöistä kattavamman luetteloinnin alta.

Sisäiset tekijät:

- Työntekijöiden välinpitämättömyys

Tällä on mahdollista tuottaa peruuttamatonta vahinkoa yritykselle. Yleisin ratkaisutapa on lisätä henkilökunnan koulutusta ja tietoutta. Näin ongelma kitketään juuritasolta pois.

- Työntekijöiden käytös
  Oli kyse sitten salasanojen vahvuudesta tai käyttäjätunnusten käyttötavoista, on tunnettu tosi asia inhimillisestä heikkoudesta mitä ihmisiin tulee.
- IT-osaston puutteellisuus/puuttuminen kokonaan
  Tämä ei ole liiketoimintasektoriin sidonnainen ongelma, jokaisella yrityksellä on nykypäivänä tarve IT-osaamiselle, vaikka se olisikin vaihtelevalla tasolla.
- Ylemmän (vanhemman) johdon tuen puuttuminen
  Tietoturvallisuus tulisi olla yksi pääkohta, joka yrityksen tietojärjestelmästrategian luomiseen tulee. Sen olisi oltava samalla tasolla kuin liiketoimintasuunnitelman tärkeys.
- Riittämättömän tekninen laitteisto
  Vanhentunut teknologia aiheuttaa täysin uudenlaisia ongelmia ja vanhentunut laitteisto tulisi uusia ja päivittää tarpeen mukaan.
- Tekniset viat (ohjelmistossa/laitteistossa)
  Oikeaoppinen käyttö ennaltaehkäisee syntyviä vikoja. Olisi tärkeää pyrkiä estämään vikatilanteista johtuvien ketjureaktioiden syntymistä.
- Riittämättömät ohjelmistot
  Käytetyt ohjelmistot tulisi valita sopimaan yrityksen liiketoimintaan ja niiden toimivuuteen tulisi kiinnittää erityishuomiota.
- Sisäisten ohjeiden ja käytäntöjen puutteellisuus tai puuttuminen kokonaan
  Näillä on mahdollista estää tilanteiden syntymistä tai ainakin rajoittaa niistä mahdollisesti syntyviä vaurioita ja lisäongelmia.
- Taloudellisen tuen puuttuminen tietojärjestelmien hallintaan
  Ilman rahaa ei ole mahdollista taata sovittua tietoturvatasoa, jota tahdotaan noudattaa.

Ulkoiset tekijät:

- Sertifiointi
  Suoritetut sertifioinnit voivat antaa harhakuvaa tietoturvallisesta tilanteesta ja jopa vääristynyttä turvallisuuden tunnetta.
- Lainsäädäntö
  Yleisesti ottaen lait eivät ota kantaa uusimpiin tilanteisiin, eivätkä ne näin ollen takaa tietoturvallisuutta varsinkaan uusimpien uhkien kannalta.
- Valtiollinen tuki tietojärjestelmille

Myös valtiot ovat ymmärtäneet tarpeen tietoturvallisuudelle. Se onkin synnyttänyt jo useampia suurempia tahoja, jotka auttavat sen varmistamisessa myös valtiollisella tasolla.

- Yleinen teknologinen kehitys
  Trendien seuraaminen ei ole helppoa teknologian nopean kehityksen myötä, mutta sitä voidaan helpottaa kehittämällä IT-osaamista säännöllisesti sovitulla tavalla.

- Luonnonkatastrofit
  Katastrofit ovat uhka ihmisille, mutta samalla myös tekniselle laitteistolle, jota on käytössä. Luonnonkatastrofeihin tulisi varautua osana suunnitelmallisuutta.
- Kolmannen osapuolen epäonnistuminen
  Kumppaneiden toimintaa olisi hyvä seurata aktiivisesti ja säännöllisesti ja jopa tarkistaa virheiden varalta. Virheiden kumuloituminen ja mahdolliset ketjureaktiot saattavat suurentaa syntyneitä vahinkoja merkittävästi.

(Bolek, Lateckova, Romanova & Korcek 2016.)

Tietoturvakäytännöt tulisivat olla yrityksen toiminnan ytimessä tavalla tai toisella, koska ne auttavat määrittelemään yleisemmällä tasolla, mikä on yrityksen haluttu tietoturvantaso. Näiden käytäntöjen pohjalta luodaan yleensä erillinen tietoturvaohje, jota yksittäiset työntekijät sitoutuvat noudattamaan osana työtehtäviään. Tietoturvaohjeen voidaan katsoa olevan kokoelma yrityksen ohjeistuksia, joilla pyritään takamaan yrityksen tietoturvan aiemmin määritelty taso ja se, kuinka sitä ylläpidetään. Usein tämä ohje sisältää myös kerrontaa siitä, miten käytäntöjen toteutumista seurataan ja mitä seurauksia noudattamattomuudella voi tulla. Kyseinen tietoturvaohje on kuitenkin yksilöllinen dokumentti eri yritysten välillä ja osa yrityksistä pyrkii toimimaan myös kokonaan ilman sitä. Yrityksien tavoitteet ovat usein yksilölliset. Tämä pätee myös kasvusuunnitelmiin, jos yrityksellä sellaisia on. Tietoturvaohjeen on tarkoitus parhaimmillaan myös erotella yrityksen ja yksilön vastuiden rajat. Tätä ohjeistusta on tärkeä myös säännöllisesti tarkastella ja arvioida sen paikkansapitävyyttä. Sitä tulisi päivittää aina kun se koetaan tarpeelliseksi, jotta sen ajantasaisuudesta voidaan olla varmoja. Ohjeistuksen kehitystä tai auditointia on mahdollista myös ulkoistaa tarvittaessa, jos yritys arvioi sen heille itselleen parhaaksi ratkaisuksi. Ulkoistaminen ei kuitenkaan ole kovin suositeltava vaihtoehto. Yritykselle parasta olisi itsearvioida, parantaa ja täydentää käytäntöjään sekä ohjeistuksiaan kokemuksen kautta tulleilla muutoksilla. (Yildirim, Akalp, Aytac & Bayram 2011.)

Ehkä tunnetuin ja pisimpään yhtäjaksoisesti tehty vuosittainen tietoturvallisuutta mittaavan tutkimuksen “global information security survey (GISS)” teettää Ernst & Young (EY) niminen yritys. Tutkimukseen vastasi vuonna 2018 noin 1500 erikokoista yritystä ja niiden johtajia. Kyselyyn vastanneista johtajista ja heidän organisaatioistaan

30 % oli alle 500 hengen yrityksiä (pienimpään kategoriaan kuuluvia). Vastanneista yrityksistä oli 41 % Euroopasta. Jotain karkeita suuntaviivoja tästä siis voi mielestäni johtaa myös Suomen pk-yrityshorisonttiin. Tutkimuksen tulosten perusteella 59 % vastaajista sanoi heidän budjettinsa kasvaneen viimeisen vuoden aikana. Vastaajista 87 % sanoi tarvitsevansa kuitenkin yli 50 % isomman budjetin toimiakseen hyvin. Vain 12 % uskoo saavansa yli 25 % enemmän budjettia jatkossa. Mielenkiintoista oli myös huomata, että 76 % vastanneista totesi, että tapahtunut tietoturvaloukkaus, joka on aiheuttanut vahinkoa, olisi voitu estää täysin, jos heidän budjettinsa olisi ollut suurempi. Huolestuttavaa on lukea siitä, kuinka vain 4 % vastaajista uskoo heidän kokonaiskuvansa tietoturvaan liittyen olevan sillä tasolla millä pitäisikin. (Van Kessel 2018.)

Ponemon:n suorittama tutkimus (2017) taas käsitteli 1040 pk-yrityksen vastausta. Tutkimuksen vastaukset kerättiin Isosta-Britanniasta sekä Pohjois-Amerikasta. Kyseisen tutkimuksen perusteella 61 % vastanneista yrityksistä oli kokenut tietoturvahyökkäyksen viimeisen 12 kuukauden aikana. Yrityksistä 54 % taas raportoi, että heiltä on viety asiakas- ja työntekijädataa viimeisen 12 kuukauden aikana. Tutkimuksen mukaan vaikuttaa siltä, että tämän kokoluokan yritysten suurin uhka olisivat sen työntekijät. Huolimattomuus on yli puolen (54 %) vastanneiden mielestä pääsyy tapahtuneeseen tietovarkauteen. Noin puolet liiketoiminnalle kriittisestä datasta käsitellään mobiililaitteissa. Vastanneista 58 % toteaa, ettei heiltä löydy lainkaan tai löytyy puutteellinen hyvien salasanojen käytäntö. Vastanneista 68 % on myös sitä mieltä, ettei salasanakäytäntöjä valvota millään tavalla toteutumisen kannalta. Tutkimukseen osallistuneista 52 % ilmoitti kokeneensa jonkinlaisen kiritysohjelmahyökkäyksen (ransomware). Osallistujat arvioivat myös menojen kasvaneen vuoteen (2016) verrattuna jopa 30 %. Ne johtuivat suorasti tai epäsuorasti tietoturvaan liittyvistä asioista, esimerkiksi tietoturvahyökkäyksestä tai tai siitä johtuneeseen palvelun katkokseen. Tehokkaimmat hyökkäysvektorit pieniä yrityksiä vastaan olivat vastanneiden mukaan huijausyritykset (phishing) sekä sosiaalinen hakkerointi (social engineering). Vastanneista 48 % kertoi näistä. Seuraavana listalla tuli verkkopohjaiset hyökkäykset 43 % osuudella. (Ponemon 2017.)

Australiassa tehdyn tutkimuksen perusteella yksi ratkaisuehdotus pk-yritysten tietoturvaan olisi antaa sen työntekijöille tietoisesti enemmän vastuuta tietoturvaan liittyen. Klassisesti sen vastuun ajatellaan olevan yrityksen johdolla tai omistajilla eikä niinkään yksittäisillä palkkatyöntekijöillä. Tämäkin esitetty malli pyörii sen tosiasian ympärillä, että riskienhallinnan kannalta on kannattavinta lisäkouluttaa työntekijöitä tietoturvallisuudesta. Se johtaa hyviin tuloksiin. Tutkimuksen perusteella pk-yritysten johtajat hoitavat itse yrityksensä tietoturvaa ja pahimmillaan hoitavat kaikki yrityksen IT-ostot ilman minkäänlaista apua. Juuri tämä kyseinen tutkimus puhuu paljon siitä, kuinka pk-yritykset väistämättä toimivat tietoturvaan liittyen enemmän reaktiivisesti kuin proaktiivisesti. (Dojkovski, Lichtenstein & Warren 2007.)

Tämä tutkimustulos (Dojkovski, Lichtenstein & Warren 2007) pk-yritysten johtajista ja heidän haasteistaan antaa osviittaa siitä, miten vastuiden jakautumista tulisi tarkastella tarkemmin yrityksen kasvaessa. Luvussa 2.4 avattiin sitä, miten tietohallinnon roolitusta ja vastuunjakoa olisi hyödyllistä hyödyntää. Vaikuttaa kirjallisuuden perusteella (esimerkiksi Dojkovski, Lichtenstein & Warren 2007 ja Bolek, Lateckova, Romanova & Korcek 2016) siltä, että vastuunjaolla on merkitystä yrityksen tietoturvan tilaan ja sen kehittymispolkuun.

# 3 TULEVAISUUDEN TIETOTURVAUHKIA

## 3.1 Kohdennetut pitkäkestoiset hyökkäykset

Tutkimukseni mukaan ja siihen kuuluvien lähteiden perusteella (esimerkiksi Winkler & Gomes 2017 & Auty 2015.) voidaan olettaa kohdennettujen hyökkäyksien (Advanced Persistent Threat, APT) koostuvan sekoituksesta erilaisia hyökkäystekniikoita ja -malleja, joilla pyritään saamaan hyötyä joko välillisesti tai suoraan. Hyökkäystyypille on ominaista pitkäkestoisuus ja pyrkimys huomaamattomuuteen. Hyökkäys voi olla myös täysin yksilöity tiettyä kohdetta varten ja tästä johtuen se on tuntematon yleisimmille tietoturvaohjelmistoille, jotka tukeutuvat tunnistusmalleihin haittaohjelmissa ja niiden aiheuttamissa hyökkäyksissä. Tämä onkin pakottanut tietoturva-ajattelun muutokseen: miten voidaan ennaltaehkäistä tyyliltään tuntematonta, jopa ennennäkemätöntä, ja jatkuvaa, pitkäkestoista uhkaa?

Hyökkäyksen motivaationa voi toimia myös poliittiset syyt taloudellisten syiden lisäksi. Tarkoituksena voi olla vaurioittaa toimintaa, ryöstää tärkeää dataa tai vakoilla kohdetta. Hyökkääjälle parhaassa mahdollisessa tapauksessa hyökkäyskohde ei huomaa joutuneensa kohteeksi tai tunnista tilanteen vakavuutta. Tämä on myös kyseisen hyökkäystyypin yksi tavoitteista. Hyökkäystyylille on ominaista peräänantamattomuus eli hyökkäys jatkuu, kunnes sen voidaan todeta onnistuneen sille annetuissa tavoitteissa. (Symantec 2011.)

Kun kyse on APT-hyökkäyksestä, voidaan hyökkääjällä olettaa olevan käytössään seuraavat edut:

- Rajattomasti aikaa
- Rajattomasti voimavaroja
- Valtiorajojen tuoma kansainvälinen suoja
- Puolustus ei ole kohdeyrityksen tärkein prioriteetti bisneksen sijaan

On tärkeää muistaa, että tämän tyyppisen hyökkäyksen takana on ammattilainen, joka tekee sitä työkseen. Hyökkäyksen todentaminen on yritykselle myös hankalaa. Hyökkääjän täytyy kuitenkin:

- Saada ajettua omaa koodiaan yrityksen järjestelmässä
- Muodostetun yhteyden tulee toimia kahteen suuntaan
- Toimia niissä yrityksen osissa, joissa on mielenkiintoista tietoa

Tärkeintä olisi pitää ”pää kylmänä” ja toimia sen mukaan mikä on järkevää, eikä sen mukaan mikä tuntuu oikealta. (Auty 2015.)

Hyökkäyksen tunnistamisella on kuitenkin yleensä isompi merkitys kuin varsinaisella suojautumisella etukäteen. Tämän puolesta puhuu juuri tähän hyökkäystyyppiin kuuluva monimutkaisuus ja ainutlaatuisuus. Voidaan myös olettaa aina epäonnistumisen tapahtuvan jossain kohdassa toimintaketjua, mutta se ei yksinään tarkoita vielä onnistunutta hyökkäystä (sillä määritelmällä, että onnistuminen tarkoittaisi aiheutettua vahinkoa kohteelle tai hyötyä hyökkääjälle). Jos oletetaan hyökkääjän saavan pääsyn halutun järjestelmän verkkoon, ei se vielä suoranaisesti tarkoita hyökkääjälle mahdollisuutta viedä esimerkiksi arvokasta asiakasdataa tai mitään muutakaan, mutta sitä voidaan pitää onnistuneena ensiaskeleena kohti haluttua hyökkäystavoitetta. Kun puhutaan tunnistamisesta ja sen tärkeydestä, se ei tarkoita pelkästään teknistä monitorointia vaan myös huolellisuutta esimerkiksi taustatutkimuksissa uusien työntekijöiden kohdalla. Tähän voidaan laskea mukaan myös työntekijöiden keskinäinen tarkkaavaisuus ja velvollisuus ilmoittaa poikkeavuuksista esimerkiksi henkilökohtaisten tunnusten väärinkäytöstä yhteiskäytön muodossa tai mitä tahansa muuta vastaavaa. (Winkler & Gomes 2017.)

Ilman tapahtunutta tunnistusta ei voi olla reaktiota. Joissakin tapauksissa, kun yritys on huomannut väärinkäytöksiä (tunnistus), jättää se silti reagoimatta niihin vaaditulla vakavuudella ja samalla se menettää mahdollisuuden estää niiden toistumisen. Tähän voi olla syynä myös esimerkiksi havaitun hyökkäyksen sattumanvaraisuus, jonkun on tehtävä päätös siitä, kuinka vakavana mitä tahansa löydöksiä eli tunnistuksia pidetään ja miten niiden osalta toimitaan. Näihin prosesseihin, tunnistukseen ja reaktioon, olisi hyvä luoda vähemmän arvopohjaisia ja enemmänkin mitattavia tapoja toimia. (Winkler & Gomes 2017.)

Vastapainona termille APT Winkler & Gomes (2017) esittelee uuden termin Advanced Persistent Security (APS), jonka tarkoitus on toimia vastapainona. Termillä tarkoitetaan sitä pitkäjänteisyyttä tai pitkäkestoisuutta ja sen ylläpitämistä, mitä vaaditaan APT-hyökkäysten proaktiivisessa torjumisessa sekä onnistuneiden hyökkäysten merkkien etsimisessä osana tietoturvaa. Winkler & Gomes on luonut myös hyvän listan vähemmän tunnettuihin faktoihin tietoturvallisuuteen liittyen:

- Täydellinen turvallisuus on mahdottomuus. Kyse on enemmänkin riskienhallinnasta.
- Turvaohjelmat ovat enemmän kuin vain suojausohjelmia.
- Tunnistus ja reagointi on yhtä tärkeää, ellei jopa tärkeämpää, kuin itse suojaus.
- Turvaohjelma ei ole epäonnistunut, jos hyökkääjä pääsee sen ohi. Epäonnistuminen on vasta kun hyökkääjä on saavuttanut tavoitteensa.
- Epäonnistuminen on hyväksyttävää ja jopa odotettavaa.
- Usein keskitytään liikaa minkälaisia erilaiset hyökkäykset ovat, vaikka pitäisi keskittyä siihen miksi hyökkäys on onnistunut.

- Tappio on usein väistämätön ja hyväksyttävä, kunhan se on odotettu ja huomioitu liiketoiminnassa.
- Tunnistuksen puutteellisuus johtuu yleensä riittämättömästä tai huonosti suunnitellusta tietoteknisestä arkkitehtuurista, mitä tunnistukseen ylipäätään tulee.
- Turvabudjetti tulee ansaita ja olla laskelmoinnin lopputulos eikä sattumanvarainen arvaus.
- Tärkeimmät ja murskaavimmat uhat eivät ole monimutkaisimpia vaan pitkäkestoisia ja puolustukseen mukautuvia.
- Vastatakseen näihin, turvaohjelman tulee olla mukautuva ja proaktiivisesti valmis epäonnistumiseen sekä muokkautumiskykyinen hyökkääjään nähden.

(Winkler & Gomes 2017.)

## 3.2 Sosiaalinen media ja yritysmaailma

Sosiaaliseksi mediaksi määritellään klassisesti mikä tahansa digitaalinen järjestelmä tai alusta, jossa sosiaalinen kanssakäyminen on mahdollista ihmisten välillä ja siihen kannustetaan. Se voi olla lyhyen tiedon jakamista, esimerkiksi olotilan tai sen hetkisten ajatusten kertomista, mutta yhtä lailla verkkokauppojen arvosteluita voidaan pitää sosiaalisen median ilmentymänä. (Mennie 2015.)

Sosiaalinen media, some, on muodostunut kanavaksi, jossa voidaan huijata ja kiusata täysin uusin keinoin kuin aiemmin. Nuoret ovat alttiita vaikutuksille ja sosiaalinen media tarjoaa mahdollisuuksia paljon. Somessa on paljon tarjouksia, jotka ovat liian hyviä ollakseen totta tai ne saattavat johtaa rikokseen tai jopa rikoksen uhriksi. Somessa on mahdollista 1) esittää olevansa joku muu 2) manipuloida muiden käyttäytymistä sekä 3) käyttää koodikieltä. Näiden vakavuus riippuu täysin tavoitteista. (Chandramouli 2011.)

Sosiaalisen median riskit ovat näin ollen selkeät ja samalla on suuri tarve riskistrategialle, jossa ne pystytään huomioimaan. Riskistrategian avulla voidaan tehdä päätöksiä vaikuttavuuden ja nopeuden kannalta. Eli kun jotain tapahtuu, miten siihen reagoidaan. Riskistrategia luodaan yleensä riskiarvioinnin lopputuloksena, koska ensin yrityksen on kartoitettava, mitä riskejä he kokevat itselleen ja missä määrin. Riskistrategiaa tulisi päivittää ja arvioida myös säännöllisesti. Kuten muussakin tietoturvassa, myös sosiaalisen median käytön osalta henkilöstön kouluttaminen on hyödyllistä ja tarpeellista. (Mennie 2015.)

Kick, Contacos-Sawyer & Thomas (2015) mukaan sukupolvi Z:lla (post-milleniaalit) eli 1990-luvun puolessavälissä ja sen jälkeen syntyneillä, on oma näkemyksensä somesta, koska he eivät ole eläneet ilman internetiä. Sukupolvet eivät keskenään ole kiinnostuneita

samoista somepalveluista. Niillä on erilaiset näkemykset somepalveluiden tarpeellisuudesta. Tällä hetkellä hyökkäykset, jotka hyödyntävät esimerkiksi Facebookia eivät toimi yhtä hyvin tulevaan sukupolveen, koska he eivät käytä palvelua. Yksilöidyn hyökkäyksen kohdalla on tarvetta huomioida myös tämä yksityiskohta, jotta se saadaan onnistumaan.

Yritysmaailmassa sosiaalinen media on aina haaste. Henkilökohtaisen ja työn sosiaalisen median rajaa hämärretään entisestään palveluilla, jotka muistuttavat toisiaan, vaikka ovatkin tarkoitettuja eri tiedon jakamiseen ja eri kohdeyleisölle. Hyvä esimerkkitapaus on Facebook ja Facebook for Work. Tietoturvan näkökulmasta käyttäjän olisi tärkeä tiedostaa mihin ja kenelle tietoa on kullakin hetkellä jakamassa. Tiedon louhinta on myös mahdollista sosiaalisesta mediasta hyödyntäen markkinoilta löytyviä useita eri palveluita, joiden päätarkoituksena on kerätä vain tietoja järjestelmistä ja jalostaa siitä datasta arvokkaampaa – jopa myytävää tietoa. Tämä synnyttää myös täysin erillisen, kohteista irrallisen tietovaraston, johon on vaikeampi, jopa mahdoton, päästä vaikuttamaan. On olemassa myös yrityksiä, jotka elävät uskossa, ettei somen vaikutus yllä heihin, koska he eivät itse sitä käytä, tämä ei kuitenkaan pidä paikkaansa. (Mennier 2015.)

## 3.3 Pilvipalveluiden nykytilanne

Kun puhutaan pilvipalveluista, tarkoitetaan sillä nykyaikaista mallia, jossa palvelu varustetaan käyttöä varten. Yleensä tähän liitetään mukaan myös jaettuja (myös muiden käytössä olevia) resursseja, joita kyetään tarvittaessa skaalaamaan eli lisäämään tai vähentämään tarpeen mukaan. Resursseja voidaan skaalata koneellisesti tai minimityöllä. Tämä toimintamalli mahdollistaa myös palvelusta maksamisen käytön mukaan. Nämä mainitut piirteet toimivat yleisesti hyväksyttävän määritelmänä pilvipalvelulle. (Pearson & Yee 2013.)

Tutkimuksissani olen törmännyt muun muassa Microsoft Azure, Amazon AWS, Upcloud sekä Acquia nimisiin palveluihin. Ne edustavatkin suurimpia pilvipalvelutoimijoita tällä hetkellä vaikkakin kilpailun voidaan todeta olevan kova. Erityisenä kilpailuetuna pilvipalvelussa toimii hinta. Palveluista maksetaan vain käytön perusteella ja yleensä myös skaalaaminen on helppoa, jos palvelun tasoa halutaan nostaa suosion kasvaessa, on se yleensä mahdollista tehdä saumattomasti ja jopa viiveettä. Pilvipalvelut ovat alkaneet tarjota virustorjuntaa vakioituna osana palvelumallia ja myös datakeskukset ovat yleensä suojattuja hyvin. Verkostot pyritään peittämään ja piilottamaan kertomalla vain summittainen sijainti palvelimelle (esim. pelkkä maa tai maanosa). Myös datan salaamista tuetaan palvelimien sisällä. Tietosuojakysymykset ovat lainsäädännöllisesti vieläkin useimmissa maissa kesken. Osa EU-maista ei salli

esimerkiksi asiakasrekisterien ylläpitämistä vieraissa maissa. Yhtenä globaalin ja virtuaalisen liiketoiminnan ongelmana on siis datan siirtyminen fyysisten maarajojen ulkopuolelle tietotekniikkapalvelujen myötä.

Koska osa pilvipalveluntarjoajien tietoturvasta perustuu todellisen, taustalla toimivan teknisen toteutuksen abstrahointiin, on niiden vertailua myös haastavaa suorittaa käyttäjälähtöisesti. Haasteita aiheuttaa myös palveluiden jatkuva päivitys. Palveluntarjoajat eivät lähtökohtaisesti ole velvollisia kuvailemaan tarkasti mikä palveluissa muuttuu ja miten. Tämäkin on osa palvelujen suunniteltua turvallisuutta.

Virtualisointi on avaintekijä pilvipalvelimien arkkitehtuurissa. Se mahdollistaa niiden joustavuuden sekä toistettavuuden, jolla voidaan saavuttaa uudenlaisia hyötyjä myös tietoturvan kannalta. Lisäksi automatisointi on mahdollista täysin uusilla tavoilla kuin ennen. Pilvipalveluita voidaan lukea olevan kolmea erilaista: SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service) sekä IaaS (Infrastructure-as-a-Service). Tässä ne olivat lueteltuina pienimmästä suurimpaan. (Winkler & Meine 2011.)

Pilvipalveluiden ympärillä voidaan todeta olevan ”hypeä”, jolla tarkoittaen niiden olevan ”uusinta uutta” mitä teknologiaan ja sen trendeihin tulee. Sitä pidetään maailmanlaajuisesti välillä jopa ratkaisuna kaikkiin mahdollisiin ongelmiin sekä vanhoihin että tuleviinkin ongelmiin teknologiassa. Näin ei kuitenkaan ole. Usein mainostajat eivät myöskään mene yksityiskohtiin edustamiensa pilviratkaisuiden monimutkaisuudesta ja moniulotteisuudesta. Yksityiskohdilla voi olla suurikin vaikutus liiketoimintaan. (Pearson & Yee 2013.)

Esimerkkinä SaaS-tyyppisestä palvelusta voisi olla sähköposti, jota käytetään selaimessa. Esimerkki taas PaaS-palvelusta olisi Google App Engine, jolla voidaan luoda ja suorittaa omia sovelluksia tietämättä yhtään, miten niitä käytännössä ”ajetaan” Googlen taustajärjestelmissä. Esimerkki IaaS-palvelusta olisi Microsoft Azure, joka toimii alustana, jossa pystytään ajamaan virtuaalisia palvelimia tarpeen mukaan tietämättä ja ottamatta kantaa, miten virtualisointi on todellisuudessa toteutettu fyysisillä palvelimilla.

Pilvipalveluita voidaan lukea olevan neljä erilaista: julkinen, yksityinen, yhteisöllinen sekä hybridimallinen. Ensitöikseen yrityksen tulisi harkita oman tietonsa valossa, mikä näistä soveltuu juuri heidän turvallisuuteensa parhaiten, jos tarkoituksena on siirtyä käyttämään pilvipalvelua. Aina on olemassa myös vaihtoehto olla siirtämättä tietoa pilvipalveluun ja pitää se siellä missä se jo nyt sijaitsee. Winkler & Meine (2011) esittävät kirjassaan listan tunnistetuista turvallisuusriskeistä, joita pilvipalveluihin liittyy:

- Saatavuus – palveluun on päästävä käsiksi silloin kun niin haluaa.
- Palveluntarjoajan luotettavuus – toimijoita on paljon ja ala on suhteellisen uusi.
- Katastrofista toipuminen sekä liiketoiminnan jatkuvuus – toiminnan tulee jatkua, vaikka palveluntarjoajalla olisi katastrofi käsillä.

- Tietoturvaloukkaukset – palveluntarjoajan tulisi olla yhteydessä myös asiakkaisiinsa mahdollisista tietoturvaloukkauksista, jos niitä tapahtuu.
- Läpinäkyvyys – asiakkaan ja palveluntarjoajan välillä on pysyttävä luottamussuhde siitä, miten he toimivat kumpikin puolellaan.
- Fyysisestä saavutettavuudesta luopuminen – tietoon ei pääse käsiksi enää ”kävelemällä” sen luokse.
- Uudet riskit, uudet haavoittuvuudet – toimialue on uusi ja sitä kautta hieman tuntematon mitä se tuo tullessaan lähitulevaisuudessa.
- Lakien ja säätelyjen vaatimukset – kaikki lainsäädäntö ei vielä mahdollista pilvipalveluiden hyödyntämistä, tämä riippuu mistä tiedoista on kyse ja tulee selvittää ajoissa.

Tämän listauksen tarkoitus on luoda tärkeimmät avainkohdat, joita tulee harkita pilvipalveluihin siirtymisen kannalta mitä tietoturvallisuuteen tulee yrityksessä. (Winkler & Meine 2011.)

Tietosuojaan liittyen voidaan puhua myös pilvipalveluiden turvattomuudesta. Useimmiten tietoa on palveluissa salaamattomana ja fyysiset resurssit ovat jaettuna useamman eri asiakkaan välillä. Tämä mahdollistaa suuren mittakaavan väärinkäyttömahdollisuudet sekä mahdolliset mittavat tietovarkaudet. Tutkitusti suurimmat esteet pilvipalveluiden käyttöönottamiselle ovat juurikin pelko tiedon luottamuksellisuuden tai sen turvallisen säilytyksen menetyksestä tiedon vuotamisena. Näissä tapauksissa yritysten on kuitenkin noudatettava ajantasaisia kansainvälisiä ja valtiollisia lakeja, joiden voidaan uskoa vain lisääntyvän lähitulevaisuudessa. Nämä lait toimivat kuitenkin juurikin reunaehtoina erilaisten palvelujen toiminnalle. Tätä maantieteellistä määrittelyä (lain silmissä mutta muutenkin) häiritsee tiedon hajautus, johon vaikuttaa myös palvelun käytettävissä olevien resurssien lisääminen tai vähentäminen. Lisätyt resurssit saattavat tullakin toisen maan puolelta kuin missä muut resurssit sijaitsevat. Pilvipalveluntarjoajien tulisikin ottaa huomioon käyttäjien vaalima yksityisyyden suojaaminen jo osana pääliiketoimintaansa esimerkiksi tietojen elinkaaren suunnittelussa. Useimmiten tämä tarkoittaa myös näiden asioiden miettimistä useammalla eri toteutustasolla aina strategisista päätöksistä aina teknologiavalintoihin. (Pearson & Yee 2013.)

## 3.4 Toimialan tai yrityksen koon vaikutus yrityksen tietoturvaan

Tutkimukseni perusteella voidaan todeta pk-yrityksen toimialalla olevan merkitystä siihen, kuinka se reagoi tietoturvaan. Lähtökohtaisesti voidaan olettaa vahvasti IT:tä

hyödyntävien toimialojen toimivan paremmin ja tietoturvallisemmin kuin klassisempien toimialojen.

Tutkimukseni mukaan pienimpien yritysten eli mikroyritysten voidaan todeta hyötyvän paljon oman bisneksensä tutkimisesta ja sitä kautta myös liiketoiminnalle kriittisen datan tunnistuksesta. Ne pitävät kumppani- ja asiakaspiirinsä yleensä pienenä ja tiiviinä, josta saattaa helposti syntyä vääränlaista turvallisuuden tuntoa. Yleensä IT:n ulkoistamiseen turvautuminen on välttämätöntä toimimisen kannalta. Näiden pienimpien yritysten strateginen maturiteetti on matala, vaikka heidän IT-maturiteettinsa olisikin keskitasoa.

Keskisuurten yritysten joukossa alkaa yleensä myös strateginen maturiteetti nousta yrityksen koon kasvaessa. Tämä yleensä lisää kiinnostusta ja osaamista tietoturvaan. Tiedon keräilystä ja sen jäsentelystä on saatavana järjestelmällisempää ja varmempaa tietoa kuin koskaan aiemmin. Parhaimmillaan se johtaa hyvien käytäntöjen seuraamiseen ja hyvin vastuullisesti toimimiseen. IT:n ulkoistaminen nähdään myös enemmän optiona kuin välttämättömyytenä.

Kun yrityskoko kasvaa, tulee yritykselle äkillistä tarvetta alkaa jakaa aiemmin yhteistä vastuuta useammalle henkilölle saavuttaakseen lisää tehokkuutta, mutta samalla myös lisäten yrityksen sisäistä luottamusta. Pääliiketoiminnasta liittyen tarve jakaa yritystä erillisiin osastoihin ja selkeämpiin vastuualueisiin herää. Joko aiemmassa vaiheessa tai hieman myöhemmin osana yrityksen luontevaa elinkaarta. Eri toiminnot ja osastot yrityksen sisällä vaativat myös uudet, niistä vastaavat johtajansa. Se saattaa luoda haasteita kommunikaatioon ja sen ylläpitämiseen eri toimintojen välillä. Tämä voi tulla myös yllätyksenä, jos yrityksen kasvu on nopeasti kasvavaa. Usein organisaatiokaaviolla, eli sillä miten vastuu periytyy eri osastoille ylimmältä johdolta ja kuinka toiminnot suhteutuvat toisiinsa, on vaikutusta päätöksientekoon. Tästä on kerrottu myös aiemmin jo luvussa 2.4. Kun organisaatiokaaviota aletaan muodostamaan tai muuttamaan, on tärkeää kiinnittää huomiota, ettei vastuita jää täyttämättä, vaikka päättäjiä tuleekin ”pöytään” lisää. Strategiasta ja selkeästä visiosta on tässä kohdassa organisaatiolle eniten hyötyä.

# 4 METODOLOGIA

## 4.1 Tutkimusmenetelmä

Tämän työn empiirinen osuus käydään läpi tapaustutkimusmenetelmällä (case study). Tapaustutkimuksen ytimessä on pyrkiä kuvailevaan ja tutkivaan kertomistapaan analysoimalla tutkimusaineistoa. Tapaustutkimuksessa voidaan tutkia yksilöitä, organisaatioita tai yrityksiä. Sen tarkoitus ei ole yleistää, eikä saada aikaan yleispäteviä tuloksia. Omalla tavallaan, tapaustutkimus rikkoo normaalimpaa, normeja mukailevaa tutkimuskaavaa. Aineistossa ehkä yleensä hyödynnetään pääasiassa kvalitatiivista aineistoa, mutta siihen on mahdollista yhdistää kvantitatiivista aineistoa. Tutkimusaineisto voi olla siis useasta eri lähteestä koottua ja siten yhdistettyä yhtenäisemmäksi. Aineistoa kerättäessä luottamuksen synnyttämiselle voidaankin antaa erityistä painoarvoa. (esimerkiksi Becker, Dawson, Devine, Hannum, Hill, Leydens, Matuskevich, Traver & Palmquist 2012 sekä Benbasat, Goldstein & Mead 1987.)

Tapaustutkimuksen ydin on tutkia haluttua ilmiötä sen omassa, luonnollisessa ympäristössään. Tiedonkeruutapoja voi olla jopa muutamia eri mutta tulosten manipulointia sekä arvailua etukäteen vältetään. Ilmiön mahdollista laajuutta ei myöskään pyritä arvaamaan etukäteen. Erot ovat täten selkeitä perinteisempiin, laboratoriopohjaisiin menetelmiin, joissa tarkoituksena on kontrolloida, ja sitä kautta minimoida mahdolliset muuttujat tiedonkeruussa. Alla olevassa listassa on lueteltuna yksitoista ominaispiirrettä, joita tapaustutkimuksilla on:

1. Ilmiötä tutkitaan sen omassa ympäristössä.
2. Tietoa (dataa) kerätään useammalla eri tavalla.
3. Yksi tai korkeintaan muutama joukko (ihminen, ryhmä tai organisaatio) valitaan tutkimuskohteeksi.
4. Yksikön kompleksisuuteen kiinnitetään erityistä huomiota.
5. Tutkija nojaa vahvasti etsimisen kautta uuden tiedon löytämiseen.
6. Käytössä ei ole kokeellisia tai manipuloivia osuuksia.
7. Tutkija ei ole etukäteen erotellut pysyviä ja vaihtuvia tekijöitä.
8. Tuloksien tuottaminen on pitkälti kiinni tutkijan kyvystä yhdistellä asioita.
9. Valittu tiedonkeruumenetelmä voi tarvittaessa muuttua, jos kehittyneempi hypoteesi niin vaatii.
10. Tapaustutkimus vastaa hyvin kysymyksiin ”miksi” ja ”miten”.
11. Keskitytään erityisesti ajankohtaisiin tapahtumiin ja nykyhetkeen.

Tapaustutkimuksen päätavoite onkin juuri suorittaa tutkimusta sekä kerätä tietoa. Aineiston keräämisessä korvaamattomaksi avuksi saattaa syntyä työpari, sen on mahdollista auttaa kerätyn aineiston rikastamisessa ja sen tarkkuuden säilyttämisessä. Tutkimuksen eteneminen tulisi olla sen lukijalle selkeää ja mutkatonta seurata. (Benbasat, Goldstein & Mead 1987.)

Tärkeässä roolissa tutkimuksen aloituksessa on tutkimuskysymysten luonti eikä niiden laadinnassa tulisi kiirehtiä. Tapaustutkimuksen osalta valitut tutkimuskysymykset vastaavat usein ”miksi” ja ”miten” -tyyppisiin kysymyksiin, sekä koskettavat nykyaikaisia tapahtumia, joihin voi vaikuttaa vain hieman tai ei ollenkaan. Tutkijan tulisikin avata osana tutkimustaan todentamia syy-seuraussuhteita tai mahdollisia hypoteeseja työssään. Tutkimuksen lukemisen tulisi olla mahdollista edetä aina tavoitteista ja kysymyksistä itse oletuksiin, ja sitä kautta myös löydöksiin – lopulta päätyen mahdolliseen lopputulokseen ja loppupäätelmiin. (Benbasat, Goldstein & Mead 1987.)

Yin (1984) pohdiskelee myös yksittäisen tapauksen tutkimisen eroja monen tapauksen tutkimiseen. Hänen mielestään nimenomaan yksittäisten tapausten tutkimiseen tulisi ryhtyä, jos:

1. Kyseessä on paljastusmainen tapaus, toisin sanoen tapaus tai tilanne, joka ei aiemmin ole ollut tieteelle saavutettavissa lainkaan.
2. Kyse on kriittisestä tapauksesta, jolla testataan (todistetaan) jo hyvin muotoiltua teoriaa.
3. Kyse on äärimmäisestä tai ainutlaatuisesta tapauksesta.

Useamman tapauksen tutkimuksien suosio on kasvanut vuosi vuodelta. Yleisesti voidaan puhua niiden olevan uskottavampia ja samalla vahvempia. Samaan aikaan ne saattavat kuitenkin olla myös raskaampia ja enemmän aikaa vaativia kuin yksittäisen tapauksen tarkastelu. Olisi myös tärkeää huomioida, ettei useamman tapauksen tutkiminen vastaa isompaa otantaa samasta vaan enemmänkin montaa eri tilannetta, joissa pyritään vastaavaan toistamiseen. (Yin 1984.)

Kun valitaan kohteita tapaustutkimukselle, tulisi vaihtoehtojen olla enemmän valmiiksi mietittyjä kuin vain tilaisuuksiin ja mahdollisuuksiin tarttuvia. Alussa olisi tärkeintä määritellä tutkimusta rajoittavat tekijät sen perusteella mitä ollaan tutkimassa ja miksi. Myös suhteita voi käyttää avuksi sopivien tapausten kokoamisessa, mutta se ei saisi olla niiden lähtökohtana. Tuntemattomien tavoittelu on kuitenkin aina hieman vaativaa. Salassapidon tärkeyttä ei voi korostaa liikaa potentiaalisille kohteille. Tutkimuksesta kun ei ole tarkoitus olla heille välillistä eikä välitöntä haittaa missään muodossa. Yrityksille voidaan tarjota mahdollisesti myös näkyvyyttä nimeämällä se tutkimusaineistossa. Tapaus voidaan käsitteenä tulkita monella eri tavalla, mutta tässä

työssä, sillä tarkoitetaan yksittäistä, valikoitua yritystä. Vaikka tapauksena käsitellään koko yritystä, on tarkemman tarkastelun alaisena sen tietoturvallisuuteen liittyvät osat ja kokonaisuudet. Tässä pyritään huomioimaan myös haastateltavan henkilön omat kokemukset ja positio kyseisessä yrityksessä, jos sillä uskotaan olevan vaikutusta tulkintoihin. (Yin 1984.)

## 4.2 Tutkimuskohde ja tutkimuksen rajaus

Tutkimusempirian kohteena olivat suomalaiset pienet ja keskisuuret yritykset. Otanta oli pieni, mutta samalla monipuolinen. Tavoitteena oli saada edustajia erilaisista yrityksistä, joissa on erilaisia määriä työntekijöitä ja siinä onnistuttiin. Tarkoituksena oli pyrkiä löytämään näistä joko yhteneväisyyksiä keskenään tai mahdollisia erottuvia tekijöitä, joita voisi erikseen nimetä. Tutkimuksessa pyrittiin mahdollisesti tunnistamaan myös erilaisia tasoja eri yritysten tietoturvakäsitysten välillä. Tutkimuskohteet olivat ennalta tuntemattomia yrityksiä, jotka toimivat toisistaan myös poikkeavilla liiketoiminnan osa-alueilla. Haastatelluilla henkilöillä oli jonkintasoinen johtoasema yrityksessä ja osalla heistä oli aiempaa teknistä taustaa, mutta osalla ei. Yritysten oletetuissa maturiteettitasoissa oli myös havaittavissa eroja jo ennen varsinaista aineiston keräämistä. Tietosuojasta ei keskusteltu osana haastattelua sen tarkemmin, ellei se noussut luonnollisesti puheenaiheeksi. Kohteille korostettiin salassapitovelvollisuutta ja sitä, kuinka aineisto tullaan anonysoimaan, eikä osallistuva yritys ole siten vastausten perusteella enää tunnistettavissa lopullisessa työssä lainkaan.

## 4.3 Tutkimusaineisto ja sen keräys

Tutkimusaineisto kerättiin Suomessa, Turussa, osana ICT-Portin, Work Informaticsin & Turun yliopiston tilattua tutkimusta ”APT - ’Have you ever seen the threat?’” vuonna 2015 (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015). Aineistoa käytetään nyt tässä tutkimuksessa tarkemmin rajattuna. Tutkimusaineiston keräysmenetelmänä käytettiin puolistrukturoituja teemahaastatteluja (Hirsjärvi & Hurme 2001), joita tehtiin kaikkiaan kuusi kappaletta. Haastatteluja ei nauhoitettu, mutta ne suoritettiin parihaastatteluina, joissa toinen parista haastatteli ja toinen kirjasi samalla muistiinpanoja vastauksista ylös. Nämä vastaukset koostettiin haastattelun jälkeen yhtenäiseksi näkemykseksi yrityksestä. Kysymyksissä ja niiden järjestyksessä noudatettiin varovaisuutta johdattelussa sekä ne jätettiin yleisesti puoliavoimiksi. Kysymyksiä ei toimitettu etukäteen haastateltaville ja haastattelun ilmoitettiin olevan yleispätevä eikä vaativan mitään esivalmistelua haastateltavalta. Kysymykset muotoiltiin

englanniksi mahdollisia kansainvälisiä yrityksiä varten, mutta lopulta kaikki haastattelut suoritettiin kuitenkin suomeksi. Varsinaisia haastatteluja ei ole litteroitu jälkikäteen vaan haastattelun aikana syntyneistä muistiinpanoista luotiin johdonmukainen ja yhtenevä kertomus parityönä heti haastattelun jälkeen, jotta mahdolliset aukkokohdat saatiin tällöin täytettyä mahdollisimman pian mahdollisimman todenmukaisesti. Haastattelutilaisuus pyrittiin pitämään kaikille osallistuneille ilmapiiriltään samanlaisena rennon virallisena. Haastateltavat saivat myös esittää halutessaan kysymyksiä ja kommentteja, ne kirjattiin myös ylös osaksi kerättyä aineistoa. Haastattelijat sekä haastateltavat henkilöt olivat ennestään toisilleen tuntemattomia.

Haastattelukysymykset löytyvät teemoineen kokonaisuudessaan liitteestä A. Haastattelu aloitettiin taustatietojen selvittämisellä. Varsinaiset tutkimukseen liittyvät kysymykset jaettiin selkeyden vuoksi kolmeen eri pääteemaan: 1) infrastruktuuri, 2) tiedonhallinta sekä 3) APT-hyökkäysmenetelmä. Järjestyksen oli tarkoitus myös ohjata haastateltavaa oikeansuuntaiseen keskusteluun alusta asti. Keskusteluteemaa vaihdettiin luontevasti, mutta silti oikeassa aihepiirissä pysytellen. Haastattelut järjestettiin ajalla 1.2.2015– 22.4.2015. Tuloksia tulkitessa on tärkeää muistaa haastateltavien edustavan pääasiassa yritysten ylintä johtoa sekä sisältävän heidän henkilökohtaisia mielipiteitä. Haastateltavina toimivat seuraavilla nimikkeillä toimivia henkilöitä: toimitusjohtaja, toiminnanjohtaja, tietohallintojohtaja sekä palkkatyöntekijä. Yritykset olivat pääasiassa päätoimisia IT-yrityksiä Turusta, mutta mukana oli myös eräs asianajotoimisto sekä jälleenmyyntiin keskittynyt verkkokauppa. Nämä valitut yritykset olivat kokoluokaltaan mikroyrityksistä keskisuuriin yrityksiin lukeutuvia eli työntekijämäärältään < 250 henkeä.

Koska osa kysymyksistä oli lähellä yrityksen liikesalaisuuksia, korostettiin haastattelutilaisuuden luonnetta täysin luottamuksellisena. Aineistoa kerättäessä otettiin huomioon myös mahdollisuus annettujen tietojen ”kaunistelusta” osana yrityksen oman maineen vaalimista.

## 4.4 Haastatteluista

Tästä osiosta löytyvät suorittujen haastattelujen läpikäynnit. Yritykset ovat listattuna sattumanvaraisessa järjestyksessä, eivätkä esimerkiksi haastattelujen ajankohdan mukaan aikajärjestyksessä.

### *4.4.1 Yritys A*

Kyseessä on pieni yritys aiemmin mainitun luokittelun perusteella. Yritys on perustettu 2011 ja aloitettu yhden yrittäjän voimin, jolla oli takanaan kattava ura IT-alalta. Yrityksen päätuote on ulkoistettu tietohallintojohtaja -palvelu, jossa pienet/mikrokoon yritykset voivat vuokrata tarvittavia palveluja itselleen tältä yritykseltä – näin ollen tarjoten mahdollisimman kokonaisvaltaisen kokemuksen. Heidän oma infrastruktuurinsa on rakentunut pitkälti pienten palasten muodostamaksi kokonaisuudeksi, yrityksen toimitusjohtaja on käsin valinnut sopivimmat työkalut jotka mahdollistavat myös tasaisen kasvualustan yritystoiminnalleen. Tämä ei kuitenkaan tarkoita, etteikö heille mahtuisi uusiakin tuotteita käyttönsä aina tarpeen mukaan – työntekijät itse saavat vaikuttaa tähän niin halutessaan. Haastateltava tosin ihmettelee ääneen, kuinka vaikeaa jopa heillä, IT-asiantuntijoina, on valita sopivia järjestelmiä itselleen ja kuinka hankalaa sen on oltava toisten toimialojen asiantuntijoille, joilla ei välttämättä ole lainkaan kyseisen (IT) alan kokemusta. Hän tuo sivulauseessa ilmi, olevansa huolissaan aggressiivisista myyvistä IT-osaajista, tietämättömät voivat ostaa heiltä palveluita tietämättä paremmasta ja samalla satuttaen omaa yritystään enemmän kuin uskoivatkaan yksinkertaisella valinnalla. He ovat hänen mukaansa osa suurempaa, alustasidonnaista yhteistyöverkostoa, jossa heillä on sopimusteknisesti varmistettu (myös asiakkaidensa) liiketoiminnalle kriittisen datan pysyvän tallessa ja suojassa – jos yhden tiedot vuotaisivat, olisivat myös muiden verkoston jäsenten tiedot vaarassa. Haastateltavan mukaan he jakavat myös verkoston muiden jäsenien kanssa saman kehitysympäristön, joka on tarkoitettu erilaisten toimintojen testaukseen tarpeen mukaan. He siis pyrkivät tarjoamaan verkoston kautta kyseiselle alustalle mahdollisimman kattavan osaamisen yhtenä osana liiketoimintasuunnitelmaansa.

Haastateltavan mukaan, heillä ei ole yrityksenä mitään sen tarkempia sovittuja käytäntöjä (kirjallisia/kirjoittamattomia) liittyen varsinaiseen tiedon käsittelyyn ja sen varsinaiseen hallintaan. He käyttävät kuitenkin asiakaskohtaisten, myyntiin liittyvän tiedon tallentamiseen erillistä asiakkuudenhallintajärjestelmää (CRM), joka sijaitsee erillisellä palvelimella (ei kuitenkaan toimi pilvipalveluna). Se on samalla ostettu ulkopuolinen palvelu myös heille itselleen. Nämä tiedot eivät kuitenkaan tällä hetkellä ole Suomessa mutta tähän on lähiaikoina tarkoitus tulla muutos asiakkaidensa pyyntöjen perusteella. Haastateltava puhuu myös siitä, kuinka helppoa olisi, jos kaikki tiedot olisivat yhdessä ja samassa järjestelmässä, myös niiden suojauksen kannalta. Mainittakoon, ettei tässä yhteydessä, osana haastattelua, tule puheeksi kuinka iso riski yhden ison järjestelmän vaarantuminen olisi – haastateltava ei mainitse itse asiasta mitään osana tätä vastausta.

Haastattelukohde ei ole koskaan kuullut APT-hyökkäysmenetelmästä aiemmin, tai siitä, mikä juuri sille on tyypillistä ja tekee siitä vaarallisen. Hän ei ole tietoinen mistään

hyökkäyksistä yritystään kohtaan – näitä ei ole tullut esiin edes kahvitaukokeskusteluissa muiden työntekijöiden kanssa. Hän ei kuitenkaan vaikuta olevan huolissaan esitetystä hyökkäysmenetelmästä, vaikka se on hänelle ennalta tuntematon ja nyt selitetty auki. Tosin, käy ilmi, että hänellä on epäily vanhalla työnantajalla tapahtuneesta onnistuneesta phishing-hyökkäyksestä (eli huijaushyökkäyksestä) – mutta siitäkään ei ollut koskaan mitään konkreettista ja sen käsittely jäi vain huhupuheiden tasolle. Kyseisen tapauksen aiheuttamista mahdollisista vahingoista hän ei myöskään ollut tietoinen. Haastateltava epäilee tämän johtuvan siitä tosiasiasta, että yrityksen kaikki työntekijät ovat kokeneita tietoalan ammattilaisia mutta samalla tuumailee sen puolesta, että tämän luonteisia (tarkoittaen arkaluontoisia) asioita ei ”kerrota edes omalle vaimolle”. Hän myöntää, ettei yritys aktiivisesti työskentele tietoturvallisuuden takaamisen puolesta ja uskoo sen johtuvan oman tietotaitonsa puutteesta – samalla kuitenkin todeten tietoturvan kiistattoman sekä suuren merkityksen myös heidän yritystoiminnalleen. Hän toteaa ehkä olevan tarve tehdä jotakin myös heidän tietoturvalleen mutta ei pysty sanomaan varmaksi mitä se jokin olisi. Tämänkaltaiset ajatukset ovat haastateltavan omien sanojensa mukaan enemmänkin ”takaraivossa”, tarkoittaen niiden vaivaavan mieltä tasaisin väliajoin mutta ei jatkuvasti. Myöhemmin keskustelussa nousee vielä esiin haastateltavan omatoiminen mietintä siitä, kuinka pieni yritys he ovat ja sitä kautta loogisesti ääneen päätellen, kuinka he eivät sitä kautta hänen mielestään ”voi olla potentiaalinen kohde hyökkäyksille”.

### *4.4.2 Yritys B*

Kyseessä on pieni yritys, jonka omistaa isompi. Yritys keskittyy myymään kuluttajille sekä toisille yrityksille IT-tuotteita, heillä on niin ikään verkkokauppa kuin oma kivijalkamyymäläkin (joka sisältää samalla verkkokaupan vaatiman varaston sekä logistiikan). Heillä ei ole lähitulevaisuuden tavoitteissa muuttaa kauppaansa globaalimmaksi, kotimaan markkinat riittävät tällä hetkellä hyvin. He pitävät tärkeänä myös pelaamiskulttuuriin osallistumisen ja tekevätkin sitä aktiivisesti, se on iso osa markkinointia. Verkkokauppa on sijoitettuna pilvipalveluntarjoajalle mutta muuten yrityksen käyttämät järjestelmät tarjoaa (ja samalla sanelee) sen omistama emoyhtiö, tämä tarkoittaa kuitenkin käytännössä yhtä ja samaa palveluntarjoajaa kaikkiin tarvittaviin palveluihin. Hän mainitsee emoyhtiöllä olevan itserakennettu ERP-järjestelmä, jota myös he hyödyntävät osittain. Tämä tarkoittaa myös sitä, että kaikki tämäntyyppiset tekniset henkilöt ovat emoyhtiössä töissä eivätkä suoraa heillä itsellään koska tarvetta siihen ei synny. Ulkopuolisia toimittajia heidän tapauksessaan ei haastateltavan mukaan ole eikä ole tarkoitus tulla – hän puhuu myös vahvasti siitä, kuinka ylpeydellä he ”tekevät ja opettelevat itse, jotta saadaan varmasti hyvä laakista”.

Kysyttäessä haastateltava on kuitenkin sitä mieltä, että tarvittaessa ulkopuolisia toimijoita voitaisiin hyödyntää eli mitään ehdotonta tähän ei liity.

Yritys jatkokehittää itse omaa verkkokauppaansa eli he eivät osta kyseistä palvelua ulkopuolelta vaan heillä on omat ohjelmoijat palkkalistoillaan tähän tarkoitukseen. Käyttöoikeuksien rajoittaminen onkin helppoa tämän ansiosta, vain heillä on ylimmän tason järjestelmänvalvojan oikeudet. Järjestelmä onkin räätälöity juuri heidän tarpeisiinsa ja sitä kehitetään yrityksen kasvun ehdoilla. Yrityksellä on tarve useampaan extranet-tyyppiseen palveluun oman kaupankäyntinsä luonteen vuoksi. He tarvitsevat jokaiselle eri kanavan toimittajaan ja mahdollisesti jopa jälleenmyyjään yhteydenpito tavan joka on samalla kaksisuuntainen, sähköposti ei tule tässä haastateltavan mukaan kysymykseenkään. Kaikki hintaneuvottelut sekä tuotetiedotteet käsitellään näissä palveluissa. Haastateltava esittää hyvin itsevarmasti kuinka hyvin he ovat hajauttaneet liiketoiminnalle kriittisen datan. Heillä on oma välijärjestelmänsä tilauksiin liittyville maksuille sekä tilauksille ja niitä tilanneille – kokonaisuus on pyritty kasaamaan mahdollinen tietovuotomahdollisuus mielessä. Kaikkien järjestelmien välinen liikennöinti on haastateltavan mukaan ”salattu alan nykystandardien mukaan”. Haastateltava toteaa myös tietoturvan olevan selkeä osa heidän asiakassuhdetta.

Verkkokaupan palvelin on vielä erikseen teknisesti viritetty huomaamaan poikkeavuuksia sisäisessä toiminnassaan ja ilmoittamaan niistä eteenpäin, mahdollisen tietoturvaloukkauksen merkeissä. Kauppa itsessään tarkkailee myös mahdollisia ”outoja” tilauksia, ilmoittaen niistä tarvittaessa eteenpäin. Näin pyritään estämään muun muassa identiteettivarkauksien aiheuttamia hankaluuksia. Haastattelun kohde ei myöskään koe palvelunestohyökkäyksiä suureksi uhaksi – hän samalla myöntää heillä niitä olleen muutamia mutta taloudellisen haitan jääneen niin pieneksi ettei ”sillä ole merkitystä isomman kuvan kannalta”. Heillä on tällaisen hyökkäyksen varalta myös toimintasuunnitelma, jonka avulla palvelukatkoksen kesto pyritään minimoimaan ja asiakkaan kaupankäynti pitämään mahdollisimman sujuvana. Yleisesti ottaen yrityksen käyttämät järjestelmät (olivat ne sitten heidän omiaan tai heidän emoyhtiönsä omistamia) pyörivät ”lokaalisti” eli he eivät ainakaan vielä hyödynnä pilvipalveluita.

Haastateltavan voidaankin todeta tietävän, sekä ymmärtävän, keskitasoa enemmän tietoturvallisuudesta ja siihen liittyvistä tekijöistä. Hän kertoo myös tiedostavansa ”inhimillisen tekijän” myös omien työntekijöidensä keskuudessa – virheitä voi aina sattua. Hän mainitsee yhdeksi kyseenalaiseksi käytännöksi joidenkin työntekijöiden tavan käyttää toisen tunnuksia nopeuttaakseen jotakin työtehtävää, asia joka on kuitenkin kuulemma jo hoidossa ja aktiivisesti seurannassa. Yritykseltä löytyy myös toimintaohjeet (kirjalliset) kadonneiden laitteiden kanssa toimimiseen, niiden sammuttamiseen sekä etäpyyhintään tarvittaessa. Haastateltava nimeää oman yrityksensä heikoimmaksi kohdaksi jo aiemmin mainitun inhimillisen tekijän mutta uskoo huolellisen suunnittelun järjestelmien jatkokehityksessä/valinnassa minimoimaan sen vaikutukset itse

liiketoimintaan. Käytettyjen järjestelmien haavoittavuuksia seurataan aktiivisesti ja niihin reagoidaan yrityksen omien ohjelmoijien toimesta tarvittaessa. Haastateltava myöntää kuitenkin aiemmin olleen muutamia tapauksia, joissa on epäilty ex-työntekijöiden vieneen yrityksestä lähtiessään mukanaan jotakin sellaista dataa, joka heille ei kuuluisi. Nämä ovat kuitenkin hänen mukaansa jääneet muutamiksi ja harvoiksi poikkeustapauksiksi – käyttöoikeuksia heidän eri järjestelmiin on myös tämän jälkeen kiristetty vastaavan varalta.

Käännettäessä haastattelu varsinaisen APT-hyökkäysmallin suuntaan, ei haastateltava koe tätä erityisesti heille sopivaksi skenaarioksi. Hän ei ole aiemmin kuullut juuri tätä nimitystä mutta tunnistaa osia siitä vakavina ja samalla potentiaalisina hyökkäysvektoreina. Keskustelun lopputuloksena vaikuttaa siltä, ettei haastateltava koe kuitenkaan heitä sopivaksi kohteeksi tälle hyökkäystavalla. Hän alleviivaa myös erikseen sitä, kuinka heillä on aina pidetty arkkitehtuurisena lähtökohtana nimenomaan eristämistä, jonka pitäisi auttaa myös näissä kuvatuissa hyökkäystavoissa. ”Kun toimari [toimitusjohtaja] nukkuu yönsä rauhassa, on kaikilla muillakin mukavampaa.”

### *4.4.3 Yritys C*

Kyseessä on keskisuuri yritys, jolta löytyy toimistot kaikista Suomen suurimmista kaupungeista sekä ”hieman toimintaa myös ulkomailla”. Heidän päätoimipaikkanaan toimii kuitenkin Turku. Noin neljäsosa henkilökunnasta on haastateltavan mukaan teknistä taustaa omaavia. Turussa on selkein jaottelu roolituksessa, tekniset henkilöt ovat eroteltuna myyjistä. Yrityksen päätoiminta painottuu IT-ratkaisuiden tarjoamiseen toisille yrityksille mutta myös julkiselle sektorille. Pääasiassa tämä käsittää arkkitehtuurin sekä infrastruktuurin, kyse voi olla muutaman tietokoneen pientoimistosta tai useamman tuhannen tietokoneen suuryrityksestä – he hoitavat näitä kumpiakin. He ovat määritelleet asiakkailleen kiinteän kuukausittaisen hinnan joka laskutetaan työmäärästä riippumatta.

Haastateltava kertoo heidän käyttämien palvelinten muodostavan niin kutsutun ”palvelinfarmin”, joka sijaitsee yhdessä ja samassa paikassa. Sen avulla he pystyvät etäkäyttämään kaikkia tarvitsemiaan sovelluksia, joita palvelimilla erikseen pyörii. Tämä sisältää palveluita kuten dokumentinhallinta sekä palvelupyynnöt ja niiden käsittely. Heillä on käytössään myös perusmuotoinen asiakkaanhallintajärjestelmä, jota he pitävät ajan tasalla mutta joka aiheuttaa ongelmia suuremmissa asiakkuuksissa – niiden tietoja säilytetään myös eräässä toisessa järjestelmässä eivätkä nämä järjestelmät ole integroituina toisiinsa muuten kuin manuaalisesti. Tämän tiedon päivittäminen on täten työlästä ja virhealtista. Haastateltavan mukaan he ovat itse jatkokehittäneet jotakin vanhaa järjestelmää ja kutsuvat sitä nyt ”kotikutoiseksi SAP-järjestelmäksi” joka toimii kuitenkin kaiken ytimenä.

Pilvipalveluina he hyödyntävät ainoastaan työajanseurantaan sopivaa ulkoista palvelua sekä yrityksen viestintää tarkoitettua Yammeria (Microsoftin tarjoama palvelu, toimii pilvessä). Haastateltavan mukaan ylin johto tahtoisi hyödyntää pilvipalveluja enemmänkin mutta työntekijät ovat tätä muutosta vastaan. Pilvipalveluiden luotettavuus on kuulemma ongelma heidän mielestään. Näissäkään kummassakaan mainitussa pilvipalvelussa ei säilytetä eikä käsitellä arkaluontoista materiaalia eikä lainkaan asiakasdataa. Haastateltavan mukaan osa heidän asiakkaista on myös vaatinut osaksi sopimustaan ehdon, ettei heitä koskevaa tietoa saa lähteä Suomen rajojen ulkopuolelle. Yrityksen omasta mielestä tämäkin ajaa heidät hyödyntämään jatkossakin omia palvelimia ja palveluita, jotka sijaitsevat täysin Suomessa ja ovat heidän omassa hallinnassaan. Yrityksen omat kotisivut on myös ulkoistettu pois heidän omasta hallinnastaan.

Yrityksellä ei haastateltavan mukaan ole käytössä mitään selkeitä käytäntöjä tai ylös kirjattuja ohjeita liittyen tietoturvaan, hän kuitenkin toteaa, että tietoturvasta keskustellaan melko tasaisin väliajoin yritystoimintaan liittyen. Yrityksellä ei hänen mukaansa ole ollut mitään vakavia ongelmia tietoturvaan liittyen ja toteaa ”löysän kontrollin johtuvan ehkä juurikin siitä” mitä yrityksen tietoturvakäytäntöihin ja niiden puuttumiseen tulee. Haastateltava toteaa myös pelkäävänsä miten lisääntynyt byrokratia, mitä korkeampi yrityksen tietoturvan taso hänen mukaan seuraisi, vaikeuttaisi hänen ja hänen työkavereidensa jokapäiväistä työnsujuvuutta. Hänen mukaansa yrityksen järjestelmien ylläpitäjät ovat tehtäviensä ajan tasalla ja päivittävät järjestelmiä aktiivisesti, silloin kun se on tarpeellista.

Tärkeintä tietoa heidän asiakkaistaan on hänen mukaansa järjestelmien toimintojen kuvaukset, tietovuokaaviot sekä yleiset arkkitehtuurikuvat, joita jo suunnitteluvaiheessa on aktiivisesti tehty ja dokumentoitu talteen. Käyttöoikeudet yleisesti säilytettävään dataan ovat hyvinkin rajoitetut, ylimääräiset ihmiset eivät näe heille kuulumatonta tietoa lainkaan. Haastateltava nimeää myös heidän varmuuskopiot erittäin kriittisiksi liiketoiminnan jatkuvuuden kannalta. Myös heidän asiakkaidensa järjestelmien käyttäjätunnukset ja salasanat ovat korkealla prioriteetilla hänen mielestään. Hän toteaa samalla, ettei heidän järjestelmien varsinainen valvonta ole niin yksityiskohtaista kuin he tahtoisivat ja että tähän olisi pian tulossa muutos.

Haastateltava ei ole kuullut termiä ”APT” aiemmin. Kun kyseinen termi selitetään ja sen sisältö avataan, tunnistaa hän heille todennäköisimmän hyökkäysvektorin olevan inhimillinen virhe muodossa tai toisessa. Hänestä (onnistunut) hyökkäys ulkoverkosta ei ole todennäköinen koska ”heidän verkko on suunniteltu sitä ajatellen”. Tietoturvasta on yrityksessä nimetty vastaamaan kaksi henkilöä yhdessä, tämä muuttui hiljattain neljäksi erään asiakkaan vaatimuksesta. Haastateltava on jonkin verran seurannut mediassa liikkuneita uutisia suurista tietoturvahyökkäyksistä ja niitä tekevistä hakkeriryhmistä mutta ei pysty niitä suoraa nimeämään. Hänestä yleisesti ottaen Suomessa on

tietoturvaosaaminen yksittäiselle työntekijällä erittäin hyvällä tasolla verrattuna ”oikeastaan mihin tahansa muualle päin maailmaa”. Lopuksi haastateltava toteaa yrityksensä tietoturvan vain parantuvan ajan myötä, kun osaamista ja tietotaitoa tulee lisää.

### *4.4.4 Yritys D*

Kyseessä on pieni yritys, jonka päätoimipaikka on Turku. He ovat vasta laajentamassa Helsinkiin mahdollisuuksien mukaan. Heidän päätoimena on tuottaa asiakkailla erikokoisia ja -tyylisiä verkkopalveluita tarpeiden mukaan. He tekevät niin ikään verkkosivuja kuin myös verkkokauppoja. Asiakkaat saavat itse valita missä heidän palvelua pyöritetään, on se sitten palvelinsali Suomessa tai ”halvin mahdollinen pilvipalvelu maailmalla”.

Heillä on haastateltavan mukaan vielä muutamia palveluita pyörimässä heidän ”ikiomassa palvelinkopissa” mutta tarkoitus on siirtyä pilvipohjaisiin palveluihin täysin, jos se vain todetaan mahdolliseksi liiketoiminnan puitteissa. Eli kyseessä on käynnissä oleva muutos. Esimerkiksi kaikki myyntiin liittyvä materiaali (sopimuksia myöden) on vielä paikallisesti tallennettuna mutta kaikkien ylläpidettävien asiakastöiden varmuuskopiot taas menevät jo pilveen talteen (vieläpä kryptattuna) – tähän yrityksellä ei kuulemma ole kiire saada aikaiseksi muutosta. Kaikki yrityksen työntekijät ovat kuitenkin lähtökohtaisesti teknisiä henkilöitä, joten yrityksen IT-maturiteetti voidaan olettaa olevan suhteellisen korkea. Haastateltavan mukaan pääasiallisesti vastuussa on heidän teknologiajohtajansa (CTO) mitä tietoturvaan tulee mutta mainitsee myös muiden osakkaiden olevan vastuussa ja sitä kautta heidän tulisi olla kiinnostuneita yhtä lailla yrityksen tietoturvan tilasta ja sen toteutumisesta vaaditulla tasolla.

Haastateltava kertoo heidän yrityksellään olevan useampia yhteistyökumppaneita, joita hyödynnetään aina tarpeen mukaan. Näillä yhteistyökumppaneilla ei kuitenkaan ole mitään asiaa heidän sisäisiin järjestelmiin vaan kommunikaatio hoidetaan lähinnä sähköpostitse ja puhelimitse siltä osin mitä on tarvetta. Hän kertoo samalla, ettei yrityksellä ole suoranaisia käytäntöjä mitä tietoturvaan tulee vaan työntekijöiden oletetaan ”pärjäävän maalaisjärjellä” kuten kotonakin. Joitakin yhteisiä ohjeistuksia kuulemma löytyy mutta niiden tarkkuus ei selviä haastattelun aikana. Mitään keskitettyä hallintaa laitteistolle ei myöskään löydy, eikä sitä ole ostettuna myöskään ulkopuolelta. Työntekijöiden oletetaan itse tietävänsä mitä tarvitsevat ollakseen ”tietoturvallisia”. Haastateltava pitää itse erityisen tärkeänä sitä, ettei hänen koneelleen asenneta yrityksen toimesta mitään ylimääräistä joka ”vain estäisi tehokasta työntekoa”.

Yritykselle selkeästi kriittisin data on asiakastiedot, mukaan lukien myös niihin liittyvät käyttäjätunnukset ja salasanat. Myös kaikki myyntiin liittyvä materiaali todetaan

olevan tärkeä (jopa elintärkeä) osa yrityksen saavuttamaa kilpailuetua ja sen ylläpitämistä jatkossakin. Varmuuskopioinnin myötä myös niiden sisältämä, asiakkaan omistama, tieto voidaan olettaa olevan arvokasta ja tästä syystä se on haastateltavan mukaan myös kryptattua – hän toteaa samalla salausavainten olevan täten myös erittäin tärkeässä asemassa. Haastateltava joutuu myös myöntämään, ettei heillä ole varsinaista liiketoiminnan jatkuvuussuunnitelmaa tietoturvaloukkauksien varalta.

Termi ”APT” ei ole ennestään tuttu. Heillä ei ole haastateltavan omien sanojen mukaan ollut ongelmia kadonneen laitteiston/laitteiden kanssa tai sosiaalisen hakkeroinninkaan osalta. Haastateltavan mukaan he ovat liian pieniä tällaisiksi kohteiksi juuri nyt, tulevaisuudesta hän ei ole yhtä varma. Hän ei mielestään osaa edes nimetä yhtäkään suoranaista kilpailijaa, joka voisi hyötyä heiltä saadusta datasta liiketoiminnallisesti. Yrityksen henkilöstömäärä on niin pieni, ettei sinne ole mahdollisuutta kenenkään ”väärätahtoisen ihmisen vahingossa eksyä” – kaikki siis tuntevat kaikki. Jos (ja kun) yrityksen henkilöstömäärä kasvaa, haastateltava itse toteaa kasvavan tarpeen organisoitumiselle myös tietoturvan kannalta ja konkreettisten käytäntöjen sekä ohjeiden luonnin. Kun nämä käytännöt on luotu, otetaan ne myös ”oikeasti sitten käyttöön”. Haastateltava ei osaa kuitenkaan erikseen nimetä kenen vastuulle näiden käytäntöjen kirjoitus ja toimeenpano käytännössä tulee olemaan.

Haastateltava kertoo, ettei heidän yritystään vastaan ole suoranaisesti koskaan hyökätty mutta, että he ovat joutuneet selvittämään asiakkaidensa puolesta muutamia hakkerointitapauksia. Hän kuvailee tämän liittyvän lähinnä verkkopalveluiden ”sotkemiseen” tai alasajoon. Näissäkin tapauksissa kyse on kuulemma ollut asiakkaan omasta huolimattomuudesta ja vastuuttomuudesta. Tapaukset ovat myös olleet nopeita selvittää ja palauttaa normaalitilanne takaisin ilman sen suurempaa dramatiikkaa. Haastattelun lopussa keskustellaan vielä yleisesti tietoturvapäivitysten tarpeellisuudesta ja haastateltava toteaa heidän tarvitsevan todennäköisemmin vielä lisää monitorointia tämän suhteen asiakkaidensa palvelujen suuntaan.

### *4.4.5 Yritys E*

Kyseinen yritys on kokoluokaltaan mikroyritys ja heidän päätoimipaikka on Turussa. Heidän päätoimintaa voisi kuvata IT-huolloksi mutta unohtamatta siihen liittyvää konsultaatiota. Koska heidän työkuormituksensa on hyvin vaihtelevaa, hyödyntävät he aktiivisesti opiskelijoita osana työvoimaa ja pyrkivätkin haastateltavan mukaan vaikuttamaan positiivisesti jo tulevan tietotyön ammattilaisen ajatusmaailmaan. Heillä on asiakkaita suuruusluokassa laidasta laitaan, on isoja sekä pieniä.

Haastateltavan mukaan heidän kokemus eri toimijoiden tietoturvaosaamisesta on hyvin kirjavaa ja vaihtelevaa – hän mainitsee erityisesti terveydenhuollon olevan

”erityisen haasteellinen mitä hyviin tietoturvakäytäntöihin tulee”. Hän avaa tätä lausahdusta toteamalla vain erityisesti liimattavien muistilappujen olevan kovassa käytössä käyttäjätunnusten ja salasanojen osalta, vaikka kuinka neuvoisi tätä vastaan. Nämä käytännön kokemukset ovat haastateltavan mukaan saanut heidät tietoturvallisesti hieman ”varpailleen” ja ajattelemaan jopa hieman ylisuojelevasti omaa tietoturvaansa ja sen tärkeyttä osana liiketoimintaa.

Yrityksessä on kirjavasti käytössä sekä PC että Mac -tietokoneita. He käyttävät myös paljon vapaasti käytettävissä olevia ilmaisohjelmistoja (lähtökohtaisesti siis avoimen lähdekoodin toteutuksia), myös pilvitallennustilaa sen osalta joka ”ei siis maksa mitään”. Tämä tarkoittaa sitä, että pilvipalveluissa on myös yrityksen tietoja. Haastateltava ei ole tästä lainkaan huolissaan vaan hehkuttaa kuinka helppoa on päästä käsiksi tietoihin nopeasti ja vaivattomasti kun niitä on ripoteltuna hieman eri palveluissa tarpeen mukaan. Hänestä hän on näin ”valmistautunut selviämään mistä tahansa laiterikosta”. Heidän laitteistojen tallennustilat ovat pääsääntöisesti salattuja.

Haastateltava arvioi oman yrityksensä IT-maturiteetin oleva keskitasoa korkeampi koska ongelmanratkaisu ja konsultaatio eivät ole helppoja toimialueita (nämä ovat siis heille yrityksenä toimimisen päätoimialat). Hänen mukaansa heillä ei ole jaettuja järjestelmiä minkään toisten tahojen kanssa. Kaikessa heidän käyttämässään laitteistossa on huomioitu etäpyyhinnän tarve ja mahdollisuus. Haastateltavan mukaan yrityksellä on heidän työnsä luonteen takia myös erillinen, täysin ”eristetty” verkko, jossa käsitellään asiakkaiden laitteistoja – näin ollen heidän yrityksen verkko pysyy niistä myös fyysisesti erillään. Hänen mukaansa näin estetään muun muassa virusten hallitsematon leviäminen, jos sellainen tietokone tulee heille huollettavaksi.

Omasta mielestään haastateltava on hyvin ajan tasalla tietoturvan sekä myös yleisesti tietotekniikan trendien osalta. Hän mainitsee ”olleensa netissä niin kauan kuin se on ollut Suomessa” eikä koe tarvetta luopua tästä saavutuksesta. Omien sanojensa mukaan hän (ja hänen yrityksensä) kokee olevansa paremmin suojassa kuin yleisesti ottaen vastaavat yritykset. Se vaikuttaa siis olevan tärkeä osa arkipäivän liiketoimintaa tämän perusteella. Heillä on myös käytössä protokolla turhien paperien tuhoamisesta koska he luottavat pilvessä olevaan tietoon haastateltavan mukaan. Vaikkakaan näistä hyvistä käytännöistä ei ole haastateltavan mukaan koottuna varsinaista selkeää, erillistä ohjeistusta, ”tietävät kaikki mitä tehdä” eli sisäinen luottamus eri ammattilaisten välillä vaikuttaa vahvalta.

Haastateltava kertoo kuitenkin lopuksi heidän joutuneen yhden (tietoturva)hyökkäyksen kohteeksi. Kohteena kyseisellä kerralla toimi heidän Googlessa olevat mainokset (Google AdWords-palvelu). Yhtäkkiä he huomasivat heidän sivustokäyntien vähentyneen huomattavasti Googlen suunnalta ja samanaikaisesti heidän palvelussa määrittelemä päiväkohtainen mainostusbudjetti oli käytetty minuuteissa muutamien päivien osalta, näin ei ollut aiemmin tapahtunut ja tämä herätti epäilyksiä. Haastateltava kertoo heidän olleen tämän osalta Googleen yhteydessä, josta vain todettiin

”kaiken olevan ihan kunnossa” ja palauttaneen oudosti kuluneet varat takaisin. Kyseisen hyökkäyksen toteutustapa sekä kaikki muu siihen liittyvä jäi täysin arvailujen varaan eivätkä he yrityksessä edelleenkään tiedä mitä oikeasti tapahtui ja voiko se tapahtua mahdollisesti myös uudelleen. Haastateltavan mukaan tämä ei kuitenkaan jättänyt heille mitään erityisiä ”arpia” tai huonoja kokemuksia edes käytetystä palvelusta. Hän totesi tapahtuneen ”tavallaan kuuluvan tähän alaan” eikä vaikuttanut olevan siitä huolissaan.

### *4.4.6 Yritys F*

Yritys on kokoluokaltaan pieni ja heidän päätoimipaikka sijaitsee Turussa. Toimistoja on yhteensä neljällä eri paikkakunnalla. Heidän päätoimenaan on palvella asiakkaitaan lakiopillisissa asioissa. Asiakkuuksia heillä on pieniä sekä isoja mutta haastateltava toteaa pienempiä asiakkuuksia olevan määrällisesti enemmän kuin isompi – myös muutamia suuryrityksiä löytyy heidän asiakaslistoiltaan. Pääasiassa he toimivat yrityslain kanssa mutta käsittelevät myös muun muassa perintöasioita. Heillä on lähinnä suomalaisia asiakkaita muutamaa amerikkalaista poikkeusta lukuun ottamatta.

Haastateltavan mukaan heidän IT-maturiteettinsa on mahdollisesti keskitasoa alempana. Hänen sanojensa mukaan tähän kysymykseen vastaaminen riippuu keneltä organisaatiosta sitä kysyisi. Hän kokee suurimmaksi haasteeksi sihteerit, jotka käytännössä pyörittävät myös kaikkea arkaluontoista materiaalia, jota heidän liiketoimintaansa kuuluu. Hän mainitsee samalla alan muuttuneen siinä määrin viime vuosina (ja uskoo muutoksen jatkuvan samana), että asianajajat tekevät itse enemmän ja enemmän omia paperitöitään eivätkä delegoi niitä samalla tavalla eteenpäin kuin ehkä ennen. Haastateltavan mukaan jokaisella toimistolla on erikseen nimettynä ”IT-henkilö”, joka on enemmän kyseistä taustaa/kiinnostusta omaava työntekijä – ei siis henkilö, joka olisi palkattu nimenomaan kyseiseen työtehtävään. Vain IT-johtaja on valittu tarkoituksena toimia ”oikeasti myös teknisenä johtajana”.

He ovat valtaosin ulkoistaneet IT-palvelut, esimerkiksi juurikin laitteistojen osalta eli he eivät hallinnoi niitä itse. Haastateltava kertoo heidän myös erittäin äskettäin vaihtaneen vanhat ”lankapuhelimet” uudempaan ja samalla mobiilimpaan toimintamalliin, jonka tarkoitus on tukea yleistyvää mobiilityöntekoa vielä paremmin kuin mitä aiemmin on ollut edes mahdollista. Tämän vaihdoksen myötä heidän mobiililaitteistonsa hallinta siirtyi pilvipohjaiseen palveluun, jonka heidän valitsema operaattori tarjoaa ja samalla myös vastaa sen toiminnasta. Kaikilla työntekijöillä on omat työasemat, valtaosa suosii jo kannettavia tietokoneita mutta silti muutamia työasemia löytyy myös vielä käytöstä. Heillä on omassa sisäverkossaan myös dokumentinhallintaan tarkoitettu palvelin (varmuuskopioidaan kerran viikossa), joka sisältää myös asiakkaanhallintajärjestelmän. Tällä ratkaisulla he pyrkivät siihen, ettei mitään asiakastietoa lähtisi ulospäin heidän

yrityksestään muuta kuin sähköpostimuodossa. Heillä on nyt mobiilityön kasvun myötä kokeilussa Skype, joka mahdollistaisi etätapaamisten pitämistä niin sisäisesti kuin ulkoisestikin. He käyttävät myös joitakin valtion ylläpitämiä sovelluksia jotka liittyvät yritystoimintaan (heidän omaan mutta myös heidän asiakkaidensa). Haastateltavan mukaan heillä oli yrityksen sisällä käytössä myös intranet mutta he pohtivat juuri nyt tulisiko sen alusta päivittää vai luovutaanko sen käytöstä kokonaan.

Haastateltavan mukaan heille on useita kertoja tarjottu pilvipohjaisia palveluja. He ovat kuitenkin yrityksenä päättäneet lykätä vielä niihin siirtymistä, pääsyynä kuulemma ”taloudellisen hyödyn olevan toistaiseksi liian mitätön vaivaan nähden”. Samalla hän toteaa heillä muutaman kerran olleen ongelmia verkkoyhteyksien kanssa toimistoissaan eikä pilvipalvelujen käyttö yhdistettynä verkko-ongelmiin tunnu hyvältä yhtälöltä haastateltavan mielestä. Hänen mielestään heidän kriittisimmät järjestelmä ovat nimenomaan verkkoyhteys sekä puhelinyhteys – ilman niitä heillä ei ole liiketoimintaa. Tämä on johtanut siihen, että he ovat hyvin tarkkoja näiden kumppanien valinnassa, eivätkä ole hevillä valmiita vaihtamaan jo hyväksi todettuja yrityskumppaneita näiltä osin. Sama pätee myös varmuuskopiointipalveluun joka vie tiedot ulkoiselle palvelimelle talteen, johon ei ole pääsyä kuin yhdellä teknikolla yrityksessä joka varmuuskopioinnista vastaa.

Yksityisyys ja luottamuksellisuus ovat heidän liiketoiminnan ytimessä, eikä sitä sovi unohtaa. Jokainen asianajaja vastaa itse teoistaan tai mahdollisesta huolimattomuudesta asianajajien liitolle. Kyseinen taho määrittelee mahdollisen rangaistuksen tai selonteon mitä tapahtuneesta syntyisi. Aiemmin asianajajien liitto on antanut vain ohjeistusta liittyen henkilötietojen turvalliseen käsittelyyn mutta on viime vuosina laajentanut ohjeistusta sisältämään myös tietoturvaan liittyviä asioita – haastateltava pitää tätä pelkästään hyvänä ja toivottuna asiana joka helpottaa myös hänen työtään. Hänen sanojensa mukaan liitto tekee myös välillä pistotarkastuksia, joissa yrityksen on kyettävä esittämään heidän toimivan annettujen ohjeiden ja sääntöjen puitteissa sovitusti. Haastateltava joutuu silti myöntymään heidän vasta harkitsevan VPN-yhteyksien käyttöä sekä työntekijöiden käyttämien laitteistojen muistien salaamista – eli nämä käytännöt eivät vielä ole käytössä yrityksessä. Yleisenä ohjeistuksena kuitenkin on, ettei laitteistoilla saa olla mitään asiakastietoa vaan ne tulisi säilyttää jaetulla dokumentinhallinta-alustalla.

Haastateltavan mukaan heillä ei yrityksenä olisi selkeää liiketoiminnalle kriittistä dataa koska kaikki heidän liiketoimintansa on hyvin henkilöitynyttä yksittäisiin asianajajiin. Hän kuitenkin toteaa kaiken asiakastiedon olevan salaista ja koska kaikilla yrityksen työntekijöillä on siihen pääsy, olisivat he kaikki kootusti vastuussa, jos jotain tämän tiedon turvallisuudelle tapahtuisi. Haastateltava toteaa myös, ettei asianajajan työarkeen kuulu juurikaan tietoturvallisuuden ajattelu. Heillä on tapahtunut muutamia inhimillisiä virheitä mutta mitään selkeää vahinkoa yritykselle ei ole koskaan vielä

tapahtunut näiden osalta. Haastateltava on myös sitä mieltä, että tapahtuneiden ”vahinkojen” luonne on ollut arkipäiväinen ja toteaa ”näitä nyt vain yksinkertaisesti sattuvan aina välillä”. Hän myös toteaa heidän olevan luottamusliiketoiminnassa mukana, mikä tarkoittaisi todellisen hyökkäyksen vahingoittavan suuresti heidän liiketoimintaa koska sellainen tuskin pysyisi salassa – ”nämä piirit ovat kuitenkin pienet”.

Haastateltava ei pidä todennäköisenä heille räätälöityä hyökkäystä tai muutenkaan heitä kohteeksi suurelle hyökkäykselle. Hän toteaa heidän yksinkertaisesti olevan liian pieni hyötyyn nähden tämän osalta. Valtaosa tiedosta on myös heidän työntekijöidensä omassa päässä, joten hän ei usko saatavilla olevien tietojen arvokkuuteen edes kilpailijoilleen. Heille turvallisuutta tärkeämpi tekijä liiketoiminnassa on jatkuvuus – jos jotain tapahtuu, heidän on päästävä nopeasti takaisin jaloilleen jatkamaan liiketoimintaa kuin mitään ei olisi alun perinkään edes tapahtunut. Lopuksi haastateltava toteaa vielä heidän toimivan tietoturvan osalta hieman enemmän reaktiivisesti kuin proaktiivisesti ja jää tämän osalta miettimään tulisiko siihen saada muutosta aikaiseksi.

# 5 EMPIRIAN TULOKSET

Empirian nojalla, joka kerättiin osana Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana (2015) tutkimusta, vaikuttaa siltä, että mitä pienempi yritys, sitä enemmän se kuvittelee olevansa turvassa hyökkäyksiltä. Tämän empirian mukaan yrityksen IT-maturiteetti vaikuttaa myös sen sisäiseen ymmärrykseen tietoturvasta ja sen tarpeesta liittyen yrityksen eri toimintoihin. Vastuunkantajan oma aktiivisuus ja valveutuneisuus on vaikuttava tekijä varsinkin pienemmissä yrityksissä – jonkun on kuitenkin kannettava vastuu. Yleinen mentaliteetti pienemmissä yrityksissä on oletus yrityksen pienuuden ja mahdollisen tuntemattomuuden aiheuttamasta turvallisuuden tunteesta. Hyökkäyskohteina pidettiin lähes yksinomaan tunnettuja ja suuria yrityksiä, poissulkien pienet ja suurelle yleisölle vähemmän tiedossa olevat yritykset. Osa tästä saattaa olla myös tietoista tosiasioiden kieltämistä ja välttelyä. Kyse voi olla myös kunnia-asiasta. Yrityksen tietoturvalle onkin tunnistettavissa erilaisia tasoja ja vaiheita, joita on avattuna tässä työssä. Tässä aiemmin mainitussa tutkimuksessa, jonka osana empiria kerättiin, huomattiin seuraavanlainen jaottelu yrityksen omista näkemyksistä ja ajatuksista omasta tietoturvastaan sekä sen tilanteesta:

1. Meitä kiinnostaa tietoturva ja olemme suojautuneet uhkia vastaan
    - Realistinen maailmankuva
    - Varautuminen muutoksiin
    - Muutoksien kautta nopeasti iteratiivinen toimintatapa

2. Meitä kiinnostaa, mutta emme tiedä mitä tehdä
    - Riittämättömät resurssit (raha, taidot)
    - Valmiiden ratkaisujen hyödyntäminen parempien puuttuessa

3. Meitä kiinnostaa, mutta emme tahdo puhua asiasta enempää
    - Voidaan olettaa tietoturvatapauksia löytyvän historiasta, mutta niistä ei haluta puhua
    - Vaikein tulkita näistä rajallisten tietojen perusteella

4. Emme ymmärrä emmekä tunne olevamme turvassa
    - Vahva ulkoistaminen
    - Sokea uskominen ulkoistuksien toimintakykyyn ja -tasoon
    - Tiedostetaan ongelmien olemassaolo, mutta ei reagoida niihin

5. Ymmärrämme mutta emme ole kiinnostuneita asiasta
    - Ei välttämättä tunnistettua liiketoiminnalle kriittistä dataa

- Ymmärretään tietoturvan olevan tärkeätä mutta todetaan sen koskettavan vain muita

6. Emme ymmärrä emmekä ole kiinnostuneita ymmärtämään
    - Vaarallisin näistä
    - Yrityksen maturiteettitaso (myös IT:n) usein hyvin rajoittunut
    - Kieltäydytään näkemästä todellisuutta mitä tietoturvaan tulee

Vaikuttaa myös siltä, että yrityksen kehittyminen vaiheiden kautta ei tapahdu lineaarisesti vaan joitakin vaiheita saattaa jäädä välistä pois. (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)

Yrityksen eri vaiheisiin voidaan todeta vaikuttavan sekä viralliset että epäviralliset säännöt tai tavat toimia yrityksen sisällä. Yrityksen tietoturvastrategia tai sen puute vaikuttaa myös tähän vaiheiden välillä liikkumiseen. Yleensä tietoturvatapaukset muuttavat toimintaa proaktiivisemmaksi aiemmasta reaktiivisesta mallista, mutta myös tässä voi esiintyä taantumaa. Tätä voidaan estää selkeästi suunnittelulla ja hyvin rakennetulla koulutusmallilla, jolla tietotasoa pyritään pitämään yllä. (Sveen, Torres & Sarriegi 2009.)

Kun haastatteluissa käytiin läpi yritykselle ja sen liiketoiminnalle kriittistä dataa (eli BCI) olivat vastaukset kirjavia. Voisi todeta, että puolet haastatelluista ymmärtävät tämän konseptin ja hyödyntävät sitä osana liiketoimintaansa, mutta toiselle puolikkaalle voisi lisäkoulutus tuoda paremman ymmärryksen saavuttamista. Sitä, mitä ei ymmärrä arvokkaaksi, ei ole mahdollista suojella ja suojata tarpeeksi. Tähän ratkaisuna voisi toimia ulkopuolisen, ehkä jopa ostetun, avun hyödyntäminen.

Pk-yrityksistä ei löydy vielä tarpeeksi intoa pilvipalveluihin siirtymiseen. Haitat koetaan toistaiseksi vielä suuremmiksi kuin varsinaiset hyödyt, joita sillä saavutettaisiin. Mobiilityön hyödyt silti tunnistetaan useammassa haastattelussa, joten sen voitaneen olettaa vaikuttavan pilvipalveluihin siirtymisessä lähitulevaisuudessa. Uskon monen yrityksen harkitsevan pilvipalveluihin siirtymistä osana yrityksen luonnollista kasvuprosessia.

Tämän kerätyn empirian nojalla, voin todeta valtaosan pk-yrityksistä olettavan tietoturvan olevan kunnossa yrityksensä kaikilla osa-alueilla, jos se voidaan todeta toimivaksi yhdessä. Vaikuttaisikin siltä, etteivät yritykset ajattele toimintaansa kokonaisuutena vaan tyytyvät kaikessa hiljaisuudessa uskomaan kaiken olevan ”ihan hyvin” (Reese 2010). Tämä korostaa tarvetta luoda yhteinen ohjelma tai ohjeistus pk-yrityksen työntekijöiden keskuuteen, jotta voidaan sitoutua noudattamaan. Ohjelman tai ohjeistuksen tulee täyttää johdon sille antamat kriteerit. Lähtökohtaisesti pk-yritykset ovat yrityshierarkialtaan matalahkoja tai jopa täysin horisontaalisia (yksitasoinen), jolloin

tämän ohjelman tai ohjeistuksen muodostaminen ja toimintaan paneminen voi olla hyvinkin yksinkertaista.

Tietohallinto voi olla usein hyvin henkilöitynyt pk-yrityksissä ja se saattaakin olla täysin yksilön oman harrastuneisuuden varassa. Tietoturvaan ei ole välttämättä lainkaan erillistä budjettia, saati koko IT:n vaatimiin hankintoihin. Se on upotettuna johonkin toiseen, yleisempään budjettiin. Tämä ei ole teorian perusteella strategisesti hyvä valinta yritykselle.

Kun yrityksiltä tiedusteltiin hyväksi havaittujen käytäntöjen kokoelmia tai varsinaisia tietoturvaohjeita, löytyi niitä muutamalta yritykseltä. Varsinaista esimerkillisesti toimivaa yritystä ei otannasta kuitenkaan noussut esille. Tällä tarkoitan haastattelukohdetta, jolla olisi ollut kaikki keskivertoa paremmin hoidossa muihin yrityksiin verrattuna. Tämä kertonee karua todellisuutta pk-yritysten tilanteesta tällä hetkellä ja sekä niiden työntekijöiden että johtajien kouluttamattomuudesta. Vaikuttaa myös siltä, että tietoturvallisuus yksinkertaisesti priorisoidaan melko alas, mitä yrityksen liiketoimintaan tulee. Se nähdään vain pakollisena osa-alueena ja sen toivotaankin olevan jonkun muun hoidossa kuin yrityksen itsensä. Mielestäni voidaan todeta tämän nostavan henkilökunnan koulutuksen tarpeen tärkeäksi osa-alueeksi turvallisuuden varmistamisessa yrityksessä ja osana sen arkipäiväistä toimintaa. (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)

Kohdennetut pitkäkestoiset hyökkäykset (eli APT) eivät olleet haastatelluille henkilöille lainkaan tuttu käsite. Osa haastatelluista henkilöistä antoi viitteitä uutisissa kuultuihin hyökkäyksiin tästä kysyttäessä, mutta he eivät vaikuttaneet ymmärtävän silti, mitä itse hyökkäys tarkoitti. Kun heille selitettiin hyökkäyksen luonnetta ja sen ominaispiirteitä, vaikutti yleinen konsensus pk-yritysten kesken asiasta olevan oletus siitä, ettei se koskettaisi juuri heidän yritystään. Myös yrityksen kokoluokka mainittiin syynä tähän johtopäätökseen. Esitetyt hyökkäysvektorit (Symantecin havainnekuva) eivät myöskään herättäneet sen suurempaa epäilyksen tunnetta turvallisuudesta. Osa haastatelluista henkilöistä myönsi kylläkin murehtivansa tietoturvaa, mutta ilman konkreettista suunnitelmallisuutta tai aikomusta paneutua asiaan sillä tasolla, jolla siihen tulisi jotain muutosta yrityksessä ja sen toiminnassa. Osa myönsi myös kyseessä olevan sen luokan asioita, joita ei kerrota edes kotona. Oletettavasti he viittasivat asioiden arkaluontoisuuteen, jonka voidaan todeta lisääntyvän vain yrityskoon kasvaessa suurempiin kokoluokkiin. (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)

Yritysten kokoluokalla oli haastattelujen perusteella suurin vaikutus itseluottamukseen. Mitä suuremman yrityksen edustaja haastateltava henkilö oli, sitä itsevarmemmalta hän vaikutti vastauksissaan liittyen yrityksen tietoturvaan. Tämä saattaa liittyä myös vastuukysymykseen, joka johtoasemasta syntyy yrityksen hierarkian osalta. Kyseisen yksityiskohdan ei kuitenkaan voida todeta vääristävän vastauksia, koska niitä

kaikkia käsiteltiin tasa-arvoisesti huomioimatta yrityksen kokoa ja keskittyen nimenomaan tietoturvapuoleen. Isommat yritykset vaikuttivat myös enemmän järjestäytyneiltä ja samalla valmiimmilta vastaanottamaan ohjeistuksia ja jatkokehittämään niiden vaatimia taustatoimintoja. Suoritettujen haastattelujen perusteella taitekohtana, juuri itsevarmuuteen liittyen, voitaisiin pitää yrityksen IT maturiteettia. Kun maturiteetti saavuttaa tietyn pisteeseen, tietoturvalle ymmärretään ja annetaan lisäarvoa yrityksessä, ja samalla yrityksen ylemmästä johdosta löytyy henkilö, joka kokee olevansa siitä vastuussa tai joka asetetaan siitä vastuuseen. Kyseinen henkilö voi pienimmissä mikroyrityksissä olla toimitusjohtaja, mutta suuremmissa pk-yrityksissä kyseinen tietoturva- tai tietohallintojohtaja saattaa olla jo nimetty erikseen. Joissakin tapauksissa nämä saattavat myös olla yksi ja sama henkilö vain ja ainoastaan helppouden takia. (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)

# 6 LOPPUPÄÄTELMÄT

Nykytilanne maailmassa tietoturvan näkökulmasta on uhkaava. Voidaan todeta uhkien muuttuneen ja panosten kasvaneen entisestään. Suuremmat ja kriittisemmät järjestelmät siirtyvät kohti pilvipalveluita, muuttuen samalla näkyvämmiksi hyökkääjille. Hyökkäyksien motivaattoreina voivat toimia myös poliittiset agendat ja ne voi nähdään aseena. Yksilön tiedot ovat arvokkaampia kuin koskaan, eikä asiakasdatan merkitystä tulisi minkään yrityksen väheksyä osana liiketoimintaansa. Tietoturvaloukkausten luonne on muuttumassa monimutkaisemmaksi sitä mukaa kuin koko IT-horisontin voidaan todeta monipuolistuneen ja vain levinneen viime vuosikymmenen aikana. Tulevaisuus tämän kaiken osalta on hyvin avoin, mutta voidaan olettaa tämän kehityksen suunnan vain jatkuvan ja hyökkäysten muuttuvan siinä samalla. Hyökkäykset ovat nykyisin osa nykyaikaista sodankäyntiä. Kaikki tämä aiheuttaa suuria haasteita lainsäädännölle, jonka tulisi pysyä perässä oikeudenmukaisuuden nimissä. Yritykset siirtyvät toiminnassaan enenevässä määrin digitaaliseen muotoon.

Pk-yritysten tulisi aloittaa tietoturvan pohtiminen omassa liiketoiminnassaan. Pohtiminen voidaan aloittaa nimenomaan tunnistamalla liiketoiminnalle kriittinen data. Mitä se on ja missä se sijaitsee tällä hetkellä? Näiden kysymysten tutkinnan voi aloittaa myös lainsäädännön avulla. Toteutuuko nykystandardien mukainen tietosuoja varmasti joka vaiheessa liiketoimintaa. Kysymysten ja määritelmien valossa, yritys voi alkaa kehitellä itselleen tietoturvastrategiaa. Tutkimukseni mukaan kannattavaa olisi ryhdyttävä luomaan myös hyväksi havaittujen käytäntöjen opasta sekä prosesseja tukemaan näitä käytäntöjä, jolloin varmistetaan niiden leviäminen koko organisaatioon. Yleensä tämän sivuvaikutuksena alkaa myös kouluttaminen tai tiedon levittäminen, joka optimitilanteessa jatkuu säännöllisesti myös tulevaisuudessa. Kirjallisuuden valossa tämän toiminnan hyödyt ovat suuret. Luodut prosessit ja kartoitukset auttavat myös kriisitilanteissa selviämistä ja niiden ratkaisemisen tehokkuutta. Yleensä pk-yrityksille on kriittistä kyetä jatkamaan liiketoimintaansa mahdollisimman lyhyen katkon saattelemana, jos sellainen on syntynyt. Yrityksen digitaalisesta liiketoiminnasta on helposti saatavissa arkkitehtuurinen kuva. Se voi helpottaa tulevaisuudessa tapahtuvaa tietojärjestelmien hankintaa ja niiden tarpeiden suunnittelua ennakoivasti.

EU:n uusi tietosuojalaki, lähinnä sitä koskeneen siirtymäajan loppuminen, tuo paljon kaivattua turvaa yksittäiselle kansalaiselle liittyen tietojen sähköiseen tallennukseen ja niiden käsittelyyn. Tämä uusi laki pakottaa myös yritykset vihdoin tarkastelemaan millaisia tietoja ne käsittelevät ja säilyttävät missäkin eri järjestelmässä osana omaa liiketoimintaansa. Kyseinen laki ei jätä tulkinnanvaraa sen toteuttamiseen, vaan kaikkien yritysten ja tahojen tulee noudattaa sitä siirtymisajan päättymisen jälkeen. Tällöin voidaan nähdä sanktioiden astuneen voimaan myös käytännössä. Kansalaisille annetaan valtaa jopa tietojensa poistamiseen sellaisista järjestelmistä, joihin he eivät niitä halua.

Kaikkien yksilöiden on myös mahdollista pyytää yritykseltä listaa tiedoista, joita hänestä on tähän mennessä kerätty. Rahallisesti tämän lain aiheuttamat muutokset ja vaatimukset voivat olla merkittäviä riippuen yrityksen toimialasta. Tämä on myös mahdollistanut täysin uusien yritysten syntymisen. Ne luovat uudenlaista konsultatiivista liiketoimintaa. Oikein toteutettuna kaikella tällä voidaan pitkällä tähtäimellä saada pk-yrityksille myös säästöjä aikaiseksi parannetun tietoturvallisuuden ja korkeamman tietosuojan ansiosta. Koska kyse on lainsäädännöstä, vaihtoehtoja ei tässä käytännössä ole, vaan muutokset on toteutettava. Määrättävät sanktiot ovat tuntuvat myös pienemmille yrityksille.

Pilvipalveluista löytyy säästömahdollisuuksia erikokoisille yrityksille, mutta niiden tietoturvallisuuden kannalta harkintaa kannattaa vieläkin käyttää. Arkkitehtuurisesti on merkitystä, mitä palveluja kannattaa siirtää pilveen ja miten yritys jatkossa käsittelee tietojaan. Myös pilvipalveluntarjoajalla voidaan todeta olevan edelleen merkitystä. Pilvipalvelut ovat edelleen houkuttavia, koska ne tarjoavat kokonaisvaltaisilta ratkaisuilta vaikuttavia paketteja. Ne tuntuvat pk-yrityksistä ja niiden yrittäjistä hyviltä vaihtoehdoilta. Kyseisten palveluiden voidaan nähdä myös hyödyntävän tätä osana markkinointistrategiaansa. Vedotaan juuri kokonaisvaltaisuuteen ja helppouteen säästöjen lisäksi.

Tutkimukseni mukaan yrityksen koolla on vaikutusta sen käsitykseen omasta tietoturvallisuudestaan. Mitä isompi yritys on, sitä turvallisemmaksi se kokee itsensä. Tässä lievänä poikkeuksena voi toimia äärimmäisen pienet mikroyritykset, jotka perustelevat turvallisuuttaan vetoamalla nimenomaan kokoluokkansa pienuuteen. Suorittamani empiriatutkimuksen pohjalta, on yritysten tietoturvakäsitykselle eroteltavissa erilaisia vaiheita. Ne eivät kuitenkaan ole suoraa sidoksissa yrityksen IT-maturiteettiin, vaikka yhtymäkohtia siitä löytyykin. Tällä tarkoitan lähinnä sitä, ettei korkean IT-maturiteetin voi automaattisesti olettaa johtuvan korkean tason tietoturvan hallinnasta ja sen avulla suuremmasta käsityksestä tietoturvasta yleisesti osana liiketoimintaa. Vaikuttaa siltä, että mitä kiinnostuneempi vastuussa oleva henkilö on tietoturvasta, sitä itsevarmempana hän kykenee esittämään asioita edustamansa yrityksen osalta. (Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)

Jatkotutkimuksia ajatellen olisi hyvä valita lisää pienemmän kokoluokan yrityksiä ja tutkia onko kyseessä pelkkä poikkeama heidän luottavaisuudesta omaan tietoturvallisuuteensa. Myös enemmän pk-yrityksen kokoluokkien toista ääripäätä olisi mielenkiintoista tutkia lisää. Onko havaittavissa erityistä kokoluokkarajaa, jossa tietoturvakäsitykset muuttuvat eri yritysten kohdalla? Tälle jatkokysymyksenä voisi myös toimia erilaiset tietoturvatrendit. Nähdäänkö niiden suosioissa eroja vai pätevätkö tässä jotkin mahdollisesti aiemmin tunnistetut linjat. Suuremman otannan voidaan olettaa tarjoavan vielä luotettavampaa poikkileikkausta eri toimialojen yritysten tietoturvan tilanteista ja siitä mikä on yleiskuva eri yritysten keskuudessa, eli mikä voitaisiin tulkita tämän osalta konsensuksena. Eräs jatkotutkimuskysymys voisi myös olla, kuinka

yritysten tietoturvakäsitys tai turvallisuudentunne on muuttunut uuden tietosuojalain siirtymäajan loputtua. Myös maantieteellisesti voisi tutkia, miten hyökkäykset yleistyvät tai vaihtoehtoisesti vähentyvät, jos siirrytään kaupungeissa sijaitsevista yrityksistä pienempien kuntien yrityksiin. Onko maantieteellisen sijainnin perusteella havaittavissa minkäänlaisia eroavaisuuksia? Kiristysohjelmistoihin erityisesti keskittyvä tutkimus voisi myös olla kiinnostava ja uusia näkemyksiä avaava tutkimuskohde.

# LÄHTEET

Auty. 2004. Political hacktivism: Tool of the underdog or scourge of cyberspace? Aslib Proceedings, vol. 56(4), 212-221.

Auty. 2015. Anatomy of an advanced persistent threat. Network Security April 2015, vol. 2015(4), 13-16.

Becker, Dawson, Devine, Hannum, Hill, Leydens, Matuskevich, Traver & Palmquist. 2012. Case studies. Writing@CSU. Colorado State University. https://writing.colostate.edu/guides/guide.cfm?guideid=60 (17.3.2018).

Benbasat, Goldstein & Mead. 1987. The case research strategy in studies of information systems. MIS quarterly (September 1987), 369-386.

Bolek, Lateckova, Romanova & Korcek. 2016. Factors affecting information security focused on SME and agricultural enterprises. Agris On-line Papers in Economics and Informatics, vol. 8(4), 37-50.

Chaleff. 1995. We're drowning in e-mail. Computerworld, vol. 29(42), 37.

Chandramouli. 2011. Emerging social media threats: Technology and policy perspectives. Cybersecurity Summit (WCS), 2011 Second Worldwide, 1-4.

Dojkovski, Lichtenstein & Warren. 2007. Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. ECIS 2007 Proceedings, 1560-1571.

Eom, Kim, Kim & Chung. 2012. Cyber military strategy for cyberspace superiority in cyber warfare. Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on, 295-299.

Euroopan komissio. Käyttöopas Pk-yrityksen määritelmä. 2017. https://publications.europa.eu/en/publication-detail/-/publication/79c0ce87-f4dc-11e6-8a35-01aa75ed71a1/language-fi (17.3.2018).

Groner & Brune. 2012. Towards an empirical examination of IT security infrastructures in SME. Lecture Notes in Computer Science, vol. 7617, 73-88.

Hirsjärvi & Hurme. 2001. Tutkimushaastattelu, teemahaastattelun teoria ja käytäntö. Helsinki University Press, Suomi.

Horne, Maynard & Ahmad. 2017. Organisational information security strategy: Review, discussion and future research. Australasian Journal of Information Systems 2017, vol. 21, article number 1427, 1-17.

Jordan & Taylor. 2004. Hacktivism and cyberwars: Rebels with a cause? Routledge, Lontoo.

Järveläinen. 2012. Information security and business continuity management in interorganizational IT relationships. Information Management & Computer Security vol. 20(5), 332.

Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana. 2015. APT - 'Have you ever seen the threat'. Julkaisematon asiakasraportti. 45 sivua. Work Informatics, Turun yliopisto.

Kick, Contacos-Sawyer & Thomas. 2015. How generation Z's reliance on digital communication can affect future workplace relationships. Competition Forum 2015, vol. 13(2), 214.

Koch. 2004. Hand OverSecurity; Physical and information security have been converging, often under the control of IT. But companies are increasingly moving the role of policing security out of IT and into the hands of an independent CSO. Here's why you should consider doing the same. CIO, vol. 17(13), 1.

Lindgren & Lundström. 2015. Pirate culture and hacktivist mobilization: The cultural and social protocols of #WikiLeaks on Twitter. New Media & Society, 13(6), 999-1018.

Mennie. 2015. Social Media Risk and Governance: Managing Enterprise Risk. Kogan Page, USA.

Mitchell. 1997. Making the most of your firm's information gold-mine. Management Today, vol. 69(12).

O'Brien. 2016. Privacy and security: The new European data protection regulation and it's data breach notification requirements. Business Information Review 2016, vol. 33(2), 81-84.

Osborne & Summitt. 2006. How to cheat at managing information security. Elsevier, USA.

Pearson & Yee. 2013. Privacy and Security for Cloud Computing. Springer-Verlag, Lontoo.

Peltier. 2005. Implementing an Information Security Awareness Program. Information Systems Security, vol. 14(2), 37-49.

Raguseo, Neirotti & Paolucci. 2015. Exploring the tensions behind the adoption of mobile work practices in SMEs. Business Process Management Journal, vol. 21(5), 1162-1185.

Rees. 2010. Information security for small and medium-sized business. Computer Fraud & Security 2010, vol. 2010(9), 18-19.

Rid. 2012. Cyber War Will Not Take Place. Journal of Strategic Studies, vol. 35(1), 5-32.

Rowley. 2007. The wisdom hierarchy: representations of the DIKW hierarchy. Journal of information science, vol. 33(2), 163-180.

Schwartzel & Mnkandla. 2011. The impact of critical business data to organizations. African Journal of Business Management, 6(26), 7705-7713.

Soliman & Yousser. 2003. The role of critical information in enterprise knowledge management. Industrial Management & Data Systems, 103(7), 484-490.

Sveen, Torres & Sarriegi 2009. International Journal of Critical Infrastructure Protection 2009, vol. 2(3), 95-109.

Symantec. 2011. Advanced persistent threats: A Symantec perspective. https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (3.4.2018).

Tuomisto, Korelin & Arbab. 2012. Mobiiliteknologia ja uusi mobiilityö Pk-yrityksissä. Work Informatics, Turun kauppakorkeakoulu, Turun yliopisto.

Van Kessel. 2018. Ernst & Young: Cybersecurity regained: Preparing to face cyber attacks 20th Global Information Security Survey 2017–18. http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf (3.4.2018).

Voigt & von dem Bussche. 2017. The EU general data protection regulation (GDPR): A practical guide. Springer, Sveitsi.

Winkler & Gomes. 2017. Advanced persistent security: A cyberwarfare approach to implementing adaptive enterprise protection, detection, and reaction strategies. Elsevier, USA.

Winkler & Meine. 2011. Securing the cloud: cloud computer security techniques and tactics. Elsevier, USA.

Wright. 2016. To GDPR or not to GDPR. Computer Reseller News Sep 5, 2016, 6-7.

Xiang. 2013. Hacktivism and the first amendment: Drawing the line between cyber protests and crime. Harvard Journal of Law & Technology, vol. 27(1), 301-330.

Yildirim, Akalp, Aytac & Bayram. 2011. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management, vol. 31(4), 360-365.

Yin. 1984. Case study research, design and methods. Sage Publications, Lontoo.

# LIITTEET

## LIITE 1 Haastattelurunko (englanniksi)

### Theme 0 - The Background

- SME company's background and status quo
- What is your business area and who are your customers?
- Tell us about your history (how you got to where you are now) and how you see the future (what are your goals and "missions")?
    - When did you start doing business?
- How many employees do you have? (more relevant numbers, e.g. turnover)
    - What are your growth plans for the future?
- What are the markets (countries and industry) in which you compete?
- What is your IT-competency level?
    - Do you have a plan for restoring backups?
    - Do you have any enforced user policies?
    - (Ask about basics, such as password policies, access monitoring, using own devices, using VPN etc.)

### Theme 1 - Information Infrastructure in Small Businesses

- SME structure/infrastructure
    - Explain your IT architecture. (Are cloud services used? On-site data centres? Outside providers? How many and for what purpose? Internal network segmentation? Remote user protection/rules?)
        - What kind of IT systems does your company have? (How many?)
        - How many of these are used on a daily basis?
        - (Why do you have obsolete systems still running?)
    - How many of your employees would you say are technically orientated?
        - How have you distributed responsibilities between staff? (Related to IT tasks)
    - What kind of cloud services have you been offered?
        - What did you think about it?
        - How many Service Providers (cloud services) do you have/use?
            1. What value do they provide?
            2. How important are they for your business?
    - Do you have any inter-organizational systems?
        - What kind of data do you share with your partners? How?

        - Can you access the information systems of your subcontractors / clients?
        - How do you understand the network of connections your company has?
    - How do you handle privacy and confidentiality at work?
        - What threats are you most afraid of?
        - Have you bought any security services directly or indirectly (e.g. antivirus software bundled with a hardware purchase)?
            1. Has someone else taken care of it in your company?

**Theme 2 - Knowledge Management (Business critical information)**

- What kind of information is used at your company in daily routine work?
    - Produce? Utilize? Edit? Share?
    - What, where, when, how, etc.?
    - What would you call critical for your survival (BCI)?
- Describe your Service Level Agreement or SLA. (Do you have one? Refer to one of the cloud services mentioned earlier if necessary)
    - How long is it acceptable for a critical system to be offline?
    - Have you had issues with service downtime?
    - What if the downtime would be caused by an attack?
- How valuable do you consider your data / BCI (Business Critical Information)?
    - How do you understand the value of your BCI?
    - To whom is it valuable? (Your own company / competitors / outsiders…)
- Who has access to your BCI?
    - Do you have different access rights for different employees?
    - Do you have separated systems for BCI and non-BCI?
- Have you used any IT consultancy services (specifically Knowledge Management related?)
    - From your IT service provider perhaps?
    - From other 3rd parties?
- Do you use or have you previously used consultancy services for business improvement?
    - If yes: What kind of knowledge have you shared with the third party?
    - What kind of external services did you use?
    - How long was the relationship?

**Theme 3 - APT-organization in Small Business Context**

*Translation for APT? Is the best one "Kohdistettu hyökkäys"? Helsingin Sanomat (usually a figurehead in using correct language) translated it as "edistynyt, pitkäkestoinen hyökkäys".*

- How do you understand cybercrime / attacks?
    - Have you heard about APT-related incidents?
    - What kind of threats are you prepared for, if for any, in terms of security management of your organization?
        1. Describe your safety policy (password security, forensics…)
        2. What are your policies regarding to e.g. stolen laptops, mobile phones etc.?
        3. Do you have any policies against social engineering? Do you have any experiences?
    - How secure do you feel that your network and the business information within are?
- Have you ever heard about any groups or individuals (hackers) who you think are capable of undertaking APT activities?
    - Can you think of any specific attacks/attackers that would target your network?
    - Who would be involved in it? (Your wildest conspiracy theories come to life -- competitors, former employees...)
    - How would this impact you and your business?
- How do you see this picture? (*see below*) Can you relate your own company to it?
    - Do you think this could happen to you? Could the "characters" depicted be stealing from you?
- Now that you've seen what we mean by APT-organizations, how does it make you feel?
    - Has your point of view changed about how secure you are?
    - Is "security" relevant for you? (meaning, will you ACTUALLY go through extra effort to safeguard your BCI, even if we tell you that APT-attackers have all these ways of gathering data)

(Image source: Symantec 2011.)


(Kaukola, Koskenvoima, Tuomisto, Mölsä, Lehikoinen, Waheed, Rana 2015.)