TAMPEREEN
AMMATTIKORKEAKOULU

KYBERTURVALLISUUSKOULUTUKSEN SUUNNITTELU JA TOTEUTTAMINEN YRITYKSEN JOHDOLLE

Kimmo Antila

Opinnäytetyö
Marraskuu 2018
Yrittäjyyden koulutus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Yrittäjyyden koulutus

ANTILA KIMMO:
Kyberturvallisuuskoulutuksen suunnittelu ja toteuttaminen yrityksen johdolle

Opinnäytetyö 124 sivua, joista liitteitä 33 sivua
Marraskuu 2018

Kyberturvallisuuden osaamisen merkitys suomalaiselle tietoyhteyskunnalle, yksityisille henkilöille, yrityksille ja kansantaloudelle on todella merkittävä ja ajankohtainen. Kyberturvallisuudessa globaali internet on keskiössä, mistä yhteiskunnan kriittinen infrastruktuuri, palvelut, teknologia ja kaikki yritykset ovat riippuvaisia.

Erittäin laajan kyberturvallisuuden aihealueen kokonaisuuden ymmärtäminen, tietoisuuden lisääminen ja aiheen kouluttaminen yritysjohdolle on haastava tehtävä, mihin tarvitaan innovatiivista, motivoivaa ja osallistavaa yritysvalmennusta. Koulutusmateriaalin sisällön on vastattava yrityksen tarpeisiin ja kriittinen liiketoiminta on turvattava kaikissa kyberhäiriötilanteissa.

Opinnäytetyön tarkoituksena oli kyberturvallisuuskoulutusmateriaalin sisällön tuottaminen, koulutuksen suunnittelu ja toteuttaminen pienen ja keskisuuren yrityksen johdolle. Tavoitteena oli, että koulutusmateriaalia voidaan hyödyntää yritysjohdon koulutuksen toteuttamisessa. Materiaalia voi soveltuvin osin käyttää eri toimialoilla, suuremmissa yrityksissä ja viranomaisorganisaatioissa. Koulutusmateriaali tuli toiminimen, Kyberkapteeni, käyttöön. Itse koulutusmateriaali ei ole julkinen liite, mutta keskeisen viitekehyksen materiaalille muodostaa luku kaksi.

Koulutusmateriaalin sisällön rakentamiseen luvussa kaksi käytettiin pääosin dokumenttianalyysiä tutustumalla laaja-alaisesti kotimaisiin ja ulkomaisiin lähteisiin sekä hyödynnettiin kirjoittajan 33 vuoden kokemusta ICT- ja tietoturvallisuusalalta, kansallisilta ja kansainvälisiltä messuilta ja alan työpajoista.

Työssä käytettiin sekä kvantitatiivisia (määrällisiä) että kvalitatiivisia (laadullisia) tutkimusmenetelmiä, kuten havainnointia, haastatteluja sekä tutustuttiin eri tahojen tekemiin kvantitatiivisiin kyselytutkimuksiin. Yritysjohtajien puolistrukturoidut haastattelut ja yrityksiin kohdistuvat turvallisuuskartoitukset toteutettiin helmikuussa 2018 ennen koulutuspilotteja. Koulutuksen suunnitteluun ja toteuttamiseen liittyvien kokeilevien pilottien yhteydessä menetelminä käytettiin systeemiajattelua, valmennusta ja aivoriihiä sekä muita osallistavia opetusmenetelmiä.

Perusteellisella taustatutkimuksella, hyvin suunnitelluilla ja toteutetuilla haastatteluilla, kyselyillä ja piloteilla saatiin toteutettua yritysjohdolle koulutusmateriaali, jonka avulla voidaan parantaa yrityksen kyberturvallisuuden johtamista, johdon kyberturvallisuustietoisuutta ja yrityksen kilpailukykyä sekä turvata yrityksen maine ja liiketoiminnan jatkuvuus. Johdon palautteet piloteista olivatkin todella positiivisia esimerkiksi innovatiivisen ja motivoivan kyberturvallisuuden johtamisen opeista.

Asiasanat: kyberturvallisuuskoulutus, tietoturvallisuus, koulutusmateriaalin suunnittelu koulutuksen toteutus, kyberturvallisuuden johtaminen

ABSTRACT

Tampere University of Applied Sciences
Master's Degree Programme in Entrepreneurship

Kimmo Antila
Designing and Implementing Cyber Security Training for Company Management

Master's thesis 124 pages, appendices 33 pages
November 2018

The significance of cyber security expertise for the Finnish community of information, private individuals, businesses and the economy is truly significant and timely. Global internet is in the heart of cyber security, from where critical infrastructure, services, technology and all businesses are dependent.

Understanding the scope of cybersecurity topics, increasing awareness and training for business management are a challenging tasks, for which innovative, motivating and participatory business training are needed. The content of the training material must be in response to the company's needs, and critical business must be safeguarded in all cyber-disturbances.

The purpose of the thesis was to produce the content of the cyber-safety training material. This includes design and implementation of the training for the small and medium-sized enterprise. The aim was to use training material in corporate management training. The material can be used in different industries, large companies as well as government organizations. The training material was made for the company called Kyberkapteeni. The training material itself is not a public appendix, but the material of the key framework is in the chapter two.

Documents analysis methodology was used in developing the educational materials. Domestic and foreign sources were widely explored. The author utilizes his 33-year experience in ICT and information security, national and international fairs and attending workshops in the field.

Data for the thesis were collected through quantitative and qualitative research methods, observation and interviews. Quantitative research conducted by different organizations was used in the thesis. Semi-structured interviews with business executives and security surveys on companies were carried out in February 2018 before pilot training. Systems thinking, coaching and brainstorming as well as other participatory teaching methods were used as experimental pilots in the planning and implementation of training.

With a thorough background study, well-designed and conducted interviews, surveys and pilots, training materials were developed for corporate management to improve the company's cyber safety management, cyber security awareness and company competitiveness to safeguard the company's reputation and business continuity. The management's feedback from the pilots was positive, for example, from innovative and motivating cyber security learning.

Key words: cyber safety training, information security, planning of training material, implementation of training, cyber security management

SISÄLLYS

1 JOHDANTO 8
1.1 Opinnäytetyön taustaa ja tutkimushaasteet 8
1.2 Työn tarkoitus ja tavoite 10
1.3 Tutkimusmenetelmät ja aikataulu sekä raportin rakenne 10
2 KYBERTURVALLISUUS YRITYSELÄMÄSSÄ 13
2.1 Dokumenttianalyysi tutkimusmenetelmänä 13
2.2 Kyberturvallisuuden merkitys yrityksille 14
2.2.1 Suojattavat arvot ja kyberturvallisuuden myytit 17
2.2.2 Kyberturvallisuuden uhkat ja niiltä suojautuminen 18
2.2.3 Voiko kyberturvallisuus olla mahdollisuus? 21
2.2.4 Sosiaalisen median merkitys kyberturvallisuudessa 21
2.2.5 Yhteenveto kyberturvallisuuden merkityksestä yrityksille 22
2.3 EU:n tietosuoja-asetuksen ja lakien sekä standardien merkitys 23
2.3.1 EU tietosuoja-asetuksen merkitys ja vaikutus yrityksille 23
2.3.2 EU -tietosuoja-asetuksen uhkat ja mahdollisuudet 26
2.3.3 Henkilötietojen käsittely ja rekisteröidyn oikeudet 27
2.3.4 Mitä johto voi tehdä tietosuojan parantamiseksi? 28
2.3.5 Lakien ja standardien merkitys kyberturvallisuudessa 29
2.3.6 Yhteenveto ja johtopäätökset 30
2.4 Kyberturvallisuuden johtaminen yrityksessä 31
2.4.1 Kyberturvallisuuden visio ja strategia sekä politiikka 31
2.4.2 Kyberturvallisuusriskien kartoittaminen ja niiltä suojautuminen . 35
2.4.3 Vastuun jakautuminen ja sen jakaminen 38
2.4.4 Asiakkaan kyberturvallisuus 39
2.4.5 Kyberturvallisuuden rakentaminen ja uhkilta suojautuminen 40
2.4.6 Verkostoituminen ja tilannekuva 41
2.4.7 Motivoiva ja innovatiivinen kyberturvallisuuden johtaminen 43
3 OPPIMISEN TEORIAT JA OPPIMISMENETELMÄT 46
3.1 Tutkimusmenetelmien vertailua ja menetelmien valinta 47
3.2 Oppimisen teoriat ja opetusmenetelmien valinta 48
3.2.1 Kognitiivinen oppimiskäsitys kyberturvallisuudessa 50
3.3 Aikuisena oppiminen ja kyberturvallisuuskoulutuksen suunnittelu 52
3.3.1 Aikuiskoulutuksen teoriaa 53
3.3.2 Koulutustilaisuuden tarkoituksen ja tavoitteiden asettaminen 56
3.3.3 Motivoiva ja osallistava oppiminen 56
3.3.4 Valmentaminen ja oppiminen tiimissä sekä ideointimenetelmät .. 57

3.3.5 Systeemiajattelu kyberturvallisuudessa 61
3.3.6 Perustelut piloteille ja pilottien analyysit 64
3.3.7 Yhteenveto 66
4 KOULUTUKSEN SISÄLTÖ JA TOTEUTUS 68
4.1 Koulutusmateriaalin sisältö ja luennon juoni 68
4.2 Muita koulutuksen toteuttamisessa huomioitavia asioita 78
4.2.1 Vaihtoehtoiset ryhmätyöt ja koulutusmateriaalin päivitys 79
5 POHDINTA JA YHTEENVETO 82
LÄHTEET 86
LIITTEET 92
Liite 1. Kyberturvallisuuden itsearvioinnin kysymyssarja 1 (15) 92
Liite 2. Yrityksen sosiaalisen median ohjeen sisältö 107
Liite 3. Kyberturvallisuusstrategian kehittäminen yritykselle 1(2) 108
Liite 4. Yrityksen kyberturvallisuuspolitiikan sisältö 110
Liite 5. Koulutukseen liittyvät pilotit ja niiden kehittäminen 1 (6) 111
Liite 6. Yritysjohtajien puolistrukturoitu haastattelurunko 1 (3) 117
Liite 7. Pilottien palautekyselylomake 1 (2) 120
Liite 8. Kyberturvallisuuskartoitus CIA:n ja 10 teesin avulla 1(3) 122

LYHENTEET JA TERMIT

APT-hyökkäys	APT (Advanced Persistent Threat) on kohdistettu haittaohjelmahyökkäys eli monivaiheinen tietoverkkohyökkäys, joka kohdistuu tiettyyn rajattuun kohteeseen ja joka tehdään haittaohjelmien sekä muiden toimintojen avulla.
Exploit kit	Ohjelmointityökalu, jonka avulla ohjelmointia osaamaton pystyy kirjoittamaan ohjelmointikoodia luomalla, muokkaamalla ja jakamalla haittaohjelmia.
Informaatioinfrastruktuuri	Tietojärjestelmien perustana olevat rakenteet ja toiminnot, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely.
Haktivismi	Hakkerin tai hakkeriryhmän kybertoimintaympäristössä harjoittama tavoitteellinen ja aatteellinen toiminta, joka on luonteeltaan rikollista.
IoT	Esineiden internetillä (Internet of Things) tarkoitetaan internet-verkon laajentumista laitteisiin ja koneisiin, joita voidaan ohjata, mitata ja sensoroida internet-verkon yli.
Kriittinen informaatioinfrastruktuuri	Yhteiskunnan elintärkeiden toimintojen tietojärjestelmien perustana olevat rakenteet ja toiminnot, joiden tehtävänä on sähköisessä muodossa olevan informaation (tiedon) lähettäminen, siirto, vastaanotto, varastointi tai muu käsittely.
Kriittinen infrastruktuuri	Rakenteet ja toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeille toiminnoille. Siihen kuuluu sekä fyysisiä laitoksia ja rakenteita että sähköisiä toimintoja ja palveluja.
Kyber	Kyber-sanaa käytetään yhdyssanan määriteosana. Sanan merkityssisältö liittyy yleensä sähköisessä muodossa olevan informaation (tietojen) käsittelyyn: tietotekniikkaan, sähköiseen viestintään (tiedonsiirtoon), tieto- ja tietokonejärjestelmiin. Vasta koko yhdyssanalla (määriteosan ja perusosan yhdistelmällä) voidaan katsoa olevan oma merkityksensä. Sanan

	kyber voidaan katsoa tulevan alun perin kreikankielen sanasta “kybereo” - ohjata, opastaa, hallita.
Kyberuhka	Mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka kohdistuu kybertoimintaympäristöön ja toteutuessaan vaarantaa siitä riippuvaisen toiminnon.
Kyberaktivismi	Yksittäisen henkilön tai ryhmän kybertoimintaympäristössä harjoittama tavoitteellinen toiminta, jolla voidaan tavoitella huomiota tai muutosta johonkin asiaan.
Kyberrikollisuus	Rikollisuus, joka muodostuu viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyistä rikoksista sekä rikoksista, jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin. Vaikutukset kohdistuvat tietojärjestelmien kautta sekä valtioihin, yksityisiin kansalaisiin että yritysten toimintaan.
Kybervakoilu	Tietoverkkovakoilua, jossa hyödynnetään tietoverkkoja, niihin liitettyjä laitteita ja ohjelmistoja. Kybervakoilussa voidaan käyttää hyväksi esimerkiksi kohdistettuja haittaohjelmahyökkäyksiä.
Malware	Haittaohjelma eli termi, josta on tullut ”sateenvarjo” termi kuvaamaan kaikkia vihamielisiä tai tunkeilevia ohjelmistoja. Haittaohjelman käsitteeseen kuuluvat tietokonevirukset, madot, troijalaiset, ransomware, spyware, adware, scareware ja muut haittaohjelmat. Haittaohjelma voi olla ilmeinen ja helppo tunnistaa tai se voi olla hyvin vaikeasti havaittava.
Phishing	Tietojenkalastelua, jossa käyttäjä huijataan antamaan henkilökohtaisia tai taloudellisia tietoja laittomasti. Tarkoitus on saada vastaanottaja asentamaan esimerkiksi linkin kautta haittaohjelma tai ohjata käyttäjä antamaan tietonsa väärennetyssä palvelussa. Phishing voi olla myös kohdistettu tietylle henkilölle (spear-phishing).
Ransomware	Kiristyshaittaohjelma, haittaohjelma, lunnasohjelma joka leviää esim. sähköpostin liitetiedoston avulla ja salaa käyttäjän tiedot vaatien maksua salauksen avaamisesta.

1 JOHDANTO

1.1 Opinnäytetyön taustaa ja tutkimushaasteet

Kyberturvallisuudesta on muodostunut megatrendi ja ajankohtainen aihe. Mediassa uutisoidaan jatkuvasti maailmanlaajuisista uhista ja haittaohjelmatapauksista. Syynä tähän on Nobelin taloustieteen palkinnon saaneen Daniel Kahnemanin mukaan se, että ihmisiä kiinnostaa yleensä negatiiviset ja huonot uutiset (Kahneman 2012, 345; Lappalainen 2015, 85–86). Media suorastaan ”mässäilee” kyberturvallisuuden negatiivisilla tapahtumilla. Yritysten ja yksityisten ihmisten onnettomuudet houkuttelevat aina katsojia, vaikka kyberturvallisuus tulisi olla positiivinen aihe, joka tuo yrityksille kilpailuetua.

Kyberhyökkäykset ovat kuitenkin ilmastonmuutoksen ja siihen sopeutumisen epäonnistumisen sekä luonnonmullistusten jälkeen neljänneksi todennäköisin ja vaikuttavin riski maailmassa, eli verkkorikollisuus on edelleen kasvava trendi. Yritykset tarvitsevat tietoa ja opastusta kyberhäiriötilanteissa kyetäkseen varautumaan uhkiin riittävällä tavalla. (Global Risks Report, 2018; Yrityksiin kohdistuvat kyberuhat 2015.)

Kyberturvallisuudesta on olemassa useita erilaisia määritelmiä, joista osuvin lienee professori Martti Lehdon (2018), joka määrittelee kyberturvallisuuden globaaliksi ja moniulotteiseksi tieto- ja kommunikaatioverkoksi, mihin sekä ihmiset että koneet voivat kytkeytyä kiinteän tai liikkuvan päätelaitteen avulla ja toimia siellä virtuaalisesti. Lehdon ja monen muunkin asiantuntijan mukaan kyberturvallisuus on laajempi käsitys kuin perinteinen tietoturvallisuus (luennot Lehto 2018; Limnèll 2016; kirjoittajan kokemukset). Yritysmaailmassa kyberturvallisuus luonnehditaan tilaksi, jossa yrityksen arvokkaat tiedot ovat turvassa ja toiminta ei keskeydy tai vaarannu, vaikka sen tietoverkkoihin kohdistuisi kyberhyökkäys (Yrityksiin kohdistuvat kyberuhat 2015, 6).

Perinteisellä tietoturvallisuudella tarkoitetaan niitä teknisiä ja hallinnollisia järjestelyjä ja toimenpiteitä, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja (käytettävyys) saatavuus (Suomen kyberturvallisuusstrategia 2013, 13). Henkilön tietosuojalla tarkoitetaan taas henkilön yksityisyyden turvaamista esimerkiksi henkilötietojen asianmukaista käsittelyä sekä suojaamista oikeudettomalta ja luvattomalta käytöltä (Henkilötietolaki 22.4.1999/523 32 §). Tietoturvallisuudella siis tarkoitetaan niitä käytännön

toimenpiteitä, esimerkiksi henkilöstön kouluttamista, millä pyritään henkilön tietosuojan toteuttamiseen yrityksessä.

Yrityksen johdon rooli on ensiarvoisen tärkeä kyberturvallisuuden rakentamisessa ja sen jalkauttamisessa organisaatioon. Sanotaan myös, että ihminen on kyberturvallisuuden heikoin lenkki, joten koulutuksella yritys voi helposti, nopeasti ja kustannustehokkaasti parantaa omaa kyberturvallisuuttaan.

Tutkimustuloksista, kokemuksista ja asiantuntijoiden kommenteista voidaan päätellä, että kyber- ja tietoturvallisuudesta 80 % on loppukäyttäjän oikeaa asennetta, toimintaa ja hallinnollisia toimenpiteitä, jotka sisältävät kouluttamista ja päivittäisten toimintatapojen ohjeistamista. Loput 20 % on teknistä suojaamista, kuten palomuuri- ja virustorjuntaohjelmistojen käyttöä. (Kodin kyberopas 2017, 12; kirjoittajan kokemukset.) Perusratkaisuna tulee olla kyberturvallisuuden osaamisen parantaminen (Lehto 2016, luento). Edellä mainitusta huolimatta pienistä yrityksistä vain 4 %:lla oli vahvistettu alan koulutus- ja harjoitusohjelma (Yrityksiin kohdistuvat kyberuhat 2016, 66).

Tutkimustuloksiin perustuen opinnäytetyön pääpaino on kyberturvallisuuden hallinnollisissa ohjeissa, määräyksissä ja oikeissa toimintatavoissa eli kognitiivisessa kyberturvallisuuden kerroksessa, joka kyberturvallisuusprofessori Limnèllin (2016) mukaan sisältää ihmisen ongelmanratkaisukyvyn ja tulkintaympäristön sekä informaation merkityssisällön ymmärtämisen ja tulkinnan (Limnèll 2016, luento). Kyberturvallisuuden tekninen aihealue rajattiin pääosin työn ulkopuolelle.

Keskeisenä tutkimushaasteena oli rajata laajasta materiaalista ne kyberturvallisuuden aihealueet, jotka yrityksen johdon tulee hallita, osata ja ymmärtää sekä tunnistaa ne opetusmenetelmät, joiden avulla yritysjohdon kyberturvallisuuskoulutus suunnitellaan ja toteutetaan. Yritysjohdon koulutus ja ohjeistus sekä asennekasvatus ovat avainasemassa, jotta johto sitoutetaan kyberturvallisuuden johtamiseen sekä vision ja strategian luomiseen yritykselle. Yritysjohdon tulee myös tuntea keskeiset ja yleisimmät kyberturvallisuusuhat ja niitä vastaan suojautuminen.

Työssä käytettiin laajasti dokumenttianalyysiä tutustuen ja analysoiden sekä keräten kyberturvallisuudesta taustatietoa kansallisista ja kansainvälisistä lähteistä, kuten tutkimuksista, raporteista, luennoilta ja messuilta. Tärkeän lisänäkökulman työhön toi kirjoittajan

33 vuoden kokemukset ICT -alasta[1] ja tietoturvallisuudesta sekä sähkövoima-alasta puolustusvoimien tiedustelulaitoksella ja ilmavoimissa, missä hän toimi mm. tietohallinto- ja tietoturvallisuuspäällikkönä sekä teknisenä tietoturvallisuusvastaavana.

1.2 Työn tarkoitus ja tavoite

Opinnäytetyön tarkoituksena oli kyberturvallisuuskoulutusmateriaalin sisällön tuottaminen, koulutuksen suunnittelu ja toteuttaminen pienen ja keskisuuren yrityksen johdolle. Tavoitteena oli, että koulutusmateriaalia voidaan hyödyntää yritysjohdon koulutuksen toteuttamisessa. Johdon tehtävä on saada aikaan tilanne, jossa jokainen yrityksen työntekijä saa kyberuhkista riittävän hyvän kokonaiskuvan ja selkeitä toimintaohjeita. Koulutusmateriaali on tarkoitettu lähinnä pienille ja keskisuurille yrityksille, mutta sitä voi soveltuvin osin käyttää myös viranomaiset ja suuremmat yritykset. Koulutusmateriaalin avulla voidaan parantaa yrityksen kyberturvallisuuden johtamista, johdon kyberturvallisuustietoisuutta ja yrityksen kilpailukykyä sekä turvata yrityksen maine ja liiketoiminnan jatkuvuus.

1.3 Tutkimusmenetelmät ja aikataulu sekä raportin rakenne

Tutkimusmenetelminä työssä käytettiin sekä laadullista (kvalitatiivista) että määrällistä (kvantitatiivista) tutkimusta, koska yhdistettynä menetelmät tukevat ja täydentävät toisiaan parhaiten. Tutkittavasta ongelmasta tai aiheesta luodaan parempi ymmärrys, kun ei keskitytä vain yhteen menetelmään. (Tuomi & Sarajärvi 2018, luku 2.5.) Hyvin suunnitelluilla tutkimusmenetelmillä eli haastatteluilla, kyselyillä ja piloteilla saatiin toteutettua yritysjohdolle yleishyödyllinen koulutusmateriaali.

Erityisesti luvussa kaksi dokumenttianalyysillä oli keskeinen merkitys, koska materiaalia oli paljon eri lähteistä ja kaupallisen yrityksen tekemän tutkimuksen puolueettomuus oli aina arvioitava. Työssä toteutettiin sekä dokumenttien sisällön analyysiä että sisällön erittelyä, koska tarkoituksena oli informaatioarvon lisääminen, aineiston selkeyttäminen, mikä mahdollisti luotettavien johtopäätöksien ja yhteenvetojen tekemisen.

[1] Sanoista Information and Communication Technology, jonka suomennos on tieto- ja viestintäteknologia.

Dokumenteista saatu aineisto ryhmiteltiin aihealueittain ja pyrittiin selkeyttämään ja tiivistämään sitä.

Luvussa kolme tutkimusmenetelminä käytettiin pääsääntöisesti ryhmä-, strukturoituja haastatteluita eli lomakehaastatteluita ja osin puolistrukturoituja haastatteluja, koska niihin sisältyi syvähaastattelun piirteitä. Yritysjohdon haastatteluja, koulutuksien palautekyselyitä ja niiden analyysejä käytettiin hyväksi yrityksen johdolle suunnatun kyberturvallisuuskoulutuksen suunnittelussa ja toteutuksessa. Koulutusmateriaalia täydennettiin kolmen erillisen pilottikoulutuksen tuloksien perusteella ja itse pilotteja kehitettiin systeemiajattelun avulla. Materiaalia kehitettiin myös koulutuksen jälkeen tehdyissä ryhmätöissä (aivoriihi) toteutetun havainnoinnin avulla ja koulutuspalautteen kyselylomakkeiden perusteella (kuvio 1). Työssä käytetyistä tutkimusmenetelmistä on tarkemmat kuvaukset lukujen kaksi ja kolme alussa.

Koulutuspilotit toteutettiin kuvion 1 mukaisesti (liite 5 s. 111–116) syyskuussa 2017 sekä maalis- ja elokuussa 2018. Liitteessä 5 on kuvattu myös systeemiajattelun käyttäminen pilottien kehittämisessä. Ennen pilotteja toteutettiin helmikuussa 2018 yritysjohdon puolistrukturoitu haastattelu ja yrityksien kyberturvallisuuskartoitus (liite 6)

Aikataulullisesti opinnäytetyön valmistelun voidaan katsoa alkaneen ennen YAMK-opintojen alkua, jo vuoden 2017 alussa, alan materiaaliin tutustumisella ja 2017 syyskuussa ICT-startup -kurssin avoimella ryhmähaastattelulla – työpajalla (pilotti 1), joka liittyi silloisen koulutusmateriaalin sisällön ja ulkoasun kehittämiseen.

KUVIO 1. Opinnäytetyön rakenne ja aikataulu sekä prosessin kuvaus

Opinnäytetyön toisessa luvussa käsitellään tarkemmin dokumenttianalyysin merkitystä alalle ja luvun avulla lisätään yritysjohdon kyberturvallisuustietoisuutta käsittelemällä kyberturvallisuuden merkitystä yrityselämässä, lakien ja asetusten tuomia vaatimuksia sekä kyberturvallisuuden johtamista yrityksessä. Luvusta muodostui aihealueen laajuuden vuoksi selkeästi tavanomaista pidempi, koska se muodostaa varsinaiselle kyberturvallisuuden opetusmateriaalille keskeisen sisällön ja viitekehyksen. Luvussa esitettyjä liitteitä yritysjohto voi käyttää hyväkseen kyberturvallisuutta rakennettaessa ja johdettaessa. Luvun liitteitä ovat kyberturvallisuuden itsearvioinnin kysymyssarja, sosiaalisen median ohje, yrityksen kyberturvallisuusstrategian ja -politiikan sisältö.

Kolmannessa luvussa käsitellään tarkemmin laadullisen tutkimuksen menetelmiä, oppimisen teoriaa ja oikean opetusmenetelmän valintaa kyberturvallisuuskoulutuksen toteuttamiseen. Luku vastaa kysymykseen, kuinka johdon kyberturvallisuuden oppiminen onnistuu parhaiten, jotta turvallisuuskulttuuri oikeasti muuttuisi parempaan suuntaan? Lisäksi käsitellään koulutukseen liittyvää suunnittelua ja pilotteja sekä aikuisen oppijan ominaispiirteitä ottaen huomioon motivaation ja osallistavan oppimisen merkityksen. Luvun lopussa käsitellään myös systeemiajattelua pilottien kehittämisessä, mikä toi uuden ajatuksen systeemiajattelun hyödyntämisestä kyberturvallisuuden kokonaisuuden ymmärtämiseen ja johtamiseen yrityksissä.

Neljännessä luvussa käydään läpi koulutusmateriaalin sisällysluettelo ja koulutuksen toteutus. Luvussa kuvataan pääosin koulutusmateriaalin sisällysluettelo perustellen samalla sisällön merkitys yritysjohdolle. Oppija siis ymmärtää koulutuksen tarkoituksen. Keskeistä oli lisätä johdon kyberturvallisuuden tietoisuutta ja käsitystä siitä, miten johdon tulisi johtaa kyberturvallisuutta ja mitä johdon tulisi tehdä kyberturvallisuuden parantamiseksi ja rakentamiseksi yrityksessä. Koulutusmateriaali ei ole julkinen, mutta sen sisältö koostuu pääosin luvusta kaksi.

Pohdinnassa analysoidaan miten materiaalin tuotossa onnistuttiin ja vastasiko sen tulokset työn tarkoitusta ja tavoitetta. Luvussa käsitellään yhteenveto ja johtopäätökset kyberturvallisuuden merkityksestä, lakien ja asetusten tuomista mahdollisuuksista sekä kyberturvallisuuden johtamisesta. Pohdintaosuudessa tarkastellaan, miten tarkoituksen ja tavoitteen saavuttamisessa onnistuttiin analysoiden oma toiminta työhön liittyen viitaten tulevaisuuteen sekä jatkotyöhön.

2 KYBERTURVALLISUUS YRITYSELÄMÄSSÄ

Tässä luvussa käsitellään dokumenttianalyysiä tutkimusmenetelmänä sekä kyberturvallisuuden, EU tietosuoja-asetuksen, lakien ja standardien merkitystä yrityksille. Luvun tarkoitus on luoda viitekehys opinnäytetyölle muodostaen taustamateriaalia kyberturvallisuuden koulutusmateriaalille. Luvussa käsitellään myös kyberturvallisuuden uhkia, mahdollisuuksia, johtamista ja sosiaalisen median merkitystä yritysten kyberturvallisuudelle ja menestymiselle sekä samalla lisätään johdon kyberturvallisuustietoisuutta.

2.1 Dokumenttianalyysi tutkimusmenetelmänä

Kvantitatiivisessa tutkimuksessa tukeuduttiin sekä kotimaisiin että ulkomaisiin kyberturvallisuusalan tutkimuksiin käyttäen hyväksi dokumenttianalyysiä. Kyselyt oli suunnattu kuluttajiin ja yritysjohtajiin määrän vaihdellessa 700:sta jopa useisiin satoihin tuhansiin. Dokumenttianalyysillä on keskeinen merkitys kyberturvallisuusalaa tutkiessa, koska materiaalia oli paljon eri lähteistä ja kaupallisen yrityksen tekemä tutkimuksen puolueettomuus oli aina arvioitava. Dokumenttianalyysi (2014) on sisällön analyysiä ja sisällön erittelyä. Tässä työssä käytettiin molempia ja tarkoituksena oli informaatioarvon lisääminen, aineiston selkeyttäminen selkeiden ja luotettavien yhteenvetojen aikaansaamiseksi. Osin dokumentit analysoitiin myös numeroiksi ja kaavioiksi ja ilmisisällön lisäksi pyrittiin analysoimaan piilossa oleva viesti. Dokumenteista ja haastatteluista saatu aineisto ryhmiteltiin aihealueittain unohtamatta selkeyttämistä ja tiivistystä. (Ojasalo & Moilanen & Ritalahti 2014, 136–137, 139.)

Dokumenttianalyysin valintaa kyberturvallisuusalan tutkimusmenetelmänä puoltaa materiaalin laajuus ja erilaisuus esimerkiksi toimialojen erilaisista uhkakuvista. Laajan materiaalipohjan ja erilaisten uhkakuvien läpikäynnin avulla voidaan yrityksen johdolle antaa mahdollisimman objektiivinen ja laaja-alainen ymmärrys aiheesta.

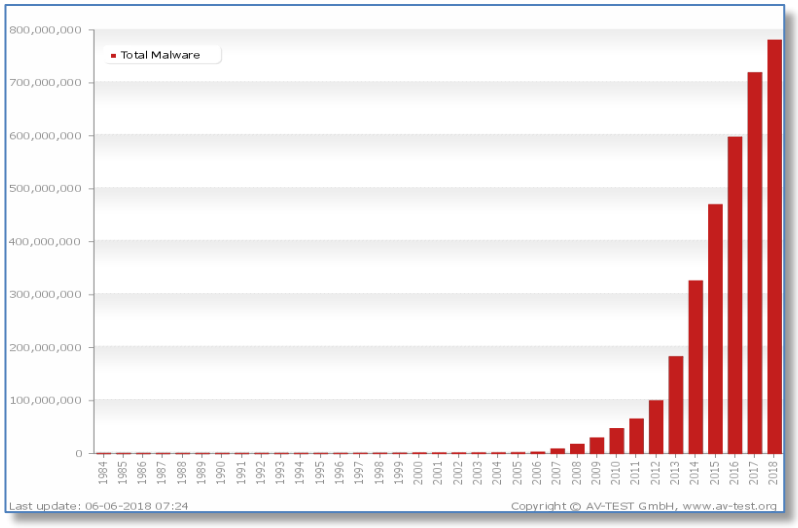
2.2 Kyberturvallisuuden merkitys yrityksille

Kyberaktivismi, -rikollisuus ja -vakoilu ovat lisääntyneet jatkuvasti. Hyökkäyskohteet on valittu ja tiedusteltu tarkoin ja monet rikolliset ovat ammattilaisia ja osaavia. Heillä on käytössään pitkälle kehitettyjä, monimutkaisia, huomaamattomia haittaohjelmia ja hyökkäystekniikoita, joita vastaan on joskus jopa mahdoton suojautua. Hyökkääjiä on usein mahdoton tunnistaa tai löytää. Lisäksi uhkien vaikuttavuus kohteeseen toteutuu yleensä lyhyessä ajassa, mutta niiden eskaloitumisen nopeus ja ajallinen kesto saattaa vaihdella esimerkiksi muutamista päivistä moniin vuosiin. Teknologian, kuten tekoälyn kehittyminen, tietotekniikan levittäytyminen, IoT-tekniikan yleinen lisääntyminen ovat luoneet aivan uusia haavoittuvuuksia ja mahdollisia hyökkäyskohteita yritysten kybertoimintaympäristössä. (Suomen kyberturvallisuusstrategia 2013, 17–18.)

Kyberuhkat jaetaan kyberaktivismiin (kybervandalismi, haktivismi), -rikollisuuteen, -vakoiluun, -terrorismiin ja -operaatioihin, joista lähinnä kolme ensimmäistä kohdistuu yrityksiin (Suomen kyberturvallisuusstrategia 2013, 18). Kybervandalismi on anarkiaan, kaaokseen ja haitantekoon tähtäävää toimintaa, jossa esimerkiksi internettiä käytetään kommunikaatiokanavana. Kyberrikokset tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai ne kohdistuvat verkkoihin ja järjestelmiin. Kyberrikoksia ovat kybervakoilu, kuten yritysvakoilu, laittoman sisällön julkaiseminen sähköisissä viestimissä tai palvelunestohyökkäykset ja hakkerointi. (ITKP0002 Johdatus kyberturvallisuuteen 2016.)

Yrityksiin kohdistuva kybervakoilu on erittäin yleistä, koska valvontaa ei ole, jollakulla on hyökkäykseen motiivi tai vain siksi, että vakoilua on helppo tehdä. Yrityksiä vastaan kohdistuvan hyökkäyksen yleisin motiivi on taloudellisen hyödyn tavoittelu, varkaus, petos, kiristys tai vandalismi. Hyökkäys voi olla massahyökkäys, kohdistettu hyökkäys tai sen takana voi olla jopa valtiollinen toimija, jolloin se voi kohdistua suureenkin yritykseen. Rikollisella on tarkoitus hankkia tietoja yksityisiltä ihmisiltä, yrityksen työntekijältä ja saada omalle yritykselle esimerkiksi kilpailuetua (ITKP0002 Johdatuskyberturvallisuuteen.) Kyberturvallisuutta ei tule kuitenkaan nähdä yrityksille pelkästään uhkana. Kyberosaaminen Suomessa -raportissa (2016) muistutettiin, että kyberturvallisuudesta muodostuu yrityksille liiketoiminnan varmistaja ja kilpailuetu. Lisäksi se on oma kasvava liiketoiminta-alansa. (Kyberosaaminen Suomessa 201, 45–47).

Hyökkäykset ovat mahdollisia, koska korjattavaa ja puutteita löytyy yritysten turvallisuusprosesseissa ja -johtamisessa, toiminnan jatkuvuuden turvaamisessa ja toipumisessa. Järjestelmissä ja ohjelmistoissa on haavoittuvuuksia. Lisäksi kybermaailman ja ihmisten avoimuus sosiaalisessa mediassa mahdollistavat hyökkäykset maailmanlaajuisesti. (ITKP0002 Johdatus kyberturvallisuuteen 2016; Hiltunen E & K 2014, 226–228.) Haittaohjelmien lisääntyminen on ollut huimaa ja kehitys näyttää jatkuvan. Asian voi todeta seuraavasta esimerkistä eli yhden yrityksen tuottamasta AVG-raportista.



KUVIO 2. Haittaohjelmien lisääntyminen vuosittain (AVG -raportti 2018)

Nykypäivän yleisistä turvallisuuden huolista mainittakoon erilaiset väkivallanteot kouluissa, turvapaikanhakijoiden kasvu, presidentinvaalien kyberuhkat, Ukrainan kriisi, terrori-iskut. Suomikaan ei ole enää turvallisuuden ”lintukoto”. Uhat vaikuttavat meidän turvallisuuden tunteeseemme ja kyberturvallisuudessa turvallisuuden tunteella on suuri merkitys. Perustuslainkin mukaan jokaisella suomalaisella on oikeus turvallisuuteen. (1336/2997; Limnèll & Rantapelkonen 2017, 15–18.)

Haittaohjelmatutkimusten mukaan Suomi on tietoturvallisuuden kärkimaa (Peltomäki & Norppa 2006, 135–136). Euroopan mittakaavassa meillä on vähiten tietoturvallisuuspoikkeamia eli 0,29 %, kun keskiverto luku Euroopan maiden kesken oli 0,87 % (Kybersää sähköposti 3.11.2017). Uhkat tulee kuitenkin ottaa tosissaan, koska saatamme menettää omaisuutemme toimiessamme väärin kybermaailmassa. Kyberturvallisuuskeskuksen (2017) mukaan jokaisessa yrityksessä tulisi miettiä, mihin internetiä yrityksessä käytetään

ja millaisia palveluita tai tuotteita siellä myydään. On ajateltava tilannetta, jossa nettiyhteys ja kaikki tiedot ovat kadonneet. (Viestintävirasto 6.11.2017.)

Identiteettivarkauksilla, kuten käyttäjätunnuksien tai salasanojen kalastelulla, rikollinen voi mustata yrityksen maineen, kiristää, tehdä luottokorttiostoksia, tyhjentää pankkitilin, nostaa lainan tai tehdä laskuhuijauksen. Hyökkäys voi kohdistua myös sosiaaliseen yhteisöön, verkkokauppaan tai työpaikkaan. Tietovuodot eli luottamuksellisen tiedon välittäminen tai vuotaminen eteenpäin saattavat aiheuttaa yritykselle jopa miljoonien eurojen tappiot. (ITKP0002 Johdatus kyberturvallisuuteen 2016.) Maailmassa joutuu kyberhyökkäyksen kohteeksi 18 ihmistä joka sekunti (Lehto 2018, luento). Yksilöön kohdistuvia kyberhyökkäyksiä ei saa vähätellä, koska hyökkäykset heijastuvat monesti välillisesti tai suoraan yksilön työhön tai yrityselämään. Jos yksilö ei osaa tai halua toimia oikein yksityiselämässään, on hänen vaikea tehdä sitä työpaikalla.

Kauppakamarin tutkimusten mukaan sekä pienten että keskisuurten yritysten pahimmat uhat olivat 2015 67 %:sti kalasteluyritykset ja haittaohjelmat, kun 2016 ongelmaksi muodostuivat kiristyshaittaohjelmat ja luottamuksellisen tiedon vuotaminen (Yrityksiin kohdistuvat kyberuhat 2015 & 2016, 9, 8; eMarketer 2016). Vaaditaan valppautta, koska rikolliset keksivät aina uusia hyökkäyskeinoja vanhojen tilalle. Myös ENISA:n tutkimusten mukaan uhkat muuttuvat aina vuosittain (ENISA Report 2017, 9).

Internetin sisällöstä 90-99 % on syvää nettiä (Deep Web), jossa on pankkien, hallitusten ja erilaisten yritysten salattua verkkoliikennettä. Syvästä netistä vain pieni osa on pimeää internetiä (Dark Web), jolla tarkoitetaan rikolliseen toimintaan käytettävää internetin osaa. Dark Web:istä puolet toimii kyberrikollisten omana laittomana kauppapaikkana, mikä halutaan pitää piilossa. Dark Web:issä on rikollisten palveluita, kuten edullisia hakkerointityökaluja, joiden käyttäminen ei vaadi merkittävää koodausosaamista. TOR -verkossa rikollisen data kuljetetaan niin usean solmupisteen kautta, että on mahdoton tutkia, mistä se on peräisin ja mikä on sen päämäärä. Facebook- tai Twitter-tilin hakkerointi maksaa 130 $, gmailin hakkerointi 162 $, organisaation postilaatikon hakkerointi vain 500 $, Winlocker-kiristysohjelman käyttö 10-20 $. (Netin pimeä puoli 2018. Sub; Lehto 2018, luento.) Rikollisuus on siirtynyt fyysisestä maailmasta nettimaailmaan.

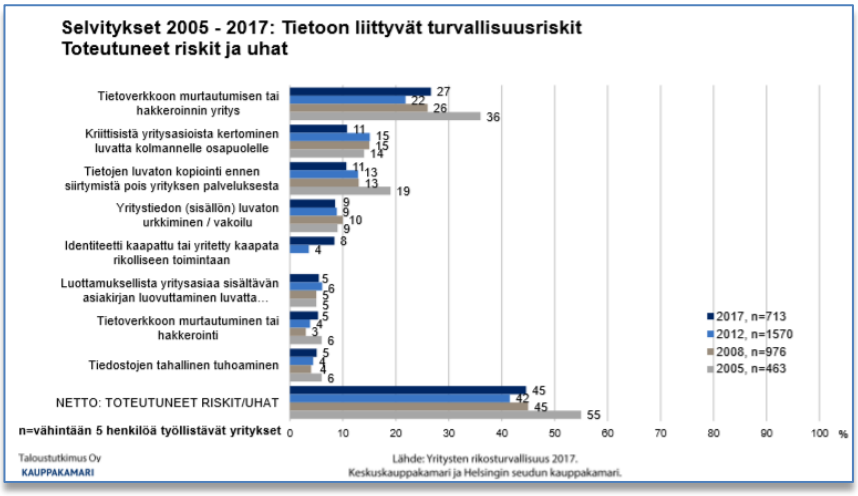
2.2.1 Suojattavat arvot ja kyberturvallisuuden myytit

Jokaisella yrityksellä on suojeltavaa henkilötietoa, dataa ja päätelaitteita. Kaikki tiedot sovellusmateriaalista, palkkalaskennasta, tarjouskirjeistä ja työsopimuksista ovat arvokkaita. Immateriaalioikeudet, kuten patentit, tavaramerkit tai uusimmat tuotesuunnitelmat antavat rikolliselle aina mahdollisuuden saada taloudellista etua. Tieto on liikesalaisuutta – aarretta – jonka menettäminen voi olla tuhoisaa yritykselle. Pelkästään Googlen avulla rikollinen pystyy pienistä tiedon jyväsistä muodostamaan kokonaiskuvan, jota hän käyttää hyväkseen kyberhyökkäyksissä.

Usein oletetaan, että tietojamme ei hyödytä varastaa tai sanotaan, että ystäviä, liikekumppaneita tai kavereita ei vakoilla. Puhutaan kyberturvallisuuden myyteistä, mutta kaikki tieto on kuitenkin arvokasta. Kysymys on vain ajasta, jolloin sosiaaliseen mediaan syötetty tieto onkin liiketoiminnan tai yksilön kannalta arvokasta, koska yritys tai yksilö saattaa tulevaisuudessa olla yhteyskunnallisesti tärkeässä roolissa ja tieto joutuu tarkempaan tarkasteluun. Yleinen ajatus on myös, että kyberturvallisuuden voi rakentaa, ostaa myöhemmin järjestelmän päälle tai koko kyberturvallisuuden voi ulkoistaa, mutta tällöin kustannukset nousevat usein kohtuuttoman suuriksi. (Kööpenhamina Cybersummits 2016; Lehto 2018, luento; Hyppönen 2017, luento.)

ICT-alan sanonta, *”paras palomuuri on puolimetriä ilmaa”*, ei pidä enää paikkansa. Haittaohjelmat ovat niin älykkäitä ja monimutkaisia, että ongelmia ei pysty välttämään, vaikka verkot erotetaankin internetistä. Ohjelmistopäivityksissä tietoa joudutaan siirtämään, jolloin virheellisellä toiminnalla tietoa voidaan varastaa eristetystä verkosta. Ei ole olemassa myöskään täysin turvallista järjestelmää, ohjelmistoa tai käyttöjärjestelmää, koska niissä on haavoittuvuuksia, joita ei ole vielä löydetty tai havaittu.

Rikollisilla on aina uusia hyökkäyskeinoja yrityksiä vastaan. Identiteetin kaappaamisesta (2017) näyttää tulevan nopeasti vakava rikoksentekomuoto, jonka uhreina ovat sekä yksittäiset henkilöt että yritykset. Näissä tapauksissa yritystä on yleensä haluttu erehdyttää maksamaan pieniä tai isoja summia rikollisen tilille. (Yritysten rikosturvallisuus 2017, 23.)



KUVIO 3. Tietoon liittyvät riskit (Yritysten rikosturvallisuus 2017, 23)

Yritysjohtajien ja nuorison haastattelujen (2018) perusteella kyberturvallista toimintaa estää käyttäjien laiskuus. Kauppakamarin raportin mukaan suurimpana esteenä turvalliselle toiminnalle ovat käyttäjien piittaamattomuus uhista sekä niihin liittyvän tiedon ja henkilökunnan tietotaidon ylläpitämisen riittämättömyys (Yrityksiin kohdistuvat kyberuhat 2016, 13). Vuosien kokemusten perusteella pahimmat ongelmat syntyvät puuttuvista ja puutteellisista käyttö-ohjeista sekä ohjelmien huonosta käytettävyydestä.

2.2.2 Kyberturvallisuuden uhkat ja niiltä suojautuminen

Jokaisen yrityksen on otettava huomioon liiketoiminnassaan kyberturvallisuuden merkitys. Isommilla yrityksillä on mahdollisuus palkata alan parhaat osaajat. Pienten yritysten on pakko turvautua konsultteihin, mikä lienee heille hyvä ratkaisu. Monissa yrityksissä ja organisaatioissa kyberturvallisuuden tehtävät kohdennetaan ICT-alan asiantuntijoille tai päälliköille, joilla on kuitenkin enää hyvin vähän resursseja ja aikaa alalle. Oman toimen ohella tehtävän työn tekeminen ei ole enää tehokasta. Kyberturvallisuutta on todella vaikea kehittää ja ylläpitää, jos alalle ei ole nimetty lainkaan kokopäiväistä vastuuhenkilöä. (Yrityksiin kohdistuvat kyberuhat 2015, 36–37.)

Kyberturvallisuus ei ole yleisesti vain ICT-alan asiantuntijoiden ongelma, vaan myös markkinoinnin ongelma. Markkinoinnista vastaavan tulee tietää missä tärkeät tiedot ovat ja miten niitä suojataan. Tiedon käsittelyssä käytettävät työkalut ovat keskeisiä hakkereiden kohteita eli uhkia, jotka on tunnistettava. Johdon on tehtävä strateginen päätös

kyberturvallisuuden parantamiseksi. Tietoturvallisuuspäällikkö vastaa alan koulutuksen järjestämisestä. Koulutus on toteuttaa siten, että markkinointi-, tietohallinto- ja turvallisuusjohtaja yhdessä kartoittavat keskeiset koulutettavat asiat, kuten markkinoinnin tiedon turvaaminen, pääsynhallinnan ja turvallisen etätyön tavat. (eMarketer 2016.)

Vuodesta toiseen yrityksen suurimat kyberturvallisuusuhat tulevat 53-60 %:sti edelleen organisaation sisältä (Yrityksiin kohdistuvat kyberuhat 2015; Lehto 2018, luento). Kyberturvallisuuden heikoimmaksi lenkiksi sanotaankin yrityksen omaa henkilöstöä. Henkilöstöstä voi kuitenkin tehdä kyberriskien parhaimman torjuntakeinon kouluttamalla säännöllisesti ja harjoittelemalla myös käytännössä. Lyhytkin tilanteenmukainen harjoitus riittää kehittämään suojautumismenetelmiä ja -keinoja. (Tietoturvaopas yrityksille 2016, 11; Vahti-teemaviikko 2017.) Yleensä yrityksessä aliarvioidaan lyhyen harjoituksen merkitys kyberturvallisuuskulttuurin kehittämisessä. Kauppakamarin raportin mukaan yrityksistä noin 90 % ei ole koskaan harjoitellut mitenkään suunnitelmiensa toimivuutta (Yrityksiin kohdistuvat kyberuhat 2016, 64).

Kaikenkokoisissa yrityksissä keskeiset ensimmäiset toimenpiteet kyberturvallisuusriskien vähentämiseksi voivat olla esimerkiksi:

- Määritellään keskeiset turvallisuusperiaatteet ja panostetaan koulutukseen.
- Yrityksen tiedot varmuuskopioidaan ja palautusprosessi testataan.
- Järjestelmät päivitetään, kybertilannekuva luodaan ja sitä valvotaan.
- Riskejä vähennetään monikerroksisella suojauksella, kuten kaksivaiheisella tunnistuksen käyttöönotolla, sisällönsuodatuksella, palomuureilla jne.
- Tietoturvaloukkauksiin varaudutaan vähentämällä riskien todennäköisyyttä ja minimoimalla toteutuneen riskin vahinko.
- Suunnitellaan liiketoiminnan jatkuvuus ja varaudutaan kriisitilanteisiin ennakolta. (Tietoturvaopas yrityksille 2016, 11–15.)

Kyberturvallisuuden tilan arviointi on jatkuva prosessi. Tärkeintä, yrityksen koosta riippumatta, on kuitenkin liiketoiminnan jatkuvuuden suunnittelu, joka sisältää yrityksen prosessien ja palveluiden riskien arvioinnin, kyberturvallisuuspolitiikan ja -suunnitelmien luomisen sekä prosessit toteutuneiden riskien vaikutuksen minimoimiseksi (Harris 2016, 94). Jos liiketoiminnan jatkuvuutta ei pystytä turvaamaan, yrityksen on siirryttävä katastrofin hallintaan. Liiketoiminnan jatkuvuuden hallinta on oltava prioriteetissa

ensimmäisenä. (Harris 2016, 94–95.) Pääasiallinen huolenaihe tulee olla henkilökunnan osaamisesta ja selviytymisestä. Johdon on annettava asialle tukensa.

Kyberturvallisuushäiriöihin varautumisesta on tehtävä ajattelutapa ja se on otettava huomioon heti yrityksen jokaisen hankkeen ja projektin alussa. Kyberturvallisuustoimet tulee myös rakentaa sisään kaikkiin yrityksen prosesseihin, laitteisiin ja järjestelmiin. (Tietoturvaopas yrityksille 2016, 16–17.)

Kyberturvallisuushäiriöiden vastatoimissa kannattaa keskittyä henkilöstön kouluttamiseen. Työntekijöiden on uskallettava ilmoittaa myös itse aiheuttamistaan häiriöistä. Näin luodaan parempaa turvallisuuskulttuuria, koska jokainen tekee virheitä. On myös nimettävä vastuutaho, joka huolehtii tietoturvallisuuspoikkeamien ja verkkorikosten käsittelystä ja niiden ilmoittamisesta johdolle, viranomaisille ja kyberturvallisuuskeskukselle. Vastuuhenkilöille on annettava valtuudet verkostoitumiseen alan muihin yrityksiin ja viranomaisiin. Ilmoittamalla rikoksista kaikkien yritysten tilannekuva paranee. (Tietoturvaopas yrityksille 2016, 17.)

Yrityksen johdolta vaaditaan selkeitä linjauksia ja ohjeita kyberturvallisuuden parantamiseksi. Koulutukseen panostamalla sosiaalinen urkinta voidaan estää, koska käyttäjien manipuloiminen arkaluonteisen tai luottamuksellisen tiedon urkkimiseksi on todella yleistä. Sisäverkon saastuminen voidaan estää sisällönsuodatuksella, kuten vertaisverkkojen ja aikuisviihde- ja pelisivujen liikenteen estämisellä. (Tietoturvaopas yrityksille 2016, 18). Verkkoliikenteen säännöt tulee olla selkeät ja yksinkertaiset, mutta niiden ei saa hankaloittaa tai hidastaa työn tekemistä, koska tällöin sääntöjä helposti rikotaan.

Yrityksen järjestelmät kannattaa suojata kaksinkertaisella tunnistautumisella, jossa verkkoon pääsemiseksi tarvitaan vahvan salasanan lisäksi esimerkiksi henkilökohtainen toimikortti ja PIN-koodi, sormenjälkitunnistus tai iiriksen skannaus. Kun käsitellään tai siirretään mobiililaitteilla tai USB-tikuilla luottamuksellista tietoa internetissä, tulee aina käyttää salausta huomioiden että laiteet ovat myös anastusherkkiä ja helposti hukattavia. (Tietoturvaopas yrityksille 2016, 18.) Eräs tämän päivän uhista on myös työntekijöiden omat laitteet, joihin on kiinnitettävä yrityksissä erityistä huomiota.

Yksi tapa kartoittaa yrityksen uhat on suorittaa kyberturvallisuuden itsearviointi. Tietoturvaoppaan (2016, 20–36) kysymyssarjaa jatkojalostaen liitteessä 1 (s. 92–106) on

esitetty kartoitukseen liittyvät kysymykset, joihin vastaamalla saadaan kokonaiskuva kyberturvallisuudesta. Vastauksien avulla kartoitetaan kyberturvallisuuden tasoa ja ohjataan yritystä kohti parempaa valmistautumista kyberturvallisuusuhkiin.

2.2.3 Voiko kyberturvallisuus olla mahdollisuus?

Asiakkailleen palveluita tai tuotteita myydessään yritysten on asetettava asiakasymmärrys keskiöön. Asiakkaan arvontuotantoprosessissa on erittäin olennaista, miten yritys voi olla avuksi asiakkaan huolien ja ongelmien, kuten turvallisuushuolien poistamisessa. Asiakas ei halua ostaa pelkästään tuotteita tai palveluja, vaan myös ongelmanratkaisuja. Palveluissa ja tuotteissa tulee olla arvokasta sisältöä. Aina asiakas ei välttämättä osaa tunnistaa mikä palvelussa tai tuotteessa huolettaa, mutta yritysjohto voi parantaa omaa palveluaan tai tuotettaan vastaamalla oheisiin arvolupauksen määrittämiseen helpottaviin kysymyksiin:

- Millaista arvoa yritys ja sen palvelut tai tuotteet tuottavat asiakkaille ja sisältävätkö ne turvallisuutta?
- Minkä asiakkaan ongelman tuote tai palvelu ratkaisee?
- Minkä asiakkaan perustarpeen yritys tyydyttää?
- Millaista tuoteportfoliota yritys tarjoaa eri asiakkaille? (Helenius 2016, 29–30.)

Maslow’n tarvehierarkiankin mukaan turvallisuus on yksi perustarpeistamme, joten jokaisen kysymyksen kohdalla vastaukseksi voimme ajatella kyberturvallisuuden lisäämisen sekä huomioimisen tuotteissa ja palveluissa. Yritysten tulisi keskittyä omissa palveluissaan asiakkaan turvallisuuden tunteen kasvattamiseen – sisäänrakennettuun turvallisuuteen – jolloin kyberturvallisuudesta tulee mahdollisuus.

2.2.4 Sosiaalisen median merkitys kyberturvallisuudessa

Massamediaan verrattuna nykypäivän sosiaalinen media (some) ”valeuutisineen” on yrityksille lähes mahdotonta hallita. Kuka tahansa voi perustaa oman median ja julkaista oikeaa tai valheellista sisältöä. Somen vuorovaikutus- ja keskustelumahdollisuudet sekä sen luonne on monelta monelle. Yrityksen maine tai brändi voidaan mustamaalata jo yhdellä videolla tai twiittauksella. Tilannetta voidaan tosin päivittää, joten maineen

korjaaminenkin on mahdollista. (Verkkouutiset 2018; Juslèn 2011, 197, 201.) Somessa voidaan varastaa kilpailijoilta tietoa tai levittää väärää tietoa ja saatu hyöty nähdään suurempana kuin kiinnijäämisen riski (Stanford yliopisto 2016; Verkkouutiset 2018). Uhkiin ja mahdollisuuksiin liittyen yritysten tulisi luoda hyvät ja tiiviit (korkeintaan kahden sivun pituiset) säännöt ja ohjeet, miten henkilöstö voi käyttää sosiaalista mediaa. Yrityksen sosiaalisen median ohjeen sisällöstä on esimerkki liitteessä 2 s. 107 (Leino 2012, 162–164).

Johdon on hyvä nimetä yrityksessä somevastaavat, jotka reagoivat heti epidemian lailla leviäviin ajatuksiin tai sisältöihin eli ”viraali-ilmiöihin”. Varsinkin, jos ilmiöt ovat yrityksen imagon kannalta negatiivisia. Tosin asiakkaiden vapaaehtoisesti levittämä tieto voi olla myös positiivinen asia yrityksen kannalta. ”Viraali-ilmiö” on kuitenkin joko tehokas voimavara tai uhka, jota on vaikea hallita (Juslèn 2011, 212).

Kun yritys käyttää sosiaalista mediaa asiakkaiden kuunteluun ja yleensä keskusteluun yhteisöpalveluissa, blogeissa ja keskustelufoorumeissa, tulee siitä mahdollisuus ja se voi korvata jopa kyselyt ja muut asiakastutkimukset. Parhaassa tapauksessa keskustelupiiri ryhtyy suosittelemaan yrityksen palveluita. (Juslèn 2011, 219,220,221.) Keskustelufoorumeilta kuulee myös, mikä asiakkaita kyberturvallisuudessa yleensä huolestuttaa. Parhaiten yritys menestyy, jos se onnistuu somen avulla saamaan suosittelijat aktiiviseksi mainostamaan yrityksen kyberturvallista tai tietoturvallista palvelua.

2.2.5 Yhteenveto kyberturvallisuuden merkityksestä yrityksille

Internet on osa kybertoimintaympäristöä ja takaa yrityksille vapaan informaatioväylän ja markkinoinnin työkalun. Samalla se kuitenkin heikentää sekä yritysten että asiakkaiden turvallisuuden tunnetta. Paras lopputulos saadaan, jos yrityksellä on halu tulla tunnetuksi osaavana, menestyvänä ja erityisesti luotettavana kyberturvallisen palvelun tai tuotteen tarjoajana. Yrityksellä tulee olla tahto näyttää, että heillä käsitellään asianmukaisesti ja kyberturvallisesti asiakkaan henkilötietoja eli halutaan parantaa asiakkaan turvallisuuden tunnetta. Eräs yrityksen toimitusjohtaja mainitsi vakavalla ilmeellä, että *kyllä meille on todella tärkeää yrityksemme imago* (Yrittäjien haastattelut 2017).

Digitalisaation avulla yksityisistä ja julkisista palveluista saadaan kyberturvallisuus huomioiden helppokäyttöisiä ja turvallisia. Kyberturvallisuuden merkitys tulee kasvamaan, koska esineiden internet, robotisaatio, keinoäly ja tiedolla johtaminen ovat alati kehittyviä aloja. Kyberturvallisuus on sisäänrakennettava palveluihin, jotta kustannukset eivät myöhemmin nouse liian suuriksi. Lisäksi palveluilta vaaditaan luotettavuutta, koska se on liiketoiminnan peruselementti.

Kybertoimintaympäristön hyödyntäminen rikollisuudessa on yleensä edullisempaa kuin tavanomaisten talousrikosten tekeminen, koska rikollinen voi aiheuttaa harmia mistä tahansa joutumatta kiinni. Työkalut haittaohjelmien tekemiseen ovat usein ilmaisia ja helppokäyttöisiä ja murtautumis- ja vakoilutyökalut ovat kenen tahansa käytettävissä.

Osaavat yrittäjät näkevät kyberturvallisuuden mahdollisuutena ja voimavarana kilpailukyvyn parantamisessa. He näkevät sen vahvistuvana liiketoiminnan alana, jossa turvallinen kybertoimintaympäristö helpottaa yrityksen oman toiminnan suunnittelua, minkä asiakkaatkin huomaavat lisääntyvänä turvallisuuden tunteena. Kyberrikollisuus (2017) aiheuttaa koko yhteiskunnalle ja sen palveluille vakavia uhkia, mutta yrityksien on kehitettävä omaa osaamista ja koulutettava henkilöstöään, jotta mahdollisuudet voittavat uhat. Kybermaailmassa ratkaisee osaamisen taso. (Limnèll 2017, luento.)

2.3 EU:n tietosuoja-asetuksen ja lakien sekä standardien merkitys

Kyberturvallisuutta ohjaa lakien ja asetusten sekä alan standardien lisäksi voimakkaasti 25.5.2018 sovellettavaksi tullut EU:n tietosuoja-asetus. Nämä luovat pohjan kyberturvallisuuden ja tietoturvallisuuden rakentamiselle. Seuraavissa alaluvuissa käsitellään lakien, asetusten ja standardien merkitystä ja vaikutusta yritysten toimintaan ja kilpailukykyyn.

2.3.1 EU tietosuoja-asetuksen merkitys ja vaikutus yrityksille

EU:n tietosuoja-asetuksen keskeinen tavoite on ajantasaistaa ja yhdenmukaistaa tietosuojaa koskevaa sääntelyä Euroopassa ja vastata teknologian huimaan kehitykseen, kuten tekoälyyn ja globalisaatioon liittyviin henkilötietojen kehitystä koskeviin haasteisiin (2016/679, 1 artikla; Oikeusministeriön julkaisu 4/2017, 9). Samanlaiset ja yhtenäiset

säännöt yritysmaailmassa tuovat oikeudenmukaisuutta ja parantavat tietosuojaa, koska säännöt ovat nyt kaikille samat.

Asetus tulee parantamaan kyber- ja tietoturvallisuutta sekä tietosuojaa, kuten rekisteröidyn oikeuksia. Jatkossa ne huomioidaan jokaisessa tietojärjestelmähankkeessa ja suunnittelussa heti ensimmäisestä askeleesta asti niin, että turvallisuus on sisäänrakennettuna kaikkiin rakenteisiin, laitteisiin, ohjelmistoihin ja palveluihin. Asetus tuo kustannussäästöjä, koska jälkikäteen muutoksien tekeminen järjestelmiin ja toimintoihin on kallista ja usein jopa mahdotonta. (Oikeusministeriön julkaisu 4/2017, 13, 23.) Aika ja asetusta täydentävä Suomen kansallinen laki näyttävät, miten ”lain henki” vaikuttaa yritysten turvallisuuskulttuuriin. Asetuksen tavoite on selkeä. Tuoda markkinoille positiivista ja tervettä kilpailua, vaikka toisenlaisiakin näkemyksiä on esitetty.

Henkilötietolain ansiosta olemme tietosuojan osalta Euroopan kärjessä. Suomessa on aina huolehdittu hyvin yksilön oikeuksista ja yksityisyydestä. Yksityiselämän suoja on perustuslainkin mukaan perusoikeutemme – ihmisten yksityisyys turvataan eli ”kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton” (Perustuslaki 1999/731/10§). Lait ja asetukset velvoittavat, että asiakkaiden henkilötietoja käsitellään yrityksissä asianmukaisesti ja niitä myös suojataan.

Tavoiteasetelmassa EU:n tietosuoja-asetuksen tulisi olla yritykselle mahdollisuus lisätä kilpailukykyä, luotettavuutta ja henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä. Asiakkaiden osalta asetus parantaa erityisesti rekisteröityjen oikeuksia valvoa henkilötietojensa käsittelyä. (2016/679, 1 artikla; Oikeusministeriön julkaisu 4/2017, 9.)

Tietosuoja-asetus koskee myös pieniä ja keskisuuria yrityksiä sekä julkista sektoria riippumatta henkilötietojen käsittelyn laajuudesta, käsiteltävien tietojen luonteesta tai käytettävästä teknologiasta. Sen täytäntöönpanoa ohjaa tuntuvat sanktiot, jonka valvontaviranomainen voi määrätä rekisterinpitäjälle ja/tai henkilötietojen käsittelijälle, jos vaatimuksia laiminlyödään. Sakkojen enimmäismäärä on merkittävä, jopa 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta. (Oikeusministeriön julkaisu 4/2017, 9; Vahti-raportti 1/2016, 30.)

Kauppakamarin tutkimus kuitenkin osoittaa, että alle 50 hengen yrityksistä vain 29 % oli varautunut asetuksen vaatimuksiin, 49 % ei ollut varautunut lainkaan ja 22 %:lla ei ollut

kokemusta asiasta tai ei vain osannut sanoa. Rakennusalalla lähes 60 % yrityksistä ei ollut varautunut asetukseen lainkaan. (Yritysten rikosturvallisuus 2017, 19.)

Keskeisiä tietosuoja-asetuksen tietosuojaperiaatteita ovat henkilötietojen käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus. Rekisterinpitäjän on myös osoitettava, että tietosuojaperiaatteita noudatetaan, mikä on merkittävä ero aikaisempaan. (Oikeusministeriön julkaisu 4/2017, 12.) Paremman suunnittelun lisäksi yritykseltä vaaditaan nyt huolellisempaa henkilötietojen ja tietoturvallisuuden dokumentointia.

Henkilötietojen suojaamiseksi käytetään teknisiä ja organisatorisia toimenpiteitä, kuten käytön valvontaa, tietojen salausta, henkilöstön koulutusta, ohjeita ja määräyksiä (Vahti-raportti 1/2016, 22). Lukuisat suojautumisen keinot liittyvät siis perinteiseen tietoturvallisuuteen. Yritykset tekevät kuitenkin päätökset, mitä keinoja ne käyttävät huomioiden kustannukset, käytössä olevan tekniikan, käsittelyn luonteen ja laajuuden, asiayhteyden ja riskit (Oikeusministeriön julkaisu 4/2017, 13). Menetelmien yhdisteleminen on suosittua, mutta kustannusten pienentämiseksi tulisi suosia koulutusta ja ohjeita, koska ne ovat helppo, yksinkertainen ja nopea ratkaisu. Lain mukaan ne eivät kuitenkaan aina riitä.

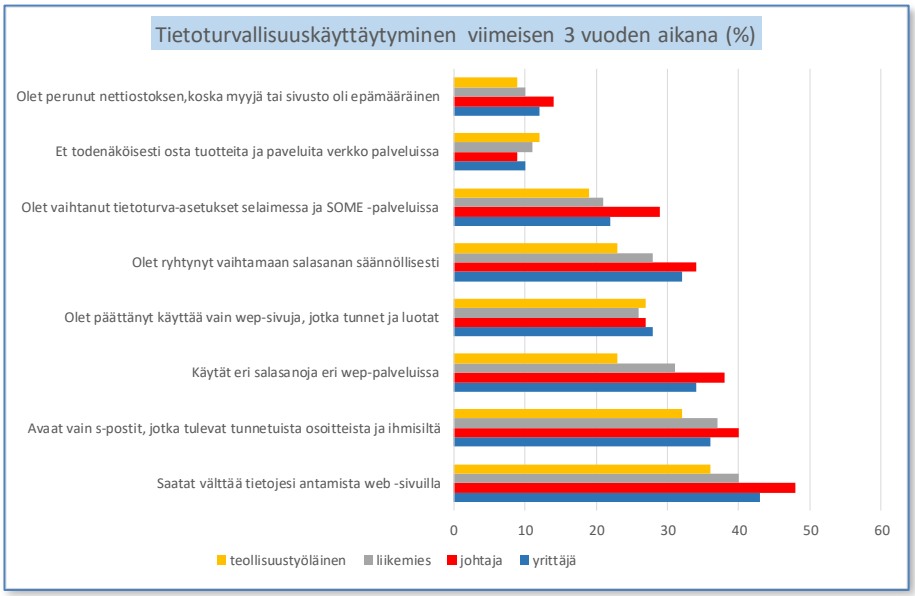
Järjestelmä- ja sovelluskehittäjälle asetus tuo haasteita rekisterinpitäjän velvoitteiden toteuttamiseksi. On esimerkiksi selvitettävä, miten suostumus kysytään tai henkilötietoja siirretään järjestelmästä toiseen. (Vahti-raportti 1/2016, 34.) Asetuksen vaatimat velvoitteet tunteva ja asiakasta arvostava yritys toteuttaa vaatimukset ohjelmistoissa automaattisesti, koska asiakas olettaa, että ohjelmisto täyttää lakien ja asetusten antamat tietosuojavelvoitteet.

Yrityksen tulee nimittää myös henkilötietojen käsittelyyn tietosuojasuojavastaava. Vaatimus ei ole kaikille yrityksille ehdoton, mutta asia tulee selvittää aina tapauskohtaisesti. Viranomaiselle ja julkishallinnolle vaatimus on ehdoton (2016/679/EU.) Asetus antaa mahdollisuuden myös yhteiseen tietosuojavastaavaan, mikä tuo pienille yrityksille varmasti kustannussäästöjä ja yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten (Oikeusministeriön julkaisu 4/2017, 35).

2.3.2 EU -tietosuoja-asetuksen uhkat ja mahdollisuudet

Tietoturvayritykset arvioivat asetuksen heikentävän kyberturvallisuutta, koska kyberrikollisten jäljittäminen vaikeutuu ja yritykset ovat vähemmän halukkaita jakamaan tietojaan uusista uhista, koska asetus ei siihen kannusta. (Krebsonsecurity 2018.) Kyberrikollisten jäljittäminen on vaikeaa, joskus jopa mahdotonta. Jokin yritys saattaa nähdä kilpailuedun myös siinä, että pitää tiedon keskeisestä uhasta omana tietonaan. Ikävien yllätysten välttämiseksi asetusta tulee kuitenkin noudattaa. Tietoturvallisuusasiantuntija Mikko Hyppösen mukaan asetuksen voimaantulo saattaa lisätä kyberrikollisuutta ja kiristystä, koska se tavallaan hinnoittelee henkilötiedot (Hyppönen 2017, luento).

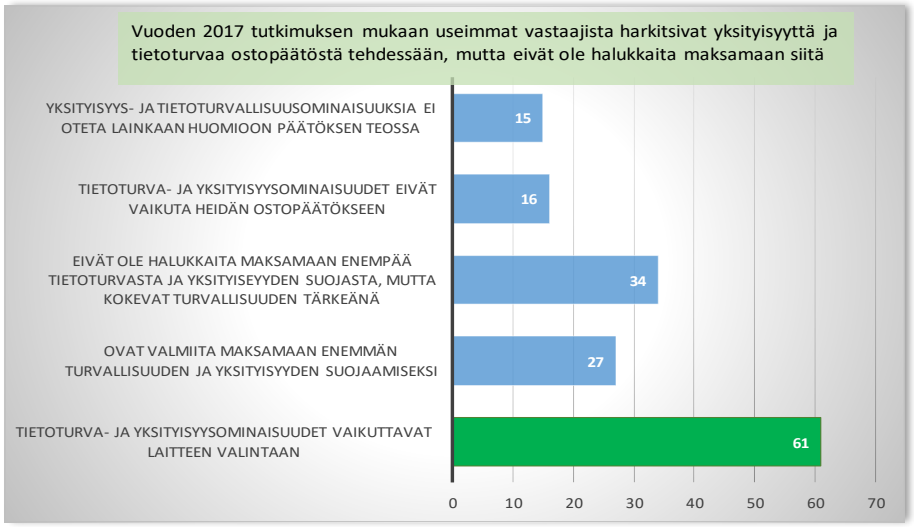
Asetuksen tuomia mahdollisuuksia tukee laaja EU:n tutkimus, jossa vastaajia pyydettiin valitsemaan ne vaihtoehdot, joita he olivat tehneet viimeisten kolmen vuoden aikana tietoturva- ja yksityisyydensuojaongelmiin liittyen. Kuvion 4 mukaan Suomessa johtajien ja yrittäjien asenne on tietoturvallisempi verrattuna muihin. Lähes 50 % saattaa välttää tietojen antamista web -sivuilla. Noin 10 % suomalaisista on perunut nettiostoksen, koska myyjä tai sivusto oli epämääräinen. Lähes 30 % käyttää vain tuntemiaan ja luotettavina pitämiään palveluita. (Special Eurobarometer 460 2017, 108.) Johtajien tulisi erottua vielä selkeämmin omalla turvallisella käytöksellään, koska esimerkissä on voimaa.



KUVIO 4. Johdon tietoturvallisuuskäyttäytyminen viimeisen 3 vuoden aikana[2]

[2] Tutkimuksessa haastateltiin kaikkiaan 27000:a eri maiden kansalaista.

Laitteiden ostopäätöstä tehdessään kansalaiset ovat huolissaan turvallisuudestaan, mutta maksuhalukkuus on vielä melko vähäistä. Tutkimuksen mukaan tietoturvallisuudella ja tietosuojalla on yhä suurempi merkitys kuluttajan ostopäätökseen, kuten kuviosta 5 nähdään. (Special Eurobarometer 460 2017, 109.)



KUVIO 5. Turvallisuuden vaikutus ostopäätökseen (Special Eurobarometer 460, 109.)

Identiteettivarkaudet eli henkilötietojen oikeudeton käyttö ovat lisääntyneet, mikä korreloi suoraan tilauspetosten määrään. Rikoksen uhrille ongelmat ovat kohtuuttomat, koska tietovuotoa ei voi peruuttaa. (Vaarat netissä 2018. Yle & Fem.) Yritysten tehtävä on estää tilauspetoksia suosimalla verkkopankkitunnistautumista nettiostosten yhteydessä.

Asetus tuo kuitenkin lukuisia madollisuuksia, kuten kilpailuetua Suomelle, koska tietosuojasta on aina pyritty huolehtimaan. Se tuo läpinäkyvyyttä ja avoimuutta henkilötietojen käsittelyyn parantaen rekisteröityjen oikeuksia. Se lisää sisäänrakennettua tietoturvallisuutta ja tietosuojaa. Lisäksi se kannustaa tekemään laadukkaampia ohjelmistoja.

2.3.3 Henkilötietojen käsittely ja rekisteröidyn oikeudet

Henkilötietojen keräämiseen tulee olla selkeät perusteet, kuten asiakassuhde. Tietoja on käsiteltävä asianmukaisesti ja asiakkaan kannalta läpinäkyvästi. Suostumus on annettava selkeästi kirjallisella, sähköisellä tai suullisella lausumalla, josta käy ilmi rekisteröidyn

vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn. (Oikeusministeriön julkaisu 4/2017, 19–22.)

Asetuksen (2016/679/EU, artiklat 12–22) mukaan uudet rekisteröityjen oikeudet ovat

- oikeus poistaa henkilötiedot eli ”oikeus tulla unohdetuksi”
- oikeus määrätyissä tilanteissa siirtää henkilötiedot järjestelmästä toiseen
- oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta, kuten selkeän kuvauksen tapahtuneesta, tietosuojavastaavan yhteystiedot tai muun yhteyspisteen.

Yrityksessä on suunniteltava, miten mainittu tietoturvaloukkaus tunnistetaan, ilmoitetaan, selvitetään ja dokumentoidaan (Oikeusministeriön julkaisu 4/2017, 33). Ohjeistukset henkilötietojen käsittelystä tulee olla myös selkeät ja käytännönläheiset.

2.3.4 Mitä johto voi tehdä tietosuojan parantamiseksi?

Yrityksessä on tehtävä tietotilinpäätös eli kartoitus, joka on kokonaiskuva henkilötietojen käsittelyn tilasta. VM:n ohjeen (2017) mukaan tietotilinpäätös on dynaaminen dokumentti, joka tukee yrityksen tehokkuutta, vaikuttavuutta ja kilpailukykyä. Se tulee suhteuttaa yrityksen toiminnan ja koon mukaisesti ja siinä kuvataan yrityksen henkilötietovarannot, tietosuojaperiaatteet, toimintaan liittyvät henkilötietovirrat, henkilötietojen käsittelyn oikeusperusteet, tietoturvallisuus ja riskien hallinta. Se antaa johdolle, työntekijöille, asiakkaille ja sidosryhmille sekä valvontaviranomaiselle selkeän kokonaiskuvan yrityksen tietojenkäsittelyn nykytilasta toimien täten johtamisen tukena, mittarina ja toiminnanohjauksen välineenä. (Laadi tietotilinpäätös 2012, 3,6,9.)

Tietotilinpäätös kannattaa tehdä, koska tieto on yritykselle arvokas ja keskeinen sekä jatkuvasti kasvava tuotannon tekijä, jonka ympärille kehittyy jatkuvasti uusia palveluja (Laadi tietotilinpäätös 2012, 4). Tietotilinpäätös parantaa myös tietojenkäsittelytavan noudattamista, koska tietohallintolaki (621/1999 18 §) edellyttää, että käsiteltävän henkilötiedon saatavuus, suoja ja laatu turvataan. Tietosuojaa parannetaan siis tietoturvallisuuden kautta ja ohjeena on kerätä vain tarpeellinen henkilötieto.

Yrityksessä arvioidaan myös henkilötietojen käsittelyyn liittyvät riskit ja toimenpiteet riskien minimoimiseksi ottaen huomioon henkilötietojen määrän ja laadun, kuten erityiset henkilötietoryhmät (Laadi tietotilinpäätös 2012, 4–5). Paras keino riskien lieventämiseen on suojata sekä työntekijöiden että asiakkaiden henkilötietojen koko elinkaari.

Asiakkaille suunnatuilta palveluilta ja järjestelmiltä tulee edellyttää luottamuksellisuutta, eheyttä, käytettävyyttä ja vikasietoisuutta. Suojaamisen lisäksi henkilötietojen käsittelyä tulee seurata ja valvoa. (Oikeusministeriön julkaisu 4/2017, 31.)

Tietotilinpäätöksen lisäksi yrityksen nettisivuille tulee tehdä tietosuojailmoitus, millä osoitetaan, että asiakkaan tietosuojasta huolehditaan. Ilmoitus on yrityksen tietosuojan näyteikkuna, jonka kautta asiakas tutustuu yrityksen tietosuojaan. Ilmoitus (rekisteriseloste) kannattaa tehdä, vaikka siitä ei suoraan mainita asetuksessa, koska artiklassa 30 annetaan laajat informaatiovelvoitteet henkilötietojen käsittelystä (2016/679/EU). Ilmoitus ei saa olla teknistä ”kapulakieltä”, vaan tekstiä, jonka kuka tahansa ymmärtää. Ilmoitus voidaan toteuttaa esimerkiksi havainnollisena videona tai kuvana, jolloin yritys erottuu edukseen muista.

2.3.5 Lakien ja standardien merkitys kyberturvallisuudessa

Lakien ja asetusten lisäksi tietoturvallisuutta ja kyberturvallisuutta ohjaavat vahvasti alan standardit, jotka eivät ole velvoittavia, mutta niiden merkitystä kyberturvallisuudelle ei tule väheksyä. Yrityksen asiakkaan kannalta on aina parempi, jos palvelut ja tuotteet, joita kuluttaja ostaa ovat turvallisia ja standardien mukaisia.

ISO/IEC 27000 standardit antavat hyvät suuntaviivat kuinka tietoturvallisuuden hallintajärjestelmää tulisi yrityksessä rakentaa ja ylläpitää. Standardeissa annetaan ohjeet kuinka yrityksen tulee suunnitella, käyttöönottaa ja ylläpitää tietoturvallisuuspolitiikkaa, prosesseja ja tekniikkaa hallitakseen riskit, jotka kohdistuvat yrityksen kallisarvoisiin arvoihin ja tietoihin. Standardisarjat ISO/IEC 27000-27008, 27011, 27014-27015, 27031-27035, 27037 ja 27799 käsittelevät jokainen tarkemmin tiettyä alaa, kuten ICT-alaa, riskien hallintaa tai liiketoiminnan jatkuvuutta. Standardeista ISO/IEC 27032 käsittelee tarkemmin kyberturvallisuutta. Paljon käytetyn ISO/IEC 27001 tietoturvallisuusstandardin avulla voidaan rakentaa ISMS (Informaation Security Management System) eli tietoturvallisuuden hallintajärjestelmä, joka on kokoelma käytäntöjä ja menettelytapoja yrityksen arkaluonteisten tietojen ja järjestelmien hallintaan. (Harris 2016, 16–18.) Standardien lisäksi yritysmaailmassa ovat osittain käyttökelpoisia VM:n vahti-ohjeet, joissa on otettu huomioon lakien, asetusten ja standardien vaatimukset.

Tietosuoja-asetuksen lisäksi kyberturvallisuuden juridiikkaan liittyy paljon lakeja, joista mainittakoon tietoturvallisuusasetus (681/2010), laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), laki viranomaisen toiminnasta julkisuudessa (621/1999), laki turvallisuusselvityksistä (177/2002), laki yksityisyyden suojasta työelämässä 759/2004 (työelämän tietosuojalaki), arkistolaki (831/1994) ja tietoyhteiskuntakaari (TYK, 917/2014), joka ohjaa sähköisen viestinnän tietosuojaa.

2.3.6 Yhteenveto ja johtopäätökset

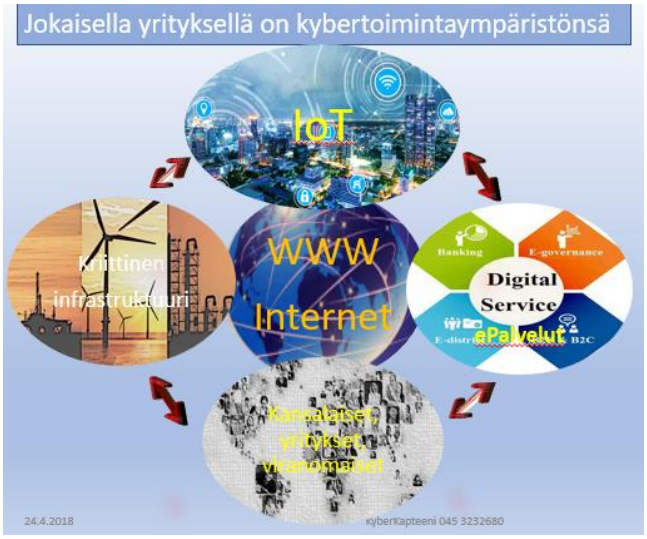
EU:n tietosuoja-asetus on velvoittava lainsäädäntö, joka kehittää yritysten kilpailukykyä sekä velvoittaa samalla yrityksen johtoa sitoutumaan tietosuojan parantamiseen tietoturvallisuuden kautta. Tietosuojan parantaminen vaatii tiedon eheyden, käytettävyyden ja luottamuksellisuuden turvaamista. Luotettavuus on asiakkaalle keskeinen digitaalisten palveluiden ominaisuus. Asetuksen vaatimat toimenpiteet voi tehdä tietotilinpäätöksessä, joka antaa kokonaisvaltaisen näkökulman yrityksen tietovarannoista ja johto voi käyttää sitä työkaluna moneen asiaan.

Asetuksen ansiosta tietosuoja ja tietoturvallisuus käsitteinä lähenevät toisiaan. Tietosuoja tavallaan asettaa vaatimukset ja tietoturvallisuudella vaatimukset toteutetaan. Yritykselle tulisi myös kirjoittaa yhteinen tietosuojapolitiikka, jossa kuvataan vastuut ja keskeiset tavoitteet sekä johdon tahtotila. Tietosuojaselosteet tai tietosuojailmoitukset voi tehdä erikseen omalle henkilöstölle ja asiakkaille. Keskeisimmistä järjestelmistä kannattaa edelleen tehdä rekisteriselosteet. Jokaisella toimialalla on myös henkilötietojen käsittelyyn liittyen erityispiirteet. Ei siis ole olemassa yksiselitteisiä ja yhtenäisiä, kaikille toimialoille sopivia ohjeita, millä menetelmillä henkilötietoja tulisi suojata.

Tietosuoja-asetus haastaa yritykset riskien minimointiin, hyvän maineen rakentamiseen, kansalaisten ja kuluttajien luottamuksen säilyttämiseen. Yrityksen tulisikin kirjata tietosuojapolitiikkaansa tavoitteeksi mielellään ylittää lain ja asetusten antamat vaatimukset, jotta se saavuttaisi kilpailuetua muihin nähden. Kyseessä voi olla pienikin kohteliaisuusteko asiakkaan tietosuojan parantamiseksi. Tietosuojasta ja tietoturvallisuudesta huolehtimisesta tulee ja on tullut jo osa hyvää, luotettavaa ja turvallista palvelua.

2.4 Kyberturvallisuuden johtaminen yrityksessä

Kyberturvallisuuden johtaminen edellyttää, että yritys tunnistaa sille ominaisen kybertoimintaympäristön, jota on kuvattu kuviossa 6. Kybertoimintaympäristössä keskiössä on internet. Sen ympärillä olevilla osakokonaisuuksilla on paljon keskinäisriippuvuuksia, jotka johdon tulee sisäistää ja ymmärtää.



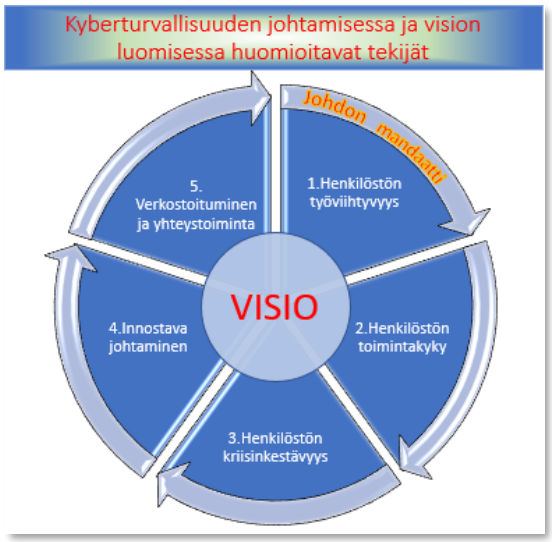
KUVIO 6. Yrityksen kyberturvallisuusympäristö (Lehto 2018, luento, muokattu)

Seuraavissa alaluvuissa käsitelläänkin kyberturvallisuuden johtamista yrityksen vision, kyberturvallisuusstrategian ja -politiikan, riskien hallinnan, vastuun, uhkien tunnistamisen ja niiltä suojautumisen sekä verkostoitumisen osalta. Lisäksi käsitellään kyberturvallisuuden rakentamista ja kartoitusta yrityksessä sekä alan innovatiivista johtamista.

2.4.1 Kyberturvallisuuden visio ja strategia sekä politiikka

Jokaisella yrityksellä tulisi olla kyberturvallisuuden visio kirkkaana mielessä. Vision ominaispiirteitä voivat olla esimerkiksi seuraavat: 1) Asiakasta kyetään palvelemaan kaikissa kriisitilanteissa, vaikka yrityksen tietojärjestelmät olisivat kyberhyökkäyksen kohteena. 2) Kyberturvallisuuden visio on yhtenevä yrityksen vision kanssa. 3) Työntekijöillä on käytössään luotettavat, toimivat, ajanmukaiset ja tietoturvalliset ICT-järjestelmät sekä liiketoiminnan kannalta tärkeimmät työkalut ovat kahdennettu ja varmennettuja.

Vision luomisessa ja yleensä kyberturvallisuuden johtamisessa on keskeisiä taustatekijöitä, kuten ihmisten innostava johtaminen, verkostoituminen, henkilöstön työviihtyvyys, toimintakyky ja kriisinkestävyys. Lisäksi johdon mandaatti visiolle on ehdoton.



KUVIO 7. Yrityksen kyberturvallisuuden johtamisen ja vision tekijät

Kybertoimintaympäristössä muutokset tulevat nopeasti eri kyberhyökkäysten ja haittaohjelmien muodossa, mikä edellyttää yrityksiltä nopeaa, läpinäkyvää ja paremmin koordinoitua – johdettua – toimintaa sekä yrityksen sisällä että yhdessä muiden yritysten ja viranomaisten kanssa (Suomen kyberturvallisuusstrategia 2013, 4). Yrityksen ylimmän johdon tulee määritellä kyberturvallisuuden strateginen linjaus ja ohjaus kohdentamalla taloudelliset ja inhimilliset resurssit. On nimettävä kyber- tai tietoturvallisuusvastaavat ja kyberturvallisuuden johto, jolla tulee olla käytössään luotettava ja reaaliaikainen kyberturvallisuuden tilannekuva. (Suomen kyberturvallisuusstrategia 2013, 4,38; Tietoturvaopas yrityksille 2016, 10.) Tilannekuvaa kootaan erityisesti viranomaisilta ja julkisista lähteistä. Luonnollisesti kyberturvallisuuden ”tiimin” koko tulee suhteuttaa yrityksen kokoon ja toimintaan.

Yrityksen kyberturvallisuuden toimintamallia on hyvä rakentaa Suomen kyberturvallisuusstrategian (2013) mukaisesti seuraavien periaatteiden avulla:

1. Sekä yrityksen että asiakkaiden kyberturvallisuus perustuu koko yhteiskunnan ja yrityksen omiin tietoturvallisuuden teknisiin ja hallinnollisiin järjestelyihin.
2. Yrityksellä on käytössään tarkoituksenmukaiset, riittävät ja turvalliset tietojärjestelmät ja tietoliikenneverkot, joiden käyttöä harjoitellaan kriisien varalta.

3. Yrityksen tulee seurata kyberturvallisuuskeskuksen jakamaa tilannekuvaa.
4. Viranomaisten ja yritysten välinen yhteistyö on oltava jatkuvaa, vastuunjako selkeää ja yritysten toiminta tulee perustua lakiin ja asetuksiin.
5. Kyberturvallisuus on kiinteä osa yrityksen kokonaisturvallisuutta. (Suomen kyberturvallisuusstrategia 2013, 5.)

Erityisesti kilpailukyvyn parantamiseksi yritysten tulisi panostaa voimakkaasti kyberturvallisuuden koulutukseen, harjoitteluun, tuotekehitykseen ja tutkimukseen sekä asiakkaan turvallisuudentunteen lisäämiseen.

Johdon on näytettävä omalla toiminnallaan, että se sitoutuu kyberturvallisuuteen ja ymmärtää sekä tukee yrityksen riskien hallintaa, jotka ovat keskeisiä tekijöitä menestykseen. Johdon strategisia linjauksia tai tavoitteita ovat: 1) Tilannetiedon parantaminen olemalla aktiivisesti yhteydessä kyberturvallisuuskeskukseen. 2) Kehittämällä osaamista kouluttamalla ja harjoituttamalla asiantuntijoita ja henkilöstöä haavoittuvuuksien havaitsemiseen sekä kyberuhkien torjumiseen. 3) Kehittämällä ohjeistusta ja koulutusta jatkuvasti. 4) Toteuttamalla yrityksessä riskien kartoitus ja tunnistamalla tärkeimmät suojattavat arvot tai materiaalit. 5) Varmistamalla johdolle ajantasainen kyberturvallisuustilannekuva ja yrityksen kyky suojautua sekä toipua kyberhäiriötilanteissa. (Suomen kyberturvallisuusstrategia 2013, 7–9.) Johtaminen ei onnistu vain toimistosta käsin, vaan johdon on näkyvästi osoitettava kiinnostuksensa osallistumalla mm. riskien hallintaan ja valvontaan sekä kehitettävä yrityksen turvallisuuskulttuuria omalla esimerkillä.

Kyberturvallisuusstrategian toteuttamisen pohjana voidaan käyttää Suomen kyberturvallisuusstrategian (Suomen kyberturvallisuusstrategia 2013, 38–40) jatkuvan parantamisen prosessiajattelua – toimintatapamallia, jonka käynnistämiseen tarvitaan ehdottomasti yrityksen johdon tuki ja mandaatti, josta on tarkempi kuvaus liitteessä 3.

Yleinen virhe on panostaa liikaa tekniikkaan, kun pitäisi keskittyä yrityksen kriittiseen tietoon. Yrityksen kyberturvallisuuspolitiikan tulisikin sisältää paljon käytännön asioita. Näitä ovat uhka- ja riskianalyysi, ratkaisut uhkilta suojautumiseen, vastuiden määrittelyt, aineellisten ja henkisten resurssien määrittely, seuranta, valvonta, auditointi ja harjoittelu. Johdon on huomioitava avaintehtäviä jaettaessa sopivuus tehtävään ja erityisesti henkilön motivaatio alalle. Kyberturvallisuuspolitiikka pitää myös jalkauttaa henkilöstön toimintatapoihin. (Lehto 2018, luento; Tietoturvaopas yrityksille 2016, 16.) Lyhyesti määriteltynä politiikan tulisi sisältää ainakin johdon tahtotila kyberturvallisuuden toteutumisesta,

vastuista ja kehittämisestä. Politiikan tavoite voi olla turvata yrityksen tuotannolle kriittisten tietoteknisten järjestelmien toiminta ja kriittisen tiedon saatavuus. Kyberturvallisuutta parannettaessa kannattaa ryhtyä parantamaan asioita tietoturvallisuuden eli tiedon eheyden, luotettavuuden ja saatavuuden kautta, jotka ovat hyvin käytännönläheisiä suojautumiskeinoja. Liitteessä 4 on tarkempi kuvaus kyberturvallisuuspolitiikan sisällöstä (Cybersecurity Essentials, luku 2.4).

Yrityksen johto vastaa myös siitä, että sietokyky kyberuhkia vastaan mitoitetaan yrityksen tavoitteiden mukaisesti. Yrityksellä on oltava ennakointi- ja varautumiskykyä kyberhäiriötilanteissa sekä toipumiskykyä häiriön jälkeisessä tilanteessa. (Suomen kyberturvallisuusstrategia 2013, 4,19.)

Esimerkiksi käytettävyyden takaamiseksi yrityksellä tulee olla kyky poistaa viat ja häiriötekijät, tunnistaa virheet ja viat nopeasti. On pyrittävä korkeaan kriittisen tiedon käytettävyyteen. Kriittisiltä järjestelmiltä vaaditaan kyberresilienssiä – kyberuhkien sietokykyä eli kykyä selvitä, vastustaa ja palautua haitallisesta kybervaikuttamisesta. Uhkan saattaa muodostaa luonnonkatastrofi, työntekijän inhimillinen virhe, levyjärjestelmän rikkoutuminen, sabotaasi, ohjelmistovirhe, varkaus tai sähkökatkos, joista tulee pyrkiä torjumaan pahimmat ja todennäköisimmät. (Cybersecurity Essentials, luku 6.1.)

Järjestelmien osalta koko turvallisuuden perusta rakentuu siihen, miten hyvä tilannekuva yrityksellä on omista laitteista. Jokainen mahdollisen turvallisuusriskin sisältävä verkkolaite, palvelin, ohjelmisto on kartoitettava ja tunnettava. On tunnistettava ja luokiteltava suojattavat asiat, tieto ja materiaali. Perinteinen ICT-alan tapa parantaa turvallisuutta on vakioida ja standardisoida yrityksen käytössä olevat laitteet, ohjelmistot, mikä helpottaa ylläpitoa ja laskee kustannuksia, koska laitekannasta ei muodostu kirjavaa.

Jos tärkeäksi tunnistettu arvo on tieto, voidaan tiedon luokittelussa ottaa mallia esimerkiksi valtionhallinnosta (Vahtiohje 2/2010, tietoaineistojen luokittelu). Kriittinen ja yritykselle salainen tieto voidaan luokitella salaiseksi tai luottamukselliseksi ja muu tieto julkiseksi. Yritys voi luokitella tiedon myös sen mukaan, kuinka arvokasta, herkkää tai kriittistä tieto on toiminnan kannalta. Tietoturvallisuuden peruskäsitteet eli saatavuus, luottamuksellisuus ja eheys, tulee myös priorisoida tilanteen ja toimialan mukaan. Lisäksi kaikelle tiedolle on aina määritettävä omistaja.

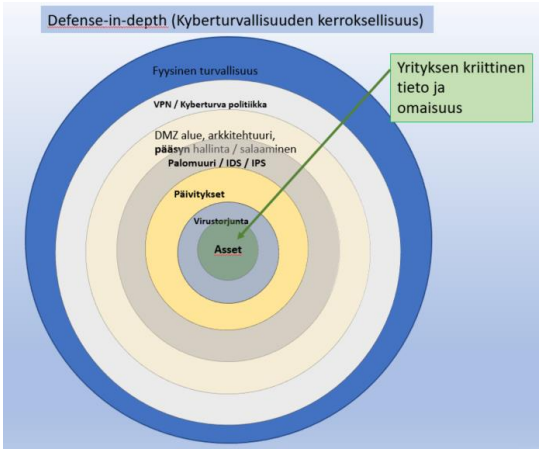
2.4.2 Kyberturvallisuusriskien kartoittaminen ja niiltä suojautuminen

Yleisin tapa riskien analysointiin on käyttää laadullista riskianalyysiä, jossa riskille arvioidaan sen vaikuttavuus ja toteutumistodennäköisyys. Työ kannattaa tehdä tiimeissä, jotta saadaan mahdollisimman laaja näkemys riskiarvioon. Mikäli päädytään arviossa punaiselle alueelle, on kyseessä vakavampi riski. (Cybersecurity Essentials 6.2.)

Category	Frequent - 5	Likely - 4	Occasional - 3	Seldom - 2	Unlikely - 1
Catastrophic - 4	20	16	12	8	4
Critical - 3	15	12	9	6	3
Marginal - 2	10	8*	6	4	2
Negligible - 1	5	4	3	2	1

KUVIO 8. Riskikartoituksen tekeminen (Cybersecurity Essentials 6.2.)

Kartoituksen jälkeen riskien toteutumista ja niiden vaikutusta on pystyttävä pienentämään. Riski voidaan myös hyväksyä, jos sen vaikutukset ovat pienet. Muita keinoja ovat valvonnan lisääminen, toimintatapojen muuttaminen tai pääsyn rajoittaminen jne. Hyvä keino riskien pienentämiseksi on suojauksen monikerroksellisuus. Kerroksien tulisi olla myös monimuotoisia ja erilaisia. Turvallisuusratkaisun pitäisi näkyä ylläpitäjälle helppona ja yksinkertaisena, mutta rikolliselle monimutkaisena. Rikolliselle ei kannata koskaan paljastaa omia haavoittuvuuksia, kuten mitä käyttöjärjestelmiä ja ohjelmistoja yritys käyttää. Yksittäinen ”heikko lenkki” voi olla jokin prosessi, ohjelmisto, laite tai mikä tahansa vikaantumispaikka, joka vaarantaa yrityksen liiketoiminnan. (Cybersecurity Essentials 6.2; Kyberturvallisuuden nykytila 2017, 18; Harris 2016, 9.)



KUVIO 9. Kyberturvallisuuden monikerroksellisuus [3]

[3] Cybersecurity Essentials materiaalista ja muista kappaleen lähteistä tehty kuvio.

Kyberriskien toteutumisen ennalta arvaamattomuuden vuoksi on tärkeää, että yritys toteuttaa jatkuvaa riskienhallintaa ottaen huomioon sekä reaalimaailman fyysiset riskit että sähköisen kybermaailman virtuaaliset riskit. Uhat tulevat sekä ulkopuolelta että sisäpuolelta. Ulkopuolelta tulevia uhkia ovat tulipalot, maineriskit ja yritysvakoilu sekä yleisimpinä sähköpostilaatikon kautta tulevat haittaohjelmat tai tiedonkalasteluviestit, joissa voi olla hämäyksenä yritysten logolla varustettuja laskuja tai kiireellisiä maksupyyntöjä. Erilaiset kiristyshaittaohjelmat salaavat yrityksen tärkeät tiedostot ja rikolliset vaativat lunnaiden maksamista niiden palauttamiseksi. Sisäpuoliset uhat katsotaan johtuvan oman henkilökunnan toiminnasta tai virheestä. Uhkien syntymiseen on voinut vaikuttaa myös yhteistyökumppani, asiakas tai jopa maailmapoliittinen tilanne. (Yrityksiin kohdistuvat kyberuhat 2015, 6; Tietoturva nyt! 2017, ”Ei koske meitä”.)

ICT-alan toimijan, IBM:n, mukaan vuonna (2015) 60 % yritysten kyberuhista oli organisaation sisäisiä joko tahallisia tai tahattomia. Uhkien jakautuminen saatiin noin 81 miljoonan tietoturvatapahtuman perusteella. (Cyber Security Intelligence 2016, 12; Lehto 2018, luento.) Yli puoleen tietoturvatapauksista pystytään näin ollen vaikuttamaan pelkästään henkilöstön kouluttamisella.

Professori Lehto jakaa kyberturvallisuuden riskit kahdeksaan kategoriaan, joita ovat ohjelmistoihin, laitteistoihin ja datan luotettavuuteen liittyvät riskit, kyberturvallisuuspolitiikan, -tilannekuvan, -ymmärryksen ja -osaamisen puute sekä inhimilliset riskit, joita käsitellään seuraavissa kappaleissa. (Lehto 2018, luento.)

Jopa 10 % kaikista ohjelmistoista sisältää ohjelmistovirheitä ja peräti 40 % niin sanotuista luotetuista sivustoista käyttää haavoittuvia ohjelmistoja, joita käytetään haittaohjelmien jakamiseen. (Lehto 2018, luento; IBM. Security Intelligence. 8.2.2018.) Yritykset ottavat isoja riskejä maineensa kustannuksella, joten ohjelmistojen laatuun on syytä kiinnittää enemmän huomiota. Ohjelmistoihin ja tietokantojen tietoturvallisuuteen voidaan halutessa tehdä paljon tarkistuksia, joiden avulla kyberturvallisuus paranee.

Laitteistoihin liittyvistä riskeistä uutisoidaan usein mediassa ja yleensä ne ovat vakavia, koska rikollisella on pääsy järjestelmään vahvoilla oikeuksilla. Rikollinen saa esimerkiksi

30 sekunniksi valvomatta jääneen yrityskannettavan etähallintaan, koska miljoonissa kannettavissa on AMT -haavoittuvuus[4] (F-secure 2018. Uutinen).

Tiedon räjähdysmäinen kasvu (Bigdata) heikentää datan luotettavuutta, joka toteutuessaan saattaa tekoälyratkaisut ja koneoppimisen tulokset epäluotettaviksi (Lehto 2018, luento). Hyvin hallitut ja tarkasti suunnitellut tietokannat toki parantaa tiedon eheyttä, järjestelmien vakautta ja suorituskykyä sekä helpottaa ylläpitoa.

Kyberturvallisuuspolitiikan ja -tilannekuvan puute ovat yleisiä ongelmia, koska tutkimusten mukaan vain 8 % yrityksistä kykenee erittäin nopeaan ja 11 % nopeaan kyberhyökkäysten havainnointiin. Vain 21 %:lla yrityksistä on yksi yhteinen näkymä datavarantoihinsa (Lehto 2018, luento). Riski on vakava, koska ilman kybertilannekuvaa ja -politiikkaa yrityksellä ei ole kyberturvallisuutta.

Kyberturvallisuuden ymmärryksen ja osaamisen puute näkyy yrityksissä esimerkiksi siitä, että 58 % johtajista ja 25 % työntekijöistä lähettää vahingossa luottamuksellista tietoa väärille henkilöille. Jopa 87 % johtajista saattaa ladata yrityksen luottamuksellista tietoa henkilökohtaiseen sähköpostiin ja pilvipalveluun. Johtajista myös 63 % käyttää samoja salasanoja eri palveluissa. Kyberturvallisuusosaajien puute on iso ongelma ja asiantuntijoista on jatkuva kilpailu. Kyberturvallisuudessa koulutus on kuitenkin syytä aloittaa johtajista. (Lehto 2018, luento; Yritysjohtajien haastattelut 2018.)

Inhimillisen riskin muodostaa esimerkiksi se, että jopa 20 % ihmisistä on halukkaita myymään oman salasanansa kolmannelle osapuolelle ja 44 % myisi salasanan, jos hinta olisi 1000 dollaria. Lisäksi vain 28 % kuluttajista myöntää vaihtaneensa salasanan kyberturvallisuushyökkäyksen tapahduttua. (RSA:n asiakastutkimus 2017; Lehto 2018, luento.)

Tietämättömyys omista datavarannoista ja kybertilannekuvan sekä osaamisen puuttuminen ovat usein myös esteenä turvalliselle toiminnalle. Lähinnä ei osata soveltaa ohjeita, ohjeita ei löydy tai niitä ei ole. Johto voi katsoa, että tietoturvallisesti laadukas ohjelmisto tai palvelu aiheuttaa liian suuret kustannukset. Kyberturvallisuuden tärkeyttä ei haluta

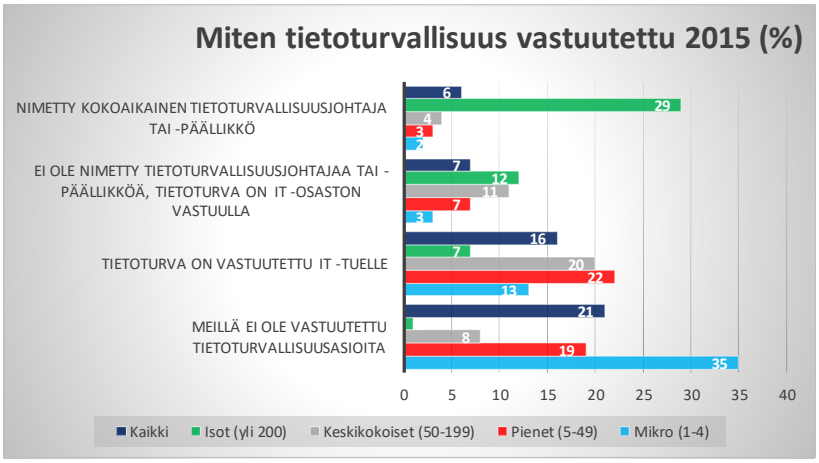
[4] Intel Active Management Technology -hallintajärjestelmä (AMT) -haavoittuvuuden vuoksi rikollinen pääsee etäyhteydellä samaan tietovarantoon, minkä käyttäjä näkee ja enempäänkin. Suojauskeino on vaihtaa AMT-salasana tai ottaa se pois käytöstä, mutta jos salasana on jo vaihdettu tuntemattomaksi, on rikollinen todennäköisesti jo käynyt koneella.

ymmärtää, sitä ei tiedetä tai sen laiminlyönnin aiheuttamia riskejä ei tunneta. (Haaja 2018, luento; Kirjoittajan kokemukset.) Puutteelliset ja puuttuvat ohjeet, tietämättömyys, välinpitämättömyys ja siihen liittyvät laiminlyönnit sekä yleinen kiire ovat olleet kyberturvallisuuskulttuurin kehityksen esteenä jo pidemmän aikaa. Koulutuksella ja asianmukaisella ohjeistuksella riskien toteutumista voidaan vähentää.

2.4.3 Vastuun jakautuminen ja sen jakaminen

Termi ”kyber” ohjaa keskustelun usein teknisille asiantuntijoille, vaikka kyberturvallisuus kuuluu kaikille ja johto vastaa vastuun jakamisesta ja henkilöresurssien kohdentamisesta (Yrityksiin kohdistuvat kyberuhat 2015, 6, 35).

Iso haaste kyberturvallisuuden organisointiin liittyen on vastuunjako johtotasolla. Alalle ei haluta tai osata, uhista huolimatta, kohdistaa riittävästi aikaa, henkilö-, ja taloudellisia resursseja. Vuoden 2015 tutkimuksessa vain 6 % kyselyyn vastaajista ilmoitti palkanneensa kokopäiväisen tietoturvallisuusjohtajan tai -päällikön. Pienillä yrityksillä vastaava luku oli vain 3 % ja keskikokoisilla 4 %. 19 %:ssa pieniä yrityksiä tietoturvallisuutta ei ollut vastuutettu lainkaan ja keskikokoisissa yrityksissä luku oli 8 %. Keskimäärin 21 %:ssa pieniä ja keskikokoisia yrityksiä vastuu siirrettiin ICT-alalle. (Yrityksiin kohdistuvat kyberuhat 2015, 35–37.) Erot isojen ja pienten yritysten välillä olivat selkeät, eikä vastaava vuoden 2016 raportti osoittanut muutosta parempaan.



KUVIO 10. Vastuun jakaminen[5] (Yrityksiin kohdistuvat kyberuhat 2015, 37, muokattu)

[5] Yrityksiin kohdistuvat kyberuhat 2015 -tutkimuksesta oleellinen tieto koottu oheiseen kaavioon.

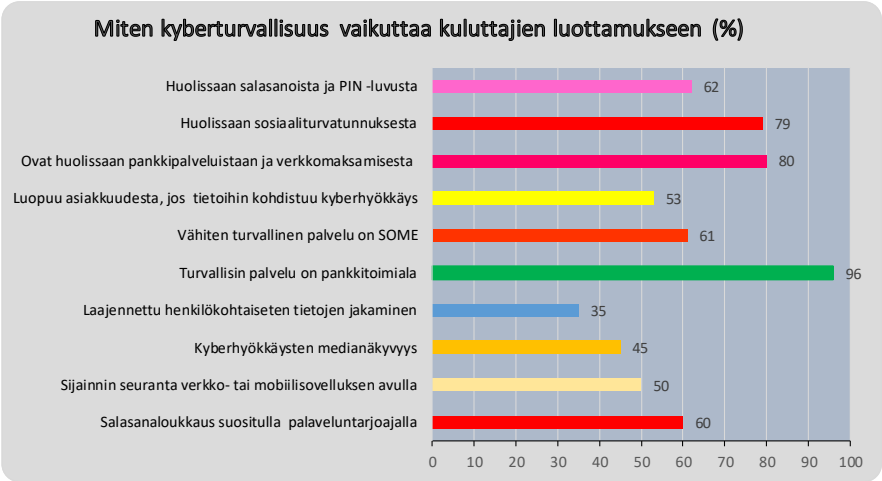
Yritysjohdon on sitouduttava kyberturvallisuuteen ja annettava jatkuvaa tukea alalle kohdentamalla mm. tehtäviin motivoitunutta henkilöstöä. Jotta kyberturvallisuus toteutuisi, ylimmän johdon on määriteltävä kyberturvallisuuden tavoitteet, vastuut ja yleiset toimintaperiaatteet. Jokainen hanke tai projekti vastaa omalta osaltaan kyberturvallisuuden toteutumisesta. Johto myös vastaa ulkoistettujen ICT-palveluiden kyberturvallisuudesta huolehtien että sopimuksiin on kirjattu palvelun tuottajan vastuut.

Tieto- tai kyberturvallisuuspäällikkö vastaa kyberturvallisuuden toteutumisesta yrityksessä. Hän ohjaa ja koordinoi kyberturvallisuutta yhteistyössä turvallisuus-, ICT-, henkilöstöalan sekä tietoturvallisuudesta vastaavien toimijoiden kanssa. Katakrin (2015) mukaan tehtävä tulee olla päätoiminen ja henkilön vastuulla on luonnollisesti kehittää ja ylläpitää yrityksen tieto- ja kyberturvallisuutta ohjeistamalla, kouluttamalla, raportoimalla ja toimimalla alan asiantuntijana sekä vastaamalla yrityksen tilannekuvan luomisesta ja ylläpidosta. (Katakri 2015, 5–12.)

Esimiestehtävissä toimivat vastaavat yhdessä henkilöstön kanssa kyberturvallisuudesta kaikissa työpisteissä. Esimiehet varmistuvat omasta ja työntekijöiden kyberturvaohjeiston hallinnasta, osaamisesta ja ohjeiden mukaisesta toiminnasta. He puuttuvat epäkohtiin ja vääriin menettelytapoihin. Hyvä ja motivoiva esimies näyttää esimerkkiä kyberturvallisesta toiminnasta, kannustaa työntekijöitä osallistumaan koulutuksiin ja turvallisempiin työskentelymenetelmiin. Jokainen myös vastaa yrityksen järjestelmien ja välineiden asianmukaisesta käytöstä, tietoaineiston ja materiaalin suojaustason mukaisesta käsittelystä ja säilytyksestä. Kaikki ovat velvollisia tekemään havaituista poikkeamista tarvittavat ilmoitukset.

2.4.4 Asiakkaan kyberturvallisuus

Kuluttajien luottamusindeksitutkimuksessa jopa 53 % asiakkaista kertoi luopuvansa asiakkuudesta, jos heidän tietoihinsa kohdistuu kyberhyökkäys, kuten tiedon vuotaminen tai katoaminen. 80 % kuluttajista oli huolissaan pankkipalveluistaan ja verkkomaksamisesta. Kuviossa 11 on kuvattu myös muita kuluttajia huolestuttavia uhkia (RSA 2017.)



KUVIO 11. Kuluttajien luottamukseen vaikuttavat kyberuhat (RSA 2017.)

61 % vastaajista piti somea vähiten turvallisena palveluna ja 60 %:a huolestutti salasanaloukkaus suositulla palveluntarjoajalla. Lisäksi 93 % asiakkaista halusi olla mukana valitsemassa, miten heidän henkilökohtaiset tietonsa ja tilinsä suojataan verkossa. 88 % vastaajista olisi halukas käyttämään perusteellisempaa kirjautumista, jos se parantaa turvallisuutta. (RSA 2017.) Kyberturvalliset palvelut on nähtävä mahdollisuutena ja some keskeisenä markkinapaikkana tulee olla kyberturvallinen.

Yritysten kannattaa panostaa kyberturvallisiin palveluihin ja sisällyttää turvallisuus tuotteisiin valmiiksi. Asiakas odottaa, että ostettu palvelu tai tuote on valmiiksi turvallinen ja tietosuoja on huomioitu ilman lisäkustannuksia. Pienten yritysten kilpailuetu voi olla myös tuote tai palvelu ilman digitalisaatiota (Kilpinen 2008, 124). Strategian kehittämisessä yrityksessä tulee tunnistaa ne perinteiset ajattelun urautumat ja epäloogisuudet, jotka usein estävät innovatiivisen kehitystyön (Kilpinen 2008, 127). Kyberturvallisuutta parannettaessa on uskallettava muuttaa nämä urautuneet tavat ja siirtyä epämukavuusalueelle, jolloin on mahdollisuus löytää uusia ja odottamattomia ideoita kokonaisturvallisuuden kehittämiseksi. Ilman digitalisaatiota tuote tai palvelu on ehkä kyberturvallisempi.

2.4.5 Kyberturvallisuuden rakentaminen ja uhkilta suojautuminen

Kyberturvallisuuden rakentamisessa on huomioitava kyberturvallisuuden uhat, jotka kohdistuvat ihmisiin, prosesseihin ja teknologiaan ja haavoittuvuudet, jotka niihin liittyvät. Maineen ja yrityksen arvojen suojelemiseksi tulee toteuttaa erilaisia vastatoimenpiteitä, kuten aiemmin mainitut toimintaohjeet, määräykset, politiikka, riskien hallinta ja

suojausteknologiat jne. (Lehto 2018, luento.) Kyberturvallisuuden rakentamisen peruspilarit ovat luottamuksellisuus, eheys ja saatavuus. Sanoista käytetään lyhennettä CIA eli Confidentiality, Integrity ja Availability) (Harris 2016, 3–4).

Kyberturvallisuus tulee huomioida jokaisessa tietojärjestelmähankkeessa ja kaikessa suunnittelussa heti ensimmäisestä askeleesta asti niin, että se on sisäänrakennettuna rakenteisiin, laitteisiin, palveluihin ja järjestelmiin. Johdon rooli ja sitoutuminen ovat erityisen keskeisessä asemassa. Koulutus on sekä nopea että halpa keino lisätä ja rakentaa yrityksen kyberturvallisuutta, ja sitä kautta lisätä kilpailuetua sekä turvata yrityksen maine. (Limnèll 2016, luento; Yrityksiin kohdistuvat kyberuhat 2015, 7; The Guardian news 2015.) Kyberturvallisuuden rakentamisessa on myös aina osattava priorisoida.

Kyberturvallisuuden hallinnan menetelmät voidaan jakaa ennaltaehkäiseviin, tunnistaviin, korjaaviin, varoittaviin, korvaaviin ja toipumisen menetelmiin. Niitä on opittava käyttämään oikein tiettyjä riskejä ja uhkia vastaan. Ennaltaehkäisevä suojautuminen jaetaan karkeasti fyysisiin, teknisiin ja hallinnollisiin suojautumismenetelmiin. Yrityksen fyysisiä suojautumiskeinoja ovat mm. aidat ja tilaturvallisuus (ovien lukitukset). Teknisiä keinoja ovat mm palomuurit, pääsynhallinta ja salaaminen. Hallinnollisia keinoja ovat aiemmin mainitut kyberturvallisuuspolitiikka, koulutus, tehokas ja oikeudenmukainen palkkausjärjestelmä, työntekijöiden taustojen selvitys, hallitut irtisanomisprosessit, tiedon luokittelu sekä yleisen turvallisuuskulttuurin kehittäminen. (Harris 2016, 9–11.)

Kyberhäiriötilanteiden hallinta voidaan jakaa varautumiseen, tilannekuvan muodostamiseen, torjuntaan ja palautumiseen (Suomen kyberturvallisuusstrategia 2013, 22). Tietoturvatapahtumien yhteydessä on erityisesti huomioitava viestittämisen vaikeus, jotta yrityksen maine ei vaarannu mahdollisissa haittaohjelmahyökkäyksissä. Yrityksellä tulee olla valmiit suunnitelmat, vaikka tilanteisiin on vaikea etukäteen valmistautua.

2.4.6 Verkostoituminen ja tilannekuva

Yrityksen johdon tulee varata kyberasiantuntijoille riittävästi aikaa yhteyksien luomiseen oman toimialan ja kyberturvallisuusalan vertaisryhmiin, kumppaneihin ja erityisesti valvontaviranomaisiin, joilta saa ajanmukaista tietoa nykyisistä ja tulevista uhkista. Suhteita tarvitaan mm. haittaohjelmakriisien yhteydessä. (Tietoturvaopas yrityksille 2016, 10.)

Yrityksille tärkein yhteistyötaho on kansallinen kyberturvallisuuskeskus, joka palvelee viranomaisia, yrityksiä ja kaikkia kansalaisia. Keskuksen tehtäviin kuuluu mm. yritysten tukeminen laajoissa kyberhäiriötilanteissa. Keskeisimmät palvelut ovat kybertilannekuvan luominen, ylläpitäminen ja jakaminen kiinteässä yhteistyössä keskusta tukevan verkoston kanssa. Yrityksen asiantuntijoiden on liityttävä keskuksen sähköpostijakeluryhmiin, jolloin he saavat joka kuukausi ”kybersää”-tiedotteen ja muita teknisiin haavoittuvuuksiin liittyviä päivitysohjeita. (Suomen kyberturvallisuusstrategia 2013, 23–24; Tilannekuva.) Aktiivista yhteystoimintaa ja tiedonvaihtoa kannattaa lisätä, koska jaettu tilannetietoisuus useampien toimijoiden välillä on tehokas keino uhkien torjunnassa. Alan parhaat ja turvallisimmat käytännöt kannattaa ottaa mahdollisimman nopeasti käyttöön ja ilmaisiin palveluihin tutustumalla yritys voi pienin askelin parantaa omaa turvallisuuttaan.

Verkostoitumisen hyödyistä mainittakoon vuoden 2018 TOP5-uhat ja suojautumiskeinot (Kyberturvallisuuskeskus 16.1.2018). Ohjeet on julkaistu erikseen sekä yksityishenkilöille että organisaatioille. Ohessa on esitetty yrityksille kohdennettu kuva 2.

KUVA 1. TOP5-uhat ja TOP5-ratkaisut organisaatioille (Kyberturvakeskus 2018.)

Kybertilannekuva muodostuu myös teknisen valvonnan ja seurannan datasta sekä erilaisista henkilöstön havainnoista, tiedusteluista, aiemmista kokemuksista ja niistä tehdyistä analyyseistä sekä muista verkostoista, kuten sosiaalisesta mediasta saaduista tiedoista.

2.4.7 Motivoiva ja innovatiivinen kyberturvallisuuden johtaminen

Kyberuhkien tehokas torjunta edellyttää laadukasta suunnittelua ja ennakointia sekä innovatiivista johtamista. Sanotaan, että yritysten strategian tulee olla ketterä, kaikkien tulee reagoida yhdenmukaisesti kohti samaa päämäärää ja toiminnan tulee perustua vahvaan osaamiseen. Samat periaatteet pätevät myös kyberturvallisuuden johtamiseen ja kyberhäiriötilanteisiin tulee pystyä reagoimaan nopeasti. Jotta johtaminen olisi yhtenäistä, on tilannekuvan oltava reaaliaikainen ja laadukas. Lisäksi tiedonkulku on aina varmistettava. (Kilpinen 2008, 10, 36–38; Suomen kyberturvallisuusstrategia 2013, 19–22.) Kun johto omaksuu koko johtamisen ketjun ja siihen liittyvät keskeisimmät tehtävät ja huomioi asiakkaiden luottamuksen säilymisen ja huolenaiheet, yrityksen kilpailukyky paranee.

Kyberturvallisuus ei ole tuote, vaan itsessään prosessi, jonka johtaminen on sisäänrakennettu organisaation prosesseihin. ICT-asiantuntijat voivat toimia kyberturvallisuudessa vastuullisina, mutta yksin he eivät siinä menesty. Vastuuta ei vain voi ”työntää” ICT -alalle. Henkilöstöä on organisoitava kyberturvallisuusalalle niin, että sillä on tosiasialliset mahdollisuudet selvitä työkuormastaan. Jokainen toimialajohtaja johtaa kyberturvallisuutta yrityksen johdon antaman vision ja strategisten linjausten mukaisesti. Kun kyberturvallisuutta osataan johtaa normaalissa päivärytmissä, yritys toipuu tositilanteessa paremmin ja nopeammin erilaisista kyberhyökkäyksistä.

Toiminnan jatkuvuuden suunnittelu on viime kädessä johtajien vastuulla. Kyberhäiriötilanteista huolimatta yrityksen päätuotantolinjan toimivuus tulee varmistaa varamenetelmällä. Yleinen virhe on rakentaa uudelle ilmiölle, kuten kyberturvallisuudelle, yritykseen oma ”siilorakenne”, jonne tärkeä, johtamiseen liittyvä tilannetieto, osaaminen ja henkilöstö kerätään. Sen jälkeen kuvitellaan, että asia on hoidettu kuntoon. Turvallisuus ja kyberturvallisuus ovat kuitenkin meidän kaikkien asia.

Alan koordinointi ja asiantuntemus yrityksessä tulee olla vahvaa ja on verkostoiduttava alan viranomaisten ja yritysten kanssa. Sekä pienissä että isoissa yrityksissä kyberturvallisuusstrategia ja -arkkitehtuuri tulee rakentaa liiketoiminnan ehdoilla ja suhteuttaa toimenpiteet yrityksen kokoon. Asioiden mittaamiseen on hyvä rakentaa yksi isompi karkean tason mittari ja useampia pienempiä teknisiä mittareita. Yhden ison edistysaskeleen sijasta kannattaa tehdä pienempiä parannuksia ja korjauksia vision saavuttamiseksi. On

osattava priorisoida. Lisäksi ICT-palveluita tai -järjestelmiä hankittaessa on vaadittava toimittajalta kyberturvallisuutta. Henkilöstön koulutus datan suojaamiseksi on aina kustannustehokkaampaa kuin kalliiseen teknologiaan sijoittaminen.

Petteri Kilpinen kertoo kirjassaan (Kilpinen 2008, 33–34), miten yritysjohtajan tulisi jokapäiväisissä tehtävissään johtaa. Pitkällä aikavälillä on keskityttävä keinoihin, joilla kaikissa kehityshankkeissa keskitytään arvon kasvattamiseen. Varmistetaan, että yrityksen strategia, tuotteet, palvelut tai brändi ovat loppukäyttäjän mielestä ainutlaatuisia ja turvallisia. Mahdollistetaan yrityksessä työntekijöiden motivaation säilyminen tehtäviinsä ja aivojen monipuolinen käyttäminen. (Kilpinen 2008, 1, 33–34.) Ohjeita voi käyttää kyberturvallisuuden johtamiseen huomioimalla ne järjestelmien suunnittelussa heti ensimmäisestä palaverista alkaen. Kaikkiin hankkeisiin nimetään vastuullinen kyberturvallisuusasiantuntija. Tuotteisiin lisätään aina myös palveluominaisuuksia, kuten tietoturvallisuutta ja tietosuojaa, jotka tuovat kaikille lisäarvoa. Palveluiden tietosuojaan panostetaan, jotta esim. EU -tietosuoja-asetuksen vaatimukset täyttyvät – mielellään jopa ylittyvät. Kannustetaan työntekijöitä innovatiivisten kyberturvaratkaisuiden toteuttamiseen, josta seuraa yritykselle todellista arvoa. Nimetään oikeat ihmiset oikeisiin tehtäviin, jolloin heillä säilyy työhönsä ”sisäinen palo”. Ja otetaan myös tavoitteeksi käsitellä jokaisessa johtoryhmän kokouksessa kyberturvallisuuden aihealue sekä asiakkaiden että omien työntekijöiden näkökulmasta.

Kilpinen esittää kirjassaan myös (2008, 55–56) viisi luovan johtamisen oivallusta, joihin on ohessa täydennetty kaikkiaan kahdeksan jokapäiväistä kyberturvallisuuden johtamisen oivallusta: 1) Läpinäkyvässä globaalissa yritysmaailmassa, bittien maailmassa, ei tule tehdä sellaista, mikä ei kestä päivänvaloa. 2) Valehtelusta jää verkossa melko nopeasti kiinni. 3) Kyberturvallisuudelle on määriteltävä yrityksessä suurempi tarkoitus (visio), johon työntekijät voivat sitoutua ja luotava mahdollisuus toteuttaa tuota tarkoitusta tai jopa parantaa sitä. 4) Kyberturvallisuudessa on pyrittävä pitempiaikaisiin tuloksiin. 5) Yrityksen strategisten suunnitelmien on oltava pitkäaikaisia ja kvartaaliajattelun sijasta niiden on katsottava vuosien päähän. (Kilpinen 2008, 68.) 6) Kyberturvallisuusstrategian on lähdettävä ylimmän johdon sitoutumisesta ja se on integroitava koko yrityksen ydinstrategiaan. 7) Yrityksen ja työntekijöiden on haastettava itsensä kehittämään kyberturvallisempia menetelmiä ja toimintatapoja. Muuten ei tapahdu turvallisuuskulttuurin kehittymistä, vaan ihmiset vain tyytyvät noudattamaan heille annettuja tietoturvallisuusohjeita, vaikka tietäisivät ohjeiden olevan vanhentuneita tai mahdottomia noudattaa. 8)

On uskallettava murtaa alan tabuja ja kehittää uusia vaihtoehtoisia menetelmiä ja strategioita (Kilpinen 2008, 62).

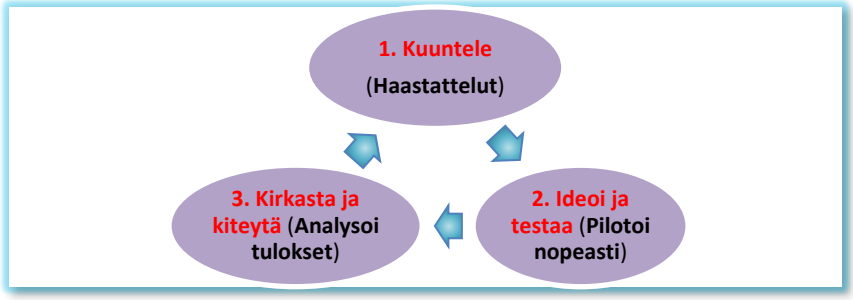
Menestykseen ei päästä matkimalla muita – on uskallettava muuttua. Katse on oltava muilla toimialoilla, uudessa teknologiassa, muuttuneissa arvoissa tai kuluttajien käyttäytymisessä. (Kilpinen 2008, 134.) Sosiaalinen media on yhä isommassa roolissa ja maineen menetys siellä saattaa viedä yrityksen suuriin vaikeuksiin. EU:n tietosuoja-asetuksen vaikutuksista ei ole vielä käytännön tapauksia, mutta vuoden 2018 loppupuolella saatamme nähdä jo ikäviä tapauksia.

3 OPPIMISEN TEORIAT JA OPPIMISMENETELMÄT

Tässä luvussa käsitellään haastatteluiden, pilotoinnin ja muiden kvalitatiivisten tutkimusmenetelmien soveltuvuutta kyberturvallisuuden koulutukseen sekä vertaillaan oppimisen teorioita. Luvussa kuvataan kuinka johto oppii parhaiten kyberturvallisuutta. Ennen koulutusta valmentajan tulee siis löytää oma opetusteoriansa, ketä ja miksi sekä mitä hän on opettamassa? Tämän jälkeen tulee koulutusta ryhtyä vain rohkeasti kokeilemaan esimerkiksi pilotoinnin avulla. Luvun tavoitteena on valita parhaat oppimiskäsitykset ja opetusmenetelmät johdon kyberturvallisuuden kouluttamiseen yrityksissä, jotta koulutusmateriaalia voidaan hyödyntää parhaalla mahdollisella tavalla koulutuksessa ja turvallisuuskulttuuri kehittyisi parempaan suuntaan. Kyberturvallisuuden opettaminen ja jalkauttaminen yrityksissä on usein haastavaa, koska aihe koetaan ICT-alaan liittyvänä tekniseksi.

Luvussa käsitellään lisäksi koulutuksen suunnittelua ja koulutuspilotointeja sekä niistä tehtyjä analyysejä systeemiajattelun periaatteita noudattaen. Pilottien tulokset ja analyysit on kuvattu tarkemmin liitteessä 5 ja yrittäjien haastatteluiden kysymykset on kerrottu liitteessä 6. Systeemiajattelua voidaan käyttää myös yleisesti yrityksen kyberturvallisuuden johtamisessa, mikä tulee esille luvussa.

Kyberturvallisuuskoulutuksen suunnittelu noudattelee myös yleistä palvelumuotoilun prosessia kuvion 12 mukaisesti. Kohderyhmän kuunteluun avoimet haastattelut olivat erinomainen keino. Ideoinnissa ja testaamisessa nopeat pilotit ovat tutkimuksissakin osoittaneet tehonsa. Lopuksi pitää muistaa kirkastaa eli tässä tapauksessa analysoida piloteista ja haastatteluista saadut tulokset.



KUVIO 12. Palvelumuotoilun (suunnittelun) yleinen prosessi (Verho 2014, 18–20.)

3.1 Tutkimusmenetelmien vertailua ja menetelmien valinta

Kvantitatiivinen eli määrällinen tutkimusmenetelmä antaa kuvan mitattavien ominaisuuksien välisistä eroista ja suhteista eli se vastaa kysymykseen kuinka paljon, miten usein ja kuinka moni? Lisäksi tutkimustulos on objektiivinen eli tutkija ei vaikuta tutkimustulokseen. Tietoa tarkastellaan numeerisesti. Tutkittavia asioita ja niiden ominaisuuksia käsitellään siis kuvaillen numeroiden avulla. (Vilkka 2007, 13–14.)

Kvalitatiivinen eli laadullinen tutkimus mahdollistaa tutkimuskohteen henkilöiden vapaamuotoisen kertomuksen kokemuksistaan ja mielipiteistään tutkimuskysymykseen liittyvästä aiheesta. On tarkoitus päästä syvemmälle tutkimusongelman ytimeen eli haastateltavan ajatuksiin ja kokemuksiin. (Tilastokeskus 2018, käsitteet; Ojasalo & Moilanen & Ritalahti 2014, 104–105.) Ei siis tutkita niinkään numeroaineistoa ja tilastoja (Tuomi & Sarajärvi 2018, 16).

Edelliseen liittyen työssä haluttiin esimerkiksi pilottien palautelomakkeeseen sekä kvantitatiivisista että kvalitatiivista tutkimusotetta, koska jo aiemmin todettiin kyseisten tutkimuksien tukevan toisiaan. Tämän vuoksi palautelomakkeeseen lisättiin avoimia kysymyksiä ja palaute kysyttiin myös avoimella keskustelulla.

Koulutuksen suunnittelussa ja tutkimusmenetelmissä keskityttiin enimmäkseen kvalitatiivisiin eli laadullisiin tutkimusmenetelmiin, joita olivat esim. teema-, avoin- ja ryhmähaastattelut, koska kyberturvallisuus aiheena on laaja-alainen ilmiö ja työssä haluttiin ymmärtää sitä paremmin ja kokonaisvaltaisemmin. Kun halutaan paljon tietoa aiheesta, on haastattelurunko (liite 6 s 117–119) toimitettava johdolle hyvissä ajoin etukäteen ennen haastattelua. (Ojasalo ym. 2014, 104–105; Tuomi & Sarajärvi 2018, 84–90.) Lisäksi haluttiin selvittää yrityksen todellinen turvallisuustilanne ja siihen haastattelut ovat hyvä keino kyberturvallisuusympäristön moniulotteisuuden ja keskinäisriippuvuuksien johdosta. Tutkimuksessa pyrittiin myös laadullisen tutkimuksen tapaan tekemään harkinnanvaraisia näytteitä ja tutkimuskohteet valittiinkin harkitusti (Ojasalo ym. 2014, 105). Koulutusta järjestettäessä kohderyhmänä oli yrityksen johto, johon ensimmäiset haastattelut ja kartoitukset kohdennettiin. Valmentajan osallistuminen on laadullisessa tutkimuksessa kohdistettava kohderyhmän toimintaan (Ojasalo ym. 2014, 105). Aivoriihi -ryhmätöiden yhteydessä valmentaja pystyy hyvinkin osallistumaan toimintaan ja tekemään osallistuvaa havainnointia tai seuraamaan tilannetta ulkopuolisena. (Ojasalo ym. 2014, 104, 114).

Koska kvantitatiiviset ja kvalitatiiviset tutkimusmenetelmät toimivat parhaiten yhdistettynä toisiinsa (Tuomi & Sarajärvi 2018, luku 2.5), työn johtopäätökset ja pohdinta on tehty sekä laadullisen että määrällisen tutkimuksen perusteella.

Haastatteluja käytettiin, koska haluttiin kerätä nopeasti syvällistä tietoa esimerkiksi johdon haasteista (Ojasalo ym. 2014, 106–107). Toteuttamiskelpoisia haastattelumuotoja juuri kyberturvallisuusalalle ovat ryhmä- ja strukturoitu haastattelu (lomakehaastattelu), joita voidaan käyttää yrityksen johtoryhmän haastattelussa ja koulutuspilottien yhteydessä palautetta kysyttäessä (Ojasalo ym. 2014, 111–112; Hirsjärvi & Hurme 2006, 43–45). Tietoturvallisuuskartoituksen ja johdon ensimmäisen kohtaamisen yhteydessä haastattelut olivat puolistrukturoituja (liite 6).

Haastattelujen avulla saatiin myös tukea ja vertailua yleiselle kyberturvallisuuden kvantitatiiviselle tutkimukselle sekä tietoa yritysjohdolle kyberturvallisuuden merkityksestä. Avoimilla ryhmähaastatteluilla saadaan arvoa koulutusmateriaalin sisällölle ja ulkoasulle. Tästä on hyvänä esimerkkinä ICT-startup -ryhmän haastattelu 2017 liitteessä 5. Myös syvähaastattelut olivat tarpeellisia, koska kyberiskun kokenut johtaja kokee yleensä tilanteen nolona ja henkilökohtaisena ja tilanne vaatii avoimuutta (Ojasalo ym. 2014, 108–109). Haastatteluja ja lomakekyselyitä täydennettiin havainnoinnin avulla tehden esimerkiksi systemaattista tarkkailua aivoriihityöskentelyn aikana ja myöhemmissä keskusteluissa. Havainnointi soveltuu hyvin kyberturvallisuuteen ja siihen liittyvään ihmisten käyttäytymiseen sekä mielipiteen ilmaisuun (Ojasalo ym. 2014, 114).

3.2 Oppimisen teoriat ja opetusmenetelmien valinta

Opettamiseen ja oppimiseen liittyvät erilaiset oppimiskäsitykset eli oppimisen teoriat. Niitä ovat behavioristinen, kognitiivinen ja humanistinen oppimiskäsitys, konstruktivismi sekä konnektivistinen oppimistapa. Teoriat on kuvattu seuraavissa kappaleissa.

Behavioristisen oppimiskäsityksen juuret ovat luonnontieteellisessä ajattelussa ja oppiminen ymmärretään ulkoisesti säädeltävänä käyttäytymisen muutoksena. Oppimiskäsityksessä ei tueta oppijan valmiuksia ajatella ja ymmärtää opeteltavia asioita. (Sava 1993, 18.) Opettajan tai valmentajan tehtävä on siirtää tietoja ja valmiita malleja suoraan oppilaille. (Sahlberg & Leppilampi 1994, 21-25; M&J von Wright 2003, 148–149).

Kognitiivinen oppimiskäsitys on tiedon prosessointia, jossa oppija tai kuulija on erilaisen tiedon aktiivinen käsittelijä, koska hän vastaanottaa, valikoi, taltioi, tulkitsee sekä aktiivisesti kehittää ja havainnoi tietoa. (Lindblom-Ylänne & Nevgi, 2003,16.) Voidaan myös puhua mielekkäästä oppimisesta. Oppijan mielessä syntyy ongelma tai tiedollinen ristiriita, koska taidot ja tiedot eivät riitä tilanteen ratkaisemiseen. Oppija oppii samalla oman oppimisensa kriittistä arviointia.

Humanistisessa eli kokemuksellisessa oppimiskäsityksessä tiedon prosessoinnin lisäksi oppiminen perustuu oppijan kokemuksiin, pohdintoihin, kykyyn arvioida omia kokemuksiaan ja omaa oppimistaan uuden oppimisen pohjaksi, minkä perusteella kokemukset voivat myös muuttua ja laajentua. (Rauste-von Wright 1997, 17; Kupias 2001, 16.) Lisäksi oppimiseen liittyy motivaatio, vapaa tahto ja vastuu omasta oppimisesta.

Konstruktivismi on oppimiskäsitys, jossa oppiminen nähdään aktiivisena tiedon rakentamisen prosessina eli tieto ei siirry, vaan oppija rakentaa sen itse uudelleen, jolloin aiemmat tiedot ja kokemukset sekä käsitykset säätelevät sen mitä hän asiasta havaitsee ja miten hän sen tulkitsee. Oppimiskäsityksessä vuorovaikutuksella on keskeinen rooli. (von Wright & Soini 2003, 156–157, 162–163.)

Konnektivistinen oppimistapa tapahtuu verkkoympäristössä. Siinä oppiminen nähdään tiedonrakentamisena, johon verkostot ja yhteistoiminta integroituvat keskeisesti ja oppimisessa hyödynnetään teknologiaa erilaisissa digitaalisissa ympäristöissä. Tunnusomaista on, että oppiminen ja tieto pohjautuvat mielipiteiden moninaisuuteen ja erilaisuuteen. Oppija on myös jatkuvasti aktiivinen, hakee, rakentaa ja jakaa tietoa muiden kanssa sosiaalisessa mediassa, kuten YouTubessa ja Facebookissa. (Oppimiskäsitykset, Jamk.)

Kyberturvallisuuden kouluttamisessa ja oppimisessa käytetään varmasti kaikkia edellä mainittuja oppimiskäsityksiä, mutta kuitenkin vähiten behavioristista oppimiskäsitystä. Seuraavaksi käsitellään hieman laajemmin kognitiivista oppimiskäsitystä, johon tämän työn aihetta on rajattu ja jonka myös asiantuntijat ovat valinneet kybermaailman tasomalliin (Kyberturvallisuuden kansallinen osaaminen 2015, 7–8).

3.2.1 Kognitiivinen oppimiskäsitys kyberturvallisuudessa

Sana kognitiivinen tarkoittaa tietoa koskevaa tai tiedollista (esimerkiksi ilmauksessa kognitiivinen oppiminen). Psykologiassa termiä käytetään viittaamaan tajunnan sisältöön, tiedostukseen tai havainnointiin. Tietotekniikassa puhutaan tällöin tekoälystä. Kognitiivinen oppiminen on oppimiskäsitys, joka sopii hyvin kyberturvallisuuden ja aikuisten kouluttamiseen sekä valmentamiseen.

Kognitiiviseen oppimiskäsitykseen perustuvassa opetuksessa opetus nähdään oppimisen systemaattisena ohjauksena, ei vain tiedon välittämisenä ja esittämisenä. Sana kognitiivinen tarkoittaa kybermaailman tasomallissa kognitiivista kerrosta eli kerros kuvaa ihmisen informaation ymmärrysmaailmaa, maailmaa, jossa informaatio tulkitaan ja henkilökohtainen ymmärrys ja käsitys muodostetaan. (Kyberturvallisuuden kansallinen osaaminen 2015, 7–8.)

Kognitiivisessa opetuksessa pyritään saamaan aikaan kuulijoiden keskuudessa ajattelua ja pohdintaa, jonka avulla ymmärretään ja opitaan eli tällöin tiedon prosessointi korostuu. Tavoitteet asetetaan yleensä väljästi ja opetuksessa pyritään opetuskokonaisuuksiin. Käytetään kuulija -ja opiskelijakeskeisiä toimintatapoja, ryhmäpohdintoja, aivoriihiä, parityöskentelyä, projekteja ja oppimistehtäviä perinteisten tenttien asemasta. Kognitiivisessa opetuksessa nähdään keskeisenä myös tiedon käsittely. (Oppimiskäsitykset, Jamk.)

Yrjö Engeström on kuvannut kirjassaan täydellisen oppimisprosessin mallia siten, että prosessi voidaan jakaa osatekijöihin, joista kukin vaatii oppijalta määrätynlaisia oppimistekoja. Hänen kuvaamansa kuusi oppimisvaihetta ovat: motivoituminen, orientoituminen, sisäistäminen, ulkoistaminen, arviointi ja kontrolli. (Oppimiskäsitykset, Jamk.)

Opettajan tai luennoijan tulee suunnitella ja toteuttaa opetus siten, että siinä käytetään opetuksellisia tehtäviä joustavasti ja monipuolisesti, sillä ehdotonta oikeaa opetuksellisten tehtävien järjestystä ei ole. Opettajan tai valmentajan haastava päämäärä on saada aikaan täydellisen oppimisen turvaava kokonaisuus. (Oppimiskäsitykset, Jamk.)

Usein kyberturvallisuuden jalkauttamisessa tai kouluttamisessa yrityksessä käytetään myös Engeströmin (2004, 60) kirjassaan mainitsemaa ekspansiivista oppimista, joka ei ole suoraviivaista, vaan etenee moniaskelisena kehänä eli oppimissyklinä. Kyseinen

sykli, prosessi, muodostui huomaamatta myös koulutusmateriaalin kehittämisprosessista, joka on kuvattu luvun 4 kuviossa 15. Ekspansiivisessa oppimisessa törmätään ajoittain yllättäviin esteisiin ja ristiriitoihin, jolloin joudutaan ottamaan askelia taaksepäin ja tuloksia saatetaan saavuttaa vasta kuukausien tai vuosien päästä. (Engeström 2004, 60–63.)

Kyberturvallisuusalalla ja monella muulla työelämän alueella oppijakeskeiset opetusmenetelmät ovat keskiössä ja esimerkiksi vuorovaikutus ja dialogin mahdollistaminen ovat suuri osa valmentamista. Tavoitteet on kuitenkin asetettava mielellään yhdessä, jotta kuulijat saavat opetuksesta tarvitsemansa. Ryhmäpohdinnat, avoin keskustelu, erilaiset työpajat ja aivoriihet ovat hyviä opetusmenetelmiä ja ongelmanratkaisutapoja, kun suunnitellaan yritysjohdon kyberturvallisuuskoulutusta. Kyberturvallisuuteen liittyen johdolla on monia vaikeita päätöksiä, joiden ratkaisemiseen De Bonon hattumenetelmä, lootuskukka, aivoriihi, systeemiajattelun periaatteet ja muut osallistavat oppimismenetelmät ovat käyttökelpoisia. Näistä kerrotaan enemmän luvussa 3.3.

Johdon motivoiminen alaan on tärkeää, koska uhkat yritykselle ovat suuret. Ilman kuulijan motivaatiota on vaikea saada esitettävälle asialle kiinnostusta ja tämä on haaste valmentajalle. Kyberturvallisuuden esimerkkitapaukset, kuten opettavaiset, uhkaavat ja pelottavat videot voisivat toimia motivoinnin keinoina. Orientoitumisvaiheessa johdolle on tärkeää, että kyberturvallisuuden laaja aihealue tulee ymmärretyksi ja kuulijalle muodostuu selkeä kokonaiskuva alasta, uhkista ja suojautumiskeinoista. Samalla kuulija ymmärtää keskeiset toimintamallit ja osaa kytkeä yksityiskohdat kokonaisuudeksi. Ryhmätehtävissä kuulijoiden tulisi osata jo muodostaa oman yrityksensä suojautumismalleja.

Engeströmin mainitsemat oppimisvaiheet muodostavat valmentajalle selkeitä opetuksellisia tehtäviä, joista voidaan mainita kyberturvallisuusalalle muutamia: 1) Kuulijat on ensinnäkin motivoitava ja valmistettava uuteen aiheeseen. 2) Koulutusmateriaali on valmisteltava huolellisesti ja kuulijoiden orientointi tehdään mielellään yhdessä heidän kanssa. 3) Kyberturvallisuusalan uuden tiedon välittäminen ja kokonaiskuvan täydentäminen lisätiedoilla käyttäen eri opetusmenetelmiä. 4) Johdon kannalta keskeisten kyberturvallisuuden aiheiden kertaaminen, kuten yrityksen uhkien ja suojautumismenetelmien priorisointi aivoriihessä. 5) Luentomateriaalin jäsentäminen loogiseen järjestykseen. 6) Harjoittelusta muistuttaminen, koska sen avulla organisaatio saavuttaa ja näkee myös todellisen suorituskykynsä. 7) Kyberturvallisuusalan tiedon soveltaminen käytäntöön, joka usein avautuu kuulijoille vasta vuoropuhelun ja käytännön esimerkkien avulla.

Luennoitsijan on myös jollakin keinolla selvitettävä, miten hyvän kokonaiskuvan, ymmärryksen tai toimintamallin johto sai koulutuksesta. Nämä kysymykset on syytä koota palautekyselyyn, jotta johto myös itse osaisi arvioida omia taitojaan ja tietämystään. Monessa yrityksessä on myös käytössä kyberturvallisuus- tai tietoturvallisuusalan verkkokoulutustesti, jolla säännöllisesti päivitetään ja ylläpidetään osaamista.

Kirjoittajan kokemuksien perusteella voidaan todeta, että kyberturvallisuuden kouluttaminen vaatii myös laaja-alaista osaamista eri tekniikan aloilta kuten tieto-, tietoliikennetekniikasta, tietoturvallisuudesta, sähkövoima-alasta, radiotaajuustekniikasta, turvallisuusalasta yleensä, LVI-tekniikasta ja IoT-laitteista. Lisäksi tulee tutustua kyseisen toimialan liiketoimintaan.

Monet muutkin oppimiskäsitykset soveltuvat hyvin kyberturvallisuuden valmentamiseen ja opettamiseen. Ominaisuuksiensa puolesta siihen soveltuu muun muassa humanistinen eli kokemuksellinen oppiminen, missä oppimiseen liittyy myös motivaatio, vapaa tahto ja tässä tapauksessa johdon oma vastuu oppimisestaan. Myös konstruktivismi ja esimerkiksi verkkoympäristössä tapahtuva konnektivistinen oppimistapa soveltuvat hyvin alan oppijoille. Kyberturvallisuusalan uhat ja suojautumiskeinot muuttuvat nimittäin jatkuvasti ja oppiminen tapahtuu osin sosiaalisessa mediassa. Verkottuminen ja yhteistoiminta sekä niihin liittyvä tiedon jakaminen ja saaminen tapahtuu sosiaalisen median eri kanavissa. Konstruktivismin osalta jokainen johtaja rakentaa mielessään itselleen tulkintoja kyberturvallisuuden laajasta kokonaisuudesta ja eri osa-alueiden merkityksestä toisiinsa.

3.3 Aikuisena oppiminen ja kyberturvallisuuskoulutuksen suunnittelu

Seuraavissa luvuissa käsitellään aikuiskoulutuksen teoriaa ja nivotaan se myöhemmissä alaluvuissa kyberturvallisuuden koulutukseen ottaen huomioon koulutustilaisuuden tarkennettu tarkoitus ja tavoitteet, motivoiva ja osallistava kyberturvallisuuden oppiminen sekä systeemiajattelu. Tässä luvussa tarkastellaan myös hyväksi havaittuja tiimioppimisen menetelmää, kuten aivoriihen ja muiden ideointimenetelmien sopivuutta kyberturvallisuuden työpajoihin ja ryhmätöihin.

3.3.1 Aikuiskoulutuksen teoriaa

Oppimistutkimuksen uranuurtajat, professorit Marjaliisa Rauste-von Wright ja Johan von Wright ja mainitsevat kirjassaan (2003), että aikuiset poikkeavat oppijoina nuorista ja lapsista. Havainnollistavana esimerkkinä he esittävät Knowlesin jo 1970 luvulla kehittämän andragogiikan, jonka perusoletukset eli aikuisena oppimisen erityispiirteet ovat:

1) Aikuiset muuttuvat kypsyessään riippuvuudesta kohti itsenäisyyttä ja itseohjautuvuutta.
2) Aikuinen voi käyttää oppimisen resurssina aikaisempaa monipuolista ja yksilöllistä elämänkokemustaan.
3) He pitävät oppimista mielekkäänä, koska sillä on välitöntä sovellusarvoa ja oppiminen suuntautuu ongelmien ratkaisemiseen.
4) Aikuisen oppimisvalmiudet liittyvät monesti hänen yhteyskunnalliseen rooliinsa.

Andragogiikan ja muissakin aikuiskoulutuksen suuntauksissa avainkäsitteitä ovat itseohjautuvuus ja ymmärtämisen tärkeys oppimisessa. Konkreettisena lähtökohtana on useimmiten Lewinin malli, jossa kuvataan miten oppimisessa ymmärtämisellä on keskeinen rooli eli tärkeää ei ole faktojen hallinta ja yksittäiset tiedot, vaan se organisoitu tieto- tai taitorakenne, johon ne sisältyvät. Pystymme siis perustelemaan esimerkiksi tapaa, jolla käytämme käsitettä (von Wright M&J & Soini 2003, 77–78, 165–166.). Tässä tapauksessa tuo käsite on kyberturvallisuus.

Aikuiskoulutuksessa on kehitetty paljon koulutusohjelmia, joissa korostetaan omien kokemusten reflektoinnin merkitystä eli mietiskellään ja pohditaan mitä opittiin, koska syvällinen oppiminen edellyttää teorian ja käytännön ymmärtämistä. Tieto myös organisoituu paremmin, mitä enemmän alasta jo tiedetään. Aikuisten kokemuksellisten tietojen ollessa laajempia, ne ovat myös usein syvälle juurtuneita, mikä voi vaikeuttaa sellaisen uuden tiedon omaksumista, joka ei ole nivottavissa olemassa olevaan tietoon. (von Wright M&J & Soini 2003, 78–79.) Liian juurtuneita käsitteitä tai automatisoituja rutiineja on vaikea muuttaa. Kyberturvallisuuden oppimisessa valmentajan tulee huomioida edellinen lähestymällä kyberturvallisuutta tietoturvallisuuden näkökulmasta.

Aikuiselle uuden oppiminen voi tuntua jopa ahdistavalta. Suhtautuminen muutokseen voi olla pelottava tai haasteellinen, jolloin on tärkeää ympäristön sääntöjenmukaisen toiminnan odotukset. Toisaalta aikuisiällä motivaatiolla on yhä suurempi merkitys uuden

oppimisessa. Lisäksi koulutuksessa on syytä silloin tällöin muistuttaa, että oppiminen on elinikäinen prosessi. (von Wright M&J & Soini 2003, 79–80.)

Kyberturvallisuusalan koulutuksen ja materiaalin sisällön suunnittelussa sekä opetusmenetelmiä ja teorioita tarkastellessa päädyttiin siihen, että johdon koulutuksessa on tuotava esille keskeiset kyberturvallisuusalan uhat, suojautumiskeinot, termit ja muut aihealueet eli lisättävä johdon kyberturvallisuustietoisuutta. Johdon on saatava vastaus siihen, miten kyberturvallisuutta parannetaan, jotta liiketoiminnan jatkuvuus on turvattu ja kyberturvallisuus antaisi yritykselle kilpailuetua. Johdon on itse ajateltava aktiivisesti haasteita ja etsittävä niihin ratkaisut oman organisaation osaamisesta ja hyvistä työmenetelmistä, kuten aivoriihestä, verkostoitumisesta, työpajoista jne.

Oppimisen osalta havaittiin jo 1950 -luvulla, että ihmisen tiedonkäsittelykapasiteetti on melko vaatimaton. Uuden aiheen, kuten kyberturvallisuuden, omaksuminen saattaa olla haasteellista sekä oppijalle että valmentajalle. Suosituksena on, että Power Point -esityksessä yhdellä sivulla tulee esittää enintään kolme pääasiaa (Lappalainen 2015, 139). Aihetta esitettäessä valmentajan tulee pysähtyä painottamaan keskeisiä ja tärkeitä aiheita. Valmentajan on huomioitava, että oppiminen vie aikaa, koska oppiminen on itseasiassa aivojen hermoverkkojen yhteyksien muuttamista (Lappalainen 2015, 140).

Jokaisella valmennettavalla on kapasiteettirajoitukset tarkkaavaisuuden osalta ja sanotaankin, että ihminen kykenee seuraamaan vain yhtä asiaa kerrallaan (Lappalainen 2015, 139). Tekstin määrä dioissa on minimoitava. Tästä asiasta mainitsivat myös pilotteihin osallistuneet. Vanha sanonta – ”kuva kertoo enemmän, kuin tuhat sanaa” – pitää edelleen paikkansa. Kuulijoiden muistaminen tehostuu aina, kun valmentaja käyttää kielellisen koodin lisäksi kuvallista, näköaistiin perustuvaa koodia (Lappalainen 2015, 137; ICT-ryhmän haastattelut 2017). Koulutuksen suunnittelussa käytettiin hyväksi myös piloteista saatuja kokemuksia ja analyysejä, joista on mainittu tarkemmin liitteessä 5.

Kuten jo aiemmin todettiin, suuretkaan investoinnit kyberturvallisuuden teknologiaan eivät auta, jos henkilöstö on kyberturvallisuuden heikoin lenkki. Kyberturvallisuuden koulutus ja harjaannuttamisohjelma on yritykselle elintärkeä ”vakuutus”. Työntekijä ei välttämättä tee tarkoituksellisesti tietoturvatapahtumaa, vaan usein se johtuu tietämättömyydestä ja osaamattomuudesta. Henkilöstön ja johdon koulutusohjelman voi toteuttaa

usealla eri tavalla painottaen aina samalla harjoittelua. Koulutuksessa tulisikin huomioida seuraavia asioita:

- Koulutus ja yleinen kyberturvallisuustietoisuus tulee tehdä osaksi henkilöstön jokapäiväistä toimintaa.
- Johdon tulee myös sitoa kyberturvallisuus osaksi työn vaatimuksia ja suoritusarviointia.
- Motivoidaan innokkaat alan harrastajat henkilökohtaiseen koulutukseen.
- Henkilöstölle tulee myös järjestää säännöllisiä kyberturvallisuuden harjoitteita, jolloin kyberturvallisuudesta saadaan jatkuva prosessi.
- Jatkuvaa osaamisen kehittämistä on tuotava jokapäiväisiin toimintatapoihin, koska uhat ja rikollisen tekniikat sekä keinot muuttuvat nopeasti. Hyvä keino osaamisen jatkuvaan kehittämiseen on pitää yllä tietotaitoa vuoden aikana tehdyllä suunnitelmallisella koulutuksella esimerkiksi 2-4 kertaa vuodessa. Alalla on myös verkkokursseja, joihin kannattaa tutustua.

Kyberturvallisuuskulttuurin jatkuva kehittäminen ja johtaminen vaatii johdon sitoutumista sekä myös koko henkilöstön osallistumista esimerkiksi järjestettävälle yrityksen kyberturvallisuuden koulutuspäivälle. Koulutusten yhteyteen järjestetyt alan työpajat, seminaarit ja aivoriihet auttavat lisäämään tietoisuutta uhista ja suojautumiskeinoista sekä yleistä tietoisuutta kyberturvallisuudesta. Erityisen keskeistä on kouluttaa uudet työntekijät kyberturvallisuuskulttuuriin, koska heidän tietämättömyytensä saattaa aiheuttaa korvaamattomia vahinkoja. Lisäksi omasta henkilöstöstä on löydettävä ne innokkaimmat, jotka haluavat kouluttautua asiantuntijoiksi.

Jo 1989 ilmestyneen National Institute of Standard and Technology eli NIST:n oppaan mukaan yritysjohdolle tulisi:

- kouluttaa tietoisuutta tieto- ja kyberturvallisuudesta
- kouluttaa tieto- ja kyberturvallisuuden suunnittelun ja johtamisen toteuttaminen sekä tietoturvallisuuspolitiikan ja tietoturvallisuuden menettelyt ja käytännöt
- esitellä ainakin varautumissuunnittelua ja järjestelmien elinkaaren hallintaa. (Computer Security Training Guidelines 1989, 6–8.)

Hieman ovat painotukset muuttuneet noista ajoista, mutta yllättävän hyvin NIST:n luoma koulutusstandardi on pitänyt pintansa ja tulevissa luvuissa nähdään, mitä erilaisia osakokonaisuuksia standardiin on tässä opinnäytetyössä lisätty.

3.3.2 Koulutustilaisuuden tarkoituksen ja tavoitteiden asettaminen

Opinnäytetyön tarkoituksena oli kyberturvallisuuskoulutusmateriaalin sisällön tuottaminen, koulutuksen suunnittelu ja toteuttaminen pienen ja keskisuuren yrityksen johdolle. Itse opetustilaisuuden osalta tarkoitus on aina sama, mutta joka kerta tulee suunnitella tarkennettu opetustarkoitus. Se vaihtelee yrityksen toimialan ja kohderyhmän mukaisesti. Tämän todistivat myös pilottien palautteet ja yrittäjien haastattelut. Koulutuksen sisällössä tulee aina huomioida erot kyberturvallisuuden painotuksissa kohderyhmän mukaan. Esimerkiksi tiedon luottamuksellisuus, eheys ja saatavuus priorisoidaan eri tavalla finanssi-, laki- ja ICT-alalla tai teollisuudessa.

Tarkennettu opetustarkoitus on suunniteltava antamaan yrityksen johdolle perusteet kyberturvallisuuden johtamiselle ja turvallisuuskulttuurin kehittämiselle. Tilaisuuden tavoitteena on luonnollisesti parantaa yrityksen kilpailukykyä markkinoilla. Itse opetustilaisuudessa kuulijoille on syytä tuoda heti esille opetustavoitteet, joita ovat

- tuntea kyberturvallisuuden peruskäsitteet ja alan määritelmät
- tuntea yrityksen oma kybertoimintaympäristö ja kuulijan oma rooli
- osata johtaa kyberturvallisuutta yrityksessä
- tuntea kyberturvallisuuden uhat ja riskit sekä osata suojautua niitä vastaan
- ymmärtää kyberturvallisuuden merkitys yrityselämässä ja yleensä jokapäiväisessä elämässä sekä
- lisätä johdon kyberturvallisuustietoisuutta.

3.3.3 Motivoiva ja osallistava oppiminen

Nykypäivän opettajat ovat pikemminkin valmentajia kuin opettajia tai asiantuntijoita. Oppimisen ja asian sisäistämisen kannalta tiimityöskentely ja opiskelijan motivaatio sekä osallistava oppiminen ovat keskeisessä asemassa. Tampereen ammattikorkeakoulun lehtoreiden Rami Lehtisen ja Mira Grönvallin kehittämän motivoivan oppimisen MiRaMi -konseptin (2016) mukaan opiskelijat oppivat ja motivoituvat parhaiten 4-5 hengen työryhmissä. Konseptissa opiskelijoille on tarkoitus antaa nimenomaan valmiudet työelämään. (Grönvall & Lehtinen 2016, 2–5.) Menetelmässä yhdistyy moni kognitiivisen, humanistisen (kokemuksellisen) ja konnektivistisen oppimiskäsitysten hyvät puolet.

Voidaan katsoa, että menetelmä sopii hyvin myös yrityselämän kyberturvallisuuden ryhmätyöskentelyyn.

Koska kyberuhkilta suojautuminen jaetaan yrityksen osalta ulkoisilta ja sisäisiltä uhkilta suojautumiseen, on näiden aiheiden kouluttamiseen myös keskityttävä. On painotettava, että sataprosenttista suojaa tai täysin teknisesti haavoittumatonta järjestelmää ei pystytä rakentamaan, joten suojautumisessa on keskityttävä kykyyn havaita ja reagoida kyberpoikkeamiin riittävän nopeasti ja tehokkaasti. Kun henkilöstö saa itse esimerkiksi aivoriihessä ryhmätöinä ideoida keinoja ja välineitä miten toimia kyberturvallisesti, saadaan heidät osallistumaan ja sitoutumaan parempaan turvallisuuskulttuuriin.

Henkilöstön kouluttaminen ennakoivaan tunnistamiseen ja tapahtumien kokonaiskuvan muodostamiseen on keskeistä, jotta esimerkiksi yrityksen kriittisen tuotantojärjestelmän outo tai epätavallinen käyttäytyminen havaitaan riittävän ajoissa ja siihen reagoidaan oikein. Yrityksen eri toimipisteissä käytössä olevan verkottuneen järjestelmän outo käyttäytyminen saattaa johtua haittaohjelmasta tai tavallisesta teknisestä viasta, mutta tärkeintä on madaltaa henkilöstön ilmoituskynnystä kyseisissä tilanteissa, jotta katastrofilta vältytään.

Koulutusta voi kehittää myös pelillistämisellä, josta esimerkkinä Hoxhunt -yrityksen (2018) kehittämä palvelu, missä työntekijät saadaan innostumaan ja kehittämään omaa kognitiivista ja turvallisempaa ajattelua. Yritys on monen muun alan asiantuntijan ajatuksien tavoin vienyt palkitsemisen käytäntöön kehittämällä aiheeseen ohjelmiston, koska usein miten rikolliset käyttävät sosiaalista hakkerointia rikosten tekemisessä. Ohjelmisto valmentaa tietokoneen käyttäjän aivot haittaohjelmia vastaan ja opettavaa vaikutusta kehuu myös arvostettu tietoturvallisuusasiantuntija Mikko Hyppönen. Kyseessä on tietoturvahyökkäyksiä simuloiva ohjelmisto, joka opettaa yritysten työntekijöitä tunnistamaan kyberrikollisten käyttämiä huijauksia. (Hoxhunt 2018, yrityksen blogi.)

3.3.4 Valmentaminen ja oppiminen tiimissä sekä ideointimenetelmät

Hyödylliset yhteisölliset ideointi- ja tiimityömenetelmät sopivat hyvin kyberturvallisuuskoulutukseen, koska ne soveltuvat luovaan ongelmanratkaisuun. Ilman innovointia minkä tahansa alan kehittäminen yrityksessä taantuu. Koulutustilanteeseen on luotava avoin,

positiivinen, vuorovaikutteinen ilmapiiri, missä ryhmätyöskentelyllä sekä verkostoitumisella on keskeinen merkitys.

Monista ideointimenetelmistä käyttökelpoisia ja tunnetuimpia ovat aivoriihi, ”lootuskukka” ja ”kuusi ajatteluhattua”. Nämä menetelmät soveltuvat myös kyberturvallisuusalalle. Kaikille menetelmille (2014) on tyypillistä poistaa normaalit ajattelun rajoitukset, motivoitua jakamaan hullutkin ideat ja kehittää muiden ideoita. Aivoriihi eli ideointipaja on luovan ongelmanratkaisun standardimenetelmä, jossa valmentajan johdolla 6-12 henkinen ryhmä ideoi uusia lähestymistapoja tai ratkaisuja kyberturvallisuuden haasteisiin. (Ojasalo ym. 2014, 160.) Ratkaisut saattavat olla hyvinkin yksinkertaisia, edullisia ja käyttäjäystävällisiä.

Ennen työpajaa aihe ja tavoitteet on hyvä rajata. Tässä valmentajalla on tärkeä rooli. Keskusteluvaiheessa, tuloksia ja syntyneitä ideoita tarkasteltaessa valmentajan tulee selkeästi jakaa puheenvuorot, jolloin kaikki pääsevät sanomaan mielipiteensä. Jokaisella on mahdollisuus antaa idealle tai päätökselle + tai - merkki, jolloin eniten merkkejä saanut idea on toteuttamiskelpoisin. (Ojasalo ym. 2014, 161).

De Bonon yksinkertaisessa ja helpossa ”kuusi ajatteluhattua” -menetelmässä ryhmätyön tekijät pakotetaan ajattelemaan monipuolisesti ja luovasti ilman riitelyä ja väittelemistä. Menetelmä antaa mahdollisuuden ajatella käsiteltävää aihetta vaiheittain eri tavalla, jolloin ajattelu ei mene sekaisin ja ryhmä aikaansaa rakentavan päätöksen. Menetelmässä on käytössä kuusi eriväristä ajatteluhattua. Sinisellä hatulla määritellään aihe, valkoisella jokainen tuo esille aiheeseen liittyvät tosiasiat. Punaisella hatulla jokainen tuo esiin aiheen tuomat tuntemukset (intuitiot). Keltaisella hatulla ajatellaan vain mahdollisuuksia. Mustalla hatulla ajatellaan aiheen uhkia ja ongelmia. Vihreällä hatulla jokainen tuo esille parhaat ideansa ja uudet ratkaisut mahdollisiin ongelmiin. (Ojasalo ym. 2014, 165–166.)

Erilaisista ideointimenetelmistä useampi on toteuttamiskelpoinen, mutta tähän opinnäytetyöhön valittiin ICT-startup -kurssilla 2017 hyviä kokemuksia saanut brainwriting eli hiljainen aivoriihi, jossa ideointi tapahtuu 4-6 hengen ryhmissä ilman keskustelua. Kukin kirjoittaa itsenäisesti paperille kolme ideaa viiden minuutin aikana, jonka jälkeen paperi annetaan ryhmässä seuraavalle, joka jatkojalostaa edellisen ideoita ja kirjoittaa uusia. Näin syntyy paljon melko pitkälle kehittyneitä ideoita, jonka jälkeen ryhmä valitsee yhteisessä keskustelussa parhaat ideat jatkokehittelyyn. (Ojasalo ym. 2014,161.)

Menetelmän etuna on, että se antaa myös hiljaisille henkilöille mahdollisuuden tasavertaiseen osallistumiseen ja helpottaa eri organisaatiotasojen ja toimialojen henkilöiden työskentelyä, josta syntyy yleensä parhaat ideat ja päätökset. Henkilöstö myös sitoutuu yhdessä tehtyihin ideoihin ja päätöksiin, koska kaikki ovat osallistuneet niiden tekemiseen. (Ojasalo ym. 2014, 161–162.) Valmentajalla on ideointihetkellä keskeinen rooli. Hänen on oltava herkkä huomaamaan ryhmien ongelmat ja ohjattava työskentelyä jakamalla puheenvuoroja.

Aivoriihessä on muutamia perussääntöjä. Ideoita ei voida arvioida tai tuomita liian nopeasti. Kannustetaan hulluilta ja liioitelluilta vaikuttavia ideoita. Ideoiden määrä korvaa laadun. Lisäksi kehitetään muiden ideoita, mahdollistetaan osallistuminen ja pidetään jokaista ideaa arvokkaana. (Ojasalo ym. 2014, 163.)

Kyberturvallisuusalan ryhmätöitä suunniteltaessa on valmentajan oltava tarkkana tehdäänkö arviointia vai ideointia, koska liian aikainen arviointi tyrehdyttää ideoinnin. Usein ideoija tyrmää liian aikaisessa vaiheessa omat ”hullut” innovatiiviset suojautumiskeinot. Luovassa ajattelussa on siis tiedostettava, että määrä eli lukuisat ideat synnyttävät laadukkaita kyberturvallisuuden suojautumiskeinoja.

Edellä mainitun MiRaMi-konseptin valmentamiseen ja opettamiseen liittyvät perusperiaatteet ovat:

1. Otetaan huomioon enemmän oppilaiden tarpeet kuin opettajan tarpeet.
2. Itsenäisen työskentelyn ja perinteisen opetuksen sijasta käytetään enemmän ryhmätyöskentelyä ja valmentamista.
3. Etäopiskelun ja virtuaalisuuden sijasta käytetään enemmän valmentajan läsnäoloa ja yhteydenpitoa oppilaisiin.
4. Yhden päivän aikana keskitytään monen aiheen sijasta vain yhteen aiheeseen.
5. Pienten harjoitustehtävien sijaan käytetään enemmän projektioppimista ja projekteja yleensä.

Arvoina MirRaMi-konseptissa ovat luottamus, kunnioitus, yhteistyö, valmentaminen, innostus ja läsnäolo (Grönvall & Lehtinen 2016, 3.) Voidaan todeta, että sekä konseptin perusperiaatteet että arvot ovat sellaisenaan hyödyllisiä myös yrityksen kyberturvallisuuskoulutuksen suunnittelussa ja toteutuksessa. Lisäksi MiRaMi -konseptia puoltaa selkeät havainnot paremmista oppimistuloksista, motivaation lisääntymisestä ja opiskelunsa keskeyttäneiden merkittävästä vähenemisestä. Ensimmäisen opiskeluvuoden jälkeen

keskeyttäneiden määrä väheni 50 %:a ja hakijamäärä koulutukseen lisääntyi 127 %:a (Grönvall & Lehtinen 2016, 6).

Myös kyberturvallisuuden koulutuksessa konseptin perusperiaatteet ovat selkeästi käyttökelpoisia. Kuulijoiden ja asiakkaiden tarpeiden on aina oltava etusijalla. Ryhmätyöskentelyn liittäminen yrityksen kyberturvallisuuskoulutuspäivään on hyödyllistä, koska silloin voidaan keskittyä yhteystyössä samaan aiheeseen. Valmentajan läsnäolo on tärkeää, jotta tarvittaviin alan polttaviin kysymyksiin saadaan heti vastaus. Valmentajan tehtävä on myös luoda luottamusta sekä kuulijoiden keskuuteen että valmentajan ja kuulijoiden välille. Ilman luottamusta kyberturvallisuuden kehittäminen on vaikeaa. Koulutuksesta ja sen kehittämisestä tulisi muodostua yritykselle pidempiaikainen kehitysprojekti, jonka käynnistämisessä johdolla on keskeinen rooli. Omassa yrityksessään kyberturvallisuuden tiimin jäseniä valittaessa johto voi käyttää MiRaMi -konseptin periaatteita (Grönvall & Lehtinen 2016, 5–6).

Kokemuksesta voidaan sanoa, että tiimissä oppiminen on monin verroin antoisampaa kuin yksin ”ahertaminen”. Sosiaalisessa kanssakäymisessä opimme enemmän muilta ja muut oppivat meiltä. Lappalainen korostaa kirjassaan (2015) luovan ideoinnin välineitä eli De Bonon ”ajatushattua”, aivoriihiä, proaktiivisia kysymyksiä jne. (Lappalainen 2015, 78). Valmentamisessa kuulijat tulee saada ajattelemaan luovasti ja itsenäisesti. On siis annettava mahdollisuus kysymyksille, vuorovaikutukselle ja ryhmätöille. Monesti puhutaan tällöin kyberturvallisuuden työpajoista.

Työryhmät kannattaa muodostaa erilaisista kyvykkyyksistä, koska erilaiset jäsenet täydentävät toisiaan ja luovat innovatiivisia haasteita (Lappalainen 2015, 79). Usein aivan erilaisesta lähtökohdista tulevat henkilöt osaavat tehdä niin sanottuja ”tyhmiä” tai oikeita kysymyksiä, jotka saavat varsinaisen asiantuntijan ajattelemaan aivan uudella innovatiivisella tavalla. Kun jäsenten luovuus ja kokemus sekä erilaiset näkemykset kohtaavat, syntyy mahdollisuus uudenlaisiin kyberturvallisiin ratkaisuihin ja niiden hyödyntämiseen. Yksinkertaisin keino erilaisten kyvykkyyksien yhdistämiseen on luvunlasku eturivistä, koska useimmiten yrityksessä samankaltaisesti ajattelevat ja samalla osastolla tai samankaltaisissa tehtävissä työskentelevät hakeutuvat lähelle toisiaan.

3.3.5 Systeemiajattelu kyberturvallisuudessa

Systeemiajattelun ensimmäisiä uranuurtajia oli Daniel Kahneman, jonka mukaan ihmisen aivot toimivat järjestelmällä yksi ja/tai kaksi. Tutkimuksien mukaan järjestelmä yksi toimii meillä automaattisesti ja nopeasti, vähäisin tai ei oikeastaan minkäänlaisin ponnistuksin. Kansankielellä puhutaan intuitiosta – ajatuksesta, joka tulee ensimmäisenä mieleen ja tuntuu heti oikealta tai väärältä. Päätös tuntuu tai tulee vaistonvaraisesti. Intuitiivisessa heuristiikassa on olennaista huomata, että jätämme yleensä vastaamatta vaikeisiin kysymyksiin ja vastaamme mieluummin helpompiin kysymyksiin. Yleensä, kun edessämme on vaikea kysymys tai ongelma, emme edes huomaa, että muutamme itse kysymyksen asettelua. (Kahneman 2012 12, 22, 30, 40.) Heuristinen systeemin yksi opittu toimenpide on esimerkiksi haittaohjelman tunnistamisen ja havaitsemisen jälkeen tehtävät toimenpiteet, jotka ovat sinänsä hyödyllisiä taitoja osata.

Järjestelmä kaksi kiinnittää aivoissamme huomiota ponnistusta vaativiin mentaalisiin toimintoihin, jotka edellyttävät monimutkaisia laskutoimituksia, keskittymistä, tarkkaavaisuutta tai valinnan tekemistä (Kahneman 2012, 30, 40). Kyberturvallisuudessa käyttäjällä voi olla edessään haaste, miten toimia edistyksellisen kalastushaittaohjelman suhteen? Tai miten huomioida kustannusten ja suojauksen kattavuus ICT-alan hankkeissa tai toteuttaa yrityksen riskikartoitus? Samaan haasteellisen ajattelun kategoriaan kuuluu myös kaikkien kyberuhkien joukosta sen uhkan löytäminen, joka on suurin uhka laajasta uhkakirjastosta. Pahimmat uhkat jäävät huomaamatta, jos käytämme vain intuitiota.

Voidaan todeta, että turvallisuuskulttuurin kehittämiseksi intuitiivinen ajattelu ei aina toimi. Kahnemanin (2012) mukaan – jos spontaani ratkaisutapa ei toimi eikä asiantuntijan tai heuristista ratkaisua ei löydy tai tule mieleen – on hyvä vaihtaa hitaampaan, harkitumpaan ja työläämpään ajattelun muotoon (Kahneman 2012, 11–25, 22.)

Patrian tietohallintojohtaja DI Sari Torkkola antaa Lean-ajattelusta kertovassa kirjassaan (2017) useampia esimerkkejä yrityksien toimintatavoista ja tietohallinnon ja muiden toimialojen välisistä yhteistyön ongelmista (Torkkola 2017, 18–131). Niitä voi hyvinkin verrata kyberturvallisuuden ja eri toimialojen väliseen yhteystyön kitkaan.

Lean-ajattelussa määritellään eri toimialojen yhteistyö jatkuvaksi vuorovaikutussuhteeksi esimerkiksi kyberturvallisuuden ja liiketoiminnan välillä. Yhteisenä tavoitteena on lisätä

kyberturvallisuuden ja liiketoiminnan suorituskykyä. Torkkolan mukaan (2017) yhteistyö koostuu neljästä päätekijästä, joita ovat kumppanuus, yhteiset tavoitteet, yhdenmukaisuus ja toimitusvarmuus. Yhteistyö on lisännyt tietohallinnon suorituskykyä 54 %. (Torkkola 2017, 85.) Samat päätekijät toimivat myös kyberturvallisuuden kouluttamisessa ja johtamisessa, koska yleensä tieto- ja kyberturvallisuus on aiheuttanut aina yrityksessä muutosvastarintaa. Valmentajan ja johtajan tulee saada siis aikaan eri osapuolien välille win-win tilanne eli tilanne, jossa molemmat osapuolet voittavat.

90-95 % yrityksen suorituskyvystä tulee ihmisten vuorovaikutuksesta ja systeemistä, jossa he työskentelevät. Ilman vuorovaikutusta yhteistyön taso on heikko, asiat eivät suju ja ristiriidat ja kustannukset yleensä kasvavat. Johdon tulee pyrkiä muuttamaan systeemiä, jolloin se pystyy vaikuttamaan 95 %:iin hallittavista asioista saaden aikaan oikeita tuloksia. (Torkkola 2017, 91–92, 95.) Johdon on siis ajateltava kyberturvallisuuden johtamista kokonaisvaltaisemmin keskittymällä vuorovaikutukseen ja yhteistyöhön.

Yleisesti systeemi voidaan nähdä siis itsenäisten osien muodostamana verkostona, joka tekee töitä yhdessä saavuttaakseen systeemin päämäärän. Systeemiajattelussa yksinkertaistetaan monimutkaisia asioita käsittelemällä kokonaisuutta korkeammalla abstraktiotasolla ja tutkitaan osien välisiä yhteyksiä jatkuvalla vuorovaikutuksella. Ei siis tutkita itse osia vaan unohdetaan pienet yksityiskohdat. (Torkkola 2017, 96, 104–105.)

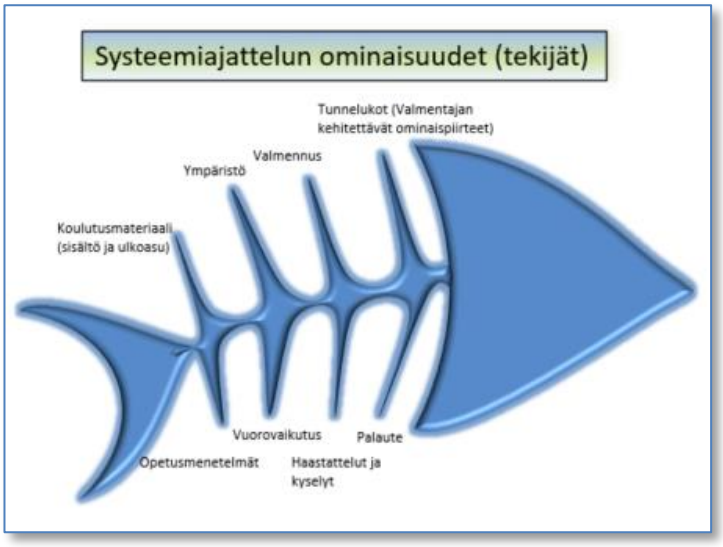
Yrityksen johtaja on vastuussa systeemitason muutoksesta. Systeemiajattelun perusperiaatteita ja kulmakiviä ovat: 1) Systeemillä on oltava päämäärä ja tärkein tehostamisen paikka on osien vuorovaikutuksessa. 2) Systeemissä on yksi tekijä, joka rajoittaa systeemin toimintaa. 3) Systeemit toimivat syy-seuraus -suhteiden vaikutuspiirissä. 4) Useat eitoivotut oireet johtuvat muutamasta juurisyystä. 5) Keskeisimpiä systeemin rajoitteita ovat säännöt ja linjaukset. 6) Ajan kuluessa ja systeemin ympäristön muuttuessa ongelmanratkaisu rämettyy. (Torkkola 2017, 96.)

Mitä enemmän systeemin osat ovat riippuvaisia toisistaan, sitä enemmän tarvitaan niiden välillä yhteistyötä, kommunikointia ja kokonaisuuden johtamista (Torkkola 2017, 96). Valmentamisessa ja koulutuksen kehittämisessä on selvää, että vuorovaikutus ja palautteen saaminen sekä kirjallisesti että suullisesti ovat analyysin avaintekijät. Myös kyberturvallisuuden johtamisessa yritysjohdon on omaksuttava systeemiajattelun merkitykset ja mahdollisuudet.

Systeemiajattelun kulmakiviä käytettiin työssä liitteessä 5 esitettyjen kyberturvallisuuskoulutuksen pilottien keittämisessä. Torkkolan (2017) mukaan systeemiajattelussa on aina ymmärrettävä kouluttajan oma rooli osana koulutusmateriaalin kehittämistä. On oltava valmis muuttamaan linjauksia ja toimintatapoja, jos se auttaa suorituskyvyn parantamisessa. Aivan keskeistä on ymmärtää ja hyväksyä, että omalla käyttäytymisellä on vaikutus toisiin osapuoliin ja sitä kautta takaisin itseen, tässä tapauksessa kouluttajaan. On myös uskallettava muuttaa systeemiä, jos tavoitteita ei savuteta. Lisäksi usein heikkoudet paljastuvat omasta ajattelutavasta tai virheestä. (Torkkola 2017, 97.)

Koulutuksessa on oltava selkeä tavoite jatkuvaan koulutusmateriaalin kehittämiseen ja koulutuspilottien parantamiseen, jotta asiakas saavuttaa liiketoiminnalleen todellista arvoa. Koulutusmateriaali ja pilotointi kehittyvät, jos valmentaja toteuttaa huolellisesti palautteen kysymisen ja on vastaanottavainen kuulijoiden mielipiteille ja kommenteille.

Yrityksessä systeemin ominaisuuksia voivat olla esimerkiksi tiedon laatu, organisaation rakenne ja roolit, henkilöstön määrä ja osaaminen, linjaukset, toimintatavat, menetelmät, tietojärjestelmät, mittarit, palkitseminen ja johdon käyttäytyminen. Näistä 3-5 on kriittisiä ominaisuuksia tai tekijöitä, jotka ratkaisevat saavutetaanko tavoite. Ominaisuuksista voidaan rakentaa Ishikawa-kaavion mukainen systeemin malli eli kalanruotokaavion mukaiset raaka-aineet, jotka systeemi tarvitsee toimiakseen (Torkkola 2017, 97–98, 101.) Kyberturvallisuuden kouluttamisessa on ymmärrettävä kokonaisuuteen ja lopputulokseen eniten vaikuttavat tekijät tai ominaisuudet, jotka on esitetty kuviossa 13.



KUVIO 13. Koulutukseen liittyvät systeemiajattelun tekijät (Torkkola 2017, muokattu)

Voidaan todeta, että systeemi koostuu kyseisistä raaka-aineista ja pullonkaulateorian mukaisesti jokin ominaisuuksista saattaa myös olla heikoin lenkki tai kriittinen tekijä. Systeemin suorituskykyä tulee tietenkin parantaa juuri heikoimman lenkin kohdalta. Heikoin lenkki saattaa myös liikkua systeemissä. (Torkkola 2017, 98–99.) Kyberturvallisuusalalla pullonkaulaksi muodostuu helposti koulutusmateriaalin sisällön päivittäminen, koska muutokset kybermaailmassa ja rikollisten hyökkäystavoissa muuttuvat nopeasti. Sen vuoksi on vain päätettävä keinot, joilla haasteesta selvitään kohtuullisella investoinnilla ja työpanoksella. Kyseinen pullonkaula on myös koulutettavan yritysjohdon kannalta merkittävä, koska uudet uhkat saattavat jäädä havaitsematta. Pullonkaulan vaeltaessa myös tekijästä toiseen on ymmärrettävä, että koulutuspilottien testauksia (iterointia) tulee jatkaa eikä se yleensä pääty koskaan.

Mistä tahansa aiheesta voidaan siis systeemiajattelun keinoin hahmottaa kokonaisuus, joka helpottaa ja selkeyttää tavoitteeseen pääsemistä. Mielenkiintoista on huomata systeemiajattelusta, että suurin osa systeemin rajoitteista on sääntöjä ja linjauksia (Torkkola 2017, 104). Näin voidaan ajatella olevan myös kyberturvallisuuspolitiikassa. Politiikkaa tehdessä on kiinnitettävä huomiota tähän ”sudenkuoppaan”. On myös estettävä systeemin ympäristön muuttuessa optimiratkaisujen rämettyminen. Sen vuoksi mm. kyberturvallisuusohjeita on päivitettävä jatkuvasti.

3.3.6 Perustelut piloteille ja pilottien analyysit

Palveluita ja tuotteita innovoidessa asiakas ja hänen ongelmansa tulee kohdata todellisessa ympäristössä. On tiedettävä, mikä asiakkaita huolettaa ja valvottaa. Innovoinnissa ja onnistuneissa palveluissa ihmisläheisyys ja käyttäjän suoran toiminnan havainnointi on keskiössä, jossa voidaan käyttää mm. nopeaa pilotointia ja testaamista, ryhmäkeskusteluja, haastatteluja ja kyselyjä sekä uskallusta haastaa vanhat toimintatavat. Tutkimukset osoittavat, että nopea palaute mahdollistaa tuotteen tai palvelun testaamisen ja kehittämisen edelleen. Muuten idean toimivuus on arvailujen varassa. Palvelua kehitetään sen käyttäjille. Menestystarinat ovat osoittaneet, että aktiivinen suhde käyttäjiin edistää tuotekehityksen onnistumisia. (Ruckenstein & Suikkanen & Tamminen 2011, 75, 83–89, 95.) Kyberturvallisia palveluita ja tuotteita syntyy vain, jos asiakasta kuunnellaan ja osataan asettua hänen asemaansa. Edellisen perusteella työssä päädyttiin kehittämään ja suunnittelemaan koulutusta pilottien, haastatteluiden ja ryhmätöiden avulla.

Kaikki opinnäytetyöhön liittyvät pilotit toteutettiin yrityksessä systeemiajatteluun perustuen liitteen 5 (s. 111–116) kaavioiden periaatteita ja prosessia noudattaen. Liitteen 5 alun kuvauksen mukaisesti kouluttaja kehitti itselleen systeemiajattelun avulla koulutuspilottien jatkuvan kehittämisen mallin päätyen alkutilanteesta ja vaiheesta 1 aina vaiheeseen 2, jossa prosessiin lisättiin esimerkiksi valmentajan itsensä tunteminen, johtaminen, positiivisuus, läsnäolo, oppijan kuunteleminen, tiimityö ja inspiroiva johtaminen. Liitteessä 5 on kerrottu myös tarkemmat analyysit koulutuspiloteista 1, 2 ja 3.

Pilotissa 1 (s.112) on kerrottu ICT-startup -ryhmän avoimen ryhmähaastattelun tulokset. Avoin haastattelu (työpaja) kohdistui silloiseen 29.9.2017 tehtyyn kyberturvallisuuskoulutusmateriaalin sisällön ja ulkoasun arviointiin.

Pilotissa 2 (s.113–115) koulutus toteutettiin viranomaisorganisaation keskijohdolle, josta saatiin paljon palautetta koulutusmateriaalin sisällön kehittämiseksi ja positiivista signaalia ryhmätöiden jatkamiseksi. Aivoriihen tuloksena löydetään paljon ehdotuksia ja ratkaisuja, joita ei tavanomaisessa jokapäiväisessä kiireessä tule ajatelleeksi.

Pilotissa 3 (s.115–116) koulutus toteutettiin alle 10 hengen yritykselle, jossa oppijoina oli johtoryhmän neljä jäsentä. Tilaisuudesta muodostui valmentajan systeemiajattelun tuloksena jo selkeästi avoimempi ja vuorovaikutuksellisempi kuin edellisestä. Tulokset ja analyysi on kerrottu tarkemmin liitteessä 5.

Piloteissa tehdyn havainnoinnin ja palautekyselyiden perusteella kuulijat haluavat oppia ja kuulla kyberturvallisuuden uhkien todellisista tapauksista. Erityisesti, jos valmentaja pystyy lisäämään esitetyn uhan kohdalla aiheeseen liittyvän tarinan tai videon. Palautteen yhteydessä huomattiin myös koulutuksen ekspansiivisen oppimisen voimanlähde eli ristiriidat ja negatiivinen palaute, jotka eivät ole kielteinen tai torjuva ilmiö vaan yleensä kyberturvallisuuden ja koulutuksen kehittämisen perusta. Palautteesta kävi ilmi myös, että esitysmateriaalin visualisointi tai videoiden käyttö on ainakin osin suotavaa, mutta varsinkaan iäkkäämmät eivät halua opiskella aihealuetta pelkästään videon välityksellä. Oppijat haluavat, että tilaisuus on vuorovaikutuksellinen ja ilmapiiri on mahdollisimman avoin sekä toimialueelle kohdistettu. Johdon haastatteluista ja palautekyselyistä saatavien tuloksien avulla on mahdollista ”räätälöidä” koulutusmateriaalin sisältöä toimialueelle sopivaksi ja koulutustilaisuuden tarkoitus ja tavoitteet voidaan myös kohdentaa johdolle

tarkemmin. Moni oppija toivoo myös konkreettisia ja toimialakohtaisia kyberturvallisuusohjeita.

Luennoitsijan on hyvä lähettää materiaali myös ennen esitystä kuulijoille, jotta he voisivat halutessaan tutustua siihen etukäteen. Kuulijan on aiheeseen etukäteen tutustuessa helpompi muodostaa kokonaiskäsitys, koska se täydentyy myös itse opetustilaisuudessa valmentajan puheen aikana. Oppiminen on prosessi, jossa aihe syventyy jokaisella kerralla, kun aihe kerrataan. Johtajan miettiessä esimerkiksi yrityksen keskeisiä riskejä valmentajan kertomat uhat saattavat muuttaa lopullisia suojautumiskeinoja ratkaisevasti.

3.3.7 Yhteenveto

Oppimisen osalta valmentajan on syytä painottaa koulutuksessa, että yrityksen johdon ei tarvitse olla valmentajan kanssa täysin samaa mieltä kyseisen yrityksen kyberturvallisuusratkaisujen ajatuksista, koska jokaisessa yrityksessä on omanlaisensa toimintakulttuuri. Riittää, kun kyberturvallisuusratkaisuissa ajatukset ovat samansuuntaiset, koska edistys on aina kiinni innovaatiosta, havainnoista ja suunnittelusta.

Piloteista havaittiin, että paras keino koulutuksen suunnitteluun ja kehittämiseen ovat nopeat pilotoinnit ottaen huomioon systeemiajattelun osatekijät ja mahdolliset heikoimmat lenkit, kuten koulutusmateriaalin päivityshaaste, johon löytyi vastaus liitteen 5 systeemiajattelusta. Pilotoinnin ja koulutusmateriaalin kehittäminen on jatkuva prosessi.
Kyberturvallisuus on niin laaja ja monitahoinen käsite, että yhdestä ajatuksesta (systeemi yksi) suojautumisen keinot eivät saisi tulla. Ajatusten on koostuttava useammasta tietoisesta kokemuksesta ja ajatuksesta. Monesti emme edes tiedosta, että ajatuksemme ovat tulleet yhdestä tietoisesta ajatuksesta. Valmentajan tärkeä tehtävä onkin saada johto ajattelemaan asioita pidempään, harkitummin ja kokonaisvaltaisesti systeemillä kaksi. Kyberturvallisuudessa on tärkeä yrittää parantaa turvallisuuskulttuuria eli myös yrityksen käytävillä ja kahvihuoneessa tapahtuvaa keskustelua, jotta tunnistaisimme, ymmärtäisimme arvioinnin ja valinnan virheitä sekä muissa että itsessämme. Tämän dialogin parantamiseksi johdolla on iso rooli ja huonoista arvioinneista, valinnoista sekä päätöksistä voidaan päästä eroon tai ainakin niistä johtuvia vahinkoja voidaan rajoittaa.

Systeemiajattelu kyberturvallisuuden rakentamisessa on keskeistä, jotta johto kykenee muodostamaan selkeän kokonaiskuvan aiheesta. Kouluttajan on tuotava asia esille puheessaan ja painotettava kyberturvallisuuden rakentamisessa priorisoinnin merkitystä, jossa kokonaisuuden kannalta on ensin laitettava kuntoon kriittisimmät tuotannon kannalta keskeiset tekijät. Kaikkia uhkia ei pystytä torjumaan heti ja joitain riskejä pitää pystyä sietämään. Varmasti moni meistä käyttää systeemiajattelua huomaamattaan jokapäiväisessä elämässään ja yrityksen johtamisessa, mutta harva ymmärtää asian tärkeyttä erilaisten prosessien kehittämisessä.

4 KOULUTUKSEN SISÄLTÖ JA TOTEUTUS

Tässä luvussa perustellaan, miksi koulutusmateriaalissa esitetyt sisällysluettelon kuvan 3 mukaiset aihealueet on päätetty ottaa mukaan johdon koulutusmateriaalin. Luvun tarkoitus on kertoa, mitä johto oppii. Lukuun on poimittu erittäin laajasta kyberturvallisuuden aihealueesta yrityksen johtamiselle merkitykselliset kyberturvallisuusaiheet. Lisäksi luvussa kuvataan koulutuksen toteuttamisessa huomioitavia asioista ja käsitellään luennon lopuksi toteutettavia ryhmätöitä ja niihin liittyviä aiheita.

4.1 Koulutusmateriaalin sisältö ja luennon juoni

Kyberturvallisuuskoulutusmateriaalin sisällöllä on keskeinen merkitys yrityksen johdon kyberturvallisuustietoisuutta lisättäessä. Tavoitteena on myös, että koulutuksesta saataisiin kilpailuetua markkinoilla ja yrityksen brändi ja maine pystyttäisiin turvaamaan. Yksilötasolla on myös keskeistä suojata ihmisten sekä työntekijöiden että asiakkaiden identiteetti ja henkilökohtaiset tiedot, koska vain siten lisätään turvallisuuden tunnetta ja luottamusta. Se miten kyberturvallisesti toimimme yksityiselämässä, heijastuu myös organisaation turvallisuuskulttuuriin.

Kouluttajilta jää usein kertomatta, että jokaisella on oikeus saada kyberuhkista riittävän hyvä kokonaiskuva ja selkeät toimintaohjeet. Koulutusmateriaalin sisällön osalta haaste oli iso, koska haastattelujen ja koulutuspalautteenkin mukaan luennon pituus saisi olla enintään 2-2,5h sisältäen tauot. Kiireinen yrityksen johto on saatava vakuuttuneeksi aiheen hyödyllisyydestä, vakavuudesta ja sen merkityksestä kilpailukyvylle.

Kauppakamari on omassa yrityksille kohdennetussa oppaassa painottanut, että kyberturvallisuuden koulutusohjelmaan tulisi sisällyttää ainakin seuraavia: 1) Turvallista ja vastuullista viestintää, kuten sosiaalisen median ohjeet. 2) Ohjeita luottamuksellisen tiedon tietoturvallisesta lähettämisestä julkisilla tietoliikenneyhteyksillä ja salasanojen oikeasta käytöstä. 3) Ohjeita yritykselle tärkeän tiedon katoamisen tai korruptoitumisen välttämisestä. 4) Ohjeita tiedon luottamuksellisuuden varmistamisesta sekä tiedon luokittelusta. 5) Tietoa ja ohjeita kyberrikollisuudelta suojautumisesta, miten toimia mahdollisissa

turvallisuushäiriötilanteissa ja miten vältetään urkintahuijauksien uhriksi joutuminen. (Tietoturvaopas yrityksille 2016, 19.)

Opinnäytetyön tuloksien perusteella päädyttiin sisällön osalta käsittelemään aihetta laajemmin. Johdolle suunnatusta koulutusmateriaalista on erillinen liite, joka ei ole julkinen. Sisällysluettelossa päädyttiin yksinkertaiseen ja selkeään jakoon, joka rakentuu opinnäytetyön aiempien lukujen, kirjoittajan kokemuksien sekä pilottien palautteiden perusteella kymmeneen eri kokonaisuuteen (kuva 3). Seuraavaksi kuvataan sisällysluettelon osa-alueet.

1. Johdanto (käsitteet)

Koulutusmateriaalin sisällön juoni ja rakenne on sellainen, että johdannossa kuulijat johdatellaan aiheeseen kuvaten kyberturvallisuusympäristön uhkia ja mahdollisuuksia yritysmaailmassa. Yrityksen johdon, niin kuin koko henkilöstönkin, tulee tietää ja ymmärtää kyberturvallisuuden ja kyberuhkien keskeisimmät peruskäsitteet sekä käsite-erot tietoturvallisuuteen ja tietosuojaan verrattuna. Tutkimuksen mukaan yrityksillä ei ole aiheesta riittävästi tietoa (Yrityksiin kohdistuvat kyberuhat 2015, 25–26). Yrityksen johdon tulee ymmärtää mitä riskejä haittaohjelmiin saattaa liittyä.

KUVA 2. Kyberturvallisuuskoulutuksen sisällysluettelo

Yrityksen johdolle kyberturvallisuus voidaan määritellä laajempana kokonaisuutena. Aikaisemmin keskeisiä suojattavia kohteita olivat verkot, työasemat ja palvelimet. Kyberympäristössä mukaan tulevat kaikki yhteiskunnan infrastruktuurin toimintakyvyn edellyttämät palvelut, esimerkiksi pankkipalvelut, sähköntuotanto ja -jakelu. Johdon rooli on ensiarvoisen tärkeää rakennettaessa kyberturvallisuutta. Ilman johdon sitoutumista

kyberturvallisuuteen turvallisuuskulttuuria ei pystytä luomaan ja kehittämään. Johdon on ymmärrettävä kyberturvallisuuden merkitys yrityksen toiminnalle. Johdon on sisäistettävä, miksi kyberturvallisuuteen tulee panostaa. Jokaisella yrityksellä on myös oma kybertoimintaympäristönsä, josta löytyvät ne haavoittuvuudet, jotka johto sitoutuu korjaamaan.

Kognitiivinen kerros on kyberturvallisuuden kerroksista se, jonka avulla turvallisuutta pystytään jo parantamaan. Työntekijöiden ja koko henkilöstön inhimillinen ongelmanratkaisukyky, osaaminen sekä informaation merkityssisällön ymmärtäminen ja tulkinta ovat avainasemassa kyberturvallisuutta rakennettaessa. Kaikki ovat omalta osaltaan vastuussa järjestelmien asianmukaisesta käytöstä ja ohjeiden noudattamisesta. Kyberturvallisuus terminä ja sen eri toimialueet on ymmärrettävä. Kuulijalle tämä hahmottuu parhaiten kuvina, joihin itse termi on sijoitettu. Näin kuulija ymmärtää käsitteen laajuuden ja mihin kyberturvallisuus liittyy. Osaavan ihmisen merkitys kyberturvallisuudessa on tuotava kuulijalle esille, sillä se on yrityksen tärkein voimavara. Yksittäisiin alan termeihin ei tosin kannata juuttua, koska ne avautuvat tarkemmin opiskelun edetessä. Tärkeintä on, että kuulijat sisäistävät aiheen merkityksen yritykselleen, sen maineelle, kilpailukyvylle ja brändille. Edellä esitetyn vuoksi esityksen johdanto aiheesta on normaalia pidempi eli diat 1-15. Näistä kahdeksaan keskitytään syvällisemmin.

2. EU:n tietosuoja-asetus, lait ja standardit

Tässä osa-alueessa johdolle tuodaan esille lakien, asetusten ja standardien merkitys, koska kyber- ja tietoturvallisuus sekä tietosuoja perustuvat ja rakentuvat viime kädessä näihin peruspilareihin. Asetukset ja standardit luovat kyberturvalliselle toiminnalle pohjan ja raamit. Tietosuoja-asetuksessa painotetaan rekisteröityjen oikeuksia. Asetuksessa on määritelty lukuisia rekisteröidyn oikeuksia, kuten saada pääsy omiin tietoihin, oikeus henkilötietojen oikaisemiseen, oikeus tulla unohdetuksi, oikeus siirtää henkilötiedot järjestelmästä toiseen, oikeus vastustaa tietojensa käsittelyä ja profilointia sekä oikeus saada ilmoitus henkilötietojen tietoturvaloukkauksesta.

Yrittäjän kannalta tietosuoja-asiat tulee huomioida nykyaikaisia digitaalisia palveluita tarjottaessa, mikä tuli esille myös johdannon dioissa kuluttajien tietoturvakäyttäytymiseen liittyen. Erityisesti on huomattava asetuksen tuomat uudet rekisteröidyn oikeudet ja mahdollisuudet, jotka EU:n tietosuoja-asetus tuo yrityksen kilpailukyvyn parantamiseksi. Lisäksi yrittäjille ja viranomaisille tulevat rekisterinpitäjän velvoitteet ja

osoitusvelvollisuus. Mahdollisista rikkeistä aiheutuneet sanktiot on tuotava esille unohtamatta asetuksen tuomia mahdollisuuksia. EU:n tietosuoja-asetusta käsitellään hieman laajemmin aiheen ajankohtaisuuden, vaikuttavuuden ja yrityksen kilpailukyvyn parantamisen vuoksi. Kuulijoiden on ymmärrettävä asetus mahdollisuutena eikä uhkana. Asetuksen tuomia uhkia ei tule toki unohtaa tai vähätellä.

3. Johdon rooli (vastuut, resurssit jne.)

Tässä osa-alueessa käsitellään johdon roolia ja kyberturvallisuuden vastuunjakoa yrityksessä. Aiheeseen liittyy useampi dia, koska johdon rooli on keskeinen koko yrityksen kokonaisturvallisuuden kannalta. Johdon rooli ulottuu kaikkiin sisällysluettelon osakokonaisuuksiin, joita ovat resurssien luominen, mandaatin antaminen kyberturvallisuusstrategian ja vision sekä riskienkartoituksen toteuttamiselle. Johto vastaa myös viime kädessä, että liiketoiminnan jatkuvuuden suunnitelmat on toteutettu ja harjoiteltu sekä yrityksen tilannekuvan muodostamisesta. Lisäksi johto on aktiivisena tukemassa verkostoitumista kyberturvallisuusalalla. Omalla esimerkillään johto kannustaa myös muita, osaa toimia oikein erilaisissa kyberturvallisuuden häiriötilanteissa ja osaa suojautua uhilta. Esimerkin voimaa on syytä korostaa johdolle.

Aiheet pyritään esittämään mahdollisimman havainnollisina kuvina ja avaamaan avointa keskustelua. Aiheiden sisäistäminen johdolle on ensiarvoisen keskeistä, kuten oppimisen teorian luvussa on kuvattu. Tavallaan johdon rooli, vastuut ja tavoitteet tulee sisältyä kaikkeen mitä kuulijoille esitetään. Johto ottaa kokonaisvastuun yrityksen turvallisuudesta ja mahdollistaa kyberturvallisuudelle sekä henkiset että taloudelliset resurssit. Esimiehet toimivat esimerkkinä omalla toiminnallaan ja ovat vastuussa työntekijöidensä kyberturvallisuusosaamisesta.

Johdon on myös sisäistettävä yrityksensä kyberturvallisuusriskit ja osattava hallita ne jatkuvalla johtamisella ja mittaamisella. Tärkeimmät suojattavat kohteet ja varat on tunnistettava ja kartoituksessa niihin kohdistuneet uhat tunnistettava. On osattava priorisoida ja suojauduttava tärkeimpiä uhkia vastaan, juuri niitä uhkia, jotka ovat todennäköisimpiä ja joiden vaikutus on vakava. Lopuksi on toteutettava uhkia vastaan riittävät vastatoimet eli reagoitava uhkiin. Suojautumiskeino voi olla hallinnollinen tai tekninen tai niiden yhdistelmä. Kyberturvallisuuden johtamisen kuviin on hyvä pysähtyä tekemään kysymyksiä esim. vakavimmista uhista. Lisäksi tulee painottaa systeemiajattelun merkitystä kyberturvallisuuden johtamisessa yrityksessä, josta on esimerkkinä materiaalista kuvio 14.

KUVIO 14. Kyberturvallisuuden johtamisen ketju

Yksilötasolla on tuotava esille asiat, jotka estävät kyberturvallista toimintaa, jotta johto voisi puuttua olennaiseen. Eikä tule unohtaa sisäänrakennetun kyberturvallisuuden välttämättömyyttä heti alusta lähtien.

Systeemiajattelun lisäksi johdon tulee ymmärtää kyberturvallisuuden johtamisessa ja rakentamisessa priorisoinnin merkitys sekä kokonaisuuden hahmottaminen, koska kaikki prosessit, tuotteet, palvelut ja vastuut muodostavat laajan kokonaisuuden, jossa on paljon keskinäisriippuvuuksia.

Johdon tulee siis tehdä kaikkensa kyberturvallisuuden ja tietosuoja hyväksi, koska maineen tai kallisarvoisen brändin menettäminen saattaa olla yritykselle kohtalokasta. Julkisten toimijoiden osalta maineen menetys syö merkittävästi viranomaisten uskottavuutta ja luotettavuutta ja sitä kautta heikentää kansalaisten turvallisuudentunnetta.

4. Kyberturvallisuuden visio, strategia ja politiikka

Osa-alueessa 4 johdolle kuvataan aiemmissa luvuissa esille tuodut kyberturvallisuuden visio ja strategia sekä kyberturvallisuuspolitiikka. Monelle pienemmän yrityksen johtajalle aiheet saattavat tuntua liian raskailta. Valmentajan on kuitenkin selkeästi tuotava esille niiden merkitys ja mahdollisuudet huomioiden toimenpiteiden laajuus yrityksen kokoon suhteutettuna. Muistutetaan, että kyberturvallisuus rakennetaan tietoturvallisuuden ja CIA-periaatteiden kautta huomioiden turvallisuusrakentamisessa kerroksellisuus, joka voi sinänsä olla jo yrityksen strateginen linjaus.

Vision luomisen ja strategian kehittämisen esittämiseksi ja aiheen ymmärtämiseksi on esitettävä havainnolliset ja prosessia kuvaavat kaaviot, jotta aihe ei koettaisi liian suuritöiseksi pienelle yritykselle. Kyberturvallisuuspolitiikasta tulee mainita esimerkkeinä mitä kaikkea se voi sisältää. Näitä ovat muun muassa yrityksen järjestelmien etäkäytön käytännöt, kuvaus haittaohjelmatapauksien käsittelytavasta ja prosesseista sekä kuvaukset yritysten järjestelmien hyväksytyistä käyttötavoista. Aiheesta on kerrottu enemmän liitteessä 4.

5. Kyberturvallisuuden tilannekuva ja verkostoituminen

Tässä osa-alueessa johdolle muistutetaan verkostoitumisen merkityksestä kyberturvallisuuden tilannekuvan rakentamisessa. Kannustetaan johtoa liittoutumaan ja verkostoitumaan muiden yrittäjien kanssa sekä erityisesti liittymään kyberturvallisuuskeskuksen toimialakohtaisille sähköpostilistoille. Yhteistyötä eri viranomaisten, yhdistysten ja yritysten kanssa kannattaa painottaa unohtamatta nykypäivän sosiaalisen median merkitystä yrityksen kilpailukyvylle ja maineelle. Esimerkiksi kyberturvallisuuden twitter-tililtä saa melko reaaliaikaista tietoa yrityksen käyttöön.

Varsinkin pienten ja keskisuurten yritysten tulee tuntea myös viranomaisten roolit. Verkostoitumisesta ja kybertilannekuvan luomisesta vastaa viime kädessä yrityksen johto. Kyberturvallisuuskeskus on viranomainen, jolta saa neuvontaa, jos epäilee joutuneensa hyökkäyksen kohteeksi tai haluaa varautua uhkien varalta.

Verkostoitumalla yritykset voivat selvittää itselleen yhteyskunnalliset vastuunjaot kyberturvallisuuden alalla saaden samalla tärkeää tietoa säädöksistä ja alan yhteistoimintamallista. Kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välistä vastuunjakoa, joka perustuu asetuksiin, lakiin ja säädöksiin sekä sovittuun yhteistyöhön. Suomessa on luotu kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja kaikkien muiden toimijoiden välinen tehokas yhteistoimintamalli. Se on herättänyt kiinnostusta koko maailmassa (Saarimäki 11.1.2018). Yritysten kannalta tärkeimmät viranomaiset ovat Viestintäviraston kyberturvallisuuskeskus ja lainsäädännön osalta tietosuojavaltuutetun toimisto.

6. Riskien kartoitus ja liiketoiminnan jatkuvuus

Tässä osa-alueessa käsitellään yritysturvallisuuden kokonaisuus, josta nähdään, että riskien hallinta tulee heti strategian jälkeen. Esityksessä painotetaan, että riskienhallinta on

oltava jatkuvaa ja suunnitelmallista. Tuodaan esille yksinkertainen riskienkartoitusmalli, joka ottaa huomioon riskin toteutumisen todennäköisyyden ja sen vaikuttavuuden. Yritystutkimuksien perusteella riskit jakaantuvat enemmän sisäisiin kuin ulkoisiin, mikä vaikuttaa selkeästi yritysjohdon kyberturvallisuuden johtamiseen. Riskikartoituksen ja liiketoiminnan jatkuvuuden kannalta on tuotava esille erilaiset riskit ja parhaat käytänteet liiketoiminnan jatkamiseksi. Riskien kartoituksessa yrityksen johdon on oltava myös aktiivisesti mukana. On syytä pysähtyä pidemmäksi aikaa erilaisten kyberturvallisuusriskien kohdalla, jotta kuulijat ehtivät ajatella hieman pidempään oman yrityksensä mahdollisia riskejä. Tosiasia, että riskit tulevat noin 60-prosenttisesti yrityksen sisältä, on tuotava johdolle esille selkeillä tutkimustuloksilla.

7. Kyberturvallisuuden uhat ja niiltä suojautuminen

Seitsemännessä osa-alueessa erilaisilla toteutuneilla tapauksilla ja esimerkeillä elävästä yrityselämästä on tarkoitus saada kuulijat ajattelemaan asioita pidempään ja systemaattisesti. Tarkoitus on tuoda esille avoimesti omia haittaohjelmatapauksia, koska niiden ennaltaehkäisyyn valmentajan on annettava suojautumiskeinoja ja toimintamalleja. Johdolle opetetaan vaiheittain, miten haittaohjelmatartunnan saa yleisimmin internetselailussa tai sähköpostin liitetiedoston kautta, joten käyttäjän toimenpiteillä on suojautumisessa suurin merkitys.

Kyberturvallisuuden yleisluonteiset ohjeet sopivat luonnollisesti myös yrityksen johdolle, koska johtohenkilöt ovat tavallisten käyttäjien tavoin tietojärjestelmien käyttäjiä ja heillä on jopa suurempi riski päätyä kyberrikollisen kiinnostuksen kohteeksi. Kokemuksien ja havaintojen mukaan tietojen urkinnat kohdistuvat yleensä niihin, joilla on luottamuksellista tietoa enemmän tai joilla on siihen pääsy. Heitä ovat esimerkiksi ICT-järjestelmien ylläpitäjät, pääkäyttäjät, yrityksen päättäjät ja rahan siirroista vastaavat henkilöt.

Monet yritykset mieltävät kyberturvallisuuden pelkästään tekniseksi asiaksi. Ne toteuttavat perusinfrastruktuuriin liittyen ensimmäisenä tekniset turvallisuustoimenpiteet eli ottavat käyttöön palomuurin ja antivirusohjelmiston sekä kannettaville tietokoneille ja muille mobiililaitteille tarkoitetun pääsynhallinta- ja käyttöoikeusjärjestelmän. Toimenpiteet ovat hyviä ja monesti tarpeellisia hankintoja, jos ne tehdään kustannustehokkaasti. Silti ensin tulisi laittaa kuntoon yrityksen hallinnolliset määräykset ja toimintaohjeet ja vasta sen jälkeen käynnistää mittavammat laitehankintojen suunnitelmat.

Lunnastroijalaisten suhteen yleinen ohje on, että lunnaita ei missään nimessä kannat maksaa, koska se ei takaa salauksen purkua (Kyberturvallisuuskeskus 2015). Valitettavaksi trendiksi ovat muodostuneet myös hyökkäykset pilvipalveluihin. Liian moni yrittäjä käyttää kriittisten tietojen tallennukseen suojaamattomia pilvipalveluita ja monet ovat joutuneet kiristyshaittaohjelman tai tietovuotojen uhriksi. (Yrittäjien haastattelut 2017; Motherboard artikkeli 2018, 1).

Haittaohjelmatartunta saadaan usein internetselailun yhteydessä niin sanotun exploit-kitin välityksellä. Exploit-kit on verkkosivustolta käsin toimiva haittaohjelman jakelualusta, joka selvittää hetkessä sivustolla vierailevan kävijän tietokoneen haavoittuvuudet. Yleisimmät haavoittuvuudet liittyvät ActiveX-komponentin[6] liitännäisiin, kuten Java:n tai Adobe Flash ohjelmistoon. Kyseistä haavoittuvuutta apuna käyttäen exploit-kit murtautuu tietokoneeseen ja asentaa haittaohjelman selailijan huomaamatta. Haittaohjelmia voi tarttua sähköpostin liitteitä avattaessa, somesta, pikaviestimistä tai siirrettävästä mediasta, kuten USB-muistitikulta. USB-tikku on ulkoisista medioista ehkä vaarallisin, koska se ei vaadi aina edes käyttäjän klikkausta (Lehto 2018, luento; Yrityksiin kohdistuvat kyberuhat 2015. 6,19,24–26; ITKP0002 Johdatus kyberturvallisuuteen 2016.) Kyseiset aiheet on avattava johdolle animaation avulla ja kerrottava samalla suojautumiskeinot.

Kaikki tuntevat sähköpostien linkkien ja liitteiden riskit, mutta silti työntekijät ja johtajat avaavat niitä olematta varmoja lähettäjästä tai sähköpostissa esitetyn asian oikeellisuudesta. Rikollisen lähestyminen sähköpostin avulla on edelleen yleisin keino etsiä työntekijöiden inhimillisiä heikkouksia ja sitä kautta päästä yrityksen verkon sisälle. Paras suojautumiskeino on edelleen siis henkilöstön kouluttaminen ja heidän turvallisuustietoisuutensa sekä asenteidensa parantaminen ja viestien salaaminen. Hyökkäysmenetelmän havainnollistamiseksi ja suojaustoimenpiteiden sisäistämiseksi esitetään materiaalissa diat, jotka kertovat hallinnolliset ja yleiset tekniset suojausmenetelmät.

Kyberuhkia vastaan suojauduttaessa oleellista on henkilöstön kyky tunnistaa ja raportoida epäilyttävä ja poikkeava toiminta esimerkiksi yrityksen verkossa. Henkilöstöllä tulee olla aina kyky noudattaa turvalliseen järjestelmien käyttöön liittyvää ohjeistusta, jotka tulee olla helppolukuinen, selkeä ja mahdollisimman lyhyt.

---

[6] Toinen nimi Windows-käyttöjärjestelmässä käytetylle Component Object Model (COM) -tekniikalle. COM-komponentit ovat uudelleenkäytettäviä ohjelmistokomponentteja.

Johdolle on painotettava, että myös phishingiä eli tietojen kalastelua sekä haittaohjelmahyökkäysten uhkia ja niiden toteutumista voidaan vähentää antamalla henkilöstölle valistavaa kyberturvallisuuskoulutusta, ajantasaista ohjeistusta ja turvallisia toimintatapoja. Phishing on ollut kyberturvallisuuskeskuksen uutisissa jo useamman vuoden. Yritysten verkostoituminen, aktiivinen tiedottaminen ja tiedonvaihto eri alan toimijoiden ja asiantuntijoiden kesken on jo sinänsä hyvä suojautumiskeino.

Sekä käyttäjille että johdolle on muistutettava sosiaalisen median käytöstä liitteen 2 s. 107 mukaisesti. Henkisessä koulutuksessa on tuotava esille, että käyttäjän joutuessa pysähtymään ja miettimään vastaanotettavan viestin todenperäisyyttä, on kynnys yleensä ylittynyt. Aiheen diasta voidaan esittää sopiva ”kevennys” luennolla.

8. Työskentelyohjeita ja suojautumiskeinoja

Tämän osa-alueen tulee sisältää mahdollisimman paljon konkreettisia toimenpiteitä kyberturvallisuuden parantamiseksi ja kehittämiseksi. Näihin kuuluu muun muassa tiedon luokittelu erilaisissa tilanteissa ja ympäristöissä. Kyseisiä ohjeita on mainittu myös koko työn yhteydessä kuten kyberturvallisuuskeskuksen TOP5-uhat ja suojautumiskeinot.

Päätelaitteiden osalta kyberturvallisuus on loputonta kilpajuoksua kyberrikollisia vastaan. Ohjelmistovalmistajat ja laitevalmistajat vastaavat tuotteen tai palvelun kyberturvallisesta suunnittelusta, toteutuksesta sekä päivityksistä koko laitteen elinkaaren ajan, tehden mahdollisimman turvallisia tuotteita. Tämä sisäänrakennettu turvallisuus toimii, jos käyttäjäkin vastaa tuotteen tai palvelun kyberturvallisesta käytöstä, kuten:

- käyttää vain ajantasaisia ja päivitettyjä ohjelmistoja sekä käyttöjärjestelmää
- pitää selaimen liitännäiset (sovellukset, kuten Adobe flash ja Java) ajan tasalla
- käyttää luotettavia virus- ja haittaohjelmaohjelmistoja sekä palomuuria
- käyttää vahvoja salasanoja sekä kaksivaiheista tunnistautumista
- rajoittaa internetistä pääsyn kodin ja työpaikan aktiivilaitteisiin
- käyttää päätelaitetta internetissä käyttäessään vain peruskäyttäjätunnusta
- ei avaa tuntemattomista ja joskus jopa ”tutuista” sähköpostiosoitteista lähetettyjä viestejä ja niiden liitetiedostoja (Yrityksiin kohdistuvat kyberuhat 2015, 33,34; Kirjoittajan kokemukset 2000–2018.)
- poistaa käyttöjärjestelmästä tai ohjelmistoista täysin tarpeettomat ohjelmistokomponentit ja palvelut

- koventaa kannettavat tietokoneet asettamalla niihin BIOS-salasanan ja poistamalla kannettavasta tarpeettomat ulkoiset liitännät.

Kyberturvallisuuden kokonaisuuden hahmottamiseksi johdolle on syytä kerrata Elinkeinoelämän keskusliiton kyberasiantuntija Mika Suden (2018) kuvaamat keinot kyberturvallisuuden parantamiseksi: 1) Tunnistetaan tärkeä suojattava tieto ja materiaali. 2) Arvioidaan riskit ja suojattava liiketoiminta huomioiden tuotos-panos -suhde. 3) Panostetaan havainnointi- ja reagointikykyyn, koska kybertoimintaympäristö muuttuu jatkuvasti. 4) Luodaan kybertilannekuva ja koska kaikkea ei voi suojata kasvatetaan sietokykyä kyberhyökkäyksiä vastaan (kyberresilienssi). 5) Pidetään mielessä ihmiset, prosessit ja verkostot. Osaamista ja valmiuksia on kehitettävä jatkuvasti unohtamatta tässäkin opinnäytetyössä useasti mainittuja ohjeistusta, koulutusta ja kannustusta. (Susi 2018. Yritysturvallisuus.) Yrityksen kilpailukyvyn lisäämiseksi listaan voidaan lisätä myös tietotilinpäätös tai -kartoitus. Kyberrikollisen teknisiä kykyjä, motivaatiota ja älykkyyttä ei tule myöskään koskaan aliarvioida (Harris 2016, 14).

Jos yrityksen järjestelmissä on heikkouksia, rikollinen kyllä löytää ne ja osaa käyttää niitä hyväkseen. Heikkouksia ei saa piilottaa, vaan niistä tulee päästä eroon hyvillä tietoturvallisuuskäytännöillä. Esimerkkinä vaikkapa havainnot henkilöstön huonosta koulutustasosta, minkä johto usein sivuuttaa tai unohtaa. On esitettävä toimenpiteet, jotka johto voi tehdä yrityksen kyberturvallisuuden parantamiseksi ja rakentamiseksi.

9. Tulevaisuus

Yrityksen tulevaisuus määräytyy melko pitkälle siitä, miten se hallitsee esim. digitalisaation, virtualisoinnin, tekoälyn tuomat haasteet tai kyberturvallisuuden tuomat uhat ja mahdollisuudet. Vastuullisen ja tulevaisuuteen katsovan johdon tulee ymmärtää ja osata katsoa tulevaisuuteen. Tästä esitetään heille muutamia megatrendejä unohtamatta mainita kyberturvallisuuden myyttejä.

10. Ryhmätyön toteuttamien (aivoriihi)

Luennon ja siihen liittyvän mahdollisen ryhmätyön toteuttamiseksi käytettiin luvussa 3 esitettyjä oppimiskäsityksiä ja menetelmiä. Opinnäytetyön ryhmätyöksi valittiin hiljainen aivoriihi, koska tarkoitus oli saada yrityksen johto ajattelemaan kyberturvallisuutta laajempana kokonaisuutena. Aivoriihi on menetelmänä helppo omaksua ja nopeasti toteuttavissa, kunhan valmentaja esittelee ryhmätyön kulun ja hyvät puolet selkeillä kuvilla.

Aivoriihen toteutuksesta on hyvä mainita heti koulutuksen alussa, jotta kuulijat voivat valmistella mielessään parasta mahdollista ryhmätyön aihetta, jonka tekemisestä yritys saisi innovatiivisia ja kustannustehokkaita keinoja kyberturvallisuuden ja kilpailukyvyn parantamiseksi. Ryhmätyön toteuttamisessa valmentajalla on aivan keskeinen rooli luvussa 3 kuvattujen periaatteiden mukaisesti. Valmentajan on mietittävä muutamia ryhmätyön aiheita, jotka sopivat yritykselle ja kyseiselle toimialalle.

4.2 Muita koulutuksen toteuttamisessa huomioitavia asioita

Johdon osallistamiseksi ja vuorovaikutuksen lisäämiseksi on hyvä antaa opetustilaisuuden alussa tehtävänanto johdolle. Juvonen (2017) neuvoo blogissaan, että kuulijoita pyydetään laittamaan liimalapuilla oman osaamisensa ja tietämyksensä tason eri aiheita käsitteleville janoille, joissa toisessa päässä käsite oli tuttu ja toisessa tuntematon (Juvonen 2017. Blogi). Termit pilottikoulutuksissa olivat kyberturvallisuus, tietoturvallisuus ja tietosuoja. Näin myös valmentaja sai kuulijoista yhdellä silmäyksellä osaamisen tason, joka helpotti esitettävien aiheiden kertomista ja painotusta. Itse luennolla tulee antaa aina mahdollisuus kysymyksille ja esimerkiksi kuulijoiden ”ääneen ajattelulle” aiheesta. Tilaisuudesta tulee näin vuorovaikutuksellisempi.

Luennon jälkeen opitut aihealueet on vietävä mahdollisimman nopeasti käytäntöön, koska ymmärtäminen ja sisäistäminen syvenee, kun oppija rakentaa aiheesta itselleen kokonaisuuden aikaisempiin kokemuksiin ja tietoon perustuen. Valmentamisessa käytetään luvussa 3 esitettyjä oppimiskäsityksiä yhdistäen kognitiivisen, konstruktivistisen, humanistisen (kokemuksellisen) ja konnektivistisen oppimiskäsitysten hyviä puolia ottaen huomioon piloteissa hyväksi havaittuja oppimismenetelmiä, kuten osallistava opetus, ryhmätyöt ja aivoriihityöskentely. Välittömän, luennon jälkeisen ryhmätyön avulla yrityksen johto saavuttaa myös itselleen tilaisuudesta asetetut tavoitteet ja syventää oppimaansa. Tarvittaessa osallistavaan opetukseen voidaan käyttää aiemmin mainittua hattumenetelmää, mikäli johdon tulisi tehdä esimerkiksi kyberturvallisuuteen liittyvä vaikea päätös. Ryhmätöiden valmisteluun täytyy huomata varata myös aikaa, koska menetelmät eivät ole aina kaikille tuttuja ja silloin valmentajan rooli on suuri ryhmien koordinoinnissa ja ohjauksessa. Ryhmätöissä ja työpajoissa kuulijoiden mielipiteet ja ajatukset tulisi saada hyödynnettyä yrityksen oman toimintatavan kehittämiseksi. Vaikka valmennettavien

siirtyessä jokapäiväiseen arkeen, opetus usein unohdetaan, keskeinen kyberuhka jää huomioimatta tai hyödylliset suojaustoimenpiteet jäävät selvittämättä.

Osallistavan oppimisen mahdollistamiseksi luennon jälkeen lisättiin pääsääntöisesti hiljainen aivoriihityöskentely (työpaja), jotta kuulijoiden mielessä olevasta asiasta muodostuisi konkreettisia tuloksia yritykselle. Työskentelytapa on tuttu monesta alan seminaarista. Paras hyöty työpajasta saadaan, jos aiheet liittyvät yrityksen ajankohtaiseen haasteeseen, kuten riskien kartoitukseen, suojattaviin kohteisiin tai innovatiivisiin suojautumiskeinoihin. Mikäli on tarkoitus tehdä yrityksessä pidempiaikainen kyberturvallisuusalan projekti, valmentaja voi vinkata MiRaMi-konseptin tiimijaosta, jossa jokaiselle ryhmän jäsenelle annetaan tietty vastuualue.

Oppimisen osalta ihmiset on saatava ajattelemaan luovasti tai lateraalisesti eli samansuuntaisesti. Meidän ei tarvitse olla asioista kuitenkaan samaa mieltä. (Lappalainen 2015, 23.) Myös kyberturvallisuudessa oppiminen ja koulutus tapahtuu ihmisten ajatuksissa, informaation, ymmärryksen ja tulkinnan ympäristössä. Koska jokaisella yrityksellä on omanlaisensa kyberturvallisuuspolitiikka, on johto saatava ajattelemaan kyberturvallisuutta laajempana kokonaisuutena ja mahdollisuutena.

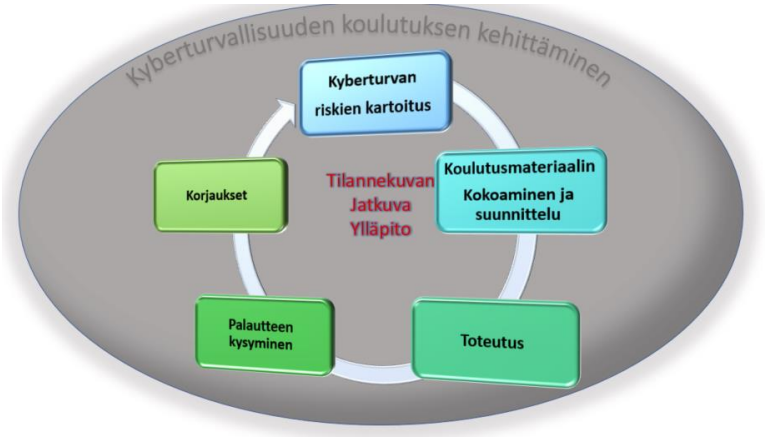
4.2.1 Vaihtoehtoiset ryhmätyöt ja koulutusmateriaalin päivitys

Aina aivoriihen aiheita ei voida kohdentaa. Tällöin yrityksen kyberturvallisuuden itsearviointi tai kartoitus voi olla ryhmätyön vaihtoehto, jos aihe pystytään selkeästi rajaamaan. Liitteessä 1 (s. 92–106) on esitetty yksinkertaiset tarkastus- ja kartoituslistat, joiden avulla yrityksen johto voi tehdä kartoituksen myös itsenäisesti. Tarkastuslistojen pohjina on käytetty mm. tietoturvaoppaan listoja, joita kirjoittaja on muokannut parhaan näkemyksensä mukaisesti (Tietoturvaopas yrityksille 2016, 21–36). Kyberturvallisuuskartoituksen kysymysten avulla johto voi tunnistaa oman yrityksensä kyberturvallisuuden vahvuuksia ja puutteita sekä löytää valmentajan ohjaamana ratkaisuja kyberturvallisuuden kehittämiseksi. Parhaan tuloksen kartoituksesta saa, jos koulutuksen pitäjä on vastaamassa johdon kysymyksiin. Pilottien kokemuksien perusteella kysymykset liittyvät koulutuksen aihealueeseen ja erilaisiin parhaisiin käytäntöihin, kun johto miettii mahdollisia suojautumiskeinoja ja menetelmiä. Kartoituksessa muodostuu myös selkeä tehtävälista yrityksen kyberturvallisuuden kehittämiseksi.

Toiseksi vaihtoehtoiseksi ryhmätyön aiheeksi valittiin kyberturvallisuuden rakentaminen tietoturvallisuuden avulla, joka sopii pienille ja keskisuurille yrityksille. Tällöin yrityksen turvallisuuskulttuuria rakennettaessa käytetään apuna tietoturvallisuuden määritelmää, jossa yritykselle tärkeää tietoa ja tiedon ominaisuuksia pohditaan tiedon luottamuksellisuuden, eheyden ja saatavuuden eli niin kutsutun CIA:n avulla. Tietoturvallisuus siis pidetään mielessä jokaisessa kymmenessä teesissä tai haasteessa. Tietoturvallisuus ja turvallisuuskulttuuri tuodaan yrityksen prosesseihin − yrityskulttuuriin. Ajatus on alun perin johdettu kyberturvallisuuskeskuksen verkkojulkaisusta (20.10.2017) *"Kartoita ja leivo tietoturva osaksi yrityskulttuuria - apuna CIA ja 10 teesiä"*. CIA ja 10 teesiä on kuvattu tarkemmin liitteessä 8 (s. 124–126).

CIA eli tiedon luottamuksellisuus, eheys ja saatavuus tulee muistaa yrityksessä asettaa aina myös tärkeysjärjestykseen. On kysyttävä siis, mikä niistä on yritykselle tärkeintä? Esimerkiksi Google asettaa tärkeämmäksi tiedon luottamuksellisuuden ja käytettävyyden. Amazonilla tärkein kriteeri on käytettävyys, koska ilman sitä ei tapahdu myyntiä. Pienillä yrityksillä aihe on keskeinen, koska tuotos-panos -suhde on myös aina otettava huomioon eli kyberturvallisuuden hyödyt ja kustannukset tulee olla aina tasapainossa (Susi 2018, verkkosivut). Yritysturvallisuudessa korostuu erityisesti henkilöstön kouluttaminen, turvallisuustietoisuuden lisäämisen ja hyvän turvallisuuskulttuurin luominen. Tietoisuuden lisääminen koulutuksen avulla on mainio uhkien ennaltaehkäisevä ja estävä kontrollointikeino.

Koulutusmateriaalin päivitykseen liittyen todetaan yhteenvetona, että kyberturvallisuuden ja digitalisaation laaja-alaisuudesta ja jatkuvasta muutoksesta johtuen koulutusmateriaalin sisältö tulee muuttumaan viikoittain. Johtamisen suhteen materiaali säilyy stabiilina, mutta uhkien ja siihen liittyvä riskien kartoitus sekä tilannekuvan ylläpito ovat jatkuvia prosesseja. Systeemiajattelun periaatteita noudattaen toteutettiinkin
yksinkertain prosessikaavio materiaalin päivityssyklin toteuttamiseksi, joka on esitetty kuviossa 15.



KUVIO 15. Koulutusmateriaalin päivitysprosessi

Kyberturvallisuudessa on kyse jatkuvasta kilpajuoksusta, missä kyberrikolliset kehittävät koko ajan yhä monimutkaisempia ja innovatiivisempia keinoja rikosten tekemiseen. Kyberrikolliset seuraavat tilannetta julkisuudessa ja vanhojen tekotapojen tullessa yleisesti tunnetuksi, he keksivät uusia. Vanhentunut koulutusmateriaali olisi yrityksille epäedullista, koska tällöin ei olisi tietoa miten esimerkiksi jo tunnettuja haittaohjelmia vastaan suojaudutaan. Yrityksiltä vaaditaan siis myös omaa aktiivisuutta tilannekuvan ylläpitämiseksi. Monesti tilanteen korjaisi oma kyberturvallisuusosaaja, joka pitää mm. säännöllisesti yhteyttä kyberturvallisuuskeskuksen CERT-FI -päivystäjiin.

Koulutustilaisuuden palautteeseen on aina tutustuttava huolella. Palautekysely tulee toteuttaa aina sekä suullisesti että lomakkeiden avulla ja siitäkin tulee tehdä mahdollisimman avoin ja vuorovaikutuksellinen. Palautteesta on aina apua valmentajan koulutuksen kehittämisessä. Myös valmentaja oppii oppijoilta!

5 POHDINTA JA YHTEENVETO

Opinnäytetyön tarkoituksena oli kyberturvallisuuskoulutusmateriaalin sisällön tuottaminen, koulutuksen suunnittelu ja toteuttaminen pienen ja keskisuuren yrityksen johdolle. Tavoitteena oli, että koulutusmateriaalia voidaan hyödyntää yritysjohdon koulutuksen toteuttamisessa.

Ajantasaisen koulutusmateriaalin sisällön rakentamisessa ja suunnittelussa käytettiin hyväksi laaja-alaista dokumenttianalyysiä alan kirjallisuudesta ja tutkimuksista sekä kvantitatiivista että kvalitatiivista tutkimusotetta. Koulutusmateriaalin sisältöön koottiin johdolle keskeiset kyberturvallisuuden osa-alueet. Materiaali pilotoitiin useaan kertaan käyttäen hyväksi systeemiajattelua, haastatteluja ja erilaisia oppimismenetelmiä. Koulutusmateriaali on lähinnä tarkoitettu pienille ja keskisuurille yrityksille, mutta se soveltuu osin myös viranomaisille ja suuremmille yrityksille. Työssä toteutetun ajantasaisen koulutuksen avulla voidaan parantaa yrityksen kyberturvallisuuden johtamista, johdon kyberturvallisuustietoisuutta ja yrityksen kilpailukykyä sekä turvata maine ja tuotannon kannalta elintärkeä liiketoiminta.

Työn tarkoituksen osalta materiaalin sisältö vastaa erinomaisesti tarkoitustaan, mutta jatkossa materiaalin ulkoasu tulee tuotteistaa visuaalisemmaksi. Näin helpotetaan oppimisprosessia, sillä kyberturvallisuuden kokonaisuuden vaikutusten arviointi omalle yritykselle on haasteellista. Tavoitteen osalta tulokset ylittyivät, koska yritysjohdolta saadun palautteen perusteella asiakkaan huomioiminen esimerkiksi tietosuojan osalta lisäsi selkeästi asiakastyytyväisyyttä. Yrityksen kyberturvallisuuden ja tietosuojan parantamisella tietoturvallisuuden avulla on selkeä merkitys kilpailukyvyn edistämisessä. Kaikki tekeminen yrityksessä heijastuu nimittäin lopulta myös asiakkaaseen. Kyberturvallisuus tulee olla sisäänrakennettua eikä se saa maksaa asiakkaalle ylimääräistä.

Kyberturvallisuus on todella laaja aihealue ja sen laajuus muodostuikin työssä haasteeksi, kun tavoitteena oli välittää yritysjohdolle kokonaiskuva kyberturvallisuudesta. Keskeisiä osa-alueita jouduttiin siirtämään liitteisiin, koska niiden rajaaminen työn ulkopuolelle olisi jättänyt kokonaisuuden vajaaksi. Toiseksi haasteeksi muodostunee jatkossa materiaalin osittainen vanheneminen. Itse opinnäytetyön tekemistä helpotti merkittävästi ymmärryksen lisääntyminen erilaisista tutkimusmenetelmistä ja systeemiajattelun

sisäistäminen kyberturvallisuuden koulutuksessa, johtamisessa ja kokonaisuuden ymmärtämisessä.

Koulutuspilottien toteuttamisessa ja kehittämisessä onnistuttiin käyttämään hyvin ja tuloksellisesti systeemiajattelun periaatteita. Pilottien tuloksien ja analyysien perusteella palaute oli positiivista, mutta tulevissa koulutuksissa tulee keskittyä kyberturvallisuusohjeisiin ja -oppaisiin. Toteutuneista uhista tulee esitellä johdolle käytännönläheisiä esimerkkejä ja demonstroida vaikkapa kyberhyökkäys yrityksen päätelaitteeseen. Systeemiajattelussa yrityksissä luotetaan liian usein intuitioon eikä ajatusta uskalleta viedä systeemille kaksi. Tällöin ehkä pelätään riskejä, joita toiminnasta paljastuu. Valitaan siis helpomman ja nopeamman eli systeemin yksi tie, kun tulisi ajatella pidempään, harkitummin ja kokonaisvaltaisemmin – systeemiajattelua suosien. Systeemiajattelua kyberturvallisuudessa voidaan pitää opinnäytetyön uutena luovana aiheena, jota kannattaa tutkia vielä enemmän.

Työn aikana syntyi paljon yrityksille yleishyödyllistä kyberturvallisuuden koulutukseen, kartoittamiseen, kehittämiseen ja rakentamiseen liittyvää materiaalia ja dokumentteja, joita yritykset ja viranomaiset voivat käyttää suoraan oman toimintansa kehittämiseen. Materiaalista ja dokumenteista mainittakoon seuraavat:

- Johdon kyberturvallisuuden tietoisuuden lisääminen ja ohjeet kyberturvallisuuden systeemiajatteluun ja innovatiiviseen johtamiseen yrityksessä (luku 2 ja 3).
- Dokumenttianalyysin, pilottien, haastatteluiden ja kyselyiden avulla johdolle on suunniteltu ja toteutettu ajantasainen koulutusmateriaali.
- Laajaan yrityksen kyberturvallisuuden kartoitukseen sopiva liitesarja (liite 1) sekä ohjeet kyberturvallisuuden rakentamiseksi CIA:n 10 teesin avulla (liite 8).
- Systeemiajattelun avulla toteutettiin koulutuksen pilotoinnin kehittämisen malli sekä johdon haastattelurunko ja palautekyselykaavakkeet (liitteet 5, 6 ja 7).
- Ohjeet ja liitteet yrityksen kyberturvallisuusvision ja -strategian tekemiseen sekä kyberturvallisuuspolitiikan ja some-ohjeen kirjoittamiseen (liitteet 3, 4 ja 2).
- Vastaukset, mitä yritysjohdon tulisi tehdä kyberturvallisuuden, tietoturvan ja tietosuojan parantamiseksi ja rakentamiseksi yrityksessään (luku 2).
- Koulutusmateriaalin sisällön hyödyntäminen, joka on luvun 4 mukainen.

Yrityksen kyberturvallisuuden johtamisessa ja toteuttamisessa tulisi lähteä liikkeelle pienistä muutoksista. Tärkeintä on huolehtia yrityksen kriittisten tuotteiden ja palveluiden

sekä liiketoiminnan jatkuvuudesta erityisesti kyberhyökkäyksen tapahtuessa. Liiketoiminnan jatkuvuuden suunnittelu on erinomainen kyberturvallisuuden korjaava hallintamenetelmä, jos ja kun yritykseen kohdistuu mikä tahansa katastrofi tai haittaohjelmahyökkäys. Keskeistä on saada kybertuvallisuus yrityksen jokapäiväisiin prosesseihin ja johtamiseen. 100-prosenttista kyberturvallisuutta ei voida koskaan saavuttaa eikä yritys voi varautua kaikkiin mahdollisiin skenaarioihin tiedon häviämisestä tai katastrofeista. Suunnitelmissa on keskityttävä jatkuvuuden turvaamiseen. Tässä on huomioitava manuaalinen työ, joka sisältää harjoittelun. Henkilöstön käyttö pitää suunnitella siten, että oikeat asiantuntijat ovat oikeissa tehtävissä. Sähkön saanti on turvattava ja verkon ja palvelimien konfiguraatiot on dokumentoitava. Vaihtoehtoinen viestintäkanava on suunniteltava. Rikollisilla on motivaatio löytää aina uudet keinot rahan ansaitsemiseen, kun vanhat keinot vuotavat median välityksellä julkisuuteen.

Kyberturvallisuuskoulutuksen tulee olla kuulijoille osallistavaa, aiheen ajankohtainen ja tilaisuudessa tulisi mielellään pystyä laittamaan kuntoon jokin yritykselle kriittisen palvelun turvaamistoimenpide, esimerkiksi ohjeistuksen rungon kirjoittaminen. Strategian kannalta yritysjohdon on tärkeä linjata, mitkä toiminnot pidetään yrityksen sisällä ja mitkä ulkoistetaan. Päätöksiin tulee tietenkin paneutua huolellisesti. Internet ja kyberrikollisuus on tuonut paljon lisää uhkia, mutta kyberturvallisuuteen sisältyy myös mahdollisuuksia. Johdon tulee varautua, koska tieto on aina arvokasta. On lähettävä siitä oletuksesta, että tieto on uhattuna ja todennäköisesti jo vaarantunut.

Yrityksien tulee edelleen tiivistää yhteystyötä viranomaisten ja muiden yritysten kanssa, koska liittoutumalla kyberrikollisia vastaan pystymme turvaamaan elinkeinomme ja yhteiskunnalle kriittiset palvelut. Yksin omissa ”poteroissa” suojautuminen on hankalaa, jos tilannekuvaa kyberympäristön tilanteesta ei ole. Henkilöstön koulutus on ensiarvoisen tärkeässä asemassa, koska monen tutkimuksen mukaan yli 50-90 % kyberuhista tulee organisaation sisältä inhimillisistä virheistä. Koulutustapahtumia tulee järjestää säännöllisesti, koska ala muuttuu jatkuvasti ja rikolliset keksivät mitä innovatiivisempia keinoja varastaa yrityksen tiedot ja osaavat käyttää teknisiä keinoja sosiaalisessa hakkeroinnissa yhä taitavammin.

Kyberturvallisuuden merkitys yritysmaailmassa ei ole siis vähenemässä. Internetin ja älypuhelimien käyttö, palveluiden digitalisointi ja tiedon määrä vain kasvavat. Mobiilisovellusten käyttö älypuhelimissa ja ihmisten arjessa lisääntyy, mikä tuo tullessaan haasteita

kyberturvallisuudelle. Olemme joka hetki yhä enemmän riippuvaisia näistä palveluista ja sovelluksista. Jatkossa yritysten tulisi kustannukset ja yrityksen koko huomioiden pyrkiä käyttämään tekoälyn ja bigdatan tuomia mahdollisuuksia hyväkseen. Kyberturvallisuuden uhkat ja haavoittuvuudet ja niistä raportointi vain lisääntyy.

Tulevaisuudessa yrityksien on muistettava, että tekniikan avulla saadaan toki tietoturvariskejä pienennettyjä, mutta parhaimmatkaan palomuurisäännöt ja tietoturvallisuuskovennukset eivät estä käyttäjän tekemiä tahallisia tai tahattomia toimintatapoja tai virheitä. Kyberturvallisuutta rakennettaessa joudutaan miettimään myös kustannuksia. Kyberturvallisuus on kompromissi suojauksen kattavuudesta ja kustannuksista, joten koulutus on kustannustehokas ratkaisu.

Vaikka tekniset järjestelyt olisivat omasta mielestä täydellisiä, niin käyttäjän laiminlyönnit, piittaamattomuus ja huolimattomuus saattavat silti aiheuttaa katastrofin. Keskeisenä yhteenvetona voidaan myös todeta, että suurimmat syyt organisaation tietoturvallisuuspoikkeamiin ovat puuttuvat ja puutteelliset ohjeet, laiskuus, yleinen huolimattomuus ja monesti jopa välinpitämättömyys tietoturvallisuudesta. Lisäksi meillä ihmisillä on luontainen taipumus tehdä asiat helpommin. Usein hieman oikaisemme tai nopeutamme työntekoa. Kiire on siis myös yleinen syy laiminlyönteihin, mutta se voi olla myös tekosyy. Lukemalla opinnäytetyö voidaan yrityksen kyberturvallisuuskulttuuria parantaa merkittävästi, sillä jatkossakin turvallisuus on kiinni asenteistamme. Opinnäytetyöllä on pyritty parantamaan yrityksen kyberturvallisuuskulttuuria ja kiinnittämään huomio siihen, että jatkossakin turvallisuus on kiinni asenteista.

Kyberturvallisuuden asiantuntijoiden ja henkilöstön kouluttaminen uusina kohderyhminä on otettava tarkemman tutkimuksen alle. Koulutus tulee olla aina räätälöity kohderyhmän tarpeiden ja vaatimusten sekä yrityksen toimialan ominaispiirteiden mukaisesti. Tekniikan huima kehitys, yhteiskunnan lisääntynyt tietointensiivisyys (datan kasvu), ICT-alan ja toimintojen ulkoistaminen, tieto- ja viestintäjärjestelmien keskinäinen integraatio, avoimien verkkojen käyttö ja yhä suurempi riippuvuus sähköstä aiheuttavat yhteiskunnan kriittisille palveluille ja yrityksille todella suuret kyberturvallisuushaasteet. Näistä haasteista vain vahvimmat ja osaavimmat selviävät. Tulevaisuudessa kyberturvallisuusosaamisella ja tiedolla saavutetaan entistä enemmän valtaa.

LÄHTEET

AVG. 2018, AVTEST. The Indipendent IT-Security Institute. Luettu 5.5.2018. https://www.av-test.org/en/statistics/malware/

Cisco Networking Academyn Cybersecurity Essentials. 2012. Kyberturvallisuus erikoistumiskoulutus 2018. TK00CY85-3002 Johdatus kyberturvallisuuteen. Tampereen ammattikorkeakoulu. Tampere.

Elinkeinoelämän keskusliitto. 2018. Yritysturvallisuus. Mika Susi. Luettu 26.5.2018. https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

eMarketer. 2016, 12.12. Cybersecurity Isn't Just an IT Problem—It's Also a Marketing Problem. Luettu 19.1.2017. https://www.emarketer.com/Article/

Engeström, Y. 2004. Ekspansiivinen oppiminen ja yhteyskehittely työssä. Keuruu: Otavan Kirjapaino Oy.

ENISA eli European Union Agency for Network and Information Security, Suomeksi Euroopan unionin verkko- ja tietoturvavirasto, Viranomainen, joka perustettu 13.3.2014. ENISA Threat Landscape Report 2016 ja 2017. FINAL VERSION 1.0. January 2017. Luettu 3.3.2017. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 ja ENISA Threat Landscape Report 2017. julkaistu 15.1.2018

EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Euroopan unionin virallinen lehti 4.5.2016. Luettu 9.9.2017. http://eur-lex.europa.eu/

Eurobarometri-tutkimus (EB) 443 sähköisen viestinnän tietosuojasta. 2016. (SMART 2016/079). Ladattu ja luettu 15.4.2018. http://ec.europa.eu

European Comission. May 2017. Special Eurobarometer 460. Attitudes towards the impact of digitisation and automation on daily life. Luettu 4.3.2018. http://ec.europa.eu/public_opinion/

EU-tietosuojan kokonaisuudistus. 2016. VAHTI-raportti – 1/2016. Helsinki. Valtiovarainministeriö. Luettu 8.9.2017. https://www.vahtiohje.fi/web/guest/

Grönvall, M. & Lehtinen, R. Tampere University of Applied Sciences. Literacy Information and Computer Education Journal (LICEJ), Volume 7, Issue 4, December 2016. Luettu 1.2.2017.

Haapakangas, V. lehtori. 2018. Mitä on kyberturvallisuus. Luento 9.2.2018. Kyberturvallisuus erikoistumiskoulutus 2018. TK00CY85-3002 Johdatus kyberturvallisuuteen. Tampereen ammattikorkeakoulu. Tampere.

Haaja, J. YAMK -insinööri, kyberturvallisuusasiantuntija. Verkkopalveluiden ja palvelinten kyberturvallisuus. Luento 8.2.2018. Erikoistumiskoulutus, Kyberturvallisuus, TK00CY86-3002 Verkkopalvelujen ja palvelinten turvallisuus. Tampereen ammattikorkeakoulu. Tampere.

Harris, S., Fernando, M. 2016. CISSP All-in-One Exam Guide. Amazon EU.

Helenius, M. 2016. Koulutusyrityksen kilpailuedun kehittäminen palvelumuotoilulla. Yrittäjyys. Tampereen ammattikorkeakoulu. YAMK opinnäytetyö.

Helsingin seudun kauppakamari. 2015. Helsingissä 26.3.2015. Yrityksiin kohdistuvat kyberuhat 2015. Kyselyyn oli osallistunut 748 yritystä, joista 75% oli henkilömäärältään pieniä (alle 50 henkilöä) yrityksiä. Luettu 24.1.2018. https://helsinki.chamber.fi/

Helsingin seudun kauppakamari. 2016. Helsingissä. Tietoturvaopas yrityksille. luettu 4.2018. https://kauppakamari.fi/hankkeet/julkaisut/tietoturvaopas-yrityksille/

Helsingin seudun kauppakamari. 2016. Helsingissä 12.12.2016. Yrityksiin kohdistuvat kyberuhat. Luettu 24.1.2018. https://issuu.com/kauppakamari/docs/yrityksiin_kohdistuvat_kyberuhat_20

Henkilötietolaki 22.4.1999/523.

Hiltunen, E&K. 2014. Teknoelämää 2035. Helsinki: Talentum Oy.

Hirsjärvi, S. & Hurme H. 2006. Tutkimushaastattelu – Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hoxhunt. Ohjelmistoalan Startup -yritys. Blogi. www.hoxhunt.com

Hyppönen, M. tietoturvallisuusasiantuntija. 2017. Luento 2017. Tampereen ammattikorkeakoulu. Tampere.

Intel-tietoturvapuute sallii hyökkääjän ohittaa sisäänkirjautumistunnukset miljoonissa yrityskannettavissa. F-Secure. 12.1.2018. Luettu 13.1.2018. https://fi.press.f-secure.com/2018/01/12/

Juslèn, J. 2011. Nettimarkkinoinnin karttakirja. Tietosykli Oy: Esa Print 2011.

Juvonen, P. 2017. Näin luodaan osallistava koulutus tai muu oppihetki. Blogi. Luettu 6.6.2018 http://www.valmentures.fi/nain-luodaan-osallistava-oppihetki/

Jyväskylän yliopisto. ITKP0002 Johdatus kyberturvallisuuteen. 2016. Kyberturvallisuuskoulutus. Kuunneltu ja luettu 24.1.2018. https://peda.net/jyu/it/do/kkv

Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Puolustusministeriö. Katakrin uudistamistyötä koordinoinut ohjausryhmä 26.03.2015. Luettu 2.8.2016. https://www.defmin.fi/

Kahneman, D, 2012. Ajattelu nopeasti ja hitaasti. Alkuperäispainos. Thinking, Fast and Slow 2011. Terra Cognita Oy: Helsinki 2012.

Kekäläinen, O. Pelkkä HTTPS-varmenne ei riitä – se pitää myös olla oikein asennettu. 11.7.2016. Blogi. WP -palvelu.fi. Luettu 12.1.2017. https://wp-palvelu.fi/blogi/https-oikein-asennettu/

Keskuskauppakamari. Helsingin seudun kauppakamari yhteistyössä Huoltovarmuuskeskuksen ja Suomen kauppakamarien kanssa. Helsinki 2017. Yritysten rikosturvallisuus 2017 – Riskit ja niiden hallinta. luettu 5.2.2017. https://kauppakamari.fi/

Kilpinen, P. 2008. Liekeissä! − Miten johtaja inspiroi ihmiset syttymään muutokselle. Jyväskylä: Gummerus Kustannus Oy.

Krebsonsecurity. 18.2.2018. New EU Privacy Law May Weaken Security. Luettu 17.2.2018. https://krebsonsecurity.com/2018/02/

Kupias, P. 2001. Oppia opetusmenetelmistä. Helsinki: Educa-Instituutti Oy.

Kyberosaaminen Suomessa – Liiketoiminta-analyysi. Suomalaisten tietoturvayritysten osaaminen ja kilpailukyky eSociety-palvelujen alueella. Cybelab OY 25.11.2015, 4. Luettu 30.9.2017. http://www.kyberosaaminen.fi/materials/Cyberlab%20liiketoiminta_analyysi_final_251115.pdf

Kyberturvallisuuden kansallinen osaaminen. No. 20/2015. Martti Lehto, Aili Kähkönen, Informaatioteknologian tiedekunnan julkaisuja. Jyväskylän yliopistopaino: Jyväskylä 2015. Luettu 1.2.2017. https://jyx.jyu.fi/dspace/handle/123456789/53974

Kyberturvallisuuskeskus. 16.1.2018. Tietoturva nyt! Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. luettu 1.2.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801161310.html

Kyberturvallisuuskeskus. 30.8.2017. Tietoturva nyt! Kaksivaiheinen tunnistautuminen pelastaa paljolta - pelkkä salasana ei suojaa kaikilta uhkilta. luettu 3.2.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/08/ttn201708301327.html

Kyberturvallisuuskeskus. Julkaistu 12.10.2017. [Teema] "Ei koske meitä" -strategia ei toimi. Luettu 2.2.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/10/ttn201710121335.html

Kyberturvallisuuskeskus. 20.10.2017. [Teema] Kartoita ja leivo tietoturva osaksi yrityskulttuuria - apuna CIA ja 10 teesiä. luettu 2.2.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2017/10/ttn201710201246.html

Kyberturvallisuuskeskus. Päivitetty 18.12.2017. Tilannekuva. Luettu 23.1.2018. https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/tilannekuvajaverkostojohtaminen/tilannekuva.html

Kyberturvallisuuskeskus. Päivitetty 18.12.2017. Yhteistyöverkostot. Luettu 23.1.2017. https://www.viestintavirasto.fi/kyberturvallisuus/viestintavirastontietoturvapalvelut/tilannekuvajaverkostojohtaminen/yhteistyoverkostot.html

Kyberuhat ja niiden aiheuttajat. Jyväskylän yliopisto. https://peda.net/jyu/it/kyberturvallisuus/kkv/4kjna

Lappalainen, M. 2015. Miksi aivot sanovat ei. Opi uusi tapa ajatella. Juva: Bookwell Oy.

Lehto, M. professori. 2016. Kyberturvallisuuden tuottaminen. Luento 27.9.2018. https://peda.net/jyu/it/do/kkv/ajankohtaista. Jyväskylän yliopisto. Jyväskylä.

Lehto, M. professori. 2018. Kyberturvallisuus tänä päivänä. Luento 26.1.2018. Kyberturvallisuus erikoistumiskoulutus 2018. TK00CY85-3002 Johdatus kyberturvallisuuteen. Tampereen ammattikorkeakoulu. Tampere.

Lehto, M., Limnèll, J., Innola, E., Pöyhönen, J., Rusi, T., Salminen, M., Valtioneuvoston selvitys -ja tutkimustoiminta. Raportti julkaisu 30/2017. Kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Luettu 27.1.2018. http://tietokayttoon.fi/julkaisu?pubid=17805

Limnéll, J. & Rantapelkonen, J. 2017. Pelottaako? − Nuoret ja turvallisuuden tulevaisuus. Jyväskylä: Docendo Oy.

Limnéll, J. Kyberturvallisuus on entistä laajempi käsite. 14.9.2017. Kolumni. Luettu 30.09.2017. https://yle.fi/uutiset/3-9831451

Limnéll. J. Kyberturvallisuus osana tämä päivän turvallisuutta. Luento. 15.9.2016. ITKP0002 Johdatus kyberturvallisuuteen. Kuunneltu 24.1.2018. https://peda.net/jyu/it/do/kkv

Lindblom-Ylänne, S. & Nevgi, A. (toim.) 2003. Oppimisnäkemykset antavat perustan opetukselle. Teoksessa. S. Lindblom-Ylänne, S. & A. Nevgi (toim.) Yliopisto- ja korkeakouluopettajan käsikirja. Vantaa: WSOY.

Leino, M. 2012. Sosiaalinen netti. Kopijyvä Oy.

Motherboard. 2018. United States. Joseph Cox 14.2.2018. 'BuckHacker' Search Engine Lets You Easily Dig Through Exposed Amazon Servers. Luettu 17.2.2018. https://motherboard.vice.com/en_us/article/j5bgm3/buckhacke-amazon-server-search-engine-aws-security

National Institute of Standards and Technology, U.S Department of Commerce. Computer Security Training Guidelines. Mary Anne Todd and Constance Guitian. November 1989. Luettu 24.5.2018. https://csrc.nist.gov/publications/detail/sp/500-172/archive/1989-11-01

Netin pimeä puoli. "Dark Wep". 2018. Ohjaus: Tzachi Sciff ja Duki Dror. Tuotanto: Zygote films, Sub.doc. Esitetty Suomessa 28.1.2018 Sub. Tuottajan sivut: http://www.zygotefilm.com/our-films.html. Maksullinen ohjelma ladattavissa osoitteessa. https://vimeo.com/ondemand/downthedeepdarkweb

Ojasalo, K., Moilanen, T. Ritalahti, J. 2014. Kehittämistyön menetelmät – Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro Oy.

Oppimiskäsitykset. Jyväskylän Ammattikorkeakoulu. Luettu 7.6.2018. http://oppimateriaalit.jamk.fi/oppimiskasitykset

Peltomäki, J., Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Talentum Media Oy.
Rauste-von Wright, M. 1997. Opettaja tienhaarassa – Konstruktivisimia käytännössä. Jyväskylä: Atena.

Rautio, J. asiantuntija. Kybersää syyskuussa 2017. ”sähköpostiviesti”. SOTE CERT-FI-CIP-SOTE@LISTSERV.FICORA.FI. Kyberturvallisuuskeskus. Luettu 6.11.2017.

RSA. 2017 Consumer Cybersecurity Confidence Index. 2018. Luettu 29.1.2018. https://www.rsa.com

Ruckenstein, M., Suikkanen, J., Tamminen, S. 2011. Unohda innovointi – Keskity arvonluontiin. Helsinki: Edita Prima Oy. Luettu 2.7.2018. URL:http://www.sitra.fi

Sahlberg, P. & Leppilampi, A. 1994. Yksinään vai yhteisvoimin?: Yhdessä-oppimisen mahdollisuuksia etsimässä. Vantaa: Helsingin yliopisto.

Sava, I. 1993. Taiteellinen oppimisprosessi. Teoksessa I. Porna & P. Väyrynen. (toim.) Taiteen perusopetuksen käsikirja. : Suomen Kuntaliitto.

SecurityIntelligence. IBM. Douglas Bonderud 8.2.2018. The State of Internet Security: Rising Risk Despite Reputation and Regulation. Luettu 18.2.2018. https://securityintelligence.com/news

SecurityIntelligence. IBM. United States of America 2016. IBM X-Force Threat Intelligence Index 2016. Luettu 20.2.2018. https://www.slideshare.net/KanishkaRamyar/the-ibm-x-force-2016-cyber-security-intelligence-index

Suomen kyberturvallisuusstrategia. 2013. Valtioneuvoston periaatepäätös 24.1.2013. Turvallisuuskomitea. Helsinki: Puolustusministeriö. Luettu 20.1.2018. https://turvallisuuskomitea.fi/?s=kyberturvallisuusstrategia

Suomen perustuslaki 11.6.1999/731.

Talus A,. Autio E. & Hänninen A. & Pihamaa H. & Kantonen S. Oikeusministeriö & Tietosuojavaltuutetun toimisto. 2017. Helsinki. Oikeusministeriön julkaisu 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen? Luettu 12.1.2017. http://julkaisut.valtioneuvosto.fi/handle/10024/79316

Techfestival, KØDBYEN & COPENHAGEN, September 5-10.9.2017, ICT -Startup kurssin opintomatka Kööpenhaminaan. Cybersummits and Cyber Security and Information Warfare Summit, Thursday, Sep 7. Marisa Hinrichs.

The Guardian news. Wed 14 Oct 2015. Craig Scott. How to stop cyber-attacks on your organisation. luettu 7.4.2018. https://www.theguardian.com/public-leaders-network/

Tietohallintolaki 21.5.1999/621. https://www.finlex.fi/fi/laki/ajantasa/1999/

Tietosuojavaltuutetun toimisto. 2012. Laadi tietotilinpäätös. Helsinki. Tulostettu 1.7.2017. www.tietosuoja.fi

Tilastokeskus. 2018. Käsitteet. Luettu 20.9.2018. http://www.stat.fi/meta/kas/index.html

Torkkola, S. 2017. Lean – Asiantuntijatyön johtamisessa. Helsinki: Alma Talent.
Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi – Uudistettu laitos. Helsinki: Tammi.

Vaarat netissä. 2018. Toimittaja: Marko Hietikko. Tuottaja: Marcus Landgärds. Yle Teema & Fem. Esitetty 4.2.2018. https://areena.yle.fi/1-3797223

Vahti-teemaviikko. VM. 2.10-6.10.2017. Kuunneltu 1.2.2018. https://vm.fi/digitaalisen-turvallisuuden-teemaviikko

Valtiovarainministerin ohjeet tietoturvallisuudesta. 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta - Tietoaineistojen luokittelu. Luettu 30.1.2017. https://www.vahtiohje.fi/web/guest/tieto-ja-kyberturvallisuus-viikko-2016

Verho, T. 2014. Palvelujen muotoilua kehittäjille. Yrittäjyys. Tampereen ammattikorkeakoulu. YAMK opinnäytetyö.

Verkkouutiset. hakusanalla ”valeuutiset”. Vuoden 2018 tietoturvatrendeissä korostuvat valeuutiset ja valtion hakkerit. Ilkka Ahtokivi | 02.01.2018. Luettu 11.12.2017. https://www.verkkouutiset.fi/?s=valeuutiset.

Viestintävirasto. 11.1.2018. Kyberturvallisuuskeskuksen johtaja Jarkko Saarimäki. Ainutlaatuisella yhteistyöllä tehdään maailman parhaita tietoturvapalveluita. Luettu 1.2.2018. https://www.viestintavirasto.fi/viestintavirasto/blogit

Vilkka, H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Tampereen yliopisto. Luettu 20.9.2018. http://tampub.uta.fi/bitstream/handle/10024/98723/Tutki-ja-mittaa_2007.pdf?sequence=1

von Wright, M. & J. & Soini, T. 2003. Oppiminen ja koulutus. Juva: WS Bookwell Oy.

World Economic Forum. The Global Risks Report 2018 13th Edition. Luettu 25.1.2018. http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape

Yrittäjien haastattelut ja kyberturvallisuuskartoitukset. 2018. klo 1100-1330 5.2.2018 Pirkkala ja klo 1500-1710 12.2.2018 Narva (sisältää myös nuorison haastattelut 3 kpl).

LIITTEET

Liite 1. Kyberturvallisuuden itsearvioinnin kysymyssarja 1 (15)

Luottamuksellisen tiedon käsittely

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksen luottamukselliset tiedot tunnistettu ja luokiteltu?			
Tiedostaako henkilöstö vastuunsa luottamuksellisiksi määritellyistä tiedoista?			
Onko arkaluonteisimmat tiedot, kuten henkilötiedot suojattu tai salattu?			
Onko menettelytavoissa otettu huomioon henkilötietojen hallinnointi? (Korjaa ja avaa tarkemmin)			
Osaako henkilöstö tunnistaa ja suojata oikein luottamuksellisia ja muita tietoja?			
Onko arkaluonteisen luottamuksellisen tiedon käyttöoikeuksien haltijat luetteloitu?			
Erityiset henkilötiedot…niiden käsittely?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksen tietojärjestelmiin tehty haavoittuvuusskannausta tai penetraatiotestausta			
Onko yrityksessä tunnistettu uhkia, jotka voivat aiheuttaa häiriöitä keskeiseen liiketoimintaan, ja onko oletettujen häiriöiden vaikutukset arvioitu?			
Onko yrityksessä tehty toiminnan jatkuvuussuunnitelma, jota testataan ja päivitetään säännöllisesti?			
Suoritetaanko yrityksessä säännöllisesti kyberturvallisuuden tai tietoturvallisuuden riskiarviointeja, joiden perusteella suojaamistoimenpiteitä parannetaan ja kehitetään?			
Onko tietojen korruptoitumista tai tahallista väärinkäyttöä pyritty estämään yrityksen kaikissa toimintaprosesseissa?			
Onko yrityksessä tehty riskikartoitusta ja riskien arviointia?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksen johto budjetoinut varoja tieto- tai kyberturvallisuuteen			
Onko yrityksen johto budjetoinut varoja tieto- tai kyberturvallisuuden järjestelmähankintoihin?			
Onko yrityksen johto sitoutunut tieto-, tai kyberturvallisuuspolitiikan, ja tiedottaako se politiikasta asianmukaisesti henkilöstölle?			
Informoidaanko hallitusta ja johtoa säännöllisesti tietoturvaa koskevien toimintatapojen, standardien, käytäntöjen ja suositusten kehityksestä?			
Onko johtotasolla vähintään yksi henkilö, joka vastaa kyber-, tietoturvallisuudesta ja tietosuojasta			
Onko yrityksessä nimetty tietosuojavastaava tai muu yhteyshenkilö EU -tietosuoja-asetuksen linjausten mukaisesti			
Onko yrityksessä organisoitu kyber -tai tietoturvallisuushenkilöstöä?			

Onko yrityksellä riittävästi tieto- tai kyberturvallisuusosaamista? 4 (15)

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yritys nimennyt tietoturva-asiantuntijan tai -tiimin, joka koordinoi yrityksen omaa osaamista ja avustaa johtoa päätöksenteossa?			
Vastaako tietoturva-asiantuntija tai -tiimi tietoturvapolitiikan päivittämisestä merkittävien muutosten tai tietoturvallisuushäiriöiden perusteella?			
Onko nimetyllä tietoturva-asiantuntijalla tai -tiimillä mukana kaikissa yrityksen hankkeissa heti hankkeiden alusta lähtien ?			
Onko eri tyyppisten tietojen käsittely ja suojaus hajautettu eri vastuuhenkilöille			
Arvioiko joku ulkopuolinen riippumaton elin tai auditoija säännöllisesti tietoturvapolitiikan toteuttamiskelpoisuutta ja vaikuttavuutta sekä tietoturvatiimin tehokkuutta?			
Onko yrityksessä tehty hallinnollisia tai teknisiä toimenpiteitä estääkseen henkilöstöä tai muita sisäverkon käyttäjiä tekemästä kyberrikoksia?			

Miten yrityksessä käsitellään luottamuksellisiin tietoihin pääsevien kumppaneiden aiheuttamia tietoturvariskejä? 5 (15)

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Käytetäänkö alihankkijoiden ja kumppaneiden tunnistamiseen kuvallisia kulkukortteja?			
Onko yrityksellä toimintatapoja tai prosesseja alihankkijoiden ja kumppaneiden taustojen tarkistamiseksi?			
Estetäänkö alihankkijan tai kumppanin pääsy tiloihin ja tietojärjestelmiin automaattisesti, kun toimeksianto tai projekti päättyy?			
Tietävätkö kumppanit, kenelle ja miten yrityksessä tulee ensimmäiseksi ilmoittaa tietojen katoamisesta, varkaudesta tai haittaohjelmatapauksesta			
Onko kumppanien ja alihankkijoiden ohjelmistot ja järjestelmät tietoturvallisia ja päivitetty?			
Sisältyykö alihankkijoiden ja kumppanien kanssa solmittaviin sopimuksiin selvästi määriteltyjä tietoturvavaatimuksia tai käyttövaltuushallinnan ohjeistusta?			
Onko yrityksen tiloissa käytössä sähköinen kulunvalvonta, ja jaetaanko kumppaneille ja alihankkijoille kyseiset kulkutunnisteet?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Suoritetaanko yrityksessä säännöllisiä testejä ja pidetäänkö havaituista uhista ja haittaohjelmatapauksista (tietoturvallisuuspoikkeamat) kirjaa?			
Onko yrityksellä menettelyä, jolla arvioidaan henkilöstöstä johtuvia uhkia tietojärjestelmille, kuten epärehellisyys, sosiaalinen urkinta ja luottamuksen väärinkäyttö?			
Pyytääkö yritys tietoturvallisuuden tarkastusraportteja ulkoisilta palveluiden tuottajilta?			
Arvioidaanko tietoturvallisuustarkastusten yhteydessä erityyppisten tallennettujen tietojen hyödyllisyyttä?			
Tehdäänkö yrityksen päätelaitteisiin tietoturvallisuuden kovennuksia esim ohjelmistojen tai raudan osalta (BIOS -salasanojen määrittely, rekisteriasetukset, USB -porttien käytön rajoittaminen jne.)?			
Onko päätelaitteissa virus- ja haittaohjelmasovellukset sekä palomuuri?			
Onko yrityksessä päätelaitteiden ja verkkoliikenteen tietoturvallisuusosaajaa?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Kun uusia teknisiä järjestelmiä otetaan käyttöön, arvioidaanko niiden vaikutuksia yrityksen tietoturvallisuuteen?			
Onko yrityksellä suojaustoimia, joilla vähennetään uusien teknisten järjestelmien aiheuttamia riskejä?			
Onko uusien teknisten järjestelmien käyttöönotto dokumentoitu?			
Onko yrityksellä kumppanuussuhteita, jotka mahdollistavat yhteistyön ja kriittisen turvallisuustiedon vaihdon uusien teknisten ratkaisujen käyttöönoton yhteydessä?			
Onko yrityksessä ymmärretty, että tietoturvapolitiikka ei ole este teknisille mahdollisuuksille?			
Hallinnoidaanko yrityksessä uutta tekniikkaa tietoturvajärjestelmien kehitysmenetelmillä järjestelmien elinkaaren aikana?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Kyberturvallisuus tai tietoturvallisuuskoulutusta on annettu koko henkilöstölle viimeisen vuoden aikana?			
Opastetaanko työntekijöitä tarkkailemaan ja ilmoittamaan tietoturvaloukkauksista?			
Onko käyttäjiä ohjeistettu ilmoittamaan järjestelmien tai palvelujen turvallisuuteen liittyvistä heikkouksista tai uhista?			
Osaavatko työntekijät käsitellä luottamuksellisia henkilötietoja asianmukaisesti?			
Saavatko myös ulkopuoliset käyttäjät tarvittavaa tietoturvakoulutusta ja säännöllisiä tietoiskuja organisaation toiminta- ja menettelytavoista?			
Onko yrityksen johto saanut heille kohdennettua kyberturvallisuuskoulutusta viimeisen vuoden aikana?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksessä on annettu yleiset ohjeistukset vahvojen salasanojen käytöstä?			
Yrityksessä käytetään vahvoja ja pitkiä salasanoja ja ne ovat kaikki henkilökohtaisia. Niitä ei ole tallennettu helposti saataviin tiedostoihin. Niitä vaihdetaan säännöllisin väliajoin vähintään kerran vuodessa. Samoja ohjeita noudatetaan kaikissa päätelaitteissa (myös puhelimissa).			
Onko yrityksen järjestelmät suojattu hyvin tunkeutumiselta?			
Kaikkia henkilöstöä, myös kumppaneita, on neuvottu kirjautumaan ulos työpisteeltä poistuttaessa.			
Onko työntekijöitä ja johtajia neuvottu miten toimia sosiaalisen median urkintatapauksessa ja tunnistavatko he mahdollisen urkinnan?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko henkilöstölle suunnattu lehdistösuhteita ja sosiaalista mediaa koskevia viestintäohjeita?			
Onko yrityksessä kurinpitomenettely, jos joku rikkovat yrityksen viestintä- tai someohjeita?			
Seuraako joku yrityksessä sisäverkon liikennettä arvioidakseen yrityksen verkkomainetta ja siihen liittyviä riskejä?			
Onko yrityksessä toteutettu teknistä suodatusta siveettömän ja rikollisen verkkomateriaalin selailuun sekä lataamisen estämiseksi?			
Onko työntekijöitä ja johtajia neuvottu miten toimia sosiaalisen median urkintatapauksessa ja tunnistavatko he mahdollisen urkinnan?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Mitataanko, raportoidaanko ja seurataanko yrityksessä kyberturvallisuus- tai tietoturvallisuus asioita?			
Onko yrityksessä toteutettu tietotilinpäätös?			
Dokumentoidaanko yrityksessä tekniset häiriöt ja tietoturvatapahtumat ja pyritäänkö niiden ehkäisemään?			
Seurataanko yrityksen palvelimien ja verkkolaitteiden logeja?			
Varmistetaanko yrityksessä, että säännöksiä, lakeja ja määräyksiä noudatetaan esimerkiksi tietosuoja-asioissa (EU tietosuoja-asetus)?			
Onko yrityksellä työkaluja, joilla johto voi arvioida turvallisuusasennetta ja vähentää mahdollisia riskejä?			
Onko yrityksellä kyberturvallisuus- tai tietoturvasuunnitelma ja onko se jalkautettu koko henkilöstölle?			
Toimitetaanko seurantaraportteja ja häiriötietoja viranomaisille kuten kyberturvallisuuskeskukselle?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksen sähköisten palveluiden etäkäyttö ohjeistettu ja siihen liittyvät tekniset turvatoimet toteutettu? (Etätyössä käytetään VPN:ä ja kaksinkertaista tunnistautumista)			
Järjestelmät testataan ja tarkastetaan aina päivitysten jälkeen			
Voiko käyttäjät itse päivittää vanhat sovellukset?			
Onko päätelaitteiden sovellusten, käyttöjärjestelmien ja viruksentorjuntaohjelmien päivitykset automatisoitu?			
Osaavatko käyttäjät päivittää yritykseltä saamansa älykännykän (myös virustorjunnan)?			
Tarkistetaanko ja hallinnoidaanko yrityksessä käyttöoikeuksia säännöllisesti?			
Poistuuko työntekijän käyttöoikeudet tietojärjestelmiin ja pääsy tiloihin automaattisesti työsuhteen päättyessä?			
Onko turvaluokiteltuihin tiloihin sähköinen kulunvalvonta ja onko henkilöstölle annettu kulkutunnisteiden käytöstä ohjeistus?			

Miten asiakkaan tietosuojasta ja tietoturvallisuudesta yrityksessä huolehditaan? 13 (15)

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	KYLLÄ	EI	SILTÄ-VÄLILTÄ
Onko yrityksellä nettisivuillaan tietosuojapolitiikka (tietosuojaseloste), jossa ilmoitetaan, mitä asiakkaan tietoja kerätään?			
Onko yrityksessä nimetty tietosuojavastaava ja onko hänet koulutettu tehtäviinsä?			
Ylläpidetäänkö yrityksessä asiakasrekisteriä ja onko siitä tehty rekisteriseloste ja tietosuojaseloste?			
Onko yrityksen johto tietoinen tietosuoja-asetuksen vaatimuksista ja velvoitteista yritykselle?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Voiko omilla laitteilla käsitellä ja tallentaa yrityksen luottamuksellisia tietoja?			
Onko henkilöstö ohjeistettu käyttämään älykännykän suojakoodia ja vaihtamaan liittymän oletuksena oleva PIN-koodi sekä käyttämään kännykässä suojattua sähköpostia?			
Käytetäänkö mobiililaitteissa salausta tietojen luottamuksellisuuden ja eheyden turvaamiseksi?			
Onko omille ja yrityksen laitteille erilliset sisäverkot?			
Osaako henkilöstö tehdä yrityksen tiedostojen varmuus- ja arkistokopioita?			
Onko kriittiset tietojärjestelmät varmennettu akustolla (UPS -laitteet) sähkökatkoksien sattuessa?			
Onko yrityksessä tietojen menettämisen varalle tehty varautumis- ja toipumissuunnitelma?			
Onko varmuuskopiot useammassa fyysisessä paikassa (3 erillistä kopiota, joista yksi vuosiarkistokappale)?			

Alla olevat kysymykset ovat perustason kysymyksiä. Valkoisella pohjalla olevaan soluun voi tarkentaa vastaustaan	**KYLLÄ**	**EI**	**SILTÄ-VÄLILTÄ**
Onko yrityksessä varauduttu kyberturvallisuus- ja tietoturvallisuushäiriöihin?			
Onko yrityksellä toimintatapamenettely tai prosessi, miten toimitaan tietoturvatapahtumissa?			
Onko häiriöiden hallintaa varten tehty viestintäsuunnitelma?			

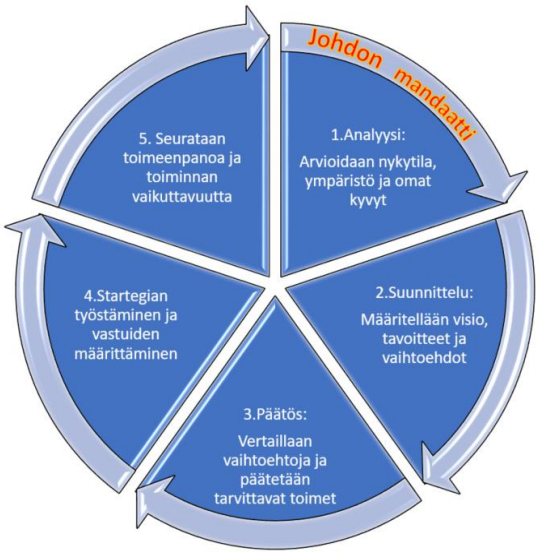
Liite 2. Yrityksen sosiaalisen median ohjeen sisältö

Sosiaalisen median ohje henkilöstölle voi sisältää mm:

- Tarkoitus on rohkaista kaikkia toimimaan sosiaalisessa mediassa.
- Monissa tehtävissä sosiaalisessa mediassa toimiminen kuuluu työn kuvaan, mutta kaikille se ei ole pakollista.
- Omaa työnantajaa ja työyhteisöä tulee kommentoida harkiten, koska ne saattavat parhaassa tai pahimmassa tapauksessa päätyä laajaan julkisuuteen.
- Keskeneräisistä hankkeista ja töistä kannattaa keskustella johdon kanssa, ennen niiden julkaisua.
- Henkilökohtaisella tasolla tulee noudattaa hyvän maun periaatteita.
- On selkeästi erotettava oma mielipide yrityksen mielipiteestä.
- Someen laitetut tiedot eivät saa vaarantaa kenenkään mainetta tai turvallisuutta, jos ne päätyvät lehden etusivulle (kyberteemapäivät).
- On otettava huomioon, että some on digiajan tori, joka on auki 24/7. (Leino 2012, 162–164.)
- On muistettava, että nettiväittelyitä ei voi voittaa sekä ICT-laitteen kautta lähetetyn viestin merkitys saattaa olla vastaanottajalle ihan toinen

Liite 3. Kyberturvallisuusstrategian kehittäminen yritykselle 1(2)

Kyberturvavallisuus strategian kehittäminen yrityksessä



Kyberturvallisuusstrategian jatkuvan kehittämisen malli (Suomen kyberturvallisuusstrategia 2013, 38–40).

Kyberturvallisuusstrategian toteuttaminen yritykselle on aivan yhtä keskeinen kuin liiketoimintasuunnitelman tekeminen. Strategia on tavallaan kuljettu polku yrityksen kyberturvallisuusvisioon. Polulla (toimeenpano-ohjelmalla) eli jatkuvalla prosessilla tulee olla tiettyjä pääkohtia tai tavoitteita. (Suomen kyberturvallisuusstrategia 2013, 38–39.)
Prosessi sisältää kuvan mukaisesti seuraavat vaiheet:

1. Analyysi, jossa saadaan perusteet jatkotyölle, arvioidaan nykytila, tunnistetaan uhkat, riskit, oma suorituskyky ja puutteet.
2. Suunnitteluvaiheessa määritellään kyberturvallisuuden visio, kyberturvallisuuskonsepti ja erilaiset vaihtoehdot (skenaariot) vision toteuttamiseksi. Otetaan suunnittelussa huomioon taloudelliset resurssit ja oma osaaminen.
3. Päätösvaiheessa vertaillaan eri vaihtoehtoja ja valitaan yritykselle sopivin tavoitetila, toimintakonsepti ja käytännön toimenpiteet tavoitteiden saavuttamiseksi. Lisäksi päätetään, mitkä ovat yrityksen kybersuorituskyvyt ja mitä toimenpiteitä tehdään niiden luomiseksi.

4. Tuottamisvaiheessa määritellään kyberturvallisuusstrategian rakenne ja se miten asiat esitetään ymmärrettävästi koko henkilöstölle ja asiakkaille. Vaiheessa määritellään myös konkreettiset tavoitteet ja vastuut. Strategiatekstin laadintaan saattaa liittyä useampia iteraatiokierroksia.

5. Toimeenpanovaiheessa strategia-asiakirja viedään käytäntöön eli toimenpide-esitykset jalkautetaan käytännön toimiksi yrityksen henkilöstölle. Toimeenpanon seuraamiseksi ja muutoksen johtamista varten luodaan kyberturvallisuuden kypsyyden mittaus- ja seurantajärjestelmä, joka voi olla esimerkiksi koulutus ja siihen liittyvän verkkotestin suorittaminen. (Suomen kyberturvallisuusstrategia 2013, 38–40.)

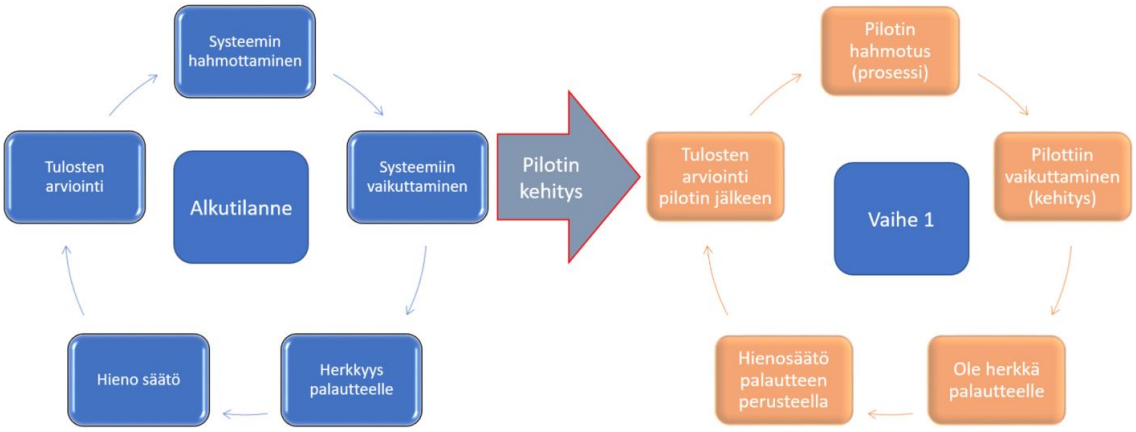
Liite 4. Yrityksen kyberturvallisuuspolitiikan sisältö

Kyberturvallisuuspolitiikan tulisi sisältää ainakin seuraavat tavoitteet ja pienellä yrityksellä se voi olla hyvinkin lyhyt ja ytimekäs:

- Annetaan keskeiset toimintaohjeet ja käyttäytymissäännöt käyttäjille ja järjestelmien ylläpitäjille.
- Määritellään tavoitteet, ohjeet ja vaatimukset yrityksen verkolle, tietojärjestelmille ja tietoturvallisuudelle
- Osoitetaan yrityksen sitoutuminen kokonaisturvallisuuteen.
- Varmistetaan yrityksen johdonmukaisuus ICT-järjestelmien toiminnassa, ohjelmistojen ja laitteistojen toiminnassa, käytössä ja hankinnoissa sekä ylläpidossa.
- Määritellään tietoturvallisuusrikkomuksien oikeudelliset seuraamukset.
- Annetaan turvallisuushenkilöstölle johdon tuki sekä henkilökunnalle ja johtajille tietoja organisaation vaatimuksista teknologialle ja tietojärjestelmien suojaamiselle. Kerrotaan, millä toimenpiteillä ja mekanismeilla yrityksessä saavutetaan turvallisuusvaatimukset.
- Määritellään tunnistus -ja todentamispolitiikka eli miten ja kenellä on pääsy yrityksen verkkoon ja järjestelmiin ja miten valtuutettujen käyttäjien identiteetti varmistetaan.
- Määritellään salasanakäytännöt, joilla varmistetaan vahvojen salasanojen käyttö ja säännöllinen vaihtaminen.
- Kuvataan organisaatiossa hyväksyttävät menettelytavat ja käytännöt, esimerkiksi organisaation hyväksyttävät verkon käyttötavat.
- Kuvataan yrityksen järjestelmien etäkäytön käytännöt, joilla määritellään turvallinen verkon käyttötapa.
- Määritellään yrityksen verkon ylläpitokäytännöt, verkkolaitteiden käyttöjärjestelmät ja loppukäyttäjien sovellusten päivitysmenettelyt. Vastuutetaan esimerkiksi käyttäjät huolehtimaan päätelaitteidensa ohjelmistopäivityksistä.
- Kuvataan haittaohjelmatapauksien (tietoturvatapahtumien) käsittelytapa ja prosessi.
- Kuvataan järjestelmien hyväksyttävät käyttötavat eli määritellään, mitä saa ja mitä ei saa tehdä, jotta väärinymmärrystä ei tapahdu. Esimerkkinä mm. kielletyt ja laittomat verkkosivustot tai sovellukset, jotka kuluttavat yrityksen tuotantoverkon kaistaa ja aiheuttavat järjestelmän epävakautta.

Liite 5. Koulutukseen liittyvät pilotit ja niiden kehittäminen 1 (6)

Opinnäytetyön piloteissa käytettiin systeemiajattelua, missä korostuu jatkuva mittaaminen ja kokonaisuuden ymmärtäminen unohtamatta kirjoittajan tai valmentajan mahdollisia tunnelukkoja. Tarkoitus on viedä systeemiajattelu kyberturvallisuusopetustapahtuman kehittämiseen kaavion mukaisesti käsittelemällä samanaikaisesti kirjoittajan tietoisuutta itsestään, itsensä johtamista, sosiaalista tietoisuutta ja suhteiden johtamista.



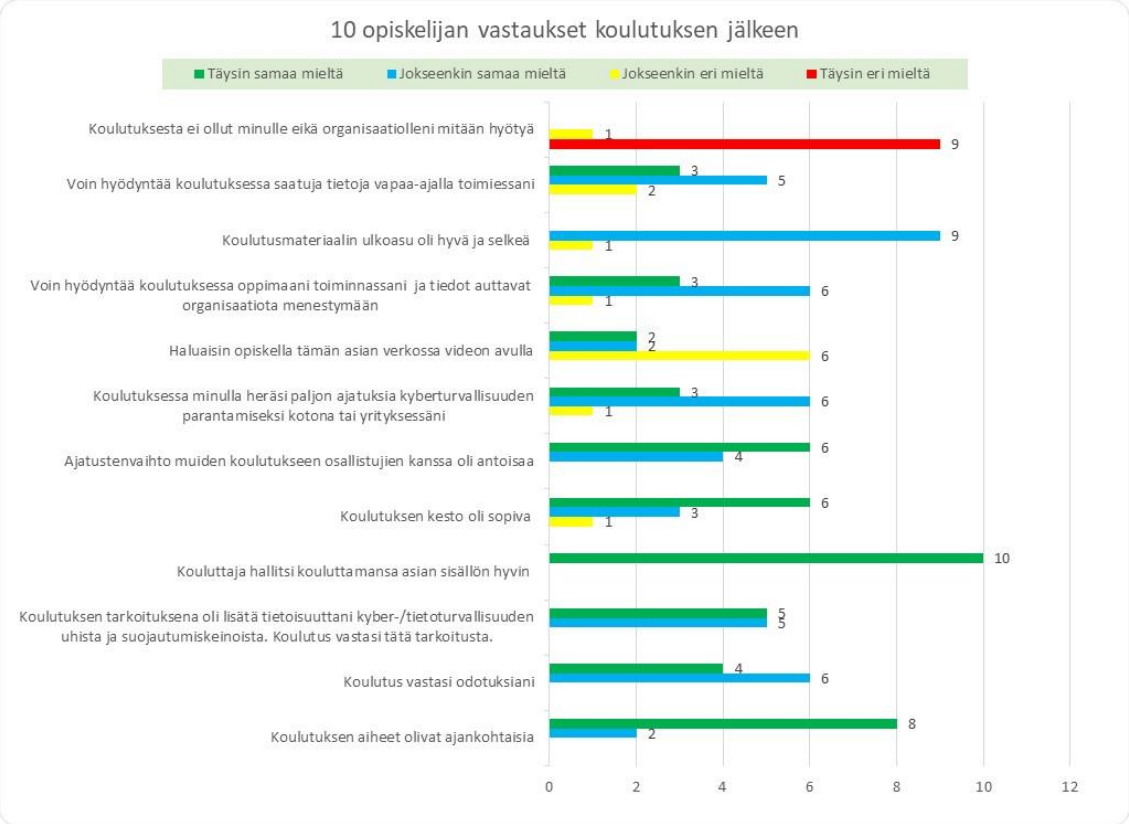
Pilotin hahmottamisen ja sen kehittämisen osalta toiminta pitää tarkastella aina uudestaan. Piloteissa tarvitaan erilaisia kuulijaryhmiä esimerkiksi viranomaisista ja yrityksistä (yleensä johtohenkilöstöä). Haastattelut, ryhmätyöt ja aivoriihet on purettava.

Palautteessa valmennettavia tulee kuunnella ”herkällä korvalla” ja antaa mahdollisuus kommentointiin. Palautteen kirjallinen osuus ei riitä, vaan se tulee kysyä myös kasvotusten, jolloin saadaan yleensä todellinen palaute. Palautekeskustelu asiakkaan kanssa voidaan toteuttaa lounaan tai kahvin yhteydessä, jolloin siitä tulee huomattavasti luontevampi ja avoimempi. Tulokset tulee dokumentoida myöhempää käyttöä varten.

1. pilotti toteutettiin 29.9.2017 klo 1700-1830 ICT-startup -yrittäjien haastattelulla ja työpajalla. Haastattelu keskittyi materiaalin sisältöön ja ulkoasuun (Proakatemia, Tampere, 8 Startup -kurssin oppilasta). Tilaisuuden palaute kysyttiin suullisesti. Haastattelu oli avoin ryhmähaastattelu, jossa pyrittiin havainnoimaan kuulijoiden kommentit mahdollisimman tarkasti:

- Tarkastettava esityksen fontit yhtenäisiksi ja tekstin oltava riittävän isoa. Ei liian paljon tekstiä yhdelle sivulle.
- Tee esimerkiksi mind-map sisällysluettelosta, josta on linkit aihealueen eri sivuille. Kuulijalle tulee saada myös näkymä, missä kohdassa esitystä ollaan menossa.
- Jaa paljon tekstiä vaativat asiat useammalle dialle.
- Uusi diojen visuaalinen ilme!
- Kyberturvallisuuden määritelmästä ja muistakin tulee saada yksi kuva ja yksi dia.
- Mieti tarkoin kohdeyleisö, koska kaikille tekniset termit eivät ole selvillä.
- Viitteet kuviin ja teksteihin tulee olla myös esityksessä.
- esityksessä tulee olla niin sanottuja ”herätesivuja” välillä.
- Keskity keräämään paljon vertailevaa taustatietoa eri lähteistä.
- Dioihin ei saa laittaa vinottain tekstejä.
- Hillityt tehosteet ovat parempia kuin kohtuuttomat ja yliampuvat tehosteet.
- Kyberturvallisuuden määritelmää voi hakea kognitiivisestä kerroksesta!

2. koulutuspilotti toteutettiin 13.3.2018 viranomaisorganisaation alijohtajille, jossa kuulijoina 10 keskijohdon edustajaa ja tilaisuuden järjestäjä. Ilman systemaattista ajattelua palautteen kysyminen ja korjaustoimenpiteet olisivat jääneet melko vähäisiksi. Palautekyselyn ja haastattelujen perusteella saatiin seuraavat kehitysehdotukset: Korjattavia asioita ovat mm palautelomakkeen ja materiaalin muokkaaminen palautteen mukaisesti (periaate: 3 min/dia, aikataulujen hienosäätö, jälkipalautteen pyytäminen järjestäjältä, suullisen palautteen kysyminen ja palautteen dokumentointi sekä analyysi.)



Koulutus pidettiin noin 1,5 tunnin luentona. Kahvitauon jälkeen pidettiin aivoriihi, jossa kuulijat ideoivat täysin uudenlaisia suojautumiskeinoja. Lopuksi jokainen ryhmä esitteli tuotoksista 3 parasta ideaa, joista keskusteltiin yhdessä. Palaute oli pääosin positiivista. Osallistujista kahdeksan olivat 30-45 vuotiaita ja siihen liittyen vähäinen halukkuus aiheen opiskelemiseen videon avulla oli pienehkö yllätys. Kuulijat haluavat selvästi opetukseen enemmän interaktiivisuutta ja vuorovaikutusta. Palautteen antoivat kaikki kuulijat, joista kaksi olivat naisia ja loput miehiä. Yhdeksälle koulutus oli suunniteltu tehtävään liittyvänä tilaisuutena, mikä kertoo siitä, että organisaatiossa huolehditaan

osaamisesta kyberturvallisuusalalla. Kyberturvallisuus nähdään siis johdon kannalta keskeisenä alana. Toisaalta viimeisen vuoden aikana peräti kuudella ei ollut lainkaan kyberturvallisuusalan koulutusta ja kolmella yksi tai kaksi koulutustilaisuutta. Koulutustilaisuudelle annettu keskiarvo oli 8,1. Asiasisältö oli hyvää ja aihe avautui kuulijoille. Kolme kuulijoista halusi kuulla enemmän käytännön esimerkkejä esimerkiksi toteutuneista uhista, mikä kertoo, että ainakaan ei haluta tehdä samoja virheitä kuin muut. Yli puolen kuulijoista (6) oli joutunut kyberhyökkäyksen kohteeksi vapaa-ajallaan. Tapaukset olivat liittyneet viruksiin, kalasteluviesteihin ja roskapostiin. Kuulijoista kolme näkee jatkuvan kouluttautumisen ja ohjeistamisen keskeisenä, koska ala muuttuu niin nopeasti. Selkeähkö kehittämisen kohde on aiheen laaja-alaisuudesta johtuen esitettävän diamäärän supistaminen, jotta myös luentovaiheessa aiheisiin olisi aikaa syventyä paremmin. Tilaisuudessa yhdelle dialle oli varattu aikaa reilu minuutti, kun pitäisi pyrkiä noin 3 minuuttiin. Kuulijoista kolme toivoi koulutukselle enemmän aikaa tai vähemmän dioja, mutta toisaalta osa myös piti aiheeseen nähden diamäärää tehokkaana. Palautekeskustelusta oli pääteltävissä, että aivoriihi uhkien suojautumiskeinoista koettiin hyödylliseksi, koska jokainen pääsi osallistumaan aktiivisesti. Suojautumiskeinoista keskustellessa koettiin keskeiseksi ongelmaksi organisaation puuttuvat ja puutteelliset ohjeet. Tästä aiheutuu turhia kyberturvallisuusriskejä ja käyttäjien ”oikomista” eli tavallaan turvallinen toimintatapa koetaan estävän ja haittaavan työn suorittamista. Jos ohjetta ei löydy riittävän nopeasti tai se on puutteellinen, ryhdytään oikomaan.

Aivoriihessä esitettyjä innovatiivisia suojautumiskeinoja olivat: 1) Osa oli kiinnostunut videon hyödyntämisessä koulutuksessa. 2) Työasemissa, järjestelmissä ja ohjelmistoissa tulisi olla niiden käyttöön liittyviä interaktiivisia kyberturvallisuusaiheisia muistutuksia. 3) Hyödyllinen ohjeistus tulisi automatisoida työn vaiheisiin liittyen, jolloin erillisten ohjeiden tarve vähenisi. 4) Kannustettiin myös avoimempaan kyberturvallisuuskulttuuriin pelottelun sijasta. Virheistä ei tulisi rankaista vaan, jos työntekijä löytää vääriä menettelytapoja tai virheitä, niistä palkitaan. 5) Myös sisäinen tiedottaminen koettiin keskeiseksi kehittämisen kohteeksi. 6) Koulutuksen merkitystä ei tule unohtaa. 7) Vara- ja vaihtoehtoisten menetelmien käyttöönotto ja harjoittelu nähtiin keskeisenä keinona. Varautumis- ja toipumissuunnitelmat ovat tässä keskeisessä asemassa. 8) Osaavan henkilöstön rekrytoinnissa ryhmät näkivät, että verkostoituminen yrityksiin, viranomaisiin, yliopistoihin ja ammattikorkeakouluihin on keskeisessä asemassa.

9) Ohjeistukset, järjestelmien ja laitteiden oikeat käyttötavat on saatava ajan tasalle. Lisäksi ohjeet on oltava riittävän yksinkertaisia. 10) Organisaatiossa voidaan suojautua hyökkäyksiltä poikkeamalla rutiineista ja helposti pääseville kohteille voidaan ladata myös disinformaatiota. 11) Monesti tietoturvalliset järjestelyt säädellään liioitelluiksi, jolloin ne vaikeuttavat omaa toimintaa eli ”ammutaan omaan jalkaan” liian ehdottomilla ohjeistuksilla. 12) Liikenteen solmukohtien suojaaminen on tärkeää. 13) Yleensä kansalaisten tietoisuuden lisääminen kyberturvallisuudesta ja somesta olisi suotavaa.

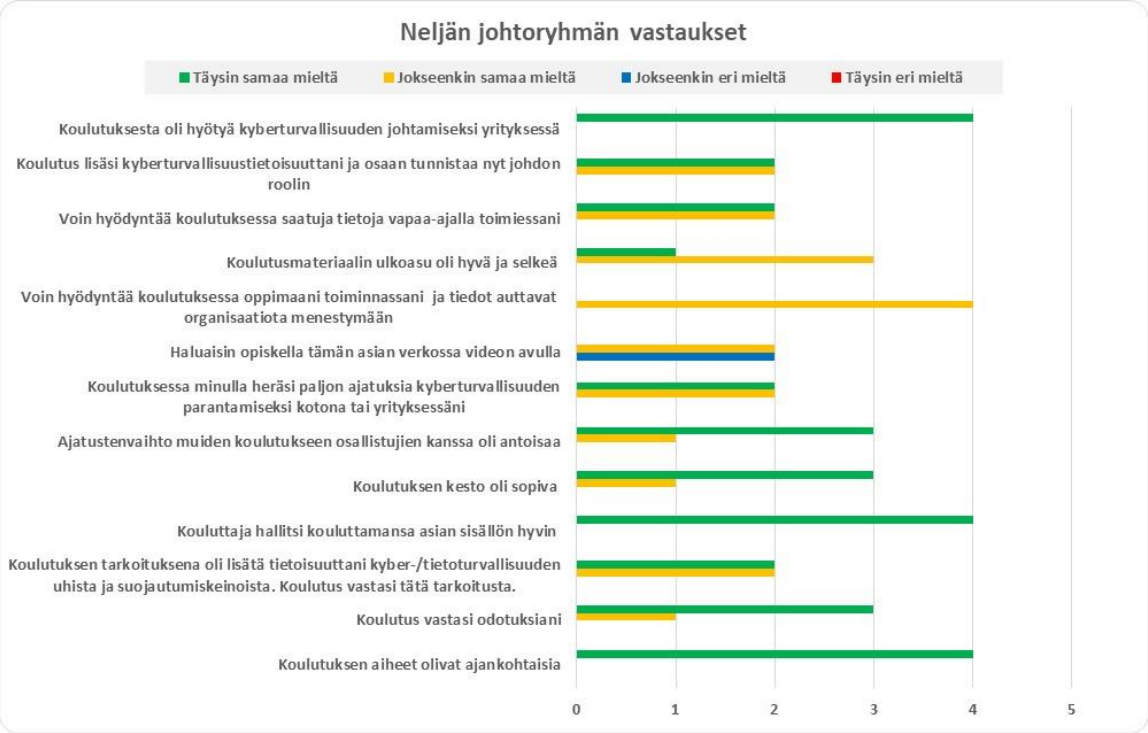
Koulutusta ja pilotteja suunniteltaessa ja toteutettaessa on huomioitava valmentajan omat mahdolliset tunnelukot eli ulkokehän kehitettävät henkilökohtaiset ominaispiirteet. Esimerkkinä voidaan mainita täydellisyyden tavoittelu, joka saattaa viedä valmentajan kaiken energian ja luovuuden. Pilotin kehittäminen tulee siis tehdä aina palautteeseen perustuen. Kaikkia kuulijoita ei myöskään aina pystytä miellyttämään, koska kuulijoiden lähtötietotasossa saattaa olla isojakin eroja.

3. pilotti toteutettiin kahden tunnin luentona yrityksen johdolle 24.8 Tampereen keskustassa. Johtoryhmässä oli neljä jäsentä ja suunniteltu luentoaika venyi kahdesta tunnista 2,5 tuntiin, koska tilaisuudesta muodostui todella vuorovaikutuksellinen ja kuulijoiden osallistaminen onnistui alussa annetun tehtävänannon johdosta. Kuulijat saivat merkata liimalapuilla oman osaamisensa ja tietämyksensä tason janoille, joiden toisessa päässä käsite oli tuttu ja toisessa päässä tuntematon. Termit janoilla olivat kyberturvallisuus, tietoturvallisuus ja tietosuoja. Näin myös valmentaja sai kuulijoista yhdellä silmäyksellä osaamisen tason, mikä helpotti esitettävien aiheiden kertomista ja painotusta. Idea osallistuvaan koulutustapahtumaan tuli Valmenturesin nettisivuilta (Juvonen 2017).

Kuten seuraavasta kaaviosta nähdään, palautteen monivalintakysymysten vastukset olivat positiivisia. Koulutus nähtiin erittäin hyödyllisenä yritykselle. Ajatustenvaihto ja vuorovaikutus muodostui todella aktiiviseksi. Aiheet koettiin ajankohtaiseksi ja koulutuksen kesto koettiin sopivaksi. Lisäksi kouluttaja hallitsi oppijoiden mielestä asiasisällön hyvin ja koulutus vastasi hyvin odotuksia. Vahvistui myös aikaisempi käsitys, että monesti nuoremmat voisivat opiskella aiheen videolta, kun vanhemmat ovat eri mieltä.

6(6)

Vuorovaikutus koetaan koulutuksessa tärkeäksi. Koulutustilaisuudelle annettu keskiarvo oli 8,75



Pilottien kehittämisen osalta kiinnitettiin erityisesti huomiota koulutuksen tuomaan hyötyyn organisaatiolle. Kaikki vastaajat olivat jokseenkin samaa mieltä eli melko tyytyväisiä. Valmentajan tulee kehittää koulutuksen sisältöä siten, että koulutuksesta saadut tiedot auttavat organisaatiota menestymään. Johdon vastaukset tulee saada tasolle, jossa he ovat täysin samaa mieltä! Samainen aihe selvisi myös avoimien kysymysten vastauksissa, joista esimerkkinä oli johdon tarve kehittää koulutuksen sisältöä enemmän omaan toimialaan ja tarve saada vielä enemmän konkreettisia toimintaohjeita sekä käytännön esimerkkejä todellisista tapauksista. Konkreettiset esimerkit lienee parasta esittää kyberhyökkäystä demonstroiden. Myös kyberturvallisuuden kokonaisuuden hahmottaminen ja ymmärtäminen koettiin oppijoiden keskuudessa haasteelliseksi, jonka ratkaisemiseksi systeemiajattelu on erinomainen työkalu.

Liite 6. Yritysjohtajien puolistrukturoitu haastattelurunko 1 (3)

Muistiorunko yrityksen johtohenkilöiden tapaamisesta ja heille esitettävistä kysymyksistä (Puolistrukturoitu kysymyslomake):

Taustaa yrityksestä (Yritysten nimiä ei kerrota opinnäytetyössä):

- johto 3-5 henkilöä
- henkilöstö alle 15

”Kyberturvallisuus ja tietoturvallisuus kartoitus” eli ensimmäiset havainnot mitkä haastattelija mainitsi (=Uhkien esille tuonti):

- Firman sivut toteutettava https:lle ja sähköpostien salaus asetusten avulla. Käyttäjän ja palvelimien välinen liikenne salataan.
- EU tietosuoja-kartoitus ja excel-kartoitustiedoston läpikäynti karkealla tasolla:
    - Onko asiakasrekisteriä? Esimerkiksi missä, kenellä siihen on pääsy, onko varmuuskopiot kunnossa ja toteutettu, onko testattu?
        - →**Dokumentoinnilla** on jatkossa pystyttävä todistamaan tietosuojavalvojalle (viranomaiselle)
    - Pyydettiin asiakasta tutustumaan alustavaan artikkeliin aiheesta: https://www.firsthatch.fi/kyberturvallisuus/eun-tietosuoja-asetus-yrityk-selle-mahdollisuus-lisata-kilpailukykya-ja-luotettavuutta/
    - Tehtävä nettisivuille tietosuojaseloste asiakkaita varten ellei ole jo tehtynä. Katso esimerkki. Asia tarkentuu tulevassa kyberturvallisuuskoulutuksessa.
    - Miten säilytetään asiakasrekisteriä?
        - Miten listat lähetetään internetissä? Salataanko sähköpostit. Annetaan ohjeet ilmaisista salausmenetelmistä, jotka kuitenkin luotettavia (esim PGP)
    - Tarvitseeko nimetä tietosuojavastaava yritykseen?
- Tietokoneet
    - USB -muistitikut (suositellaan PIN-koodillisia tikkuja)→
    - Asiakkaan dokumenttien/suunnitelmien säilyttäminen: kovalevyt, pilvessä, →varmuuskopiot
    - Onko tietokoneet ja mobiililaitteet kovennettu raudan ja softan osalta. (bios -salasanat, vahvat salasanat jne.)
    - Onko yrityksellä käytössä keskeinen tai kriittinen asiakasohjelmisto? Kenellä on siihen pääsy, salasanat ja onko siihen kahdennettua tunnistautumista?
    - Onko päätelaitteilla virus ja haittaohjelmasovellukset sekä onko käyttöjärjestelmät päivitetty sekä mitkä versiot käytössä?
    - Onko lisenssien hallinta toteutettu ja ohjelmistopäivitykset toteutettu?
    - Onko kaikista ICT-laitteista tilannetieto?
- Tietoliikenne:
    - Onko käytössä VPN
    - Onko WiFi:n asetukset kovennettu

    - Onko ICT -alan palveluntarjoajien kanssa tehty palvelusopimukset esimerkiksi vasteajoista ja palvelun laadusta tai käyttövaltuushallinnosta?
- Onko yrityksessä tehty ”penetraatiotestausta”? Jos ei, niin tehdään myöhemmin vuoden 2018 lopussa tai vuoden 2019 alussa
- Koska yrityksessä on annettu tietoturvallisuuskoulutusta → Koulutus pidetään vuoden 2018 aikana
    - Videokoulutuspaketti henkilöstölle? Onko tarpeellista?
- Miten olette toteuttaneet kulunvalvonnan?
- Onko riskien kartoitus tehty ja määritelty tärkeimmät suojattavat varat?

Laajempi kartoitus tehdään asiakkaalle sopivana ajankohtana, joka sisältää mm:

- EU:n tietosuoja-asetuksen vaatimukset (GDPR -itsearviointityökalu luonnosversion tai uudemman excel-taulukon täyttäminen→ Dokumentti koko tarkastuksesta)
    - Vai onko joskus tehty tietosuojan ja tietoturvan ”tee se itse tarkastus”
- Fyysinen turvallisuus
- Tekninen turvallisuus
- Pääsynhallinta, Käyttövaltuushallinta
- Sovellusten tietoturvallisuus
- Liiketoiminnan jatkuvuuden suunnittelu ja toipumissuunnittelun olemassaolo
- Tietoturvajohtaminen ja riskienhallinta
- Käyttöturvallisuus
- Tietoliikenne- ja verkkoturvallisuus
- Internet-turvallisuus

Keskustelu asiakkaan kanssa kyberturvallisuuteen ja tietoturvallisuuteen liittyen.

Opinnäytetyöhön ja kyberturvallisuuteen liittyen kysyttiin seuraavaa:

- Tuntemuksista?
    - Miten tietoturva koulutus tulisi teillä järjestää?
    - Onko tietoturvasta hyötyä yritykselle?
    - Valvottaako vai epäilyttääkö yrityksen tietoturvallisuusasiat?
- Näkemyksistä?
    - Miten teillä menee ihan muuten?
    - Mitä näet ympärilläsi? Miten teillä turvallisuusasiat yleensä hoidettu? kerro jotain esimerkkejä.
    - Onko teillä aiheeseen liittyviä vakuutuksia, sopimuksia (ICT-ala yleensä)
- Käytöksestä,
    - Pyritkö toimimaan tietoturvallisesti tai ajatteletko asiaa, kun työskentelet?
    - Millainen asenne sinulla on tietoturvallisuuteen tai somen käyttöön jne.
    - Mitä/miten kerrot asenteestasi muille?
- Ongelmista:
    - Onko ollut haittaohjelmatapauksia? Ja miten niistä selvittiin?

- Mitä mieltä olet videokoulutuksesta henkilöstölle ja siihen liittyvästä testistä
    - Etuna se että voidaan tehdä koska tahansa
    - Jää dokumentti koulutuksen toteuttamisesta
- Kuinka ympäristö, media ystäväsi vaikuttaa sinuun tietoturvallisuusasioissa
    - Seuraatko mediaa tietoturvan osalta?
    - Etsitkö medialta ohjeita?
    - Miten media vaikuttaa mielipiteisiin?
    - Kuka muu vaikuttaa mielipiteisiin?
- Mitkä asiat estää toimimasta tietoturvallisesti?
    - Ongelmakohdat (esimerkiksi aika, kiire)?
    - Muuta?
- Millaisia riskejä vältät?

Liite 7. Pilottien palautekyselylomake 1 (2)

PALAUTELOMAKE KYBERTURVALLISUUS KOULUTUKSESTA

1. **Koulutus johon osallistuit**: Kyberturvallisuuskoulutustilaisuus

2. **Sukupuoli**

   ☐ Nainen ☐ Mies

3. **Ikäni**

   ☐ 18–29 vuotta ☐ 30–45 vuotta

   ☐ 46–62 vuotta ☐ Yli 63 vuotta

4. **Mistä sait tietää koulutuksesta?**

   ☐ Työkaverilta

   ☐ Sähköpostitse

   ☐ Esimieheltä

   ☐ Suunniteltu koulutus tehtäviin liittyen

   ☐ Jostain muualta, mistä? _____

5. **Aikaisemmat kyberturvallisuusalan koulutukseni viimeisen vuoden aikana ☐ Ei ☐ 1-2kert ☐ 3 kertaa tai useammin**

6. **Arvioi seuraavia koulutukseen liittyviä väittämiä asteikolla 1-4. (rasti ruutuun)**

	1=Täysin eri mieltä	2=Jokseenkin eri mieltä	3=Jokseenkin samaa mieltä	4=Täysin samaa mieltä	kom-mentti
Koulutuksen aiheet olivat ajankohtaisia					
Koulutus vastasi odotuksiani					
Koulutuksen tarkoituksena oli lisätä tietoisuuttani kyber-/tietoturvallisuuden uhista ja suojautumiskeinoista. Koulutus vastasi tätä tarkoitusta.					
Kouluttaja hallitsi kouluttamansa asian sisällön hyvin					
Koulutuksen kesto oli sopiva					
Ajatustenvaihto muiden koulutukseen osallistujien kanssa oli antoisaa					
Koulutuksessa minulla heräsi paljon ajatuksia kyberturvallisuuden parantamiseksi kotona tai työssäni					
Haluaisin opiskella aiheen verkossa videon avulla					
Voin hyödyntää koulutuksessa oppimaani toiminnassani ja tiedot auttavat organisaatiota menestymään					
Koulutusmateriaalin ulkoasu oli hyvä ja selkeä					
Voin hyödyntää koulutuksessa saatuja tietoja vapaa-ajalla toimiessani					
Koulutuksesta **ei ollut** minulle eikä organisaatiolleni mitään hyötyä					

Yksityisenä henkilönä tai yrityksen edustajana olisin jopa halukas maksamaan kyseisestä koulutuksesta					

7. **Mitä mieltä olet koulutuksen sisällöstä?**

_____
_____
_____
_____

8. **Miten kehittäisit koulutusta?**

_____
_____
_____
_____

9. **Mitä ajatuksia koulutus herätti? Selvisikö organisaatiossasi selkeitä kyberturvallisuuspuutteita? Ja olivatko ne teknisiä vai koulutuksellisia puutteita?**

_____
_____
_____
_____
_____
_____

10. **Oletko joutunut koskaan kyberhyökkäyksen, viruksen, haittaohjelman, kalasteluviestin, kiristyshaittaohjelman tai muun vastaavan uhriksi ja milloin? Miten tilanteessa toimit ja toimitko mielestäsi oikein?**

_____
_____
_____
_____
_____
_____
_____
_____
_____

11. **Minkä kouluarvosanan antaisit koulutukselle (4-10)?** _____

KIITOS PALAUTTEESTA!

Luottamuksellisuus (**C**onfidentiality), joka tarkoittaa, että tietoa näkevät ja käsittelevät vain ne henkilöt, joilla on siihen oikeus. Tällöin kaikissa tietoa käsittelevissä järjestelmissä käyttöoikeudet ovat tarkoituksenmukaiset henkilön tehtäviin nähden. Se, että tieto lähetetään verkossa luottamuksellisesti, on yksi kyberturvallisuuden tärkein tavoite.
Eheys (**I**ntegrity) eli tieto ei saa tuhoutua tai muuttua vahingon tai kyberhyökkäyksen vuoksi. Varmuuskopiot ovat keskeinen tiedon eheyden turvaamiskeino. Tiedosta täytyy saada myös selville sen muutoshistoria koko elinkaaren ajalta. Eheyden tarkistamiseksi voidaan käyttää teknisesti esim. tarkistussummia. Joissakin yrityksissä tiedon eheyteen pitää kiinnittää erityistä huomiota ajatellen vaikkapa finanssi- tai terveydenhuoltoalaa. Tiedon käsittely jokaisessa vaiheessa aiheuttaa myös mahdollisen riskin eheydelle.
Saatavuus (**A**vailability) eli tieto on oltava saatavilla silloin, kun sitä tarvitaan. Usein kriittisten tietoliikenneyhteyksien ja tietojärjestelmien kahdentaminen sekä ohjelmistojen päivitys (ajan tasalla pitäminen) nähdään tiedon saatavuuden varmistuskeinoina. Monesti haittaohjelman iskiessä kriittiseen järjestelmään yritykseltä puuttuu palautumissuunnitelma ja henkilöstö tai asiakkaat eivät osaa toimia tilanteen palauttamiseksi. Tarvittaessa yksinkertaisella porttiskannauksella tai penetraatiotestauksella yrityksen kriittiset järjestelmät voidaan testata ennen kuin rikollinen pääsee hyökkäämään.

Seuraavaksi esitellään kymmenen teesiä eli haastetta, joilla kyberturvallisuuskulttuuri saadaan osaksi yrityksen toimintakulttuuria. Niiden avulla kyberturvallisuus sisäänrakennetaan yrityksen järjestelmiin, prosesseihin ja toimintatapoihin pitämällä mielessä CIA. Teesit käydään läpi säännöllisin väliajoin. Ensimmäisellä kierroksella on keskityttävä laittamaan perusasiat kyberturvallisuudessa kuntoon:

1. Tee riskien kartoitus ja löydä tärkeimmät suojattavat arvot, resurssit, tiedot ja järjestelmät. Käsitteletkö oikein henkilö-, asiakas-, tai työntekijöiden tietoja? Onko verkkosivut, sähköpostitilit, päätelaitteet ja palvelimet suojattu asianmukaisesti?
2. Tunnista, mikä tieto on yrityksesi toiminnan kannalta tärkeintä, käsitelläänkö yrityksessä esimerkiksi henkilötietoja?
3. On tiedettävä, miten tietoa yrityksessäsi käsitellään. Onko aineisto sähköistä vai paperista? Onko yrityksessä tärkeää hiljaista tietoa? Säilytetäänkö tietoa oikein ja turvallisesti esim. salattuna?

4. On tiedettävä, missä tärkeää tietoa säilytetään. Säilytetäänkö tietoa työntekijöiden omilla koneilla, kassakaapissa, palvelimilla, työpaikalla vai ulkoistetulla palvelimella? Ja ovatko tiedot turvallisessa paikassa?
5. ICT-palveluiden ulkoistus on tehtävä hallitusti, turvallisesti ja järkevästi. Punnitse siis ylläpidätkö verkkoa, palvelimia, koneita itse vai ulkoistatko palvelut.
6. Ihminen on aina heikoin lenkki eli panosta koulutukseen. Ihmisellä on luontainen taipumus tehdä asiat oikomalla ja helpommin, mikä ei aina ole tietoturvallista. Tietoturvan ja käytettävyyden hyvät tarkoitukset eivät aina kohtaa ja kustannukset tulee pitää mielessä, joten on pyrittävä tekemään hyvä kompromissi.
7. Henkilöstön ja johdon koulutus on kustannustehokkain, nopein ja helpoin tapa parantaa kyberturvallisuutta yrityksessä. Valitse siis oikeat ja motivoituneet henkilöt kyberturvan asiantuntijoiksi ja huolehdi koko henkilöstön osaamisesta. Näytä itse hyvää esimerkkiä.
8. Kun hallinnolliset toimet, ohjeet, oikeat toimintatavat on jalkautettu organisaatioon, suunnitellaan tekniset hankinnat, joista kustannustehokkaimmat ratkaisut toteutetaan ensin, esimerkiksi yrityksen kriittisen tietovarannon varmuuskopiot ja niiden testaus. Yritysten tulisi pyrkiä aina ottamaan käyttöön myös kaksivaiheinen tunnistautuminen eri palveluihin (Kyberturvallisuuskeskus: Kaksivaiheinen tunnistautuminen 2017). Siinä perinteisen käyttäjätunnus-salasana -parin lisäksi toisena varmistavana elementtinä on esimerkiksi toimikortti -pohjaiset ratkaisut esim. Google Authenticator, mobiilivarmenne tai tekstiviestitse saapuva kertakäyttösalasana. Teknisistä toimenpiteistä varmuuskopiointi on keskeinen varautumisen keino. Yleisen varmuuskopioinnin 3-2-1 -säännön mukaisesti tulisi ottaa tiedosta 3 kopiota, joista 2 eri kopioformaattia ja yhden kopion säilytys fyysisesti eri rakennuksessa. Jokavuotinen arkistokappale on säilytettävä kassakaapissa. Varmuuskopioinnista tulee tehdä yksityiskohtainen ohje, joka sisältää määräysten ja säännöstöjen mukaiset tietojen säilytysvaatimukset, joita ovat varmuuskopioiden sälytyspaikat ja -tavat, kopiointimenetelmät, vastuuhenkilöt, käyttöoikeudet, palautusprosessien toiminnan ja testauksen. On määritettävä kuinka usein varmuuskopiot otetaan, mitkä tiedot varmistetaan ja millä menetelmällä. (Tietoturvaopas 2016, 19.)
9. Päivitetään ohjelmistot, käyttöjärjestelmät, virus- ja haittaohjelmien ohjelmistot kun ne ovat saatavilla, koska päivityksissä paikataan haavoittuvuuksia ja ohjelmistojen virheitä.

10. Käydään noin kaksi kertaa vuodessa kohdat 1-9 läpi. Eli miten asiat edenneet ja miten on otettu toimintatavoiksi? Huomioidaan hankinnoissa tietoturvallisuus-vaatimukset ja nimetään niihin tietoturvavastaava. (Kyberturvakeskus, CIA ja 10 teesiä.) Tehdään kyberturvallisuudesta osa yrityksen toimintakulttuuria esim. asettamalla selkeä tavoite: ”365 päivää ilman kyberturvallisuusvahinkoa”.