LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Kyberturvallisuuden kehittäminen ja henkilöstöosaamisen kartoitus finanssialan yrityksessä

Yu, Guoxi

2017 Laurea

Laurea-ammattikorkeakoulu

Kyberturvallisuuden kehittäminen ja henkilöstöosaamisen kartoitus finanssialan yrityksessä

Guoxi Yu
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan kouluohjelma
Tradenomi (AMK)

Guoxi Yu

Kyberturvallisuuden kehittäminen ja henkilöstöosaamisen kartoitus finanssialan yrityksessä

Vuosi 2017 Sivumäärä 58

Opinnäytetyön tarkoituksena on tutkia, millaisia kyberturvallisuuden uhkia finanssialan yritys kohtaa vuonna 2017, sekä parantaa yrityksen kyberturvallisuutta henkilöstöosaamisen kautta. Opinnäytetyö toteutettiin toiminnallisena opinnäytetyönä, joka suoritettiin kansainvälisen finanssialan yrityksen suomalaisessa tytäryhtiössä. Opinnäytetyön päätutkimuskysymyksenä on ”Miten yritys voi kehittää kyberturvallisuutta henkilöstön osaamisen ja -tietoisuuden parantamalla?” Opinnäytetyössä käytettiin laadullista tutkimusmenetelmää, sillä aihealueista ei ole olemassa entuudestaan teoriaa tai historiatietoa. Tutkimuskysymykseen vastaamiseen käytettiin useita tutkimusmenetelmiä, joita olivat kirjallinen aineistoanalyysi, havainnointi ja henkilöstökysely.

Opinnäytetyössä avataan vuoden 2017 kyberturvallisuuden näkymiä esittelemällä Bangladeshin pankin ryöstö vuonna 2016, sekä kiristysohjelmien räjähdysmäinen leviäminen niin yksityisten henkilöiden päätteille, kuin yritystenkin työasemille. Lisäksi opinnäytetyössä näytetään käytännössä, miten voidaan tehdä yritykseen kyberturvallisuuden henkilöstökysely, jolla voidaan kerätä tietoa henkilöstön kyberturvallisuuden osaamisesta ja toimintatavoista, mutta toimii samalla myös opettavaisena ja mielenkiintoa herättävänä työkaluna. Samalla opinnäytetyössä on tiivistetty ISO/IEC 27001:2013, Katakrin ja VAHTI-ohjeiden sisällöt henkilöstöosaamisen kannalta, josta yritys voidaan ottaa mallia suunnitellessa omia strategioita henkilöstöosaamisen takaamiseksi.

Kiristysohjelmien nousu yhdeksi suuremmaksi turvallisuusuhkaksi on omiaan nostattamaan jokaisen työntekijän tärkeyden kyberturvallisuusuhkien torjunnassa. Niistä tuorein esimerkki on WannaCryn räjähdysmäinen leviäminen toukokuussa 2017. Tutkimuksen lopputuloksessa selvisi, että työntekijöiden osaamistasot ovat muuten hyvät, mutta epäselvää oli varsinkin yrityksen avainhallinnan ja verkkokäyttäytymisen koskevat säännöt. Henkilöstökyselystä selvisi myös, että alle puolet henkilöstö piti osaa kyberturvallisuusosaamista riittävänä ja monet olivat halukkaita saamaan säännöllisempää koulutuksia, sekä toivoivat yrityksen antavan säännöllisiä uutisiskuja uusimmista turvallisuusuhkista, mitkä ovat esillä mediassa, sekä antavan konkreettisia esimerkkejä niiden torjunnassa.

Tutkimuksen perusteella yritykselle ehdotettiin muun muassa kyberturvallisuuskoulutusten säännöllistämistä, koulutusten saatavuuden parantamista, sekä koulutuksen antaminen myös sidosryhmän jäsenille, joilla on pääsy yrityksen verkkoihin. Yritykselle ehdotettiin myös valvonnan tehostamista halutun lopputuloksen saavuttamiseksi.

Tutkimuksen lopussa todettiin, että henkilöstökysely on hyvä työkalu selvittämään henkilöstöosaamista myös kyberturvallisuuden puolella. Opinnäytetyö antaa yhden esimerkin henkilöstökyselyn tekemiseen, mutta antaa myös kehitysehdotuksia sen parantamiseen. Henkilöstökyselystä saadut tulokset ovat yrityskohtaisia, mutta itse kysely on hyvin hyödynnettävissä pienellä muokkauksella myös muille organisaatioille.

Asiasanat: Henkilöstökysely, Kyberturvallisuus, Tietoturvallisuusstandardi, Turvallisuusjohtaminen

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Abstract

Guoxi Yu

Improving Cybersecurity and Employee Awareness and Skills in a Financial Institution

Year 2017 Pages 58

The objective of this thesis is to research what threats financial institutions face in 2017, and how to improve cybersecurity in a company through employee awareness. This thesis is a functional study, and it was carried out in a Finnish subsidiary of an international financial institution. The study answers the question of how to improve cybersecurity in a company by improving employees' awareness and skills. Qualitative research was used in this thesis, because there is not any published theory in this area of research. Different research methods were used, including literature review, observation, and employee survey.

This thesis starts by elaborating the cybersecurity field in 2017 by presenting the Bangladesh Bank robbery in 2016, and ransomware that could infect both private and corporate computers. Additionally, this thesis describes how to build a cybersecurity survey for corporate use. The objective of the survey was to collect information about employees' cybersecurity skills and knowledge, and at the same time it was used for educational purposes. The thesis also includes an analysis of the ISO/IEC 27001:2013, Katakri, and VAHTI instructions. The thesis also depicts what requirements organizations have for employees' skills and knowledge. The company can use the results presented in the thesis when planning the strategies to ensure proper training for its employees.

Ransomware is one of the biggest threats in cybersecurity, and this ongoing issue further emphasises the importance of employees in stopping such attacks, as with the most recent ransomware wave in May 2017, called the WannaCry ransomware. The results from the research showed that the employees have a good understanding of cybersecurity. However, access control and web behaviour policies were still unclear for many, who answered the survey. Only about half of the employees, who answered the survey, thought that they have adequate cybersecurity skills and knowledge required for their job, and many wished for more frequent cybersecurity training. There were also demands for regular updates of latest cybersecurity threats, and concrete instructions on how to counter those threats.

Suggestions on how to improve cybersecurity in the company were given based on the research, and methods suggested included regular cybersecurity training for all internal and external employees, who have access to the company's internal networks, among other things. It was also suggested that the company should enhance supervision to achieve the set goals.

The research showed that employee survey is a working tool for a company to determine employee skills and knowledge about cybersecurity. This thesis provides one example on how to build such a survey, but it also gives suggestions on how to improve it. The results from this employee survey represent only one company, but with small adjustments, the survey itself can benefit other organizations as well.

Keywords: Cybersecurity, Employee Survey, Information Security Standard, Security Management

Sisällys

1 Johdanto

Kyberturvallisuus on tällä hetkellä paljon puhuttu aihe, ja yrityksissä siihen on panostettu vuodesta toiseen entistä enemmän. Tietoturvallisuusyritys SSP Blue:n toimitusjohtaja Hemanshu Nigam kertoi marraskuun 2015 haastattelussa, että maailmanlaajuisten kyberturvallisuusmarkkinoiden on arvioitu kasvavan 170 miljardiin Amerikan dollariin vuoteen 2020 mennessä. RT -uutissivusto kirjoitti vuonna 2015 artikkelissa World Cybersecurity Market Will Grow by $100b in Five Years, että kyberturvallisuusmarkkinoiden arvioidaan olevan vielä vuonna 2015 77 miljardia dollaria (2015). Kansalliseen ja julkiseen turvallisuuteen erikoistunut tutkimuslaitos Homeland Security Research Corp. on raportoinut omassa tutkimuksessaan, että Amerikan finanssialan laitosten kyberturvallisuusmarkkinat kasvavat nopeimmin, ja niiden yhteenlaskettu arvo ylittää vuoden 2016–2020 aikavälillä 68 miljardia Amerikan dollaria (2015). Vaikka edellä mainitut luvut ovat suuria, kukaan tuskin yllättyy siitä, että finanssiala käyttää kyberturvallisuuteen suuria määriä resursseja. Finanssiala on kyberrikollisille oiva kohde, sillä rikoksesta saatu hyöty on usein raha, jota on teknologioihin verrattuna helpompi ottaa suoraan käyttöön, ja summat voivat olla hyvinkin suuria.

Tämän opinnäytetyön tarkoituksena on parantaa yritys X:n kyberturvallisuutta henkilöstön osaamista kartoittavalla kyselyllä, joka myös herättäisi henkilöstön oman kiinnostuksen kyberturvallisuuteen. Kartoituksen pohjalta yritys X:lle tehtiin ehdotuksia kyberturvallisuuden parantamiseksi. Samalla asiakasyrityksen pyynnöstä henkilöstöosaamisen kannalta tarkastettiin myös ISO/IEC 27001 tietoturvallisuusjohtamisen standardi, VAHTI-ohjeet sekä Katakri auditointikriteeristö. Tarkastelun tarkoituksena oli selvittää, miten henkilöstöosaamisen taso varmistetaan yleisissä standardeissa ja ohjeistuksissa. Selvityksen tuloksia käytettiin myös osana yritys X:lle annettavia parannusehdotuksia.

Suomessa ei ole tällä hetkellä olemassa tiettyä kysymysrunkoa, jota voitaisiin soveltaa yritysten kyberturvallisuuskyselyihin. Opinnäytetyössä esitettyjen analyysien avulla on tehty oma kysymyspatteristo, jonka kysymykset ovat toivottavasti niin joustavia, että niitä voidaan ottaa muuallakin käyttöön. Opinnäytetyössä on perusteltu niin kyberturvallisuuden, kuin itse kyselynkin tärkeys. Mikäli olisi olemassa suomenkielinen kyberturvallisuuden runko, joka sopisi mahdollisimman monille yrityksille, se helpottaisi opinnäytetyössä esitetyn henkilöstökyselyn käyttöönottoa yrityksissä huomattavasti. Tulokset olisivat näin myös vertailukelpoisia keskenään, mikä helpottaisi yritysten välistenhenkilöstöosaamisen benchmarkingia.

2 Opinnäytetyön tausta, toteutus ja tavoitteet

Laadullista tutkimusta käytettiin opinnäytetyössä, sillä Kanasen mukaan se on paras vaihtoehto silloin, kun tutkittavaa ilmiötä ei tunneta, eikä ilmiöstä ole teoriaa (2014, 16). Hänen mukaansa laadullinen tutkimus ei pyri yleistämään kuten määrällinen tutkimus, joka taas edellyttää hyvää tietämystä tutkittavasta ilmiöstä ja teoriasta. Kirjoittaja ei opinnäytetyön alkuvaiheessa ollut löytänyt muiden suomalaisten yritysten kyberturvallisuusosaamisesta tietoa, eikä yritys X:ssä ollut tästä historiatietoa, joten laadullinen tutkimus tuntui parhaalta vaihtoehdolta. Tässä luvussa käydään läpi keskeisiä käsitteitä, opinnäytetyön taustat, tavoitteet ja toteutus, sekä rajaukset.

2.1 Keskeiset käsitteet

Seuraavaksi esitellään opinnäytetyössä esiintyviä keskeisiä käsitteitä ja lyhenteitä.

Kyberturvallisuudella tarkoitetaan sellaisten tietojen suojaamista, jotka ovat elektronisessa muodossa. Nykymaailmassa suurin osa tiedoista on sähköisessä muodossa, joten kun puhutaan tietojen suojaamisesta, puhutaan myös entistä enemmän kyberturvallisuudesta. Kyberturvallisuus pitää sisällään myös osan perinteisestä fyysisestä turvallisuudesta, sillä sähköisetkin tiedot ovat joissain tapauksessa helpompi varastaa esimerkiksi käymällä fyysisesti kohteessa ja kopioimassa tiedot suoraan koneelta. Jarno Limnéll, Klaus Majewski ja Mirva Salminen ovat todenneet kirjassa Kyberturvallisuus (2014, 31), että tietoturva oli varattu aikoinaan kuvaamaan olemassa olevan ja varastoidun tiedon turvaamista, mutta kyberturvallisuus kattoi tämän lisäksi myös tietojen liikkeen turvaamisen.

Tietoturvallisuudella tarkoitetaan sellaista tietojen suojaamista, jonka toteutuksessa useimmiten ajatellaan tietojen luottamuksellisuuden, eheyden ja saatavuuden (Confidentiality, Integrity, Availability) turvaamista (SecureWorks, 2017). Tietoturvallisuus kattaa myös sellaisten tietojen suojaamista, jotka eivät ole elektronisessa muodossa, kuten esimerkiksi paperisopimusten ja arkistojen suojaamista. Tietoturvallisuus näin ollen on kyberturvallisuutta laajempaa.

Haittaohjelmia ovat muun muassa virukset, Troijalaiset, madot, kiristysohjelmat ja vakoiluohjelmat. Haittaohjelmat tarttuvat useimmiten sähköpostin liitteistä, tai muista ladatuista tiedostoista. Haittaohjelma voi kuitenkin olla myös nettisivuissa, joista ne tartuttavat käyttäjän koneen, kun käyttäjä vierailee sivulla. (Tietoturvapalvelu, 2015).

Kiristysohjelma on haittaohjelma, joka leviää useimmiten sähköpostitse, kuten monet viruksista. Haittaohjelma saastuttaa ja lukitsee laitteen, kun ohjelma vahingossa avaa ja useimmiten salaa koko laitteen tallennustilan. Tiedostot ja laitteen saa takaisin hallintaan ainoastaan

maksamalla rikolliselle vaadittu summa. Menettelyprosessi ilmoitetaan lukitun laitteen näytöllä (Poliisi, CERT-FI & F-secure, 2013).

Standardi (normi) on käytännössä jonkin organisaation esittämä määritelmä siitä, miten tietty asia kuuluisi tehdä. Standardit syntyvät yleensä jonkin ryhmän tarpeesta saada tietynlainen normi teknisiin ratkaisuihin tai käytäntöihin**.** Useammat standardit ovat vapaaehtoisia, eivätkä ole kirjattu lakiin (BSI Group, 2015b).

SWIFT on lyhenne Society for Worldwide Interbank Financial Telecommunicationista (SWIFT, 2014). Se on yhteistyöverkosto, jonka avulla finanssialan yritykset voivat lähettää ja vastaanottaa varainsiirtoa turvallisesti, yhteisiä normeja noudattaen luotettavassa ympäristössä. SWIFT tarjoaa myös ohjelmistoratkaisuja finanssialayrityksille.

Verkkourkinta (tai tietojenkalastelu) eli **phishing**, on pääasiassa rikollisten käyttämä keino, jolla varastaa luottamuksellisia tietoja esiintymällä luotettuna tahona. Urkinta tapahtuu pääasiassa sähköpostin tai pikaviestipalvelun kautta ja kohteina on ollut niin yksityishenkilöitä, kuin yrityksiäkin. Yrityksiin kohdennettu verkkourkinta tunnetaan englanniksi myös **spear phishing** –nimisenä hyökkäyksenä. Sanastokeskus TSK ry:n mukaan termi tarkoittaa suomeksi käännettynä **kohdennettua verkkourkintaa** (2016).

2.2 Toimeksiantajayrityksen kuvaus

Tämän opinnäytetyön toimeksiantoyritys on kansainvälisen finanssialan konsernin Suomen tytäryhtiö. Konserni toimii yli kymmenessä maassa ja Suomessa sillä on vajaat 2 000 työntekijää. Koko konsernissa taas on noin neljä miljoonaa asiakasta ja lähes 20 000 työntekijää. Konsernissa on yhdistetty vanhat maakohtaiset turvallisuusyksiköt yhdeksi yksiköksi, mikä tarkoittaa sitä, että maakohtaiset turvallisuusorganisaatiot sulatettiin yhteen matriisimaiseen organisaatioon. Tässä organisaatiossa konsernin turvallisuusryhmän jäsenellä on hoidettavanaan sekä oman maan turvallisuuden osa-alueet, että konsernin tasolla vielä yksi osa-alue, kuten esimerkiksi matkustusturvallisuus tai kansainväliset toiminnot. Fyysinen turvallisuus hoidetaan eri yksikössä kuin IT-turvallisuus, vaikka toistaiseksi fyysisen turvallisuuden yksikkö huolehtii kyberturvallisuuskoulutuksista. IT-turvallisuus taas huolehtii teknisestä kyberturvallisuudesta, kuten esimerkiksi palomuureista, virustorjunnasta ja salausavaimien ylläpidosta.

Yhtiössä on käytössä osin konsernin säännökset ja osin vielä Suomen tytäryhtiön omat prosessit. Opinnäytetyön on tarkoitus ottaa kantaa yrityksen Suomen tytäryhtiön prosesseihin, mutta samalla skaalata niitä myös koko konserniin. On suunniteltu, että konserni yhtenäistäisi turvallisuusjohtamista tytäryhtiöihin niin, ettei niiden prosesseissa olisi suuria eroja, vaikka

maakohtaisia erovaisuuksia saattaa myöhemmin tulla eri maiden lainsäädännöstä tai kulttuurista johtuen. Tämä opinnäytetyö ottaa asioihin kantaa kuitenkin koko konsernin, eikä vain yhden maan yrityksen näkökulmasta, jotta ehdotukset eivät vanhenisi heti kun prosesseja aletaan tulevaisuudessa yhdistää.

2.3 Opinnäytetyön tausta ja aiheen valinta

Kirjoittaja työskenteli yritys X:ssä osana turvallisuusyksikköä. Työhön kuului finanssialan kyberturvallisuuden analysoiminen, ja sitä kautta yritys X:n kyberturvallisuuskoulutusmateriaalien päivittäminen. Analyysin tulokset paljastivat uusimpien kyberturvallisuusuhkien kohdistuvan edelleen hyvin vahvasti yritysten henkilöstöön, ja tästä syntyi ajatus opinnäytetyöstä kyberturvallisuudesta. yritys X:n turvallisuuspäällikön kanssa käydyn pohdinnan jälkeen opinnäytetyön aihealueeksi valittiin henkilöstöosaaminen. Tutkimuskysymyksestä muotoutui seuraava:

”Miten yritys voi kehittää kyberturvallisuutta henkilöstön osaamisen ja-tietoisuuden parantamisella?”

Kyberturvallisuuskoulutuksissa havaittiin suuria vaihteluita työntekijöiden ymmärryksessä kyberturvallisuudesta. Tästä lähti ajatus henkilöstökyselystä, joka opettaisi vastaajille tietyt termit, sekä herättäisi vastaajien kiinnostuksen kyberturvallisuuteen. Kyselyllä piti pystyä antamaan yritykselle hieman osviittaa vastaajien taustoista, sekä tietoa henkilöiden käyttäytymisestä ja osaamisesta. Yritys X ei ollut tehnyt kaikille työntekijöille avointa kyberturvallisuuskyselyä opinnäytetyön tekemisen ajanjakson aikana tai sitä ennen, joten idea sopi yritykselle. Toimeksiantaja halusi tehdä kyselystä työkalun, jota tiedonkeruun lisäksi voisi käyttää myös koulutuksen apuvälineenä.

Henkilöstökyselyn kysymykset suunniteltiin tarkkaan yritys X:n turvallisuuspäällikön kanssa, jotta niillä saavutettaisiin yrityksen tavoitteet. Turvallisuus tai kyberturvallisuus ei kuitenkaan ole yritys X:n päätoimiala, joten yrityksessä ei nähty tarpeelliseksi tehdä kaikille pakollista henkilöstökyselyä, vaan kysely perustui täysin vastaajien vapaehtoisuuteen. Tästä syystä, kun kyselyssä selvitettiin osallistujien tietoa kyberturvallisuudesta, vastaajille piti jäädä hyvä mieli. Turvallisuuspäällikkö korosti myös, että mikäli kyselystä tulisi liian vaikea ja haastava, kuten objektiivisesta kyselystä saattaisi tulla, työntekijöille saattaisi muodostua liian iso kynnys vastata siihen.

Henkilöstökyselyä käytettiin yrityksessä ensimmäistä kertaa vasta opinnäytetyön tekovaiheessa, ja tuloksia käytettiin työkalun parannusehdotusten tekemisessä. Yritys X:n vastuulle

jäi jatkokehittää henkilöstökyselyä, mikäli se todettaisiin hyödylliseksi. Lopullinen henkilöstökysely voidaankin nähdä kvalitatiivisen ja kvantitatiivisen tutkimuksen yhdistämisenä. Kananen (2014, 142) on esittänyt, että tähän voidaan päästä, jos määrällistä tietoa on kerätty, mutta tuloksen saamiseksi vaaditaan myös esimerkiksi havainnointia ja muuta taustaselvitystä. Opinnäytetyössä määrällisen tutkimuksen muoto, eli verkkokysely, yhdistettiin määrällisen tutkimuksen vapaisiin kommentteihin.

Opinnäytetyössä selitetään ISO/IEC 27001:2013 standardi, Katakri 2015 -auditointityökalu, sekä Vahti-ohjeet yleisesti, koska yritys X:n turvallisuuspäällikkö pyysi vertaamaan yritys X:n henkilöstön kouluttamista yleisiin standardeihin ja ohjeistuksiin, sekä kertomaan niiden erot.

2.4 Toteutus

Opinnäytetyön tavoitteena oli parantaa yritys X:n kyberturvallisuutta henkilöstöosaamista parantamalla. Opinnäytetyön muodoksi valittiin toiminnallinen opinnäytetyö. Vilkka ja Airaksinen esittelevät toiminnallista opinnäytetyötä kirjassa Toiminallinen opinnäytetyö seuraavasti: ”Toiminnallinen opinnäytetyö tavoittelee ammatillisessa kentässä käytännön toiminnan ohjeistamista, opastamista, toiminnan järjestämistä tai järkeistämistä” (2003, 9). Tässä opinnäytetyössä kehitettiin yritys X:lle työkaluksi kyberturvallisuuden henkilöstökysely, jonka oli tarkoitus järkeistää yritys X:n kyberturvallisuuskoulutusta tarjoamalla tietoa henkilöstöosaamisen tasosta, sekä kertoa työntekijöiden viimeisimmät toiveet kyberturvallisuuskoulutuksista. Kanasen mukaan kohteena olevan ilmiön ymmärtämiseksi voidaan käyttää monia menetelmiä (2014, 120), joten tutkimukseen käytettiin triangulaatiota.

Opinnäytetyö aloitettiin analysoimalla kyberturvallisuusympäristöä vuosilta 2015-2017. Lähteinä käytettiin uutisia, artikkeleita ja blogeja, jotka yhdessä antoivat kattavan kuvan kyberturvallisuuden uhkista sekä hallinnollisista haasteista yrityksille. Kanasen mukaan kaikkea sellaista aineistoa, jolla on merkitystä tutkimuksen kannalta, voidaan käyttää tutkimusongelman ratkaisussa (2014). Kirjallista aineistoanalyysia käytettiin, sillä opinnäytetyön aineista ja ympäristöstä haluttiin saada ajankohtaista kuvaa ennen varsinaisen tutkimusongelman tarkempaa rajaamista.

Kirjoittaja oli työharjoittelussa opinnäytetyön teon aikaan yritys X:ssä, joten oli luontaista kerätä tietoa myös havainnoimalla. Havainnointia käytettiin yhtenä tutkimuksen tiedonkeruumenetelmänä, sillä työharjoittelukausi antoi siihen oivan mahdollisuuden. Kanasen mukaan havainnointia voidaan käyttää tilanteissa, joissa ilmiötä ei tunneta (2014), ja tällöin se sopii tutkimusongelman tutkimiseen täydellisesti. Kanasen kirjassa Laadullinen tutkimus opinnäytetyössä esitetään erilaisia havainnointikeinoja, kuten piilohavainnointi, suora havainnointi ja

osallistuva havainnointi (2014, 66-67). Kirjoittaja havainnoi työharjoittelunsa aikana henkilöstöä yhteisön ohella, joka olisi Kanasen mukaan osallistuvaa havainnointia (2014, 66). Toiminnallisen opinnäytetyön keinona voidaan Kanasen mukaan käyttää myös osallistuvaa havainnollistamista, jolloin tutkija pyrkii saamaan aikaan pysyvän muutoksen tutkittavassa yhteisössä (2014, 67). Opinnäytetyössä osallistuva havainnointi ilmenee tapauksissa, jolloin kirjoittaja toimi kouluttajan roolissa muutamissa yritys X:n koulutustilaisuuksissa, ja näin vaikutti yritys X:n henkilöstön kyberturvallisuuskehitykseen. Samassa tilanteessa havainnoinnilla saatiin henkilöstön reaktiot ja käytös talteen jatkoanalyysia varten. Aiheanalyysin, havainnointien ja avoimien lähteiden pohjalta rakennettiin kyberturvallisuuden henkilöstökysely, joka oli tarkoitettu niin tietojen keräämiseen kuin henkilöstötietoisuuden kehittämiseen.

Kyselytutkimusta käytettiin viimeisenä tiedonkeruukeinona, jolloin sekä kirjallisen aineiston analyysin, että havainnoinnin tuloksia pystyttiin käyttämään kyselytutkimuksen luomisessa. Kyselytutkimus valittiin yhdeksi tiedonkeruumenetelmistä, sillä vastauksia haluttiin saada enemmän lyhyessä ajassa, kuin mitä haastattelua käyttämällä olisi ollut mahdollista. Tulokset kerättiin kahden viikon ajalta, jonka jälkeen ne analysoitiin ja kirjattiin tarkasti. Opinnäytetyötä kirjoitettiin pääasiassa vasta kyselytutkimuksen analysoinnin jälkeen, jotta opinnäytetyön jäsentäminen onnistuisi parhaalla tavalla. Kun kaikki vaiheet ja tulokset oli kirjattu opinnäytetyöhön, tulokset yhdessä analyysin kanssa luovutettiin yritys X:lle. Viimeisessä vaiheessa yrityksen palautteet jalostettiin jatkokehitysehdotuksiksi.

2.5 Rajaukset

Opinnäytetyön rajaukset sovittiin yhdessä toimeksiantajan kanssa heidän tarpeidensa mukaan, mutta aikarajaukset ja tietotekniset resurssit otettiin myös huomioon rajauksia sovittaessa. Työantajayritykselle oli tärkeää nostaa kyberturvallisuuden profiilia ja siksi kyberturvallisuuskyselyn luominen ja toteuttaminen olivat heille keskeisiä. Tämän lisäksi oli tärkeää katsastaa myös tietoturvallisuusstandardi ISO/IEC 27001:2013, sen sisältämät henkilöstöosaamisen osa-alueet, sekä miettiä millä tavalla yrityksen toimet niin henkilöstöosaamisessa, kuin käytännön toiminnassa sopivat yhteen standardin kanssa. Yritys X toivoi, että kirjoittaja pystyisi edellä mainitusta standardista ja muista ohjeistuksista osviittaa henkilöstöosaamisen tärkeydestä, jotta turvallisuusyksikkö pystyisi paremmin perustelemaan koulutusten tarpeet, sekä heijastamaan omaa koulutustasoa tietoturvastandardiin. ISO/IEC27001:2013:n lisäksi mukaan otettiin myös Katakri 2015 ja VAHTI-ohjeet, sillä vaikka kumpikaan ei ole standardi, ne ovat kumpikin hyvin käyttökelpoisia varsinkin suomalaisessa toimintaympäristössä.

Kirjoittajan vastuulla oli tuoda esille omat havainnot kyberturvallisuuskyselyn pohjalta, sekä tehdä tarvittaessa ehdotuksia tulevien kyberturvallisuuskoulutusten parantamiseksi, mutta

käytännön toteutukset jäivät toimeksiannon ulkopuolelle. Kirjoittajan työ oli antaa myös kehitysehdotuksia, mutta myös näiden vastaanotto ja varsinaiset kehitystoimet jäivät täysin yritys X:n vastuulle. Yritys on itse vastuussa kyberturvallisuuskyselyn kehityksestä ja sen vaikutusten seurannasta.

Tietoturvallisuusstandardin ja ohjeistusten arviointi rajattiin koskemaan ainoastaan henkilöstöosaamista, toimeksiannon ulkopuolelle jäivät kaikki muut osa-alueet. Opinnäytetyössä ei näin ollen esitetä ISO/IEC27001:2013:a, Katakri 2015:a tai VAHTI-ohjeita kokonaan, vaan ainoastaan sellaiset osa-alueet, mitkä liittyivät olennaisesti opinnäytetyön aiheeseen.

3 Kyberturvallisuus finanssialalla

Jorma Kanasen mukaan kaikkia kirjallisen aineiston muotoja voidaan käyttää laadullisen tutkimuksen tiedonkeruulähteenä (2014, 90). Koska yritys X:ssä ei oltu tehty henkilöstön kyberturvallisuusosaamisesta tutkimusta aikaisemmin, eikä aiheeseen liittyviä historiatietoja ollut saatavilla, päätettiin tutkia avoimista lähteistä saatavaa aiheistoa. Aiheistossa käytettiin uutisia, artikkeleita ja blogeja antamaan ajankohtaisin kuva kyberturvallisuuden ympäristöstä.

Kyberrikollisuus oli PWC:n raportin mukaan vuonna 2016 toiseksi eniten esille tullut talousrikoksen muoto (2016), ja finanssialan yritykset olivat rikollisille ykköskohde. Kaikki kyberrikollisuudet eivät tule ilmi, sillä rikoksen kohteeksi joutuneen yrityksen maine saattaa tahriintua. Yksi tapaus oli kuitenkin hyvin laajasti otsikoissa vuonna 2016, ja se on Bangladeshin pankin varkaus. Verkon kautta tapahtunut varkaus toi rikollisille 81 miljoonan dollarin hyödyn, mutta rikollisten tavoitteena oli yhteensä jopa miljardin dollarin saalis (Barrett, 2016).

Finanssialalle kyberturvallisuus on erittäin tärkeässä osassa, sillä yrityksen on varjeltava varainsiirtoa, omia liikesalaisuuksiin kuuluvia tietoja ja pankkisalaisuuksiin kuuluvia asiakkaan tietoja. Perinteisen turvallisuuden lisäksi finanssialalla korostetaan myös yksityisyyttä, sillä asiakkaan tietoa on suojattava kaikilta asiattomilta tahoilta, joilla ei ole virallista lupaa käsitellä kyseisten asiakkaiden tietoa. Nykypäivänä asiaton taho voi olla niin kyberrikolliset, pankin omat työntekijät, kuin erilaiset valtiolliset tahotkin.

Pankissa säilytettävä, ja pankkien sekä pankkien ja asiakkaiden välillä liikkuva raha saattaa olla ensimmäinen asia, joka tulee mieleen, kun ajatellaan finanssialan kyberturvallisuutta. On selvää, että pankin näkökulmasta omaisuuden turvaamisella on erittäin suuri prioriteetti. Perinteisiä pankkiryöstöjä sattuu Suomessa nykyään hyvin vähän. Hevonojan kirjoittaman artikkelin (2015) mukaan 2000–luvulla Suomessa on tehty 3–8 pankkiryöstöä vuodessa, eivätkä sum-

mat ole olleet merkittäviä. Suomi on säästynyt suurelta osin pankkiryöstöiltä verrattuna moniin muihin länsimaihin – esimerkiksi Ruotsissa oli saman artikkelin mukaan 110 pankkiryöstöä pelkästään vuonna 2008. Maantieteellinen sijainti ja yhteiskunnalliset olot ovat tehneet osansa pankkien turvatessa omaisuutta rikoksilta, mutta bittiaikana kumpikaan harvoin tuo erityistä suojaa. Varainsiirto tapahtuu samassa verkossa riippumatta siitä, missä päin pankit fyysisesti sijaitsevat. Tämä korostuu vielä enemmän alla olevassa Bangladesh Bankin tapauksessa, jossa rikolliset pääsivät varastamaan pankin käyttämiä tunnisteita, ja pääsivät näin siirtämään varoja oikean pankin identiteetillä.

Seuraavissa kappaleissa tullaan avaamaan Bangladeshin pankin tapausta konkreettisena esimerkkinä siitä, kuinka pankilta pystytään ryöstämään verkon kautta enemmän rahaa, kuin olisi fyysisesti mahdollista. Tapauksen analysoinnin toivotaan antavan myös pientä kuvaa siitä, kuinka monialainen ja haastava kyberturvallisuuden kenttä on finanssialalla. Lisäksi annetaan yleiskuva kyberturvallisuuskentästä, sekä arvioidaan ammattilaisten listaamia uhkia. Näiden kaikkien tarkastelujen tarkoituksena on perustella kyberturvallisuuden korostamista finanssialalla, sekä antaa syitä kyberturvallisuuden henkilöstökyselylle.

3.1 Varkaus Bangladesh Bankista ja vaikutukset finanssialaan

Bangladesh Bankin tapaus on yksi suurimmista pankkimaailmassa tapahtuneista kybervarkauksista. Vuoden 2016 helmikuussa toistaiseksi tunnistamattomat varkaat pääsivät käsiksi pankin käyttämään SWIFT-rahansiirtojärjestelmään ja lähettivät Reutersin mukaan rahansiirtopyyntöjä 951 miljoonan Yhdysvaltojen dollarin edestä (Das & Spicer, 2016). Hyökkääjät käyttivät Bangladesh Bankin identiteettiä ja lähettivät varainsiirtopyynnöt New Yorkin Federal Reserve Bankille, joka piti hallussaan Bangladesh Bankin tilejä. Neljä yhteensä 81 miljoonan dollarin arvoista rahalähetyspyyntöä Filippiineille pääsi läpi, mutta 20 miljoonan dollarin arvoinen rahapyyntö Sri Lankalle pysäytettiin, sillä eräs ryöstäjä oli erehdyksessä kirjoittanut erään yhteisön nimen väärin. ”Foundation” -sanan sijasta henkilö oli kirjoittanut ”Fandation”, ja tämä kiinnitti lähetystä reitittäneen Deutsche Bankin työntekijän huomion. Deutsche Bank ja Sri Lankan pankki ottivat yhteyttä Bangladesh Bankiin, ja rahalähetys peruttiin.

Security Managementin Megan Gates kirjoitti omassa artikkelissaan Stopping the Cyber Buck (Gates, 2017), että varkautta suunniteltiin todennäköisesti yli vuosi. Varkaus oli hämmästyttävän samanlainen kuin vuoden 2013 Bangladeshilaisen Sonali Bankin varkaus. Tutkijat epäilevätkin, että molemmissa varkauksissa saattoivat olla samat tekijät. Bangladesh Bankin varkauden jälkeisessä tutkimuksessa selvisi, että pankin varainsiirtojärjestelmistä löytyi haittaohjelma, joka oli todennäköisesti asennettu pankkiin vuoden 2016 tammikuussa. Tämä oli hyökkääjien pääasiallinen tapa kerätä teknistä tietoa Bangladesh Bankin SWIFT -varainsiirtojärjestelmän teknisistä tiedosta. The Wall Street Journalin artikkelin mukaan FBI epäili myös,

että muutamat sisäpiiriläiset saattoivat antaa hyökkääjille tietoa Bangladesh Bankin tietojärjestelmistä (Barrett, 2016).

Ryöstäjät käyttivät monia seikkoja hyväkseen, kuten esimerkiksi Bangladeshin julkisia vapaapäiviä, 4. ja 5. helmikuuta, jolloin varkaus tehtiin. Näin ryöstäjät saivat lisäaikaa, eikä Bangladeshissa huomattu rahasiirtoja heti. Sisäpiiriläisten käyttö oli myös tärkeää tietojen hankkimisessa, ja on olemassa teoria, jonka mukaan haittaohjelma olisi myös päässyt pankin järjestelmiin sisäpiiriläisten kautta (Barrett, 2016). SWIFT -varainsiirtojärjestelmän heikkoudet ovat olleet ajoittain julkisuudessa ja esimerkiksi Ylen artikkeli on paljastanut työkaluja, joiden avulla SWIFT -varainsiirtojärjestelmää voidaan vakoilla (Kokkonen, 2017a). RHEA Groupin blogi antoi ymmärtää Bangladeshin pankin varkauden osoittaneen, että siihen mennessä virheettömäksi luultu SWIFT osoittautuikin tässä tapauksessa olevan varainsiirtojärjestelmän heikoin lenkki (The Three Biggest Cyber-Attacks of 2016, 2016). Hyökkäys oli myös hyvä osoitus siitä, miten pankin identiteetin varastaminen antaa hyökkääjälle kyseisen pankin identiteettiä käyttämällä mahdollisuuden siirtää varoja lähes huomaamatta, ja samalla ohittaa kaikki muut suojaukset. Distil Networks haastatteli useita kyberturvallisuuden asiantuntijoita vuoden 2017 suurimmista kyberturvallisuuden uhista ja 451 Researchin turvallisuusanalysoija Eric Ogrenin mukaan suurin uhka vuodelle 2017 oli se, että hyökkääjä käyttäisi hyväkseen yrityksen käytäntöjä sen jälkeen, kun hyökkääjä pääsee yrityksen verkkoon (Terman, 2017). Ogrenin mukaan on paljon helpompi käyttää hyväkseen kaapattuja avaimia ja identiteettiä, kuin hyökätä ulkopuolelta väkisin. Tämä oli juuri se syy, minkä takia hyökkäys Bangladesh Bankia vastaan oli niin onnistunut. Myöskin Bangladeshin valtion kyvyttömyys rakentaa finanssijärjestelmilleen riittävän vahvat suojaukset, sekä SWIFT:in turvallisuusaukot antoivat rikollisille mahdollisuuden tehdä kymmenien miljoonien arvoisen kansainvälisen varkauden.

Vuonna 2016 oli Bangladesh Bankin varkauden lisäksi ainakin kaksi muuta julkistettua pankin kybervarkautta, joissa käytettiin hyväksi SWIFT:in heikkouksia. Toisessa hyökkäyksessä Ecuador Bank Banco Del Austro of Cuencasta oli viety SWIFT:iä käyttämällä 12 miljoonaa dollaria, kertoo Pierlugi Paganini Security Affairsin sivulta (2016).

Hyökkäys nosti hyvin julkisuuteen kyberturvallisuuden merkityksen finanssialan yrityksille, sekä sen, miten finanssialaan kohdistuva kyberhyökkäys voi vaikuttaa kokonaisvaltaisesti talousympäristöön. Gates selitti omassa artikkelissaan (2017), että New York State Department of Financial Services (DFS) otti käyttöön marraskuussa 2017 uudet säännöt, joiden pitäisi nostaa finanssialan yritysten kyberturvallisuuden minimitasoa. Säännöstelyyn kuuluvilla yhteisöillä ja yrityksillä pitää olla kirjalliset ohjeet ja prosessit niiden kolmannen osapuolen kyberturvallisuustasojen auditointiin, jotka pääsevät niiden salaisiin tietoihin. Lisäksi yrityksillä on oltava tietoturvapäällikkö (Chief Information Security Officer, CISO), jonka vastuulla on laatia

kyberturvallisuusohjeistukset ja johtaa niiden toteutusta. Niiden on myös palkattava kyberturvallisuushenkilöstöä, jonka vastuulla on tunnistaa uhat, vastata kyberturvallisuuspoikkeamista, sekä hoitaa palautuminen jo tapahtuneista vahingollisista tapahtumista. Nämä ovat pieni askel parempaan, mutta eivät välttämättä sovellu sellaisinaan kaikille tahoille.

Bangladesh Bankin tapaus korosti kuitenkin konkreettisesti, kuinka tärkeätä on luoda kyberturvallisuusjohtamisjärjestelmä, jossa on selkeät vastuuhenkilöt ja tavoitteet. Tämän lisäksi yrityksellä on oltava suunnitelma kyberturvallisuuspoikkeamille, sekä valmius toteuttaa kyseinen suunnitelma, milloin tahansa, riippumatta kansallisista vapaa- tai muista poikkeavista päivistä. Bangladesh Bankin verkkoliikennettä valvottiin ja rahaliikenteen siirtoa vakoiltiin jo kuukautta ennen itse varkautta, mutta Bangladesh Bankilla ei ollut koko sinä aikana mitään tietoa asiasta. Tämä paljastui vasta jälkiselvityksessä, joka kertoo teknisen järjestelmän ja valvonnan puutteista. Finanssialan yrityksellä joka lähettää kansainvälisiä rahansiirtopyyntöjä, on oltava sellaiset palomuurit, jotka sallivat vain hyväksyttyä tietoliikennevirtaa sisään ja ulos, sekä antaa selkeän varoituksen, kun yrityksen verkossa liikkuu sellaista tietoa joka ei ole erikseen sallittua.

Henkilöstön osaamisen korostamisella olisi ollut jonkinlainen vaikutus Bangladesh Bankin tapaukseen liittyen, mutta se tuskin olisi pysäyttänyt varkautta kokonaan. Tässä tapauksessa kyse oli jopa valtiollisesta kyberturvallisuuden laiminlyönnistä, lainsäädännöstä lähtien. Yrityksen johdolla on myös tärkeä rooli kyberturvallisuusjohtamisjärjestelmän luomisessa, ylläpitämisessä ja kehittämisen tukemisessa, mikä tässä tapauksessa oli hyvinkin puutteellista. Sisäpiiriläisen mukana oleminen oli myös varsin kriittinen osa varkaudessa, ja todennäköisesti vaikeutti varkauden valmistelun ja toteutuksen havaitsemista ja niihin reagoimista. Tapauksen tärkeimmät yksityiskohdat jäävät kuitenkin asianomistajien ja tapauksessa mukana olevien viranomaisten tietoon, sillä näiden tietojen luovuttaminen julkisuuteen ei ole Bangladesh Bankin etujen mukaista. Näin ollen monet varkauteen liittyvät tiedot ovat pelkkää spekulaatiota, mutta itse tapaus kuitenkin osoitti, etteivät pankkien rahaliikenteet ole mitenkään poissuljettua kohteita kyberrikollisuudessa. Aikaisemmat varkaudet ovat tuoneet rikollisille kymmeniä tuhansia dollareita, mutta tämä tapaus osoitti hyvin konkreettisesti, että miljoonien dollareiden varkaus onnistuu ammattirikollisilta aivan yhtä helposti. Kuvaavaa on myös se, ettei varastettua 81 miljoonaa dollaria ole onnistuttu saamaan takaisin, ja tässä vaiheessa rahat ovat hyvin todennäköisesti onnistuttu pesemään niin, ettei niiden alkuperää voi enää saada selville.

Monet yritykset laiminlyövät kyberturvallisuutta ajattelemalla, että kyseiset asiat eivät koske heitä, tai ajattelevat niitä jopa turhina menoerinä. Valitettava totuus on, että nämä tapaukset tulevat toistumaan vielä moneen kertaan, ennen kuin viranomaisten sääntely ja yritysten

omat panostukset ovat riskien vaatimilla tasoilla. Turvallisuuskenttä on ollut aina kissa-hiiri-leikkiä, mutta vaikka perinteinen fyysinen turvallisuus on monella yrityksillä kunnossa, kyberturvallisuus vaatii edelleen monilta huomattavia panostuksia ennen kuin bittipuolella päästään fyysistä puolta vastaavaan vastustuskykyyn.

3.2 Kyberturvallisuusuhat vuonna 2017

Kyberturvallisuuskenttä on fyysiseen turvallisuuteen verrattuna kohtalaisen uusi, minkä vuoksi käytännön uhat vaihtuvat useasti siitä huolimatta, että keinot niiden torjumiseen ovat lähes samat. Tässä kappaleessa avataan kyberturvallisuuden uhkia yleisesti, sekä henkilöstön osaamisen merkitystä kyberturvallisuusuhkien torjunnassa. Lähteinä käytetään lähimenneisyyden tapahtumia, sekä uutisia ja ammattilaisten artikkeleita.

Monet kyberrikollisuuden muodot käyttävät hyökkäyksissä hyväkseen laitteiden tai organisaation heikkouksia. Teknologiasivustoja selatessa tällaiset tapaukset nousevat herkästi myös otsikoihin, sillä teknologia-alan ihmiset nostavat mielellään esille seikkoja, joissa keskitytään laitteiden ja protokolien heikkouksiin. Isoissa, varsinkin finanssialojen yrityksissä tekniset haasteet ja laitteistojen heikkoudet ovat jonkin verran henkilöstöstä johtuvia riskejä helpompia paikata. Tekniset heikkoudet ovat käytännössä vain tietoteknisten ammattilaisten ongelma, ja on helppo kouluttaa pieni osa henkilöstöstä vain teknisten ongelmien ratkaisuun. Muu henkilöstö on kuitenkin usein todellinen haaste, sillä he joutuvat huolehtimaan kyberturvallisuudesta oman työnsä ohella, jolloin turvallisuus saatetaan nähdä pääasiallista työtä haittaavana hidasteena. Tästä syystä henkilöstö on edelleen monien tietoturvallisuuden ammattilaisten mielestä heikoin lenkki, kuten Steve Culp toi esiin Forbesin artikkelissa (Culp, 2016), eikä tarvitse mennä kovin kauas taakse nähdäkseen yhden käytännön esimerkin ongelman laajuudesta.

Kiristysohjelmien raju leviäminen paitsi yksityiskäyttäjien koneelle, myös yritysten omistamiin laitteisiin oli suuri ongelma vuonna 2016. Kiristysohjelmia on monenlaisia. Yleisesti ottaen haittaohjelma leviää käyttäjän laitteisiin käyttäen joko käyttöjärjestelmien heikkouksia, kuten WannaCryn kiristysohjelman tapauksessa, tai kalasteluviestin avulla, jolloin halutaan saada henkilö itse asentamaan haittaohjelman koneelle häntä huijaamalla tai erehdyttämällä. Kun kiristysohjelma pääsee asentumaan käyttäjän laitteeseen, ne piilottavat tai pahimmissa tapauksissa salaavat käyttäjän tiedostot niin, että vain rikollisten hallussa olevalla salausavaimella saadaan tiedostot auki. Yksityishenkilöille tämä voi merkitä lomakuvien mahdollista katoamista, mutta päästyään yrityksen verkkoihin kiristysohjelma saattaa johtaa merkittäviin tuotannollisiin vaikeuksiin, sekä esimerkiksi kaataa yrityksen julkisen nettisivun. Varsinkin yri-

tyksille halu maksaa on kova, sillä lukitut tiedot ja hidastunut tuottavuus voivat kustantaa yrityksille paljon enemmän kuin mitä rikolliset pyytävät. Mikäli kiristysohjelma salaa tiedostot algoritmilla, on lähes mahdotonta avata tiedostot ilman oikeaa salausavainta.

Tunnetuin tapaus, jossa kiristysohjelma lukitsi suomalaiseen organisaatioon kuuluvan laitteen, sattui helmikuussa 2016. Silloin HUS:in järjestelmissä havaittiin sen historian ensimmäinen kiristysohjelma, kerrotaan Ylen artikkelissa (Rissanen & Koivuranta, 2016). Samassa artikkelissa on myös maininta samanlaisesta tapauksesta samaan aikaan Yhdysvalloissa, missä kiristysohjelma lukitsi Hollywood Presbyterian Medical Centerin tietoverkon. Tiedossa ei ole, oliko kyseessä sama haittaohjelma. Samassa artikkelissa on myös HUS:in oma selvitys tapahtuman kulusta. Tartunta on näkynyt sairaalalle tietoverkon vikana ja IT-yksikkö oli todentanut haittaohjelmahyökkäyksen. HUS oli päättänyt, että nopein ja tehokkain tapa palauttaa järjestelmät ja hallinnolliset toiminnot olivat maksaa lunnaat ja hankkia hyökkääjiltä salausavain. Hyökkääjien vaatimuksena oli 17 000 dollaria, nykykurssilla noin 16 000 euroa, jonka sairaala myös maksoi. Hollywood Presbyterian Medical Center oli artikkelin mukaan ensimmäinen sairaala, joka myönsi maksaneensa hyökkääjälle vaaditut lunnaat.

WannaCry -haittaohjelma on aiheuttanut tuhoja ainakin 74 maassa, kirjoittaa Kokkonen Ylen uutisista (Kokkonen, 2017b). Hyökkäys tuli julki 2017 toukokuussa ja useat sairaalat Britanniassa ovat joutuneet käännyttämään potilaitaan muihin sairaaloihin, sillä potilastietojärjestelmään ei päästä käsiksi (Nurminen, 2017). Muutaman päivän sisällä WannaCry -haittaohjelma oli levinnyt entisestään jo 150 maahan ja yli 200 000 kohteeseen, kertoo EU:n poliisiviranomainen Europol Ylen artikkelissa (Kippo, 2017). Viestintävirasto huomautti Ylen artikkelissa (Strömberg & Jokiniemi, 2017), että haittaohjelma leviää erittäin tehokkaasti yrityksen sisäverkossa. Tästä voidaan päätellä, että ohjelmaa ei levitetä väkisin hyökkäämällä yrityksen palomuuria vastaan, vaan perinteisellä tavalla esimerkiksi roskapostin kautta ja vahinko alkaa monikertaistua vasta, kun haittaohjelma pääsee ensin yrityskäyttäjän omalle koneelle, josta haittaohjelma on helppo levitä muihin yrityksen verkkoihin. Tämä on hyvä esimerkki siitä, että vaikka yritykset keskittäisivät huomattavan suuria resursseja palomuureihin ja palvelunestohyökkäyksien torjuntaan, tällaiset haittaohjelmat jotka leviävät lähinnä sisäisesti käyttäjien huolimattomuuden takia voivat myös tehdä suurta vahinkoa.

Sairaaloihin kohdistuneet hyökkäykset ovat muutenkin herkkiä päätymään otsikoihin, sillä sairaaloiden toiminta on suoraan yhteydessä ihmisten hyvinvointiin. Useimmissa tapauksissa ne ovat myös julkisia toimijoita, joten ne tiedottavat asioista huomattavasti herkemmin kuin monet yksityiset tahot. Uutiset ovat vuonna 2016-2017 raportoineet useihin sairaaloihin kohdistuneita kiristysohjelmahyökkäyksiä, mutta samalla tavalla kyseiset kiristysohjelmat voivat saastuttaa minkä tahansa organisaation tietokoneet. Mielenkiintoista on se, että molemmissa Ylen

artikkeleissa kirjoitetaan, että hyökkäyksessä on hyödynnetty haavoittuvuuksia ja hakkerointityökaluja, jotka on saatu käyttöön Yhdysvaltain turvallisuusvirastoon NSA:han jokin aika sitten kohdistuneessa tietomurrossa. Haavoittuvuus oli tällä kertaa Windows -käyttöjärjestelmässä.

Poliisi, viestintäviraston kyberturvallisuuskeskus, sekä F-Secure ovat laatineet yhdessä kiristysohjelmista kertovat sivuston (2013). Sivustolla listataan pari tunnettua kiristysohjelmaa, kuten CryptoWall ja TorrentLocker, ja annetaan toimintaohjeita, jos joutuu kiristysohjelmien uhriksi. Ensimmäinen mielenkiintoinen asia on lunnaiden summa, sillä Ransomeware – sivuston mukaan tyypillinen summa on 100–150 euroa. HUS:in maksama summa on kuitenkin huomattavasti suurempi. Poliisin ja kyberturvallisuuskeskuksen mukaan ”lunnaiden maksaminen ei kuitenkaan takaa tiedostojen palauttamista ja ainoastaan kannustaa sekä tukee rikollista toimintaa.” ”Älä koskaan maksa rikollisille!”, sivu jatkaa. Kirjoittaja kysyi asiasta muutamilta tietoturvallisuuden parissa työskenteleviltä, ja yleinen kanta oli, että rikollisille maksaminen ei takaa, että he antaisivat salausavaimen vastineeksi. Toisaalta oltiin myös sitä mieltä, että monet rikolliset kohtelevat kiristysohjelmien leviämistä kuin yrityksen johtamista. Heille on taloudellisesti järkevää pidemmällä aikavälillä, jos he antavat salausavaimen vastineeksi lunnaista, sillä muuten kukaan ei maksaisi lunnaita alun perinkään. Tämä ei taas olisi hyvä rikollisten tuotoille.

SonicWallin toimitusjohtaja Bill Connor on kirjoittanut kiristysohjelmista artikkelin Forbes –sivuille, ja hänen mukaansa kiristysohjelmat ovat toistaiseksi levinneet hyvin paljolti sähköpostin liitteenä tai joissakin tapauksissa sähköpostiviestissä olevana linkkinä (2017). Connorin mukaan toisissa tapauksissa kiristysohjelma on voinut levitä myös, kun käyttäjä klikkaa saastunutta mainosikkunaa, jolloin mainokseen piilotettu haittakoodi asentaa ohjelman käyttäjän koneelle. Sähköpostin mukana virus leviää todennäköisesti massaviestinä, eli se voi levitä niin ihmisten henkilökohtaisiin sähköposteihin, kuin työsähköposteihinkin. HUS:in ja Hollywood Presbyterian Medical Centerin tapauksissa ei ole julkistettu, miten kyseisten sairaaloiden koneet olivat saastuneet, mutta Kentuckyssa sijaitseva Methodist Hospital oli saanut järjestelmäänsä samoihin aikoihin vuonna 2016 Lockey –kiristysohjelman (Kiristysohjelma iski taas sairaalaan, 2016), ja tässä tapauksessa oli varmistettu, että kiristysohjelma pääsi sairaalaan järjestelmään sähköpostin liitetiedostosta.

Kiristysohjelmat ovat olleet tavallista isompi ongelma niin yrityksille, kuin yksityisillekin henkilöille siitä syystä, että ne ovat ensimmäisiä todella tuottoisia kyberrikollisuuden muotoja, joita on alettu tarjoamaan Ransomware-as-a-Service, tai RaaS - nimellä tunnettuna palveluna. Tietoturvallisuusyhtiö SonicWallin toimitusjohtaja Bill Conner kirjoitti Forbesin sivuille RaaS:stä artikkelin, missä hän paljasti paitsi haittaohjelman pääasialliset leviämistavat, myös

kiristysohjelmien räjähdysmaisen kasvun (2017). Hän lainaa Armada Cloudin tekemää raporttia kiristysohjelmista (2016) missä arvioitiin, että kun vuonna 2015 maailmassa nähtiin neljä miljoonaa kiristysohjelman hyökkäystä, vuonna 2016 nähtiin jopa 638 miljoonaa kiristysohjelman hyökkäystä. Tämä tarkoittaa 167-kertaista kasvua vain yhdessä vuodessa.

4 Henkilöstön kyberturvallisuusosaamisen tutkiminen

Yritys X:n kyberturvallisuuskoulutukset ovat pääasiassa vapaaehtoisia. Yrityksellä oli tapana lähettää kyberturvallisuuskoulutusten jälkeen osallistujille sähköpostitse palautekysely, johon sai vapaasti kommentoida koulutuksen sisältöä, sekä toiveita tuleville koulutuksille. Vanhasta palautekyselystä oli mahdollista saada palautetta ainoastaan koulutuksiin osallistuneilta. Tämä oli ongelmallista, sillä henkilöstöltä haluttiin myös yleisiä kommentteja heidän kyberturvallisuusosaamisestaan ja toiveista päästä koulutuksiin. Yritys X toivoi tästä syystä, että kirjoittaja tekisi työkalun, jolla henkilöstön kyberturvallisuusosaamista pystyttäisiin kartoittamaan, sekä opettaa ja kerrata asioita, jotka käydään läpi varsinaisissa kyberturvallisuuskoulutuksissa.

Näistä asioista päätettiin kerätä tietoa henkilöstökyselyllä. Henkilöstökyselyn tarkoituksena oli selvittää koko henkilöstön kyberturvallisuusosaamisen taso, heidän mielipiteensä koulutuksista, sekä ehdotukset koulutusten parantamiseen. Yrityksen kyberturvallisuuden parantamiseen henkilöstöosaamisen kautta tarvitaan myös yritys X:n henkilöstöturvallisuuden peilaamista yleisiin standardeihin ja ohjeisiin. ISO/IEC 27001:sta, Katakrista ja VAHTI-ohjeista kirjoitetaan lyhyesti lopussa, jotta voidaan nähdä, mitä yleiset ohjeistukset edellyttävät yrityksiltä. Tämän lisäksi kirjoittaja käytti osana havaintoanalyysiä myös omia havaintoja yritys X:ssä vietetyn työharjoittelun ajalta, joiden tuloksia käytettiin ainakin henkilöstökyselyn vastausten tulkitsemisessa.

Yritys X:n henkilöstölle suunniteltiin ja toteutettiin kyberturvallisuuden henkilöstökysely, jonka tarkoituksena oli saada tietoa vastaajien työsuhteiden laadusta, kyberturvallisuuden osaamisesta, turvallisuussääntöjen noudattamisesta, itsearviointia omasta kyberosaamisesta, sekä palautteita ja toiveita kyberturvallisuuskoulutuksista. Kysely rajattiin koskemaan ainoastaan yritys X:n omia työntekijöitä, vaikka yrityksen verkkoon pääsivät myös monet sidosryhmät, joihin yrityksen kyberturvallisuussäännöt myös liittyvät. Yritys X halusi kuitenkin keskittyä ensin omien työntekijöidensä kouluttamiseen ennen koulutuksen ja kyselyn laajentamista.

Seuraavissa kappaleissa selitetään kyselyn taustat tarkemmin, jonka jälkeen jokainen kyselyssä oleva kysymys käydään läpi ja kerrotaan, minkä takia juuri nämä kysymykset valittiin henkilöstökyselyyn. Tämän jälkeen analysoidaan kyselystä saadut tulokset, mielenkiintoiset

havainnot, sekä annetaan kehitysehdotuksia yritykselle niin kyberturvallisuuden parantamiseksi, kuin itse kyselynkin parantamiseksi, mikäli yritys päättää myöhemmin ottaa kyberturvallisuuskyselyn säännölliseen käyttöön.

4.1 Henkilöstökyselyn rakentaminen

Opinnäytetyön kirjoitusvaiheessa ei löytynyt muita suomalaisia avoimia lähteitä, joissa olisi neuvottu vastaavanlaisen henkilöstölle tarkoitettuun kyberturvallisuuskyselyn teossa. Opinnäytetyössä käytettiin ulkomaalaisia lähteitä, mutta koska jokainen kysely on räätälöity jonkin tietyn organisaation tarpeeseen, lähdemateriaalia muokattiin yhdessä yritys X:n turvallisuuspäällikön kanssa. Pääasiallisena lähteenä käytettiin SANS Instituten sivuilta löytynyttä, opiskelijatyönä tehtyä kyberturvallisuuden henkilöstökyselylomaketta. Kyseessä oli Trenton Bondin työ, jossa hän oli laatinut kyselyn arvioimaan vastaajien turvallisuustietoisuutta (Bond, 2012). Bond oli laatinut 25 kysymystä, joissa jokaisesta vastauksesta sai tietyn määrän pisteitä. Ideana oli, että kaikkien vastaajien vastaukset pisteytetään ja pisteiden mukaan arvioidaan riskitaso asteikolla 1-5. Idea kuulosti hyvältä ja kysymyksetkin olivat hyvin lähellä niitä, jotka tämän opinnäytetyön kirjoittajalla oli mielessä. Tämän kyselyn pohja oli myös kaikista avoimista lähteistä saatavista kyberturvallisuuden kyselypohjista tähän kontekstiin käytännöllisin.

Bondin kyselyssä kysymykset olivat monivalintaformaatissa ja samaa formaattia käytettiin myös opinnäytetyön henkilöstökyselyssä. Henkilöstökyselyyn sisällytettiin monia kysymyksiä, jotka antoivat jonkinlaisen kuvan henkilöstön kyberturvallisuuden osaamistasosta. Monivalintaformaatin nähtiin voivan johtaa siihen, että vastaajat päättelisivät olemassa olevista vastausvaihtoehdoista oikean vastauksen, vaikka heillä ei olisi kysymyksestä tietoa alun perin. Tätä ei kuitenkaan nähty ongelmaksi, sillä kysely oli kaikille avoin, ei kerännyt henkilöiden identiteetistä tietoja, eikä vastaamiseen asetettu aikarajaa. Vastaajat pystyivät halutessaan etsimään oikeat vastaukset verkon kautta, mikäli he halusivat niin tehdä. Kyselyn alustuksena olevassa tekstissä tehtiin hyvin selväksi, etteivät väärät vastaukset aiheuta henkilöille mitään seurauksia. Tämän toivottiin tuovan esiin enemmän rehellisiä vastauksia sen sijaan, että vastaajat etsisivät oikeat vastaukset esimerkiksi internetistä. Monivalinnalla kyselyyn vastaamisesta saatiin helppoa ja nopeaa, mikä oli yksi tärkeä kriteeri kyselyn rakentamisvaiheessa.

Kun lähdemateriaali oli valittu, käytiin yritys X:n turvallisuuspäällikön kanssa kysymykset läpi ja arvioitiin, ovatko kyseiset kysymykset sopivia tähän toimeksiantoon. Yritys X:n turvallisuuspäällikkö antoi todella rakentavia huomioita kysymysten rakentamisvaiheessa. Koska Bondin tekemä kysely oli alun perin englanninkielinen, käännettiin kysymykset suomenkielelle. Tässä vaiheessa syntyi monia ilmaisuja, jotka hiottiin turvallisuuspäällikön avulla sellaisiksi, että ne olisivat helposti ymmärrettäviä yrityksen työntekijöille. Monet kysymykset myös karsittiin,

koska ne arvioitiin epämääräisiksi, eivätkä vastaukset olisi tuoneet kyselylle mitään konkreettista hyötyä. Yksi esimerkki tästä on Bondin kyselyssä kysymys 8, “Kuinka turvallisen tunnet työkoneesi olevan?”. Vaihtoehtoja oli kolme vastausta, ”Erittäin turvalliseksi”, ”Turvalliseksi” ja ”Turvattomaksi”. Pisteitä vastauksista tuli edellä mainitussa järjestyksessä 3, 1 ja 4, ja suuremmat pisteet tarkoittivat suurempaa riskiä. Bond perustelu tämän käytännön niin, että jos henkilö on arvioinut tietokoneen hyvin turvalliseksi, hän saattaa tehdä riskialttiita asioita, jotka vaarantaisivat turvallisuuden, kun taas henkilö, joka arvioi tietokoneen turvattomaksi, saattaa olla oikeassa, mutta samalla käsitellä tietokonetta vähemmän riskialttiilla tavalla. Turvalliseksi arvioiminen taas oli Bondin mukaan paras vaihtoehto ja samalla kertoo pienestä tietoturvallisuuden riskistä. Turvallisuuspäällikkö oli sitä mieltä, ettei henkilökunnan oma arvio tietokoneen turvallisuudesta kerro juuri mitään ja Bondin pisteytykset ja vastaukset tuntuivat täysin mielipuolisilta. Ei ole mitään todisteita siitä, että jos henkilön mielestä oma tietokoneen turvallisuus on ”erittäin turvallinen”, se aiheuttaisi nelinkertaisen riskin siihen verrattuna, että henkilön mielestä oma tietokone on ainoastaan ”turvallinen”. Tämä on totta varsinkin, kun kaikkien työntekijöiden työkoneiden asetukset on asetettu tietoteknisten ammattilaisten toimesta konsernin yhteisen linjan mukaisiksi. Tästä syystä kysymys, sen vastaukset ja varsinkin vastausten arviointi vaikuttivat hyvin hämmentäviltä.

Bondin kysely oli vuodelta 2012 ja yritysten käyttämät tietotekniset ratkaisut ovat muuttuneet viimeisten viiden vuoden aikana paljonkin. Tästä syystä sellaiset kysymykset, jotka teknisesti eivät edustaneet yritys X:n käyttämiä ratkaisuita otettiin myös pois. Esimerkiksi Bondin kyselyssä kysyttiin, onko vastaajan tietokoneen palomuuri kytketty, sekä onko kone asetettu päivittyväksi automaattisesti. Nopeasti ajateltuna nämä olivat erittäin päteviä kysymyksiä ja juuri sellaisia asioita, joita yksityisiä käyttäjiä opastetaan huomioimaan. Yritysmaailmassa on taas täysin erilaiset toimintatavat, sillä monet yritykset käyttävät yhtenäisiä palomuuri- ja virustorjunnan asetuksia, joihin käyttäjät eivät voi vaikuttaa. Nykyään jopa pienet ja keskisuuret yritykset saattavat käyttää tietoturvayritysten tarjoamia loppupäätteen suojauksia, eli Endpoint Protectionia. Näissä ratkaisuissa yritykset voivat jakaa käyttäjiä erilaisiin ryhmiin ja laatia jokaiselle ryhmälle omat säännöt. Säännöissä voidaan erikseen kieltää tai sallia nettisivut, joilla henkilöt pääsevät vierailemaan omilla työkoneilla, sekä asettaa valmiiksi työkoneiden VPN (Virtual Private Network, tai virtuaalinen erillisverkko) -yhteydet. Tämän takia yrityksen työntekijöillä ei ole enää vastuuta päivittää omia viruksentorjuntaohjelmistojaan, tai huolehtia niiden toiminnasta. Samalla tavalla kaikki muutkin päivitykset hoidetaan useissa yrityksissä keskitetysti, sillä esimerkiksi uudet Windows päivitykset voivat aiheuttaa epävakautta yritysten omien ohjelmistojen kanssa. Tästä syystä päivitykset eivät tule laajasti kaikkien tietokoneille ennen kuin yritys on rajoitetusti testannut päivityksen vaikutusta omassa käytössä oleviin laitteisiin. Suuret päivitykset porrastetaan käyttäjien kesken yritysten omien sääntöjen mukaan niin, että mahdollisissa ongelmatilanteissa kaikkien tietokoneet eivät kaadu sa-

maan aikaan. Kuten virustorjunnan ja palomuurien asetuksien kanssa, käyttäjät eivät voi juurikaan vaikuttaa käyttöjärjestelmien tai ohjelmistojen päivityksiin. Tästä syystä yritys X:n turvallisuuspäällikkö olikin sitä mieltä, etteivät teknisten ratkaisuiden takia tällaiset kysymykset sovellu yritys X:lle tehtävään henkilöstökyselyyn.

Samasta syystä poistettiin lopullisesta versiosta myös kysymys, jossa vastaajilta tiedusteltiin, voivatko he asentaa omia ohjelmia työkoneille. Turvallisuussyistä tämä on konsernissa kielletty, mutta koska tätä valvottiin estämällä käyttäjiltä teknisellä menetelmällä ohjelmien asentaminen ilman järjestelmävalvojien oikeuksia, kysymys olisi ollut aivan turha. Vaikka vastaaja olisi vastannut, että hän saisi asentaa omia ohjelmia, tämä ei olisi kuitenkaan ollut mahdollista, joten vastaus ei olisi tuonut yritykselle kyselyyn lisäarvoa.

Yritys X:n toiveiden mukaan muokattiin monia periaatteessa hyviä kysymyksiä, joita Bond käytti omassa henkilöstökyselyssään. Esimerkiksi Bondin kyselyssä oli seuraava kohta: ”Onko pomosi tai kukaan muu työpaikaltasi ikinä kysynyt sinun salasanaasi?”. Tämä kohta oli muuten hyvä ja tärkeä, mutta turvallisuuspäällikön mielestä kysymyksen asettelu ei antanut mahdollisuutta olennaisiin vastauksiin. Olennaista oli se, onko vastaaja ikinä antanut salasanaa muiden käytettäväksi. Tärkeintä ei ole, onko joku ikinä kysynyt salasanaa, vaikka sekin voi olla indikaatio huonosta turvallisuuskulttuurista. Monille nämä kaksi versiota kysymyksistä saattavat kuulostaa samalta, mutta pienetkin erot kysymyksissä voivat tuota suuriakin eroja vastauksissa ja kyselyn tuloksissa.

Monet kysymykset olivat kuitenkin sellaisinaan hyviä Bondin omassa versiossa, kuten lopullisessakin versiossa oleva kysymys ”Käytätkö samaa salasanaa niin yrityksen järjestelmiin, kuin omiin henkilökohtaisiin järjestelmiin, kuten Facebookiin, LinkedIn:iin, tai omiin sähköpostitileihin?” Tämä nähtiin tarpeelliseksi ja se hyväksyttiin kyselyyn yritys X:n toimesta.

4.2 Henkilöstökyselyn kysymykset ja taustat

Tässä kappaleessa esitetään valmis henkilöstökysely, sekä perustellaan miksi kysymykset ovat siinä muodossa kuin ne ovat lopullisessa versiossa. Kyselylomake tehtiin yritys X:n intraan SharePointin omaa kyselypohjaa käyttäen. Jorma Kananen opettaa, että kyselylomakkeen mukana on oltava saatekirje jolla ”lähestytään vastaajaa ja pyritään vastaamisen motivointiin” (2011, 46). Koska kysely tehtiin yrityksen intraa käyttäen, eikä postitettu vastaajille, ennen kyselyä henkilöt pääsivät näkemään käytännössä saatesanoja. Saatesanat pidettiin lyhyinä, jotta ne voitaisiin lukea nopeasti. Tavoitteena oli antaa lyhyt kuvaus kyselystä ja sen myös sen ylläpitäjästä. Oli tärkeää lisätä saatesanoihin tieto ylläpitäjästä siltä varalta, että vastaaja haluaisi ottaa yhteyttä ylläpitäjään lisäkysymyksiä varten. Saatesanoissa annettiin myös lyhyt kuvaus kyberturvallisuudesta, jotta vastaajat tietäisivät, minkä aihealueen kysymyksiin

he ovat vastaamassa, ja jotta keskeiset käsitteet tulisivat tutuiksi ennen kyselyyn vastaamista. Alla on lopullinen versio saatesanoista, jotka näytettiin vastaajille ennen henkilöstökyselyä. Yrityksen nimi on alla korvattu ”yritys X:llä”.

” Tervetuloa kyberturvallisuuskyselyyn! Kyselyä ylläpitää Turvallisuusyksikkö ja sen tarkoituksena on kartoittaa yritys X:n henkilöstön kyberturvallisuustietoisuutta, sekä arvioida kyberturvallisuuskoulutuksen nykytilaa. Kyselyyn vastaaminen kestää n. 10 minuuttia ja se tapahtuu täysin anonyymisti. Kiitos vastauksestasi!

- Mikä on kyberturvallisuus? Kyberturvallisuus voidaan usein tulkita tietoturvallisuuden osana, jossa keskitytään digitaalisten tietojen ja tietoteknisten laitteiden turvaamiseen. Nykyään tietoturvallisuus ja kyberturvallisuus -termejä käytetään kuitenkin usein ristiin, sillä usein niiden rajat ovat hyvin häilyvät. Tässä kyselyssä kyberturvallisuus käsitetään kokonaisuutena, johon kuuluu tietojen turvaamisen lisäksi myös kulunvalvonnan parhaat käytänteet.”

Alla on lopulliset henkilöstökyselyn kysymykset:

1. Kuinka kauan olet ollut yritys X:llä töissä?
    a. 0 – 1 vuotta
    b. 1 – 3 vuotta
    c. Yli 3 vuotta.

Tausta: Kyselyssä haluttiin selvittää, eroaako henkilöstön osaaminen työsuhteen kestosta riippuen.

2. Mikä on työsuhteesi laatu?
    a. Osa-aikainen
    b. Määräaikainen
    c. Vakituinen

Tausta: Tässä kysymyksessä haluttiin selvittää edellisen kysymyksen tavoin, vaikuttaako henkilöstön työsuhteen laatu heidän osaamiseensa.

3. Milloin olet viimeksi saanut kyberturvallisuuskoulutusta, tai suorittanut kybeturvallisuuskursseja?
    a. Alle 6 kuukautta
    b. 6-12 Kuukautta
    c. Yli 12 kuukautta
    d. En koskaan

Tausta: Tässä kysymyksessä haluttiin selvittää, milloin vastaaja oli viimeksi saanut kyberturvallisuuskoulutusta. Yritys X halusi tällä kysymyksellä kartoittaa, milloin vastaajat ovat viimeksi käyneet kyberturvallisuuskoulutuksen, vai ovatko ollenkaan.

4. Tiedätkö keneen ottaa yhteyttä, jos saat työasemaasi haittaohjelman?
    a. Kyllä
    b. Ei

Tausta: Yritys X on tiedottanut monen kanavan kautta prosessin, jota työntekijän pitäisi seurata, mikäli hän epäilee saaneensa haittaohjelman tietokoneelle. Tällä kysymyksellä haluttiin selvittää ovatko opetukset menneet henkilökunnalle perille.

5. Onko työasemasi ikinä ollut saastuneena viruksesta tai troijalaisesta?
    a. Kyllä, työasemaltani on löytynyt haittaohjelmia aikaisemmin.
    b. Ei, työasemani ei ole ikinä saastunut.
    c. En tiedä mikä on virus tai troijalainen.

Tausta: Mikäli henkilö saa koneelle haittaohjelman tai troijalaisen, käyttäjä tulee saamaan joko automaattisen viestin haittaohjelman poistosta, tai yhteydenoton IT-tuelta. Mikäli henkilö ei ole saanut mitään viestiä, hänen työasemansa ei ole saastunut viruksesta tai troijalaisesta. Tässä haluttiin selvittää henkilökunnalta, onko heillä omasta mielestään ikinä ollut virusta tai troijalaista työasemallaan. Tätä tietoa voidaan esimerkiksi verrata IT-tuen tilastoihin saastuneista koneista ja selvittää, onko henkilökunta itse ollut tietoinen kaikista kerroista, jolloin heille on tullut ilmoitus siitä, että heidän työasemansa on saastunut. Vaikka tässä on ollut vaihtoehto, että henkilö ei tiedä mikä on virus tai troijalainen, olisi ollut jälkeenpäin ajateltuna hyvä, jos tähän olisi saanut vielä vastauksen, ettei vastaaja tiedä, onko heidän koneensa ollut ikinä saastuneena vai ei. Tämä huomattiin eräiden vastaajien vapaista kommenteista vastastauksia purkaessa.

6. Oletko ikinä antanut käyttäjätunnuksesi liittyvän salasanan muille?
    a. Kyllä
    b. En

Tausta: Yritys X:llä on selkeä ja hyvin tarkka politiikka siitä, että henkilökunnan käyttäjäprofiilit ovat henkilökohtaisia, eikä kenenkään käyttäjätunnus saisi olla yhteiskäytössä. Tämä on tärkeää väärinkäytösten ehkäisemisessä. Yritys X haluaa olla varma tästä käytännöstä ja tästä syystä kysymys lisättiin, jotta vastauksista saisi selville, onko kukaan jakanut omaa käyttäjätunnusta ja salasanaa muille.

7. Oletko joskus lainannut henkilökohtaisen avaimen/kulkutunnisteen toiselle yrityksen työntekijälle?
    a. Kyllä
    b. En

Tausta: Yritys X:n henkilökunnilla on aina omat henkilökohtaiset sähköisen kulunvalvonnan kulkutunnisteet. Kulkutunnisteet ovat henkilökohtaisia, jotta jälkeenpäin voidaan selvittää, kuka on kulkenut mistäkin mihin aikaan. Tämä on erityisen tärkeää väärinkäytösten ehkäisemisessä. Edellisen kysymyksen tavoin yritys X haluaisi tietää, onko henkilökunta tehnyt tähän sääntöön poikkeuksia.

8. Jos deletoit / poistat tiedoston tai kansion, kaikki tiedot ovat pysyvästi poistettu.
    a. Tosi
    b. Epätosi
    c. En osaa sanoa

Tausta: Kun tiedosto poistetaan kovalevyltä perinteisin menetelmin, ainoastaan tiedoston sijainti poistetaan indekseistä. Käyttöjärjestelmä ei kuitenkaan kirjoita tiedoston yli mitään, joten tiedosto on edelleen luettavissa, mikäli käyttäjä osaa kaivaa kovalevyn piilotetut tiedostot. Tämä on ongelma silloin kun käyttäjä käyttää kannettavaa tietokonetta tai työpuhelinta huolimattomasti ja siinä uskossa, että hän on poistanut tärkeät tiedostot koneelta, tai jos henkilökunta antaa käytöstä poistettuja laitteita yrityksen ulkopuolelle tai ottaa niitä omaan käyttöön ilman, että kovalevyt ovat yrityksen tietoturvallisuuspolitiikan mukaisesti kirjoitettu yli tai tuhottu. Edellä mainitut tapaukset voivat pahimmillaan johtaa siihen, että yrityksen salassa pidettävät tiedot joutuvat ulkopuolisiin käsiin. Tällä kysymyksellä haluttiin varmistaa, että henkilökunta on tietoinen tästä faktasta, tai tästä luettuaan ottaisivat itse selvää asiasta.

9. Miten tunnistaa suojatun yhteyden?
    a. Kun nettisivun osoite alkaa ”http:”llä.
    b. Kun nettisivun osoite alkaa ”https:”llä.
    c. En osaa sanoa.

Tausta: Suojatun yhteyden tunnistaa, kun nettisivun osoite alkaa https:llä, kun taas normaalin suojaamattoman yhteyden tunnistaa, kun nettisosoitteen edessä on ainoastaan http://. Tämä on helppo tapa huomata esimerkiksi väärennettyjä verkkopankkisivuja. Opinnäytetyön tekovaiheen aikana tuli esiin monia tapauksia, joissa oli väärennettyjä yritysten sivuja ja ne olisi voitu huomata siitä, että yhteydet niiden sivulle eivät olleet salattuja. Asiakkaat ovat tiedustelleet asiasta myös yritys X:n henkilökunnalta ja tällä kysymyksellä oli tarkoitus varmistaa, että henkilökunta osaa esimerkiksi tämän esimerkin antamalla neuvoa asiakkaalle, miten he voivat tunnistaa väärennetyn verkkosivun. Henkilökunnan on hyvä myös itse tiedostaa tämä asia, jotta he eivät myöskään lankea väärennettyihin nettisivuihin.

10. Lukitsetko työasemasi aina poistuessasi?
    a. Kyllä, lukitsen sen aina.
    b. En lukitse työasemani, jos poistun vain lyhyeksi aikaa.
    c. Ei, en lukitse työasemani olleenkaan.

Tausta: Yritys X:n henkilökunnan sisäisen verkon tunnukset ovat henkilökohtaisia, eikä muiden ole tarkoitus päästä toisen tunnuksella yrityksen sisäiseen verkkoon. Henkilökunta on yleensä kuitenkin kirjautuneena omiin työasemiin omilla tunnuksilla, eikä aina lukitse omaa työasemaansa kahvitauolla tai kun he käyvät hoitamassa työasioita muualla. Henkilökuntaa on kui-

tenkin useasti ohjeistettu lukitsemaan aina työasemansa, kun he eivät itse ole fyysisesti työasemansa luona. Tällä kysymyksellä haluttiin selvittää noudattaako henkilökunta yrityksen ohjetta.

11. Käytätkö henkilökorttia, kun liikut työpaikan tiloissa? (Muuten kuin kassatoimihenkilönä kassapaikalla)
    a. Kyllä, pidän henkilökortin aina näkyvillä työpaikan tiloissa.
    b. Pidän henkilökorttini työpisteellä, mutta en mukana liikkuessani työpaikan tiloissa.
    c. Pidän henkilökorttini taskussa tai laukussa.
    d. Ei, en pidä henkilökorttia mukana työpaikalla.
    e. En tiedä, missä henkilökorttini on.

Tausta: Yritys X:n työntekijöille ja kaikille vierailijoille annetaan henkilökortti, jota jokaisen yrityksen tiloissa oleskelevien ja liikkuvien pitäisi pitää esillä, jotta voidaan tunnistaa asiattomasti yrityksen tiloissa liikkuvia. Yritys X:n työntekijöille on opetettu tämä asia ensimmäisestä perehdytyksestä lähtien, mutta yritys on sisäisissä tarkastuksissa havainnut puutteita tässä asiassa. Tällä kysymyksellä oli tarkoitus saada selville, kuinka monet pitävät henkilökorttia esillä ja kuinka monet jättävät kortit pitämättä mistäkin syistä.

12. Tiedätkö, mitä tietojen kalastelu, eli phishing on?
    a. Puhelinmyynti, jossa yritetään myydä erilaisia palveluita tai tuotteita
    b. Verkkourkintaa, jolla pyritään samaan haltuunsa luottamuksellisia tietoja rikollisiin tarkoituksiin
    c. Massasähköpostitus, esimerkiksi mainosviestejä osoitteisiin, johon ei ole saatu etukäteislupa
    d. En tiedä

Tausta: Tietojen kalastelu, eli phishing oli hyvin paljon esillä opinnäytetyötä tehdessä. Melkein kaikki ovat myös törmänneet siihen joko työelämässä, tai yksityisessä elämässä. Asiaa on opetettu paljon yritys X:n koulutuksissa ja tällä kysymyksellä oli tarkoitus selvittää, kuinka monella on asia hallussa.

13. Asiakas lähettää sinulle hänen saamansa mahdollisen kalasteluviestin. Mitä teet?
    a. Avaan viestin ja liitteen, jotta voin tarkastaa viestin sisällön.
    b. Poistan viestin avaamatta liitteitä.
    c. Lähetän viestin yritys X:n Phishingmail – postilaatikkoon avaamatta liitettä.

Tausta: Melkein kaikki suomalaiset yritykset ovat saaneet kalasteluviestejä. Yritys X, joka on asiakkaiden kanssa tekemisissä, on erityisen herkkä näille viesteille. Kokemus on osoittanut, että asiakas joka on saanut mahdollisen kalasteluviestin yritys X:n nimissä usein lähettää sen yritys X:n asiakaspalveluun tiedustellakseen asiasta. Tämä on sinänsä asiakkaan puolesta oikein toimittu, mutta tämä asettaa myös paineita henkilökunnalle, jotta he tunnustaisivat tällaisen viestin ja lähettäisivät sen prosessin mukaisesti oikeaan paikkaan tarkistettavaksi. On erityisen tärkeää, ettei yritys X:n työntekijä lähde itse avaamaan viestiä tai sen linkkejä ja selvittämään asiaa, sillä työntekijä saattaa näin toimiessaan saada itse haittaohjelman omalle

työasemalleen. Tällä kysymyksellä haluttiin selvittää, onko henkilökunta tietoisia tästä asiasta, sekä toimivatko he yrityksen sääntöjen mukaisesti.

14. Tiedätkö, mitä toimitusjohtajahuijaus (CEO-fraud) on?
    a. Henkilö, jolla on väärennetyt pätevyydet, hakee toimitusjohtajaksi yrityksiin
    b. Toimitusjohtajan aseman väärinkäyttö
    c. Sähköpostihuijaus, jolla rikollinen tekeytyy jonkun esimieheksi saadakseen uhria lähettämään varoja rikollisen tilille.
    d. En tiedä

Tausta: Vuosina 2015-2016 alkoi toimitusjohtajahuijaus, englanniksi CEO-fraud, rantautumaan myös suomalaisiin yrityksiin. Yritys X oli kouluttanut henkilökuntaa tunnistamaan huijauksen ja tällä kysymyksellä haluttiin selvittää, kuinka hyvin henkilökunta osaa jo tunnistaa kyseistä huijausta.

15. Työasemallani/sähköpostissani ei ole arvokasta tietoa, eikä se kiinnosta rikollisia.
    a. Tosi
    b. Epätosi
    c. En osaa sanoa

Tausta: Finanssialan yrityksen henkilökunnan pitäisi olla hyvin perillä siitä, että heidän työasemillaan ja sähköpostissaan on arvokasta tietoa ja heidän pitäisi toimia näiden tietojen suojaamiseksi tarpeellisella tavalla. Tällä kysymyksellä halutaan selvittää, onko henkilökunta tietoinen näistä seikoista.

16. Onko yritys X:llä sääntöjä siitä, millä nettisivuilla saat työasemallasi käydä?
    a. Ei, saan käydä millä tahansa sivuilla töissä.
    b. Kyllä, meillä on säännöt siitä, millä sivuilla voin käydä, mutta en tiedä niitä.
    c. Kyllä, meillä on selkeät säännöt ja osaan soveltaa niitä käytännössä.

Tausta: Yritys X:llä on selkeät ja näkyvät säännöt, millä sivuilla työntekijät saavat vierailla ja millä sivuilla he eivät saa vierailla. Vaikka monen muun yrityksen tavoin myös yritys X on suojautunut laittamalla tiettyjä internetsivustoja mustalle listalle, jolloin yrityksen koneet ovat estetty vierailemasta niillä. On myös tärkeää, että henkilökunta itse osaa olla vierailematta sivuilla sen takia, etteivät tekniset estot kaikesta huolimatta voi estää kaikkia yrityksen sääntöjen vastaisia sivuja niiden ilmaantuessa, vaan henkilökunnan tarkkuutta vaaditaan yhtä lailla. Tällä kysymyksellä haluttiin selvittää, onko henkilökunta tietoinen yrityksen säännöistä.

17. Käsitteletkö yrityssalaisuuden alaisia tietoja sähköpostitse muutoin kuin yrityksen omassa sisäisessä verkossa?
    a. Kyllä käsittelen.
    b. Ei, en käsittele.

Tausta: Yritys X turvaa tietojen luottamuksellisuuden käsittelemällä luottamuksellisia tietoja sähköpostitse vain yrityksen sisäisessä verkossa. Mikäli luottamuksellisia tietoja lähetetään

asiakkaiden sähköpostiin, viesti voidaan kaapata tiedon liikkuessa. Yrityksellä on omat tekniset ratkaisut siihen, miten asiakkaan kanssa voidaan lähettää luottamuksellisia tietoja muuten kuin sähköpostitse. Tällä kysymyksellä selvitettiin, toteutuuko tämä käytäntö henkilökunnan käytöksessä.

18. Voitko lähettää työsähköpostia omiin sähköpostitileihin (Hotmail, Gmail, Yahoo jne.), mikäli sinulla ei ole pääsyä työsähköpostiisi?
    a. Kyllä voin.
    b. En voi.
    c. En tiedä.

Tausta: Yritys X:n strategia luottamuksellisten tietojen suojaamisessa on se, että tietoja ei lähetetä ikinä suojaamattomia kanavia pitkin, eli sähköpostitse muuten kuin yrityksen sisällä. Tällä kysymyksellä haluttiin varmistaa, että työntekijät ei myöskään käytä omaa sähköpostia yrityksen luottamuksellisten tietojen lähettämiseen niissä tapauksissa, kun oma työsähköposti ei jostain syystä ole käytettävissä.

19. Käsitteletkö yrityssalaisuuden alaisia tietoja ulkopuolisissa ohjelmissa (Esim. Basecamp, Trello)?
    a. Kyllä käsittelen.
    b. En käsittele.

Tausta: Basecampin ja Trellon tapaiset ohjelmat ovat tarkoitettu helpottamaan käyttäjien projekti- ja ajanhallintaa. Kuten edellä mainittiin, yritys X on kuitenkin hyvin tarkka siitä, että luottamuksellisia tietoja säilytetään vain yrityksen omalla palvelimella. Mikäli työntekijä tallentaa huolimattomuuttaan luottamuksellista tietoa yrityksen ulkopuolisille palvelimille tai kolmannen osapuolen ohjelmistoja käyttäen, luottamukselliset tiedot voivat päätyä vääriin käsiin. Tällä kysymyksellä selvitettiin, kuinka suuri osa yrityksen työntekijöistä käsittelee yrityssalaisuuden alaisia tietoja ulkopuolisilla ohjelmilla.

20. Käytätkö samaa salasanaa niin yrityksen järjestelmiin, kuin omiin henkilökohtaisiin järjestelmiin, kuten Facebookin, LinkedIn, tai omiin sähköpostitileihin?
    a. Kyllä käytän.
    b. En käytä.

Tausta: Ihmisten kirjautumistietoja varastetaan jatkuvasti sähköisistä palveluista. Pelkästään vuonna 2016 varastettiin miljardin ihmisen kirjautumistiedot Yahoosta (Goel & Perlroth, 2016), 43 miljoonan käyttäjätiedot Weeblystä (Fadilpašić, 2016) ja 68 miljoonaa salasanaa Dropboxista (McGoogan, 2016), eikä tässä ole kuin pieni osa julkisuuteen tulleista tapauksista. Kun hakkerit saavat käyttäjien salasanat, yleensä niistä tehdään lista ja niitä voidaan käyttää mahdollisissa sanakirjahyökkäyksissä (dictionary attack), joissa salasanaa yritetään murtaa kokeilemalla miljoonia jo tiedossa olevia salasanoja. Mikäli yrityksen työntekijä käyttää samaa salasanaa kuin henkilökohtaisissa palveluissa, ja samasta palvelusta onnistutaan varastamaan

henkilön salasana, tämä asettaisi myös henkilön yritysprofiilin vaaraan. Yritys X on kannustanut henkilökuntaa olemaan käyttämättä samoja salasanoja, joita he käyttävät henkilökohtaisissa palveluissa. Tällä kysymyksellä haluttiin tietää, kuinka suuri osuus henkilökunnasta käyttää edelleen samaa salasanaa henkilökohtaisissa palveluissa ja yrityksen palveluissa.

21. Pidätkö omaa tietoturvallisuustietoisuuttasi tarpeeksi kattavana?
    a. Kyllä pidän.
    b. Osaan perusasiat, mutta lisätieto olisi tarpeen.
    c. En pidä, ja kaipaan huomattavasti enemmän tietoja kyberturvallisuudesta.
    d. En pidä, enkä kaipaa lisätietoja kyberturvallisuudesta.

Tausta: Toinen yritys X:n antamista tutkimuksen tavoitteista oli selvittää, tarjoaako yritys riittävästi koulutusta ja tukea henkilöstön kyberturvallisuusosaamiseen. Yksi mittari oli henkilökunnan oma arvio omasta osaamisesta. Tällä arvioitiin, onko yrityksen tarjoama koulutus riittävää, vai onko lisäkoulutus tarpeen. Viimeinen vaihtoehto annettiin siksi, että voitiin nähdä, onko vastaajissa sellaisia ihmisiä, joita ei kiinnosta oppia kyberturvallisuudesta, vaikka arvioikin omaa osaamista asiassa heikoksi. Mikäli tällaisia työntekijöitä on, se olisi yrityksen näkökulmasta erittäin hälyttävää.

22. Tarjoaako Yritys X riittävästi tietoa kyberturvallisuusosaamisesi varmistamiseksi?
    a. Kyllä, yrityksessä on saatavilla riittävästi tietoa kyberturvallisuudesta.
    b. Ei, en saa yrityksen kautta riittävästi tietoa kyberturvallisuudesta.
    c. (Jos et saa tarpeeksi tietoa, miksi et? Millaisia parannuksia haluaisit?)

Tausta: Tämä kysymys seuraa edellisen kysymyksen mallia ja sen tarkoituksena oli selvittää, tarjoaako yritys X henkilöstön mielestä tarpeeksi tietoa kyberturvallisuusosaamisen varmistamiseksi. Kysymys toteutettiin niin, että mikäli työntekijä valitsi vaihtoehdon b., eli ei saa riittävästi tietoa, hänelle tuli ylimääräinen kysymys tämän jälkeen, jossa hän sai vielä kysymyksen c., eli miksi ei saa, ja millaisia parannuksia hän haluaisi. Tällä haluttiin antaa henkilökunnalle mahdollisuus kertoa vapaasti mielipiteitä ja toiveita yrityksen tarjoamiin kyberturvallisuuskoulutuksiin ja -tietoihin liittyen.

23. Vapaa kommenttikenttä

Tausta: Edellisen kysymyksen c. vaihtoehto tarjosi vapaata kommentointia ainoastaan heille, jotka valitsivat vaihtoehdon b. Muille ei ollut vaihtoehtoa kommentoida vapaasti, joten kysymys 23:n tarkoitus oli antaa kaikille vielä mahdollisuus kommentoida mitä tahansa yritys X:n kyberturvallisuuskoulutuksiin ja muihin käytännön asioihin liittyvää. Tämä kysymys käytettiin myös siihen, että henkilöstö sai kommentoida myös itse kyselyä ja sen toteutusta, sekä antaa vinkkejä kyselyn kehittämiseen, tai tuoda sen puutteet esille.

4.3 Toteutus ja tulokset

Kyberturvallisuuskysely toteutettiin syksyllä 2016 ja se tallennettiin yritys X:n intraan turvallisuusyksikön sivun alle. Kyselystä tiedotettiin intran etusivun uutisissa. Kyselyä pidettiin auki kaksi viikkoa, sillä yritys X oli havainnut kokemuksesta, että sitä pidempään auki olleet kyselyt eivät enää houkutelleet vastaajia. Ennen kyselyn julkaisua kyselylle saatiin viisi vastaajaa, jotka tekivät sen alusta loppuun ja antoivat palautteita kysymyksistä ja vastauksista. Kommenttien avulla kyselyä muokattiin vielä viimeisen kerran ennen julkaisua, jonka jälkeen kysely julkaistiin kaikille yritys X:n työntekijöille.

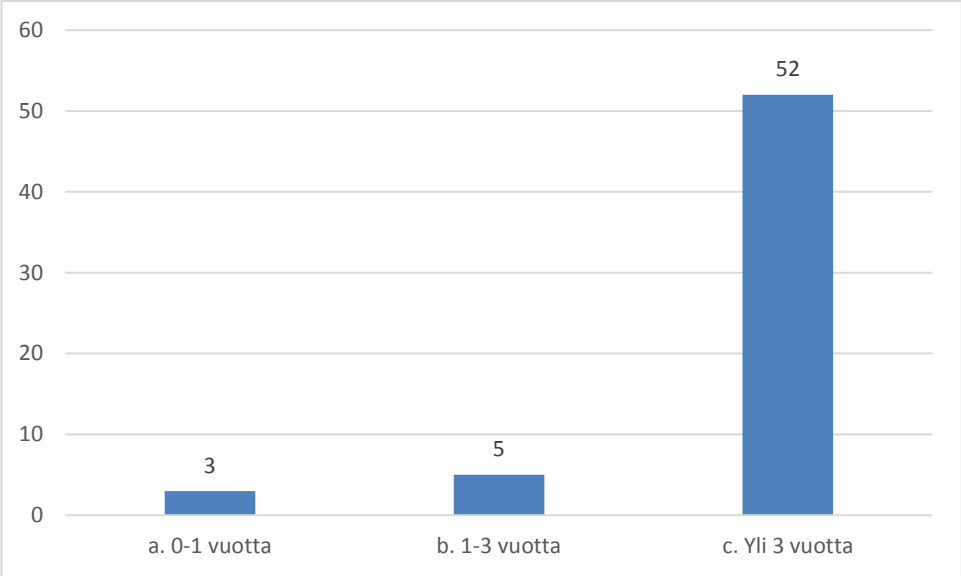
Kysely sai lyhyessä ajassa 60 vastausta ja tässä kappaleessa analysoidaan sen tuloksia laadullisin menetelmin. 60 vastausta on isossa yrityksessä hyvin vähän. Esimerkiksi vain 3 henkilöä on vastannut työskentelevänsä yritys X:ssä alle vuoden verran. Näin ollen on mahdotonta analysoida esimerkiksi alle vuoden yrityksessä työskennelleiden kyberosaamista, sillä vastaajat eivät riitä. Opinnäytetyössä keskityttiin tämän takia sellaisten vastausten tulkintaan, joihin saatiin riittävä määrä vastaajia.

Laadullisessa tutkimuksessa tutkimustulokset yhteismitallistetaan ja tiivistetään sopivaan tekstimuotoon (Kananen 2014, 99). Tässä tapauksessa tutkimuskysymykset saatiin raakadatana Microsoftin SharePointista Excel-muotoon, josta laskettiin ja tallennettiin jokaisen vastauksen määrä. Avoimet vastaukset kerättiin myös yhteen Word tiedostoon, josta pystyttiin helposti lukemaan ne kaikki ja etsimään yhteisiä tekijöitä.

Vastausten analyyseissä käytettiin prosentteja sen sijaan, että tuloksissa olisi esitetty tiettyjen vastausten todellinen lukumäärä. Tämä tehtiin helpottamaan tulosten esittelyä, sillä prosentit auttavat hahmottamaan yrityksen kannalta oikein vastanneiden osuuden suuruuden paremmin.

Koko kysymys- ja vastausluettelo vapaita kommentteja lukuun ottamatta on liitteenä opinnäytetyön lopussa. Vapaat kommentit analysoitiin ja niiden tulokset kerrotaan opinnäytetyössä, mutta itse vastauksia ei liitetty mukaan opinnäytetyöhön, sillä ne sisälsivät yrityssalaisuuden piiriin kuuluvia asioita, ja olisivat voineet paljastaa toimeksiantoyrityksen.

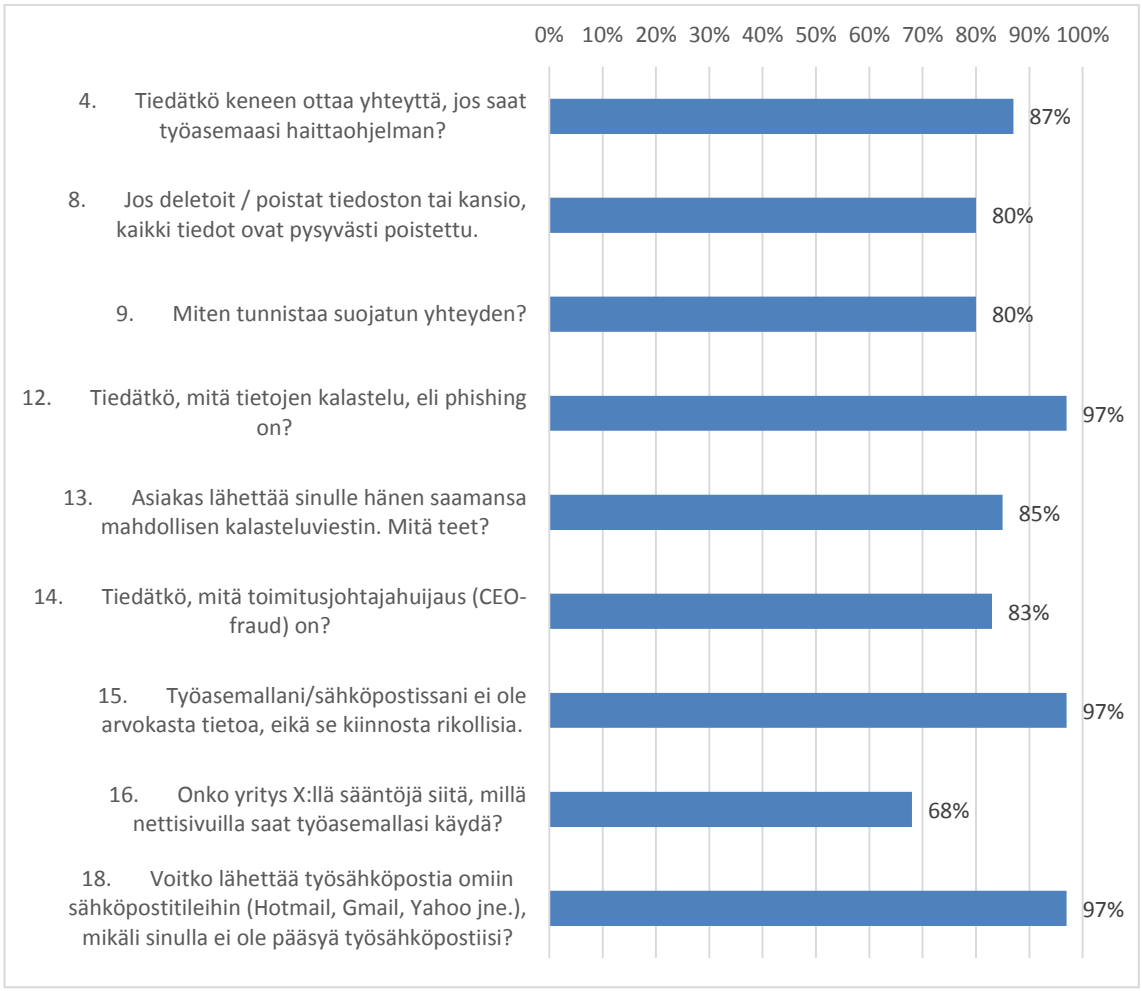
Osa vastauksista esitetään itsenäisinä kuvioina tuloksista, mutta suurin osa kerättiin kategorioittain yhteen ja tuloksissa esitetään vain oikean tai toivotun tuloksen määrää prosentuaalisesti. Avoimessa tulkinnassa avataan tuloksia enemmän, mutta kuvioiden on tarkoitus antaa selkeää tietoa nopeasti.



Kuvio 1: Henkilöstön työsuhteen kesto

Ensimmäinen tulos ei sisältänyt uutta tietoa, mutta antoi hyvän kuvan henkilöstön pysyvyydestä finanssialalla. Tämä antoi myös hyvän lähtökohdan opinnäytetyössä olevalle henkilöstökyselylle, sillä jos sitä tultaisiin toteuttamaan säännöllisesti, niin yritys kuin työntekijätkin voivat saada hyvän kuvan henkilöstön kehittymisestä. Myös vakituisten työntekijöiden määrä oli kaikista vastaajista 95%, mikä tukee työsuhteiden jatkuvuuden linjaa ja antaa hyvän lähtökohdan henkilöstöosaamisen kehittämiselle ylipäätään.

Kun edelliset lähtökohdat kertoivat lähinnä henkilöstön jatkuvuudesta yrityksessä, seuraavat kysymykset mittaavat henkilöstöosaamista konkreettisemmin. Kysymysten oli tarkoitus mitata, kuinka hyvin henkilöstö oli tietoisia kyberturvallisuusuhista ja termeistä, sekä yritys X:n säännöistä. Vastauksissa esitetään oikeat ja yrityksen haluamat tulokset prosentteina. 100% tarkoittaisi sitä, että kaikki vastaajat osasivat vastata oikein. Kuvion alla avataan enemmän jokaista kohtaa erikseen.



Kuvio 2: Henkilöstöosaamisen osio

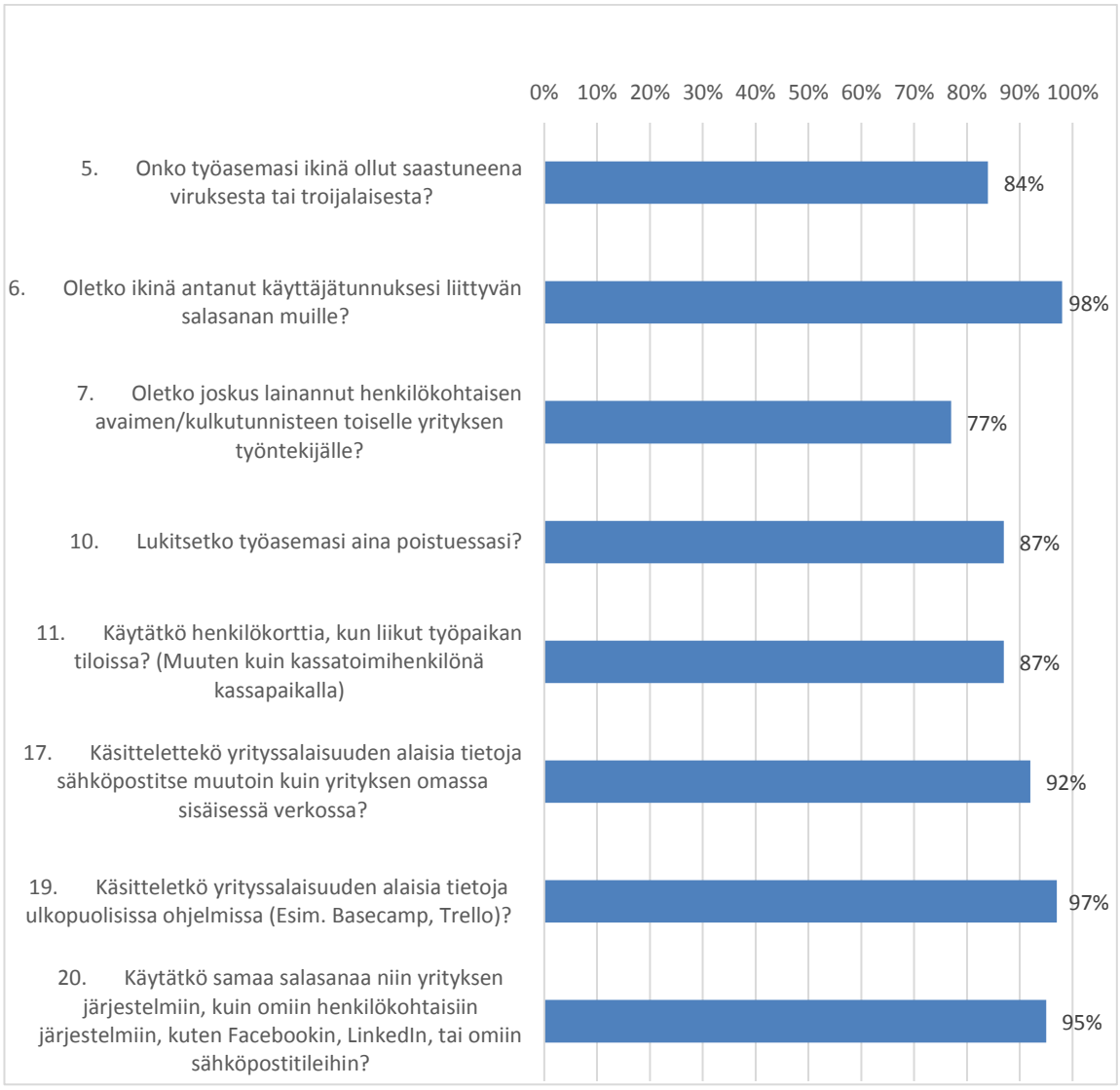
Yllä olevasta kuviosta näkee hyvin henkilöstöosaamisen tasot eri kysymyksissä. Kysymysten ei ollut tarkoitus olla vaikeita, vaan ajankohtaisia ja tärkeitä kyberturvallisuuden kannalta. Valitut kysymykset olivat siis sellaisia, joita henkilöstön pitäisi lähtökohtaisesti osata, jotta yritys X voisi saavuttaa korkeimman tavoitellun kyberturvallisuustason. Vastauksista päätellen henkilöstö on osannut vaaditut asiat pääosin erittäin hyvin. Yritys X piti yli 80% osaamistasoa erinomaisena, vaikka kehitettävää onkin.

Tilastollisesta näkökulmasta asiat vaikuttivat olevan hyvin, eikä alle 80% tuloksen alle mennä kuin ainoastaan kysymyksessä 16. Ainoastaan 68% vastaajista tiesi yritys X:n säännöt siitä, millä sivuilla saa vierailla, ja osasi myös soveltaa niitä. 30% vastaajista tiesi, että yrityksellä on säännöt, mutta eivät tienneet sääntöjä, mikä oli hyvin huolestuttavaa. Ainoastaan 2% vastaajista ei tiennyt, että yrityksellä ylipäätään on mitään sääntöjä. Tämä asia vaatii ehdottomasti lisätutkimusta siitä, minkä takia 30% vastaajista tietää säännön olemassaolon, mutta ei

ole onnistunut syystä tai toisesta löytämään oikeita sääntöjä. Lähtökohtaisesti yrityksen näkökulmasta olisi hyvä korostaa tätä asian tulevissa koulutuksissa, sekä luoda säännöt niin, että niitä olisi helpompi löytää yrityksen omilta sivuilta.

Kirjoittajan kokemus omilta ajoilta yritys X:ssä antoi sellaisen kuvan, että henkilöstön luottamus teknisiin kyberturvallisuusratkaisuihin oli hyvin suuri ja lähtökohtaisesti henkilöstö toivoi, että turvallinen työskentely pitäisi kyetä takaamaan heistä riippumatta. Tähän on voinut vaikuttaa se, että yrityksellä on käytössä teknisesti toteutettu loppukäyttäjänhallintajärjestelmä, mikä ohjelmallisesti estää työntekijöiden vierailun kielletyillä sivuilla. Tällainen järjestelmä ei kuitenkaan pysty sataprosenttisesti estämään kaikkia haitallisia sivuja. Tästä huolimatta työntekijöille saattaa tulla jopa valheellinen turvallisuudentunne, kun he vahingossa menevät joillekin sivuille ja saavat heti ilmoituksen, että kyseinen sivu on estetty yrityksen turvallisuuspolitiikan mukaisesti. Se saattaa antaa kuvan henkilöstölle siitä, että yrityksellä on säännöt millä sivuilla saa vierailla ja millä ei, mutta vapauttaa samalla henkilöstön tietämisen vastuusta, sillä teknisesti pääsy kielletyille sivuille estettiin siitä huolimatta, tiesikö käyttäjä syyn vai ei.

Jatkokehityksen kannalta yritys X:n olisi hyvä saada esimerkiksi IT-osastolta tilastoa, kuinka suuri osa yrityksen verkossa tapahtuvasta verkkoselailusta johtaa turvallisuuspolitiikan mukaisesti kielletyille sivuille, jotta voidaan saada käytännön kuvaa siitä, onko ongelma suuri vai ei. Tämän toteuttaminen käytännössä olisi kuitenkin suuri työ, sillä yritys X on osana isompaa konsernia, jonka vuoksi verkkoliikenteen hallintaa ei tehdä paikallisesti, vaan osana koko konsernin verkkoliikenteen hallintaa. Tiedon selvittäminen vaatisi konsernintason päätöksiä, joten opinnäytetyötä tehdessä tämä ei olisi ollut mitenkään mahdollista. Mikäli konserni kuitenkin päättäisi jossain vaiheessa analysoida tällaisia tuloksia, se antaisi hyvin paljon tietoa siitä kuinka hyvin ihmiset osaavat välttää omalla käytöksellään kielletyillä sivuilla vierailua, ja kuinka paljon luotetaan edelleen pelkkiin teknisiin ratkaisuihin, jotka estävät käyttäjää tekemästä virheen.



Kuvio 3: Henkilöstökäyttäytyminen

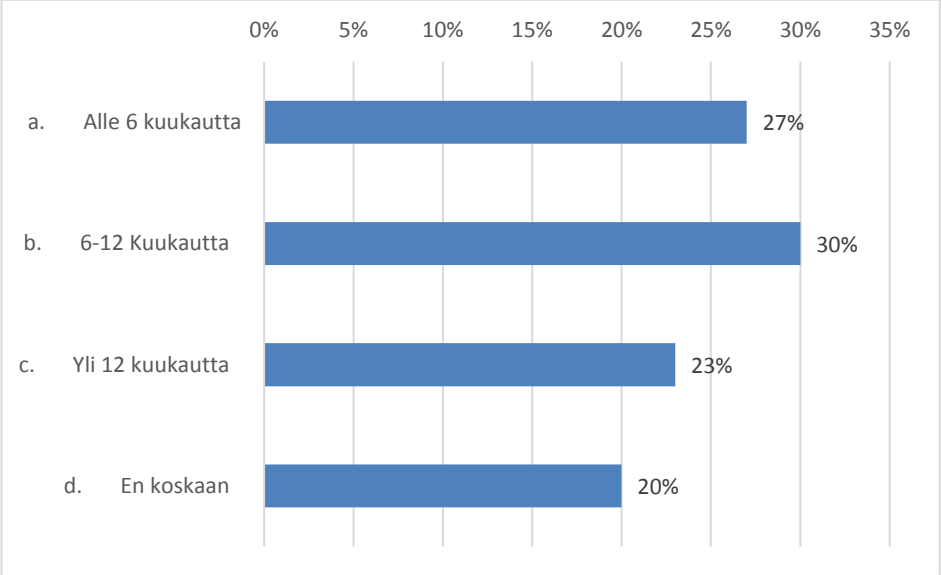
Kun edellinen kuvio käsitteli kyselyn vastauksia henkilöstöosaamisesta lähinnä tietämyksen näkökulmasta, kuvion 3 kysymykset luotiin antamaan vastauksia henkilöstön käyttäytymisestä. Tärkeimmät erot olivat, että edellisissä kysymyksissä kysyttiin osaamista ja tietoa, mutta tässä kuviossa haluttiin tietää, käyttäytyykö henkilöstö yritys X:n turvallisuussääntöjen mukaisesti. Suurin osa näistäkin vastauksista ylitti 80% oikeiden vastausten rajan, mutta näistä kysymyksistäkin voitiin päätellä monia mielenkiintoisia asioita.

Ensimmäinen huomio kiinnittyi siihen, että jopa 16% vastaajista raportoi, että heidän työasemallaan on havaittu joskus virus tai troijalainen. Tämä voi ensisilmäyksellä näyttää todellista pahemmalta, mutta se ei esimerkiksi kerro, kuinka montaa kertaa henkilön työasemalla on havaittu haittaohjelmia, tai milloin viimeksi tämä on tapahtunut. Mikäli henkilön työasemalla on kerrankin ollut virus tai troijalainen yritys X:llä työskennellessä, hän raportoisi sen tähän.

On huomioitava, että yli 87% vastaajista on ollut yritys X:llä pidempään kuin 3 vuotta, ja monilla on saattanut olla virus vain kerran koko työuransa aikana. Vaikka kertakin on tavallaan liikaa, riskienhallinnan kannalta tämä ei kuitenkaan ole odottamatonta tai kriittistä millään tavalla. Tämä ei myöskään ole puhtaasti negatiivinen asia, sillä kirjoittaja keskusteli tästä erään yritys X:n työntekijän kanssa, jolla oli vuosia sitten yhden kerran virus omalla työasemalla ja hän muisti tarkalleen, miten tapaus eteni. Tämä tapahtuma oli paitsi opettanut henkilölle, miten yrityksen viruksentorjunta tapahtui käytännössä, myös korotti hänen valppauttansa tulevissa tapauksissa, ja niiden ennaltaehkäisyssä. Koska tämä oli ensimmäinen kyberturvallisuutta koskeva henkilöstökysely koko yrityksessä, tällä kysymyksellä haettiin yleistä kuvaa siitä, kuinka monella on ollut virus työasemalla. Mikäli asiaa haluttaisiin tutkia enemmän, voidaan esimerkiksi tulevissa kyselyissä kysyä, milloin vastaajalla on viimeksi havaittu virus tai muu haittaohjelma työasemalla. Tämä antaisi enemmän osviittaa pidemmällä aikavälillä siitä, saastuvatko yrityksen työasemat nykyään enemmän vai vähemmän. Mikäli asiaa haluttaisiin tutkia enemmän tekniseltä puolelta, voidaan ottaa raportit jokaisesta saastumistapauksesta ja tutkia, kuinka kauan kesti, ennen kuin haittaohjelma huomattiin, tai mistä haittaohjelma oli tullut yrityksen työasemalle. Nämä vaatisivat teknisen puolen asiantuntemusta, sekä jälleen kerran laajemmat tilastot konsernilta, mutta voisivat antaa paremman kuvan siitä, miten tällaisia uhkia voitaisiin tulevaisuudessa torjua paremmin.

Toinen huomionarvoinen asia oli henkilöstön pitäminen kyberturvallisuutta näennäisesti tärkeämpänä kuin fyysistä turvallisuutta. 98 % vastaajista ei ollut ikinä antanut käyttäjätunnukseen liittyvän salasanaa muille, mutta ainoastaan 77% vastaajista oli pitänyt oman kulkutunnisteen itsellään. Tämä kysymys on valitettavasti kuitenkin vaikea tulkita tässä muodossa. Vaikka henkilöstökyselyn alkuvaiheessa tämä tuntui hyvin olennaiselta kysymykseltä ja periaatteessa henkilökohtaista avainta ei saa luovuttaa työkaverille käytettäväksi, totuus on kuitenkin toinen monessa pienemmissä toimipisteissä, jossa kulunvalvonta on toteutettu paljon yksinkertaisemmalla tavalla. Mikäli kyseessä on pelkkä kova-avain, henkilöstö ei välttämättä assosioi sitä yhtä henkilökohtaiseksi kuin sähköinen kulunvalvonta siitä huolimatta, että molemmissa voi olla sähköinen kulunvalvonta ja -loki. Vaikka yrityksen sääntö yksiselitteisesti vaatii jokaista käyttämään vain henkilökohtaisia avaimia ja kulkukorttia, pienemmissä toimipisteissä joissa on vain muutama työntekijä ei välttämättä nähdä kulunvalvonnan ideaa aivan samalla tavalla kuin paikassa, jossa työskentelee montaa sataa työntekijää. Riskit ovat myös erilaiset erilaisissa paikoissa, vaikka ymmärrettävästi yritys X tai konserni kokonaisuudessaan ei voi tehdä poikkeuksia sääntöihin isoissa tai pienissä toimipisteissä. Vaikka oman kulkutunnisteen tai avaimen luovuttaminen jollekin toiselle voi olla yhtä vaarallista kyberturvallisuuden kannalta kuin käyttäjätunnuksen ja salasanan luovuttaminen, käytännössä sitä ei nähdä samalla tavalla vastaajien joukossa, ja jatkossa yritys X:n kannattaisikin tutkia ilmiötä tarkemmin laadullisilla menetelmillä, jotta saadaan juurisyy selville.

Seuraavat osiot käsittelevät viimeistä osa-aluetta, eli koulutuksia. Koska tässä osiossa ei ollut oikeita tai vääriä vastauksia, tullaan kysymykset avaamaan yksitellen. Tämän lisäksi avoimista vastauksista otetaan pääelementit ja niistä tehdään lyhyt analyysi.



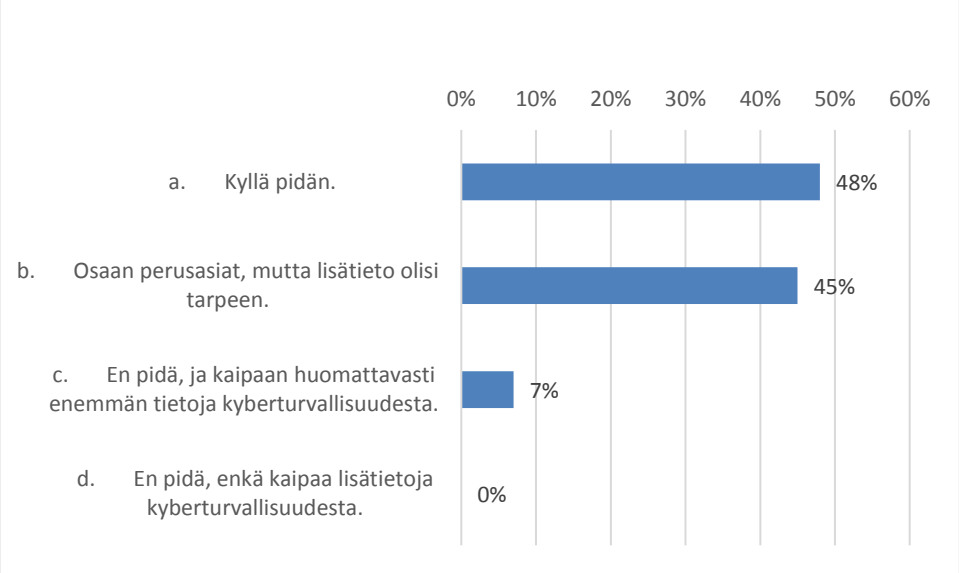
Kuvio 4: Milloin vastaaja viimeksi saanut kyberturvallisuuskoulutusta, tai suorittanut kybeturvallisuuskursseja

Kuvion 4:n vastaukset heijastivat osaltaan karuakin kuvaa kyberturvallisuuskoulutuksiin osallistumisesta yritys X:ssä. Sekä ajasta, että muista resursseista johtuen opinnäytetyön teon hetkellä yritys X:n henkilöstön ei ollut pakko osallistua kyberturvallisuuskoulutuksiin, vaikka kyberturvallisuudesta puhutaankin heti työntekijöiden perehdytyksen alussa. 20% kaikista vastaajista ja jopa 23% yli 3 vuotta työsuhteessa olleista eivät olleet omien sanojensa mukaan käyneet missään kyberturvallisuuskoulutuksissa. Tämä osoitti selkeästi, että työsuhteen pitkä kesto ei takaa sitä, että työntekijä olisi käynyt edes kerran yritys X:n järjestämässä kyberturvallisuuskoulutuksessa. Tämän lisäksi kaikista vastaajista 14% oli käynyt kyberturvallisuuskoulutuksen yli 12 kuukautta aikaisemmin.

Yritys X:n linja on ollut se, että jos työntekijä ei käy edes kerran vuodessa missään kyberturvallisuuskoulutuksessa, hänen ei voida olettaa osaavan aiheesta enää mitään. Monet voivat olla sitä mieltä, että vuosikin on liikaa. Tässä kohtaa on kuitenkin hyvä muistaa jälleen kerran, että kyberturvallisuus ei ole prioriteetti suurimmalle osalle työntekijöistä, vaan yksi osa sivutehtävistä. Hyvä puoli oli kuitenkin se, että yli puolet, eli 57% vastaajista oli käynyt kuitenkin kyberturvallisuuskoulutuksen vuoden sisällä. Tätä kaikkea piti kuitenkin vielä heijastaa henkilöstöosaamiseen ja käyttäytymiseen, joiden tulokset olivat lähes poikkeuksetta hyvät. Vaikka henkilöstöosaamisen kysymykset olivat kohtuullisen helppoja ja yksinkertaisia, tämä

heijasti kuitenkin useiden yritysten tavoitteita henkilöstöosaamisesta. Tuskin missään finanssialan yrityksissä yritetään kuitenkaan kouluttaa kaikista työntekijöistä kyberturvallisuuden ammattilaisia, vaan pelkkä kybertietoisuus ja kiinnostus riittävät jo pitkälle.

Yksi käytännöllisempi syy siihen, miksi niin monet eivät olleet käyneet edes kerran vuodessa kyberturvallisuuskoulutuksessa, oli koulutusten sijainti. Koulutuksia ei järjestetä ympäri Suomea, joten aina jää joku, joka ei päässyt paikan päälle. On olemassa itseopiskelumateriaaleja kyberturvallisuudesta, mutta se ei ole sama asia, kuin oikeassa koulutuksessa käyminen. Tämä on sellainen ongelma, mihin olisi hyvä löytää ratkaisuja, mutta onko se etäkoulutus, mihin osallistujat voisivat kuitenkin osallistua sijainnista riippumatta, vai jotain muuta, jää yritys X:n ratkottavaksi.



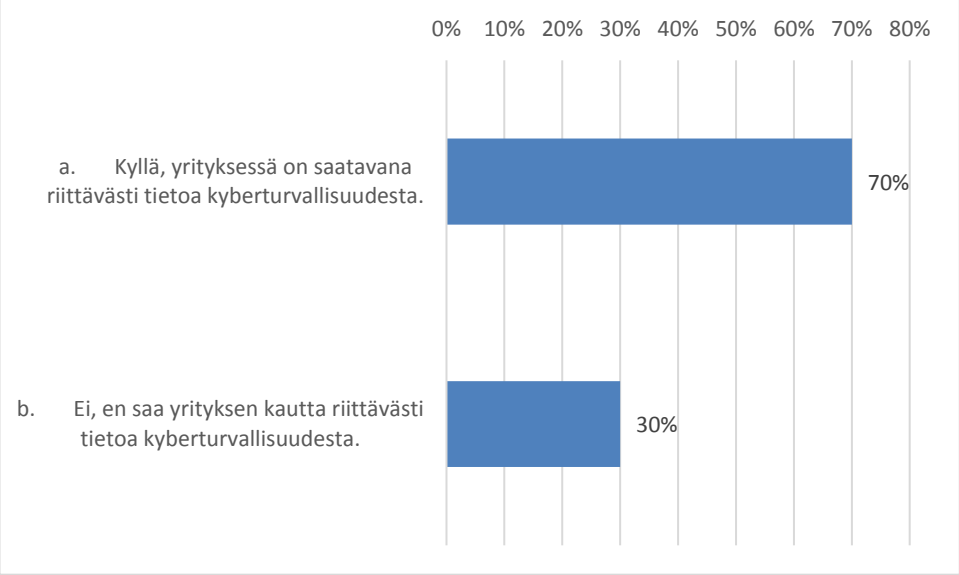
Kuvio 5: Pitävätkö vastaajat omaa tietoturvallisuustietoisuutta tarpeeksi kattavana

Kuvio 5:sta voi nähdä, 48 % vastaajista piti omaa kyberturvallisuustietoisuutta riittävänä, 45 % osasi vastausien perusteella perusasiat ja vain 7% henkilöstöstä oli sitä mieltä, että he kaipaisivat huomattavasti enemmän tietoja kyberturvallisuudesta. Vastaus D oli muotoiltu erittäin provosoivasti, joten ei liene yllätys, että siihen ei kukaan vastaajista sortunut.

Yllättävää oli sen sijaan se, että jos mukaan otettiin vastauksia pelkästään henkilöiltä, jotka olivat käyneet kyberturvallisuuskoulutuksen viimeksi joko yli 12 kuukautta sitten, tai eivät olleet käyneet sitä olleenkaan, myös heistä tasan 48 % piti omaa kyberturvallisuustietoisuutta riittävänä. Heistä 12 % kaipasi huomattavasti enemmän tietoa kyberturvallisuudesta, kun taas koko vastaajaryhmästä 7 % kaipasi huomattavasti enemmän tietoa. Vastaajaryhmä oli sen verran pieni, että tämäkin ero voisi mahdollisesti tasoittua, mikäli vastaajia olisi ollut huomatta-

vasti enemmän. On vaikea tietää mistä johtuu, että ihmiset jotka eivät olleet käyneet kyberturvallisuuskoulutuksissa pitkään aikaan pitivät omaa osaamistaan yhtä riittävänä kuin muutkin. Kyseessä voi olla henkilöstökyselyn helppous, mutta jatkoa varten olisi erittäin mielenkiintoista tutkia pelkästään henkilökunnan asennetta kyberturvallisuutta ja myöskin omaa osaamista kohtaan.

Nämä tulokset antavat myös yritys X:n turvallisuusyksikölle syytä lisätä esimerkiksi kyberturvallisuuskoulutuksia, sillä alle puolet piti omia taitoja tarpeeksi kattavina. Tämä luku olisi voinut olla erilainen, mikäli vastaajia olisi saatu enemmän, mutta jos alle puolet piti omia taitoja tarpeeksi kattavana, tehtävää on vielä paljon. Tämä luku ei yksinään silti kerro kaikkea, vaan sitä peilattiin vielä vapaisiin kommentteihin, sekä muihin olennaisiin tietoihin.



Kuvio 6: Tarjoaako yritys X riittävästi tietoa vastaajien kyberturvallisuusosaamisen varmistamiseksi

Tämä osio oli yritys X:lle hyvin tärkeä ja pisteet olivat hyvät, mutta eivät erinomaiset. Kuten edellisissä vastauksissa nähtiin, vain 48% piti omaa kyberturvallisuuden tietämystä tarpeeksi kattavana. Silti 70% vastaajista oli sitä mieltä, että yrityksessä on saatavana riittävästi tietoa kyberturvallisuudesta. Tähän voi olla monia syitä, mistä päästään vapaiden kommenttien ja vastausten vertailuun.

Neljä vastaaja oli jättänyt avoimia kommentteja kyselyn lopussa, jonka lisäksi kaikki, joiden mielestä he eivät saaneet yrityksen kautta riittävästi tietoa kyberturvallisuudesta olivat voineet jättää ylimääräisen kommentin siitä, miksi he eivät mielestään saa tarpeeksi tukea. Yrityssalaisuuden ja toimeksiantoyrityksen salassapidon vuoksi avointen vastausten sisältöä ei julkistettu sellaisenaan, mutta tässä osiossa analysoitiin niiden sisältö niiltä osin, kuin opinnäytetyön kannalta oli olennaista.

Monet vastaajat olivat kommentoineet avoimeen vastaukseen siitä, miksi he eivät mielestään saa yritys X:ltä riittävästi tietoa kyberturvallisuudesta. Vaikka eräskin vastaus oli ”En osaa sanoa tarkkaan”, monet vastaajat pystyivät antamaan hyvinkin kehittäviä kommentteja. Yksi yleinen esille noussut teema oli uusimpien kyberturvallisuusuhkien tiedottaminen henkilöstölle. Monet pitivät yritys X:n intrassa julkaistavia uutisia liian epäsäännöllisinä ja kuivina. Monet myös kaipasivat uhkien rinnalle konkreettisia vinkkejä niiden torjuntaan ja monet olivat sitä mieltä, etteivät he usko osaavansa toimia oikein omissa työtehtävissään kyberuhkien torjumiseksi. Eräs vastaaja esitti myös, että koulutusten pitäisi olla proaktiivisia ja kohdistua uusimpiin uhkiin. Hän koki, että liian usein yrityksen koulutukset sisälsivät uhkia, jotka olivat jo iskeneet, jolloin koulutus oli jo myöhäistä. On huomioitava, että kyberturvallisuudessa uhat eivät ole sidoksissa maantieteellisiin alueisiin, joten ne leviävät huomattavan nopeasti. Tämä vaikeuttaa kyberturvallisuuskoulutuksissa esitettyjä tulevien aiheiden esittämistä, sillä useimmiten kun uusimmista uhkista osataan kouluttaa tarpeeksi kattavasti, ne ovat jo valloillaan digimaailmassa. Yritys X:ssä koulutuksia voidaan suunnitella jopa puoli vuotta aikaisemmin, mutta joskus muutama päivä ennen koulutuksen alkua saattoi ilmentyä sellaisia asioita, jotka muuttivat olennaisesti koulutusmateriaalin sisältöä. Näin koulutukset vaativat hyvin paljon ajallista resurssia koulutuksen päivittäjältä, jotta ajankohtaisia trendejä pystytään seuraamaan ja tiedottamaan henkilöstöä heidän vaatimistaan ajankohtaisista kyberturvallisuusuhkista.

Myöskin uudet teknologiat nousivat vastauksissa esille, sillä monet toivoivat myös matkapuhelimien suojaamiseen liittyviä koulutuksia. Vanhoja asioita olivat massamuistien turvallinen käsittely ja eräs työntekijä toivoi sen korostamista tulevissa koulutuksissa.

Kyberturvallisuuskoulutuksia toivottiin myös järjestettävän säännöllisemmin. Yritys X:ssä oli säännöllisesti rahoitusalan koulutuksia, ja samaa toivottiin kyberturvallisuuskoulutuksista. Rahoitusalan koulutuksia oli ollut luonnollisesti enemmän, sillä se on yritys X:n pääasiallinen toimialue, kun taas turvallisuuden osa-alueet ovat aina pelkkiä tukitoimintoja. On kuitenkin tärkeää huomata, että henkilöstö heräsi vaatimaan säännöllisempiä koulutuksia ja tästä saatiin dokumentaatio. Kyberturvallisuuskoulutukset ovat aina pois työntekijöiden päätoimisesta työtehtävästä, joten niistä koituu aina myös konkreettisia kustannuksia. Kustannukset muodostuvat yritys X:ssä muun muassa työntekijän koulutusajan palkasta, hänen sijaisensa palkasta, matkustuskustannuksista ja itse koulutuksen erilaisista kustannuksista. Jotta koulutuksia voitaisiin lisätä, olisi myös tärkeää saada yritykselle dokumentoituja toiveita ja vaatimuksia lisäkoulutuksista, joita tästä henkilöstökyselystä saatiin. Mielenkiintoisena seikkana eräs vastaaja kirjoitti, että hänen mielestään kyberturvallisuuskoulutuksia pitäisi olla 1-2 kertaa vuodessa. Tämä sopi yhteen yritys X:n omienkin linjojen kanssa, jotka mainittiin opinnäytetyössä aikaisemmin. Tämän linjauksen mukaan työntekijän olisi hyvä osallistua ainakin kerran vuodessa

kyberturvallisuuskoulutukseen, jotta osaamisen taso säilyisi hyvänä. Tämä oli toistaiseksi ollut pelkkä tavoite, eikä sääntö, sillä kaikki kyberturvallisuuskoulutukset työsuhteen alussa olevaa perehdytyskoulutusta lukuun ottamatta olivat olleet vapaaehtoisia. Positiivisena puolena kyberturvallisuuskoulutuksista annettiin myös vapaissa kommenteissa kiitosta, mikä on aina hyvä, kun suunnitellaan tulevia koulutuksia.

Itse koulutuksesta annettiin myös palautetta, sillä aihealue koettiin haastavaksi monelle. Monet saavat median kautta tietoa uusimmista kyberturvallisuusuhkista, mutta niiden toivottiin olevan esillä myös koulutuksissa, sillä useat kokivat haasteelliseksi uutisissa olevan tiedon yhdistämistä omissa työtehtävissä koettuihin uhkiin. Monet toivoivat, että koulutuksen jälkeen olisi aikaa keskustella henkilökohtaisemmin kouluttajan kanssa, jotta he pääsisivät tuomaan juuri itseään vaivanneita asioita esille. Kirjoittaja oli mukana yritys X:n kyberturvallisuuskoulutuksissa ja omat havainnot vahvistivat sen, että monet eivät uskalla kysyä kesken koulutuksen, sillä aihealue on niin vaikea, että osa pelkää tyhmiä kysymyksiä. Vasta koulutuksen jälkeen uskallettiin tulla kysymään itseään eniten mietityttäviä kysymyksiä.

Koulutuksia toivottiin myöskin sen takia, etteivät monet vastaajat tunteneet kyberturvallisuuden olevan omalla mukavuusalueellaan. Tästä syystä itsenäinen opiskelu koettiin aikaa vieväksi, ja valmiit nauhoitteet riittämättömiksi, sillä niissä ei voida esittää kysymyksiä, eivätkä ne päivity riittävän usein pysyäkseen uusimpien kyberturvallisuusuhkien perässä. Yritys X:n kansainvälisyydestä huolimatta varsinkin yrityksen vanhemmat työntekijät toivoivat koulutusmateriaaleja suomenkielellä, sillä he eivät kokeneet olevansa kotonaan englannin kielen kanssa, varsinkaan tuntemattomilla aihealueilla, joissa on oma ammattisanastonsa.

4.4 Henkilöstökyselyn arvioiminen

Henkilöstökyselyä käytettiin antamaan yleiskuvaa henkilöstön kyberturvallisuusosaamisesta. Opinnäytetyössä esitettyä henkilöstökyselyä oli tässä muodossa vaikea esittää tilastollisesti, sillä vastaajia olisi pitänyt olla vähintään nelinkertainen määrä. Taustamuuttujia olisi esimerkiksi pitänyt olla vähintään viisi, ja tämä olisi ollut liikaa lyhyelle kyselylle. Sen sijaan aineisto analysoitiin laadullisilla menetelmillä. Mitään historiallista dataa tai muita vastaavanlaisia tutkimuksia ei myöskään ollut käytettävissä, sillä yritykset eivät välttämättä halua julkaista tietoja henkilöstönsä osaamisesta.

Henkilöstökyselyyn oli myös tarkoituksena sisällyttää opettavaisia elementtejä, joka tarkoitti kyllä- ja ei-tyylisiä vastauksia, sekä sellaisia, joissa oli selkeät oikeat ja väärät vastaukset. Tällaiset kysymykset taas eivät ole analysoitavissa tilastollisesti, sillä kahdesta vaihtoehdosta ei voi laskea keskihajontaa, mitä tarvittaisiin tilastolliseen analyysiin. Liukuva 1-10 asteikko taas ei sopinut erimerkiksi kysymyksiin, joissa kysytään vastaajilta, olivatko he antaneet ikinä

salasanaansa muille. Kysely sisälsi myös kaksoiskysymyksiä, esimerkiksi onko vastaajan työasemalla tai sähköpostilla tietoa joka saattaisi kiinnostaa rikollisia. Tilastollisesti kysymystä ei voida analysoida, sillä ei tiedetä tarkoittaako kyllä-vastaus sitä, oliko arvokas tieto vastaajan mielestä hänen sähköpostissaan, vai työasemallaan. Yritys X:ä kiinnosti ainoastaan se, että työntekijät tietäisivät, että heidän hallussaan on sellaisia tietoja, jotka kiinnostaisivat rikollisia, tarkoittivatpa he kumpaa tahansa. Tilastollisesta analyysia ajatellen kysymys olisi pitänyt kuitenkin jakaa kahdeksi ja sisällyttää samaa liukuvaa skaalaa, jota käytettäisiin kaikissa kysymyksissä. Henkilöstökyselyn tulokset olivat kuitenkin analysoitavissa laadullisilla menetelmillä, jolloin opinnäytetyön asettamat tavoitteet voitiin täyttää.

5 Tietoturvallisuusstandardi, yleiset ohjeet, sekä henkilöstön osaaminen

ISO/IEC 27001:2013, Katakri 2015 ja Vahti-ohjeet tarkastettiin yritys X:n toiveista, ja opinnäytetyössä katsastettiin niiden sisältö henkilöstöosaamisen ja koulutuksen kannalta.

5.1 ISO/IEC 27001:2013

ISO/IEC 27001 tarkastettiin käyttämällä Suomen Standardisoimisliitto SFS ry:n julkaisemaa teosta SFS-ISO/IEC 27001, mikä pitää sisällään ISO/IEC 27001:n alkuperäisen englanninkielisen tekstin ja suomennetun tekstin. ISO/IEC 27001:2013:n toinen julkaisija on kansainvälinen standardisoimisliitto ISO, joka tekee siitä ainoan kansainvälisesti tunnustetun tietoturvallisuuden hallintajärjestelmän standardin.

5.1.1 Yleiskatsaus

ISO/IEC 27001:n tarkoitus on luoda vaatimukset tietoturvallisuuden hallintajärjestelmään (Information Security Management System, ISMS). ISO/IEC 27001 on nimensä mukaisesti ISO:n (International Organization for Standardization) ja IEC:n (International Electrotechnical Commission) yhteystyössä julkaisema standardi, jonka kehityksestä vastasi ISO:n ja IEC:n yhteinen alakomitea, ISO/IEC JTC 1/SC 27. ISO/IEC 27001:tä edelsi BS 7799 osa 2, jonka julkaisi BSI Group vuonna 2002 (BSI Group 2002).

BS 7799 sisälsi alun perin parhaat käytännöt tietoturvallisuuden hallinnasta ja vuonna 2002 julkaistu BS 7799:n osa 2 "Information Security Management Systems - Specification With Guidance for Use" antoi tarkempaa ohjetta tietoturvallisuuden hallintajärjestelmän luomiseen, sekä liitti PDCA -syklin (Plan, Do, Check, Act) tietoturvallisuuden hallintajärjestelmiin. Alkuperäinen versio ISO/IEC 27001:2005 julkistettiin nimensä mukaisesti vuonna 2005 ja se

perustui BS 7799:n toiseen osaan. Edeltäjänsä tavoin ISO/IEC 27001:2005 keskittyi luomaan kokonaisvaltaisen tietoturvallisuuden hallintajärjestelmän, jotta tietoturvallisuuden hallinta olisi hallittua ja helpompaa organisaation johdolle. BSI Group julkaisi teoksen ISO/IEC 27001 - Information Security Management - Transition Guide 2013, joka keskittyi ISO/IEC 27001:n 2005 ja 2013 -versioiden eroihin. Teoksen mukaan vuonna 2013 julkaistu päivitys yhtenäisti ISO/IEC 27001 standardin ulkoasua vastaamaan uusimpia ISO säännöksiä. Uudistus oli helpotus organisaatioille, joilla oli käytössä integroitu johtamisjärjestelmä (integrated management system), joka soveltuu useimpiin standardeihin, kuten ISO 9001 laatustandardiin tai ISO 22301 liiketoiminnan jatkumisen hallintajärjestelmän standardiin. Toisessa muutoksessa ISO/IEC 27001:n riskienhallintaosat muutettiin vastaamaan ISO 31000 riskienhallintastandardia. Tämä taas helpotti organisaatioita, mikäli niillä oli käytössä sekä ISO/IEC 27001, että ISO 31000, ollen riskienhallinnan perusteet ovat molemmissa standardeissa yhtenäiset, kirjoittaa BSI Group niiden omilla nettisivuilla (2013).

5.1.2 ISO/IEC 27001:2013 ja henkilöstöosaaminen

ISO/IEC 27001:2013 on klassinen standardi siinä mielessä, että se ei ota kantaa käytettyihin menetelmiin, vaan ainoastaan hallinnollisiin seikkoihin, sekä johtamisjärjestelmän rakentamiseen. Koska standardi on tarkoitettu juuri johtamisjärjestelmän rakentamiseen, se ei ota liiaksi kantaa yksityiskohtaisiin asioihin. ISO/IEC 27001:2013 on hyvä myös siksi, että se korostaa riskienarvioinnin merkitystä ja antaa yrityksen itse arvioida, mihin käytännön toimenpiteisiin ryhdytään riskiarvioinnin jälkeen.

Henkilöstöosaamisesta ja koulutuksista kirjoitetaan kuitenkin A.7 Henkilöstöturvallisuus –osiossa. A.7 jakautuu kolmeen osaan, eli A.7.1 Ennen työsuhteen alkua, A.7.2 Työsuhteen aikana, sekä A.7.3 Työsuhteen päättyminen tai muuttuminen. Koulutuksista mainitaan A.7.2:ssa, ja standardissa on kirjoitettu, että tavoitteena on varmistaa, että työntekijät ja vuokratyöntekijät ovat tietoisia tietoturvallisuusvastuista ja täyttävät ne. A.7.2.2:ssa, eli Tietoturvatietoisuus, -opastus ja -koulutus –osiossa otetaan kantaa konkreettisesti työntekijöiden tietotaitoihin. Osiossa kirjoitetaan selkeästi, että ”kaikkien työntekijöiden on saatava asianmukainen tietoturvatietoisuusopastus ja -koulutus, ja heidän tietojaan organisaation käytänteiden ja menettelyjen muutoksista on päivitettävä säännöllisesti, mikäli se on heidän toimenkuvansa kannalta merkityksellistä.”

Vaikka yritykselle itselleen jätettiin päätökset käytännön teoista, on kuitenkin selkeää, että yrityksen on taattava työntekijöiden tietoturvallisuustiedot ja -taidot. Kaikkia samojen sääntöjen on myös käytettävä niin omien, kuin vuokratyöntekijöiden kanssa. Tämä oli tärkeää, sillä yritys X:llä ei ollut opinnäytetyön kirjoitushetkellä samanlaista suunnitelmaa sidosryhmien työntekijöiden kyberturvallisuusperehdytyksille siitä huolimatta, että useat sidosryhmän

jäsenet pääsivät myös yritys X:n yritysverkkoon. Sidosryhmillä on siis samanlaiset vastuut kyberturvallisuuden takaamisesta kuin yrityksen omillakin työntekijöillä.

5.2 Katakri 2015

Toinen tarkastettavaksi valittu teos oli Katakri 2015, joka on viranomaisten työkalu silloin, kun halutaan arvioida kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa. Kuten ISO/IEC 27001:2013:a, Katakri 2015:a käytetään myös yleisenä tietoturvallisuusarviointityökaluna ja ohjeistuksina yrityksissä ja yhteisössä. Ensimmäinen versio Katakrista julkaistiin vuonna 2009 ja nykyinen versio vuonna 2015.

5.2.1 Yleiskatsaus

Katakrin, eli kansallisen turvallisuusauditointikriteeristön ensimmäinen versio oli tehty osana hallituksen sisäisen turvallisuuden ohjelmaa ja sen tarkoituksena oli arvioida yrityksen tai yhteisön kykyä suojata viranomaisen salassa pidettävää tietoa. Ensimmäistä versiota tehtiin puolustusministeriön johdolla yhdessä elinkeinoelämän edustajien kanssa, mutta tämän jälkeen vastuu siirrettiin sisäministeriölle, missä valmistui päivitetty versio vuonna 2011. Katakria päivitettiin edelleen elokuussa 2012, jolloin sisäministeriö asetti neuvoa antavan työryhmän, jonka tehtävänä oli vuoden 2013 loppuun mennessä sekä päivittää Katakri, että selvittää valtiohallinnossa Katakria koskevia vastuita. Katakrin päivitystä ei kuitenkaan saatu tehtyä määräajan puitteissa, ja päävastuu Katakrin päivityksestä siirtyi tammikuussa 2014 ulkoministeriössä toimivalle Kansalliselle turvallisuusviranomaiselle (NSA).

Mikael Hakkarainen Nixusta avasi TigerTeam blogissa (Katakri III on vihdoin täällä – osa I, 2015), että Katakri 2015 on enemmänkin täysin uusi kriteeristö, kuin pelkkä päivitys, sillä merkittävä uutuus Katakrissa on riskilähtöisyys. Kun Katakrissa aikaisemmin oli hyvinkin tarkat kriteerit, joista ei voitu poiketa, antaa Katakri 2015 huomattavasti enemmän vapauksia toteutuksen suhteen. Katakri 2015 aloittaa siis riskiarvioinnin tekemisestä ja vasta tämän jälkeen miettii mahdollisia kontrolleja. Tämä lähestymistapa on hyvin samanlainen kuin ISO/IEC 27001:2013:ssa, missä lähdetään myös riskienarvioinnista. Katakri 2015 käyttääkin ISO/IEC 27001:2013:a, sekä ISO/IEC27002:2013:a lähteenä monessa osassa ja useissa kriteeristöissä viitataan myös VAHTI-ohjeisiin.

Katakri 2015:ssa on vaatimuksia aiemman reilun 160 sijaan enää vain noin 40. Myöskin aiemman neljän eri osa-alueen sijaan vaatimukset on lajiteltu kolmeen osioon: turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen turvallisuus. Ilkka Korhonen on MPY:n blogissa selven-

tänyt asiaa niin, (2015) että turvallisuusjohtamisessa varmistetaan, että toimijalla on vaadittavat turvallisuusjohtamisen valmiudet ja kyky hallinnollisen ja henkilöstöturvallisuuden osalta. Fyysisessä turvallisuudessa taas tarkastellaan fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset, jotka kattavat tietojen käsittely- ja säilytystä. Tekninen tietoturvallisuuden osa-alue taas kattaa tietojenkäsittely-ympäristön tekniset vaatimukset.

Katakri 2015 versio valittiin osaksi opinnäytetyötä, koska Katakri 2015 on VAHTI-ohjeiden lisäksi tunnetuin suomalainen tietoturvallisuuden työkalu, jota voidaan käyttää yleisenä ohjeistuksena tietoturvallisuuden parantamiseen. VAHTI-ohjeiden lailla Katakri 2015 on julkisesti saatavilla, vaikka korkein suojaustaso I onkin edelleen salassa pidettävä, eikä saatavilla julkisista lähteistä.

5.2.2 Katakri 2015 ja henkilöstöosaaminen

Katakri ottaa kantaa henkilöstöosaamiseen osa-alueessa T, turvallisuusjohtaminen. T-osio sisältää henkilöstöturvallisuus –osa-alueen, jonka T11 kohta liittyy olennaisesti henkilöstöosaamiseen.

Katakrin kohta T11, Henkilöstöturvallisuus: Turvallisuuskoulutus ja -tietoisuus, määrittää tarkasti turvallisuuskoulutusten ja -tietoisuuden vaatimukset, mutta ei ota kantaa turvallisuuskoulutusten sisältöön, eli siihen, onko kyseessä tietoturvallisuuskoulutus vai jotakin muuta. Koska Katakri on tehty viranomaisten salassa pidettävien tietojen suojaamista silmällä pitäen, siinä puhutaan turvallisuusohjeista, jotka kattavat salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt tiedon koko elinkaaren ajalta, ja että henkilökunnalle pitäisi myös järjestää koulutusta salassa pidettävien tietojen asianmukaisesta käsittelystä. Katakri jatkaa vielä, että koulutuksen pitäisi olla säännöllistä ja koulutuksiin osallistuneet henkilöt tulisi dokumentoida. Viimeisenä Katakri kertoo seuraavaa: ”Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti” (2015).

Katakri perustuu hyvin pitkälti ISO/IEC 27001:2013 standardiin, mutta ottaa mallia myös VAHTI-ohjeista. Katakri on kuitenkin ISO standardiin verrattuna paljon tarkempi vaatimuksistaan, kun ISO antaa paljon suuremmat raamit, jossa yritys on vapaa toteuttamaan omia toimenpiteitä riskienarviointien pohjalta. ISO27002:2013 sisältää kuitenkin enemmän käytännön toteutuksen esimerkkejä ja Katakri käyttääkin sitä enemmän lähteenä.

5.3 VAHTI-ohjeet

VAHTI-ohjeet ovat ensisijaisesti Suomen valtiohallinnon työkalu tietoturvallisuuden turvaamiseen, mutta samoja ohjeita käyttävät myös esimerkiksi kunnallishallinnossa ja elinkeinoelämässä. Ohjeita kehittää valtiovarainministeriön asettama valtionhallinnon tieto-ja kyberturvallisuuden ohjausryhmä, eli VAHTI. VAHTI-ohjeet syntyivät, kun valtionhallinnon tietoturvallisuusasetus tuli voimaan vuonna 2010 (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 2010). Asetuksen mukaan valtiohallinnon organisaatioiden tuli saavuttaa tietoturvallisuuden perustaso kolmen vuoden siirtymäkauden jälkeen, eli 30.9.2013 mennessä.

5.3.1 Yleiskatsaus

VAHTI-Ohjeet ovat jaettu kahdeksaan tietoturvallisuuden kehittämisalueeseen:

- Hallinnollinen tietoturva
- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikenneturvallisuus
- Ohjelmistoturvallisuus
- Tietoaineistoturvallisuus
- Käyttöturvallisuus
- Laitteistoturvallisuus

Vaikka VAHTI-ohjeet ovat tarkoitettu julkishallinnon henkilöstölle noudettavaksi, niissä myös lukee, että ohjetta voidaan soveltaen käyttää muissakin, kuin julkishallinnon organisaatiossa. VAHTI-ohjeet eroavat ISO-standardeista ja Katakrista siten, että ohjeet on tarkoitettu noudettavaksi sellaisenaan, kun taas ISO-standardit ja Katakri on tarkoitettu toteutettavaksi osana riskiarviointia. Ohjeet ovat niin tarkkoja, että niissä kerrotaan esimerkiksi millä näppäinyhdistelmällä voidaan lukita Windows työasema.

5.3.2 VAHTI-ohjeet ja henkilöstöosaaminen

VAHTI-ohjeita on paljon enemmän kuin ISO/IEC 27001:2013:n tai Katakrin osioita, sillä VAHTI-ohjeita on täydennetty vuosien varrella erilaisiin tarkoituksiin. Esimerkiksi 2/2008 on otsikoitu: Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta (Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmä, 2016). Tämän osion teemana on henkilöstöriskien ja -uhkien hallinta. Siinä korostuu monien asioiden lisäksi myös tietoturvaohjeistus, sääntöjen tiedottaminen ja valvonta, sekä koulutus. VAHTI-ohjeet listaavat myös heti alle,

että tyypillisiä korjattavia kohteita, josta yksi on tietoturvaohjeistus, ovat sääntöjen tiedottamisen ja valvonnan sekä koulutuksen puutteet.

VAHTI-ohjeista 4/2013:a on vaikeampi ottaa hallinnollinen näkökulma henkilöstöosaamiseen, sillä ohjeiden näkökulmaksi on valittu työntekijä, eikä turvallisuusjohto. Tästä johtuen ohjeet ovat hyvin tarkkoja yksittäisten toimenpiteiden tekemisessä, eivätkä neuvo kyberturvallisuuden johtamisessa. Henkilöstöosaaminen tulee esille kohdassa 4/2013, eli Henkilöstön tietoturvaohjeessa. 2. osiossa, otsikolla Tietoturvallisuuden ohjeet pähkinänkuoressa, on vielä alaotsikko 2.1. Tiedottaminen ja koulutus, jossa työntekijöitä kehotetaan seuraamaan organisaation tietoturvallisuuden tiedotteita, tutustumaan ohjeisiin ja osallistumaan tietoturvakoulutukseen. Heti seuraavaksi lisätään, että työntekijän on myös hyvä noudattaa näitä tietoturvaohjeita.

VAHTI-ohjeiden hallinnollinen osio ei eroa ISO/IEC:27001:2013:sesta paljoa, mutta työntekijöille tarkoitettu 4/2013 -osio on kuitenkin omaa luokkaansa, mikäli mikä tahansa organisaatio haluaa peilata omia tietoturvallisuusohjeistuksiaan johonkin julkiseen tietoturvallisuusohjeeseen. VAHTI-ohjeissa on paljon hyviä perusasioita, mutta ne on haudattu monien eri ohjeiden, otsikoiden ja alaotsikoiden alle. Toisin kuin ISO/IEC 27001:2013 ja Katakri 2015, Vahti-ohjeet eivät ole yksi ohjeistus, vaan kokoelma eri ohjeistuksia ja niiden sisällä on eri osa-alueita.

6 Tutkimuksen tulokset

Tulokset kyberturvallisuusympäristön analyysistä osoittivat, että uhat ovat todistetusti olleet aidot finanssialalla. Viimeisempänä nousevana trendinä on ollut selkeästi kiristysohjelmien, varsinkin WannaCry:n, kasvu ja raju leviäminen yritysympäristössä toukokuussa 2017. Keinot uhan torjumiseen ovat paitsi laitteiston ja ohjelmiston tekninen päivittäminen, myös ehdottomasti henkilöstöosaamisen kehittäminen.

On kiisteltävissä, kumpi on esimerkiksi WannaCryn haittaohjelman leviämisen estämiseksi parempi - henkilöstön valveisuus, vaiko teknisen järjestelmien päivitys. WannaCry käyttää Windowsin haavoittuvuutta, jonka korjaamiseksi julkaistiin päivitys maaliskuun puolessa välissä (Strömberg & Jokiniemi, 2017). Näin ollen on helppo sanoa, että yritysten on päivitettävä käyttöjärjestelmiään ja ohjelmiaan säännöllisesti ja nopeasti. Yritysmaailmassa päivitykset on kuitenkin testattava huolellisesti ennen niiden käytönottoa, jotta uudet päivitykset eivät aiheuta käytössä oleviin ohjelmiin virheitä. WannaCry on levinnyt pääasiassa roskapostien kautta, joten mikäli yritys ei voi ottaa uusimpia tietoturvapäivityksiä heti käyttöön, on henkilöstön rooli erittäin tärkeä kyberturvallisuusuhkien torjunnassa.

Yritys X torjuu henkilöstöön kohdistuvat uhat erilaisilla koulutuksilla ja tiedotteilla. Sekä ISO/IEC 27001:2013, että Katakri 2015 korostaa säännöllisten tietoturvallisuuskoulutusten merkitystä ja yrityksen vastuuta koulutusten ja tiedotteiden järjestämisestä. ISO/IEC27001:2013 7.2.2 -osiossa selkeästi määrätään, että niin omat, kuin sidosryhmien työntekijät on saatava tietoturvallisuuskoulutukseen, ja että heidän tietojaan on päivitettävä säännöllisesti. Yritys X:n ei voida katsoa olevan tässä tilassa, sillä 20% henkilöstöstä ei ole osallistunut henkilöstökyselyn mukaan mihinkään kyberturvallisuuskoulutukseen, ja 23% henkilöstöstä on suorittanut sellaisen yli 12 kuukautta sitten. Kyberturvallisuustilanne ja yritys X:n kyberturvallisuuskoulutus ovat päivittyneet sitä tahtia, että mikäli työntekijä ei ole vuoden sisällä osallistunut yhteenkään kyberturvallisuuskoulutukseen, hänen ei tietojaan ei voida katsoa olevan päivitetty säännöllisesti.

VAHTI-ohjeet peräänkuuluttavat myös työntekijöiden vastuuta pitää silmällä tietoturvallisuuskoulutuksia, sekä velvoittaa niihin osallistumiseen. Työnantajan on kuitenkin tultava tässä työntekijöitä vastaan, sillä työntekijöiltä ei voida edellyttää koulutuksiin osallistumista, jos esimerkiksi heitä ei ole tiedotettu kunnolla, tai jos he eivät voi työaikojen puitteissa osallistua koulutuksiin. Työntekijät on myös velvoitettu noudattamaan yrityksen tietoturvallisuusohjeita. Jos vain 87 % lukitsee työasemansa aina poistuessa ja vain 87% käyttää henkilökorttia liikkuessaan työpaikkansa tiloissa, työntekijöidenkään ei voida katsoa noudattaneen yrityksen ohjeita.

6.1 Kehitysehdotukset

Yritys X:lle annettavissa kehitysehdotuksissa otettiin huomioon kyberturvallisuuden uhat vuonna 2017, henkilöstökyselyn tulokset, sekä ISO27001:2013:n, Katakri 2015:n ja Vahti-ohjeiden analyysit:

1. Kyberturvallisuuskoulutus on pidettävä säännöllisesti ja henkilökunta on velvoitettava osallistumaan ainakin yhteen koulutukseen kalenterivuoden aikana.
2. Työntekijöiden osallistuminen kyberturvallisuuskoulutuksiin on dokumentoitava. Työntekijät, jotka eivät ole osallistuneet riittävästi kyberturvallisuuskoulutuksiin tulevat saamaan muistutuksia siihen asti, kunnes he seuraavan kerran osallistuvat koulutukseen.
3. Sidosryhmien työntekijöiden on käytävä myös yritys X:n kyberturvallisuuskoulutuksissa, mikäli heillä on pääsy yrityksen sisäiseen verkkoon. Esimerkkinä vastaanoton työntekijät.

4. Yritys X:n on tehostettava fyysisen turvallisuuden valvontaa ja esimerkiksi henkilökorttien käyttö yrityksen tiloissa on saatava sataan prosenttiin. Henkilökohtaisen kulkutunnisteen lainaamista muille on myöskin valvottava ja käytäntö kitkettävä pois.
5. Yritys X:n on säännöllisesti esitettävä uudet kyberturvallisuusuhat henkilöstölle. Samassa yhteydessä on tarjottava selkeitä ohjeita siitä, miten mainittuja uhkia voidaan konkreettisesti torjua työntekijöiden näkökulmasta.
6. Ohjeet kyberuhkien torjuntaan on saatava suomenkielisenä versiona. Kaikista koulutusmateriaaleista on tarjottava myös suomenkielinen versio.
7. Työntekijöiden osaaminen sekä tarpeet on varmistettava säännöllisillä kyberturvallisuuden henkilöstökyselyillä. Tulokset on dokumentoitava huolellisesti ja käsiteltävä henkilöstön kanssa. Yrityksen on tehtävä tulosten mukaan kyberturvallisuuteen parannusehdotuksia ja toteutettava niitä.

Edellä mainitut ehdotukset ovat opinnäytetyön kirjoittajan mukaan kohtuulliset ja opinnäytetyössä tehtyjen analyysien mukaiset. Ehdotuksia annettaessa on otettu yritys X:n toiminnan luonne, sekä organisaatiolliset mahdollisuudet ehdotuksien toteuttamiseen huomioon. Ehdotusten taloudellista rasitetta tai vaikutusta ei voida arvioida, joten niiden vaikutusten kohtuus jää täysin yritys X:lle.

6.2 Henkilöstökyselyn kehittäminen, jatkotutkimus ja käytettävyys muissa organisaatiossa

Yritys X:lle annettavissa kehitysehdotuksissa ehdotettiin, että heidän olisi hyvä ottaa käyttöön säännölliset kyberturvallisuuden henkilöstökyselyt. Kyberturvallisuus on aina osittain myös työntekijöiden vastuulla ja on tärkeää, että henkilöstön osaamista testataan säännöllisesti. Tämän lisäksi on erittäin tärkeää antaa kyselyissä myös työntekijöiden tuoda omat huolensa ja ajatuksensa esille, sillä useat heistä eivät tuo mielipiteitään aktiivisesti esille. Monet työntekijöistä kaipaavat enemmän tukea turvallisuusasioissa, joten yritys X:n on ehdottomasti jatkossakin tehtävä yhteistyötä henkilöstön kanssa, ja varmistettava, ettei henkilöstö ole yrityksen heikoin lenkki.

Henkilöstökyselyä on kuitenkin mahdollista kehittää monella tavalla. Olisi hyvä analysoida henkilöstön oman osaamisen arviointia pitkäjänteisesti. Sen sijaan, että se tehtäisiin sanallisesti, sen voisi tehdä liukuvalla 1-5 asteikolla. Tämä asteikko tulisi sisällyttää kaikkiin henkilöstökyselyihin, jotta voitaisiin tilastollisilla analyysimenetelmillä nähdä, tapahtuuko kehitystä vai ei. Myöskin monet muut kysymykset, kuten esimerkiksi työntekijän kokemus yritykseltä saatavasta tuesta, voitaisiin asettaa tälle samalle asteikolle.

Henkilöstökyselyssä tuli myös ilmi, että yrityksen työntekijät olivat lainanneet huomattavan usein avainta tai kulkutunnistetta jollekin toiselle yrityksen työntekijälle. Ilmiö on hälyttävä ja syy siihen olisi ehdottomasti tarpeellista tutkia tarkemmin. Jotta ilmiö voitaisiin kokonaan kitkeä, olisi syytä selvittää perin pohjin jatkotutkimuksella, miksi työntekijöillä on ollut tarve antaa muille oma henkilökohtainen kulkutunniste, vaikka se on yrityksessä kiellettyä.

Mikäli useammat saman alan yritykset kehittäisivät yhteisen kyberturvallisuuden henkilöstökyselyn, jota voitaisiin soveltaa useammassa yrityksessä, saataisiin korvaamaton vertaisverkosto, jossa jokainen yritys voisi mitata omia tuloksiaan muita vastaan. Jokaisessa yrityksessä on omat erikoispiirteet. Esimerkiksi tietohallintajärjestelmät voivat olla niin erilaisia, että eri yritykset vaativat eri asioita työntekijöiltä esimerkiksi virustorjunnan ja ohjelmistopäivityksien suhteen. Tästä huolimatta, mikäli joku ottaisi tehtäväkseen tutkia henkilöstöosaamista laajemmin monessa yrityksessä, olisi erittäin mielenkiintoista niin yrityksille, kuin yhteisöllekin tietää, missä tilassa yritysten kyberturvallisuuden henkilöstöosaaminen on Suomessa.

7 Yhteenveto

Opinnäytetyön tarkoituksena oli tutkia, miten finanssialan yrityksessä voidaan parantaa kyberturvallisuutta henkilöstön osaamista parantamisella. Tutkimuksesta syntyi henkilöstökysely, jota ei ole ikinä aikaisemmin käytetty yritys X:llä. Vaikka henkilöstökyselyn muotoilu oli kaukana täydellisestä ja parantamisen varaa oli useammassa kohdassa, se tuotti silti jo sellaisenaan korvaamatonta informaatiota henkilöstön osaamisesta, käyttäytymisestä, omien taitojen arvioimisesta, sekä koulutusten toiveista. Mikäli kyberturvallisuuden henkilöstökysely otettaisiin käyttöön yrityksessä säännöllisesti, siitä saadut tulokset voisivat olla entistä paremmat ja hyödyllisemmät.

Henkilöstökyselyn tuloksia peilattiin ISO/IEC 27001:2013:n, Katakri 2015:n, sekä Vahti-ohjeisiin. Vaikka mikään edellisistä teoksista ei suoraan anna vastauksia yritysten henkilöstöosaamiseen ja -johtamiseen kyberturvallisuudessa, antavat ne paljon neuvoja ja ohjeita. Ne ovat osaltaan myös armottomia, ja mikäli mikä tahansa organisaatio päätyisi joskus ottamaan niitä käyttöön, joutuisivat monet uudistamaan omaa tietoturvallisuusjohtamisjärjestelmää hyvin laajalti.

7.1 Tutkimuksen luotettavuusarviointi

Tieteellisen tutkimuksen yleiset mittarit ovat reliabiliteetti ja validiteetti, kirjoittaa Kananen (2014, 147). ”Reliabiliteetti tarkoittaa tulosten pysyvyyttä ja validiteetti sitä, että tutkitaan oikeita asioita”, Kananen jatkaa. Henkilöstökyselyn luotettavuutta lisättiin opinnäytetyössä

tehdyllä aineistotriangulaatiolla, eli henkilöstöosaamisen ja koulutusten parantamisehdotuksia peilattiin myös ISO/IEC:27001:2013:n, Katakri 2015:n ja VAHTI-ohjeisiin. Näiden yhteistuloksia käytettiin, kun yritys X:lle tehtiin kehitysehdotuksia.

Henkilöstökyselyn luotettavuus varmistettiin lisäksi riittävällä dokumentaatiolla. Kanasen mukaan riittävä dokumentaatio on yksi merkittävimmistä asioista tutkimusta tehdessä, sillä se antaa työlle uskottavuutta (2014, 153). Tästä syystä kaikki kyselyssä esitetyt kysymykset ja vastausten määrät ovat luettavissa sellaisinaan liitteissä. Tämä on tärkeää, jotta myös lukijat voivat varmistua siitä, että opinnäytetyössä esitetyt luvut ovat oikeita. Alkuperäiset tulokset ovat yritys X:n hallussa, joten myös he voivat tarkistaa opinnäytetyössä esitetyt luvut ja väitteet.

Opinnäytetyön analyysi kyberturvallisuuden uhkista vuonna 2017 varmistettiin oikeaksi käyttämällä useita lähteitä. Tavoitteena oli, että sama tulos pitäisi olla nähtävillä useita lähteistä ja tähän tulokseen myös päästiin. Henkilöstöosaamisen merkitys yrityksen kyberturvallisuudelle varmistettiin siis sekä opinnäytetyön kirjoittajan omalla havainnoinnilla yritys X:ssä työskentelyn aikana, että aiheistoanalyysillä. Lisäksi koulutusten arvioinnissa käytettiin niin ISO standardia, Katakria, Vahti-ohjeita, kuin henkilöstökyselyn tuloksiakin. Aineistoanalyysistä saadut tulokset on esitetty omassa osiossaan ja lähteet merkitty selkeästi, jotta niiden tarkistaminen olisi helppoa.

7.2 Oma kehityksen arviointi

Opinnäytetyö oli haasteellinen, sillä kyberturvallisuus ei ollut iso osa kirjoittajan koulutusta tai työtä opinnäytetyön aloittaessa. Vaikka kyberturvallisuus on ollut otsikoissa Stuxnetin ajoista lähtien, yritysten kyberturvallisuuskoulutukset ovat silti vasta kehittymässä. Tästä syystä kyberturvallisuus valikoitui opinnäytetyön aihealueeksi. Ala on kehittyvä ja moninainen, eikä opittava lopu kesken.

Opinnäytetyö kohtasi monia haasteita kirjoitusaikana. Kirjoittaja oli ollut työharjoittelussa yritys X:ssä vuoden 2016 kevään aikana, ja kun kyberturvallisuuskysely oli saatu valmiiksi, yritys X:ssä alkoi työntekijöiden lomakausi. Tästä syystä kyselyn julkaisua lykättiin toistuvasti, kunnes kysely saatiin vihdoinkin julkaistua syksyllä 2016. Kirjoittajan työharjoittelu yritys X:ssä loppui myös ennen kyselyn julkaisua, joten kyselyn julkaisu ja tietojen kerääminen olivat täysin yritys X:n vastuulla. Tämä taas teki opinnäytetyön tekemisestä hitaampaa ja vaikeampaa, kun kysymysten jalostaminen ja tuloksien saaminen ei enää onnistunut yhtä helposti, kuin jos kirjoittaja olisi ollut yritys X:ssä töissä. Aikataulun olisi pitänyt olla parempi, jotta tällainen viivästys ei olisi päässyt tapahtumaan, sillä mitä enemmän aika kului, sitä vaikeampaa oli tulosten analysointi ja palautteiden saaminen yritys X:ltä.

Lopputuloksen kannalta kysely oli hyvä, ja vastasi yrityksen tavoitteita ja toiveita, mutta parannettavaakin löytyy. Esimerkiksi yrityksessä tällaiset kyselyt olisi saatava näkyvämmäksi, jotta niihin saataisiin riittävästi vastaajia. 60:llä vastauksella tulokset antavat osviittaa, mutta eivät ole yleistettävissä koko yritykseen.

7.3 Loppusanat

Analyysi viimeisimmistä kyberuhkista kertoo karua kieltä henkilöstön suurista vastuista ja toisaalta suurista epäonnistumisistakin. Kiristysohjelmat ovat levinneet ehkä jopa ennakoitua enemmän ja kärsijöitä eivät ole pelkästään yksityiset henkilöt, vaan myös monet yritykset ovat joutuneet niiden kynsiin. Yhteinen tekijä on kuitenkin kaikissa haittaohjelmissa se, että toisin kuin palvelunestohyökkäykset, kiristysohjelmat eivät yritä yrityksen verkkoon väkisin. Ohjelman leviäminen sen sijaan luottaa vahvasti siihen, että henkilöstöstä löytyisi edes yksi heikko lenkki, joka ei ole tilanteessa valppaana. Yhdenkin väärän linkin avaaminen voi johtaa minuuteissa jopa yrityksen ydintoimintojen pysähtymiseen ja rahallisen vahingon kannalta tämä olisi katastrofaalista. Finanssialalla konkreettinen esimerkki tietojärjestelmien tärkeydestä on se, että verkkopankki ja -liikenteen pysähtyminen pankin verkossa voi aiheuttaa jopa enemmän vahinkoa kuin kaikkien pankin konttoreiden sulkeutuminen yhtä aikaa. Finanssiala on niin vahvasti mukana kansainvälisessä rahaliikenteessä, että pienetkin ongelmat yhdessä tietokoneessa voivat levitä kansainväliseksi finanssikriisiksi.

Toivottavasti myös muut lukijat hyötyvät tästä opinnäytetyöstä, joko henkilöstöosaamisen merkityksen esilletuomisen, tai konkreettisen kyberturvallisuuden henkilöstökyselyn teon kautta. Kaikkien saatujen tulosten jälkeen on täysin varmaa, että vastaavanlainen kysely olisi säännöllisesti suoritettuna arvokas mille tahansa organisaatiolle. Vaikeinta on hioa kysely sopivaksi juuri omaan käyttöön, mutta tämän jälkeen sen ylläpito on hyvin kohtuullista siitä saadun hyödyn huomion ottaen.

Lähteet

Andreasson, A & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tallinna: AS Pakett.

Gates, M. 2017. Stopping the cyber buck. Security management. 3/2017, 28-31.

Hirsijärvi, S. Remes P. & Paula Sajavaara. 2012. Tutki ja kirjoita. 15.- 17. painos. Hämeenlinna: Kariston Kirjapaino Oy.

Kananen, J. 2011. Kvantti: Kvantitatiivisen opinnäytetyön kirjoittamisen käytännön opas. Tampere: Tampereen Ylipostopaino Oy – Juvenes Print.

Laki luottolaitostoiminnasta. 610/2014.

Limnéll, J. Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. 1.7.2010/681.

Vilkka H. & Airaksinen T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi Oy.

Sähköiset lähteet

Armada Cloud. 2016. Roundup: Ransomware Statistics 2016. Viitattu 24.4.2017. http://www.armadacloud.com/roundup-ransomware-statistics-2016/

Barrett D. 2016. FBI Suspects Insider Involvement in $81 Million Bangladesh Bank Heist. Viitattu 16.4.2017. https://blogs.wsj.com/indiarealtime/2016/05/10/fbi-suspects-insider-involvement-in-81-million-bangladesh-bank-heist/

Bond, T. 2012. Employee Security Awareness Survey. Viitattu 27.4.2017. https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf

BSI Group. 2002. Launch of revised BS 7799 standard at international conference. Viitattu 21.5.2017. https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2002/9/Launch-of-revised-infosecurity-standard-at-7799-Goes-Global-conference/

BSI Group. 2013. ISO/IEC 27001 - Information Security Management - Transition guide. Viitattu 20.3.2017. https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

BSI Group. 2015a. Our history. Viitattu 2017. https://www.bsigroup.com/en-GB/about-bsi/our-history/

BSI Group. 2015b. What is a standard? Viitattu 17.5.2017. https://www.bsigroup.com/en-GB/standards/Information-about-standards/what-is-a-standard/

Conner, B. 2017. Ransomware-As-A-Service: The Next Great Cyber Threat? Viitattu 24.4.2017. https://www.forbes.com/sites/forbestechcouncil/2017/03/17/ransomware-as-a-service-the-next-great-cyber-threat/#4cc8144e4123

Culp, S. 2016. Cyber Risk: People Are Often the Weakest Link in The Security Chain. Viitattu 13.5.2017. https://www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain/#c897d812167a

Das, K & Spicer J. 2016. How the New York Fed fumbled over the Bangladesh Bank cyber-heist. Viitattu 16.4.2017. http://www.reuters.com/investigates/special-report/cyber-heist-federal/

Fadilpašić, S. 2016. Weebly hacked, 43 million user credentials stolen. Viitattu 1.5.2017. http://www.itproportal.com/news/weebly-hacked-43-million-user-credentials-stolen/

Goel, V. & Perlroth N. 2016. Yahoo Says 1 Billion User Accounts Were Hacked. Viitattu 1.5.2017. https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?_r=0

Hevonoja, J. 2015. Aseellisia pankkiryöstöjä tapahtuu muutamia vuodessa – huippuvuotena 90-luvulla jopa 114. Viitattu 17.4.2017. http://yle.fi/uutiset/3-7855263

Homeland Security Research Corp. 2015. U.S. Financial Services: Cybersecurity Systems & Services Market – 2016-2020. Viitattu 30.6.2016. http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/

IEC. 2017. About the IEC. Viitattu 17.5.2017. http://www.iec.ch/about/

ISO. 2016. About ISO. Viitattu 17.5.2017. https://www.iso.org/about-us.html

Kippo, J. 2017. Hurja kyberhyökkäys jatkuu – iskenyt jo 150 maahan ja 200 000 kohteeseen. Viitattu 14.5.2017. http://yle.fi/uutiset/3-9612491

Kokkonen, Y. 2017a. Hakkeriryhmä: Yhdysvallat vakoilee globaalia pankkijärjestelmää. Viitattu 16.4.2017. http://yle.fi/uutiset/3-9567399

Kokkonen, Y. 2017b. Tuhoisa haittaohjelma sulkee tietokoneita kymmenissä maissa – kehitetty USA:n turvallisuusvirastossa? Viitattu 13.5.2017. http://yle.fi/uutiset/3-9611520

Korhonen, I. Mikä ihmeen Katakri? 2016. Viitattu 25.3.2017. http://blogi.mpy.fi/mika-ihmeen-katakri

McGoogan, C. 2016. Dropbox hackers stole 68 million passwords - check if you're affected and how to protect yourself. Viitattu 1.5.2017. http://www.telegraph.co.uk/technology/2016/08/31/dropbox-hackers-stole-70-million-passwords-and-email-addresses/

MTV uutiset. 2016. Kiristysohjelmat jylläävät – tuttuja myös Suomen sairaaloissa. Viitattu 19.4.2017. http://www.mtv.fi/uutiset/kotimaa/artikkeli/kiristysohjelmat-jyllaavat-tuttuja-myos-suomen-sairaaloissa/6131500

Nixu TigerTeam blogi. 2015. Katakri III on vihdoin täällä – osa I. Viitattu 25.3.2017. https://www.nixu.com/fi/blogi/2015-04/katakri-iii-on-vihdoin-taalla-osa-i

Paganini, P. 2016. A third bank was a victim of cyber heist that involved the SWIFT. Viitattu 19.4.2017. http://securityaffairs.co/wordpress/47532/cyber-crime/swift-thord-cyber-heist.html

Poliisi, CERT-FI & F-secure. 2013. Ransomware. Viitattu 20.4.2017. http://www.ransomware.fi/

Puolustusministeriö. 2015. Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 21.3.2017. http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

PWC. 2016. Global Economic Crime Survey 2016. Viitattu 15.4.2017. http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey.html

RHEA Group. 2016. The Central Bank of Bangladesh heist. Viitattu 19.4.2017. https://www.rheagroup.com/news/three-biggest-cyber-attacks-2016

Rissanen J. & Koivuranta E. 2016. Verkkorikolliset tunkeutuvat sairaalan verkkoon, lukitsevat tiedostoja ja vaativat rahaa – Ovatko tietoni turvassa? Viitattu 20.4.2017. http://yle.fi/

RT. 2015. World cybersecurity market will grow by $100b in five years – report. Viitattu 15.4.2017. https://www.rt.com/usa/315147-cybersecurity-market-growth-boom/

Sanastokeskus TSK ry. 2016. kohdennettu verkkourkinta; kohdistettu verkkourkinta. Viitattu 17.5.2017. http://www.tsk.fi/tsk/termitalkoot/hakemistot-267.html?page=get_id&id=ID468&vocabulary_code=TSKTT

SecureWorks. 2017. Cybersecurity vs. Network Security vs. Information Security. Viitattu 2017. https://www.secureworks.com/blog/cybersecurity-vs-network-security-vs-information-security

Strömberg, J & Jokiniemi, E. 2017. Tuhoisasta haittaohjelmasta havaintoja myös Suomessa – "Leviää erityisen tehokkaasti työpaikkojen sisäverkossa". Viitattu 14.5.2017. http://yle.fi/uutiset/3-9611769

Suomen Standardisoimisliitto SFS ry. 2011. Mikä SFS on? Viitattu 17.5.2017. https://www.sfs.fi/sfs_ry

Suomen Standardisoimisliitto SFS ry. 2013. SFS-ISO/IEC 27001. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset, Viitattu 16.3.2017. https://online.sfs.fi/

SWIFT. 2014. SWIFT history. Viitattu 17.5.2017. https://www.swift.com/about-us/history

Tietoturvapalvelu. 2015. Haittaohjelmat ja muut uhat. Viitattu 25.5.2017. http://www.tietoturvapalvelu.info/johdanto/haittaohjelmat_ja_muut_uhat

Kuviot

Liite 1: Henkilöstökyselyn kysymykset ja vastaukset

Kysymykset	Vastausten määrä
1. Kuinka kauan olet ollut Yritys X:llä töissä?	
a. 0 – 1 vuotta	3
b. 1 – 3 vuotta	5
c. Yli 3 vuotta.	50
2. Mikä on työsuhteesi laatu?	
a. Osa-aikainen	0
b. Määräaikainen	3
c. Vakituinen	57
3. Milloin olet viimeksi saanut kyberturvallisuuskoulutusta, tai suorittanut kybeturvallisuuskursseja?	
a. Alle 6 kuukautta	16
b. 6-12 Kuukautta	18
c. Yli 12 kuukautta	14
d. En koskaan	12
4. Tiedätkö keneen ottaa yhteyttä, jos saat työasemaasi haittaohjelman?	
a. Kyllä	49
b. Ei	11
5. Onko työasemasi ikinä ollut saastuneena viruksesta tai troijalaisesta?	
a. Kyllä, työasemaltani on löytynyt haittaohjelmia aikaisemmin.	4
b. Ei, työasemani ei ole ikinä saastunut.	50
c. En tiedä mikä on virus tai troijalainen.	6
6. Oletko ikinä antanut käyttäjätunnuksesi liittyvän salasanan muille?	
a. Kyllä	1
b. En	59
7. Oletko joskus lainannut henkilökohtaisen avaimen/kulkutunnisteen toiselle yrityksen työntekijälle?	
a. Kyllä	14
b. En	46
8. Jos deletoit / poistat tiedoston tai kansio, kaikki tiedot ovat pysyvästi poistettu.	
a. Tosi	2
b. Epätosi	48
c. En osaa sanoa	10
9. Miten tunnistaa suojatun yhteyden?	
a. Kun nettisivun osoite alkaa ”http:”llä.	4
b. Kun nettisivun osoite alkaa ”https:”llä.	48
c. En osaa sanoa.	7

10. Lukitsetko työasemasi aina poistuessasi?	
a. Kyllä, lukitsen sen aina.	52
b. En lukitse työasemani, jos poistun vain lyhyeksi aikaa.	8
c. Ei, en lukitse työasemani olleenkaan.	0
11. Käytätkö henkilökorttia, kun liikut työpaikan tiloissa? (Muuten kuin kassatoimihenkilönä kassapaikalla)	
a. Kyllä, pidän henkilökortin aina näkyvillä työpaikan tiloissa.	52
b. Pidän henkilökorttini työpisteellä, mutta en mukana liikkuessani työpaikan tiloissa.	2
c. Pidän henkilökorttini taskussa tai laukussa.	4
d. Ei, en pidä henkilökorttia mukana työpaikalla.	2
e. En tiedä, missä henkilökorttini on.	0
12. Tiedätkö, mitä tietojen kalastelu, eli phishing on?	
a. Puhelinmyynti, jossa yritetään myydä erilaisia palveluita tai tuotteita	0
b. Verkkourkintaa, jolla pyritään samaan haltuunsa luottamuksellisia tietoja rikollisiin tarkoituksiin	58
c. Massasähköpostitus, esimerkiksi mainosviestejä osoitteisiin, johon ei ole saatu etukäteislupa	1
d. En tiedä	1
13. Asiakas lähettää sinulle hänen saamansa mahdollisen kalasteluviestin. Mitä teet?	
a. Avaan viestin ja liitteen, jotta voin tarkastaa viestin sisällön.	0
b. Poistan viestin avaamatta liitteitä.	9
c. Lähetän viestin yritys X:n Phishingmail – postilaatikkoon avaamatta liitettä.	51
14. Tiedätkö, mitä toimitusjohtajahuijaus (CEO-fraud) on?	
a. Henkilö, kenellä on väärennetyt pätevyydet, hakee toimitusjohtajaksi yrityksiin	0
b. Toimitusjohtajan aseman väärinkäyttö	6
c. Sähköpostihuijaus, jolla rikollinen tekeytyy jonkun esimieheksi saadakseen uhria lähettämään varoja rikollisen tilille.	50
d. En tiedä	4
15. Työasemallani/sähköpostissani ei ole arvokasta tietoa, eikä se kiinnosta rikollisia.	
a. Tosi	1
b. Epätosi	58
c. En osaa sanoa	1
16. Onko yritys X:llä sääntöjä siitä, millä nettisivuilla saat työasemallasi käydä?	
a. Ei, saan käydä millä tahansa sivuilla töissä.	1
b. Kyllä, meillä on säännöt siitä, millä sivuilla voin käydä, mutta en tiedä niitä sääntöjä.	18
c. Kyllä, meillä on selkeät säännöt ja osaan soveltaa niitä käytännössä.	41

17. Käsitteletkö yrityssalaisuuden alaisia tietoja sähköpostitse muutoin kuin yrityksen omassa sisäisessä verkossa?	
a. Kyllä käsittelen.	5
b. Ei, en käsittele.	55
18. Voitko lähettää työsähköpostia omiin sähköpostitileihin (Hotmail, Gmail, Yahoo jne.), mikäli sinulla ei ole pääsyä työsähköpostiisi?	
a. Kyllä voin.	0
b. En voi.	58
c. En tiedä.	2
19. Käsitteletkö yrityssalaisuuden alaisia tietoja ulkopuolisissa ohjelmissa (Esim. Basecamp, Trello)?	
a. Kyllä käsittelen.	2
b. En käsittele.	58
20. Käytätkö samaa salasanaa niin yrityksen järjestelmiin, kuin omiin henkilökohtaisiin järjestelmiin, kuten Facebookin, LinkedIn, tai omiin sähköpostitileihin?	
a. Kyllä käytän.	3
b. En käytä.	57
21. Pidätkö omaa tietoturvallisuustietoisuuttasi tarpeeksi kattavana?	
a. Kyllä pidän.	29
b. Osaan perusasiat, mutta lisätieto olisi tarpeen.	27
c. En pidä, ja kaipaan huomattavasti enemmän tietoja kyberturvallisuudesta.	4
d. En pidä, enkä kaipaa lisätietoja kyberturvallisuudesta.	0
22. Tarjoaako Yritys X riittävästi tietoa kyberturvallisuusosaamisesi varmistamiseksi?	
a. Kyllä, yrityksessä on saatavana riittävästi tietoa kyberturvallisuudesta.	55
b. Ei, en saa yrityksen kautta riittävästi tietoa kyberturvallisuudesta.	5
c. (Jos et saa tarpeeksi tietoa, miksi et? Millaisia parannuksia haluaisit?)	
23. Vapaa kommenttikenttä	