Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2016

Juha Mäentaus, Juhani Ruusi, Riina Välimaa

TIETOTURVA-AUDITOINNIN JÄLKEISET TOIMENPITEET TIETOTURVAN PARANTAMISEKSI

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2016 | 41

Jarkko Paavola

Juha Mäentaus, Juhani Ruusi, Riina Välimaa

TIETOTURVA-AUDITOINNIN JÄLKEISET TOIMENPITEET TIETOTURVAN PARANTAMISEKSI

Työssä tutkimme aiemmin tehdyn tietoturvakartoituksen jälkeistä tilannetta ja tietoturvan tasoa kohdeyrityksessä. Tutkimustulosten perusteella selvitämme tarvittavia toimenpiteitä tietoturvatason nostamiseksi.

Ensimmäinen osa selvittää tietoturvan ja riskienhallinnan perusperiaatteita sekä pohjustaa seuraavissa osissa käsiteltäviä aihealueita.

Toisessa osassa käsitellään laadullista tutkimusta, haastattelututkimuksen tekemistä sekä ensimmäisen tietoturvakartoituksen jälkeisen tietoturvatason kartoittamista. Tilanteen kartoittaminen tapahtui haastattelun avulla, joten haastattelukysymysten koostaminen on merkittävä osa työssämme.

Kolmannessa osassa käsitellään toimenpiteitä haastattelututkimuksesta saatujen tulosten perusteella. Lisäksi toimenpiteitä pohjustetaan teoreettisella tiedolla.
Viimeinen osa koostuu erikseen tehtävän tietoturvakoulutuksen teoriaosuudesta.

Tietoturvakoulutus aloitettiin tekemällä yksinkertainen ohjeistus työntekijöitä varten. Ohjeistus on ohjevihkonen siitä, miten tulisi toimia erilaisissa tilanteissa ja miten uhkia voi havaita. Teimme myös koulutusvideon, jonka avulla työntekijöitä opetetaan hauskalla tavalla tarkemmin varautumaan erilaisiin tietoturvauhkiin. Video tullaan näyttämään jokaiselle nykyiselle työntekijälle ja tulevaisuudessa uusille työntekijöille perehdytyksessä.

Alustavan tietoturvakartoituksen, -politiikan ja tämän opinnäytetyön johdosta luotiin yritykselle tietoturvapohja ja heräteltiin yrityksen johtoa asian tärkeydestä. Tutkimuksemme myötä kohdeyrityksen tietoturvan kehittäminen helpottuu, ja yleinen tietämys tietoturvasta parantaa jokaisen yksilöllistä suoritusta.

ASIASANAT:

tietoturva, tietoturvakartoitus, tietoturvakoulutus, auditointi, haastattelututkimus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2016 | 41

Jarkko Paavola

Juha Mäentaus, Juhani Ruusi, Riina Välimaa

MEASURES TO IMPROVE INFORMATION SECURITY AFTER THE AUDIT

The purpose of this thesis was to investigate the current level of the information security in the client company. Based on the research we developed the necessary measures to raise the level of information security in the company.

The first section explains basic principles of information security and risk management.

The second part deals with qualitative research, doing an interview study and mapping the level of information security, after the first information security audit.

The third part deals with the measures on the basis of the results of the interview study. In addition, measures are discussed and proposed by applying theoretical knowledge. The last part consists of a separate task of the theory about information security training.

The information security training for the client company was carried out by creating a guide with simple guidelines for employees. The guide is a booklet of instructions about what to do in different situations and how security threats can be detected. An educational video was created which allows employees to be taught in a fun and educational way to be prepared for various information security threats. This video will be shown to every current employee and to future employees during their orientation to the company.

The information security mapping, the information security guide and now this thesis, have created a base for information security and help corporate management increase their awareness of it. From now on, it is easy for the company to keep improving their information security.

KEYWORDS:

information security, information security mapping, information security orientation, audit, interview study

SISÄLTÖ

LIITTEET

KUVIOT

TAULUKOT

SANASTO

Auditointi	Objektiivinen ja määrämuotoinen arviointi, jolla pyritään havaitsemaan täyttääkö auditoinnin kohde sille asetetut vaatimukset.
Tietoturvallisuus	Toimet ja järjestelyt joilla pyritään tietojen, palvelujen, tietojärjestelmien sekä tietoliikenteen suojaamiseen.
Tietoturvapolitiikka	Yrityksen johdon hyväksymä dokumentti, joka tähtää yrityksen strategisten tavoitteiden pohjalta tietoturvallisuuden systemaattiseen kehitykseen.
Tietoturvariski	Vahingon vaara, joka kohdistuu tietoon, tietojärjestelmään tai tietoliikenteeseen.
Tietoturvataso	Kuvaa tietyn toimijan tasoa ohjata tietoturvatapahtumia.

1 JOHDANTO

Tietoturva on päivittäisessä työelämässä yhä keskeisemmässä roolissa tekniikan kehittyessä ja liiketoiminnan nojatessa aina enemmän sähköisiin järjestelmiin. Tietoturva-asia on kuitenkin liian monessa yrityksessä jäänyt pimentoon tai tärkeysjärjestyksessä muiden toimintojen jalkoihin.

Opinnäytetyömme on jatkoprojekti kaksi vuotta sitten samalle kohdeyritykselle tekemällemme tietoturvakartoitukselle ja -auditoinnille. Tekemämme kartoitus ja auditointi saivat kohdeyrityksen havahtumaan asian tärkeydestä. Tietoturvallisuus oli jäänyt firman koosta ja kansainvälisestä toiminnasta huolimatta taka-alalle. Näin ollen yrityksessä suhtauduttiin hyvin positiivisesti aiempiin töihimme ja tietoturvaa haluttiin saada edelleen paremmalle tasolle.

Työmme varsinaisena tarkoituksena oli kartoittaa, missä tilassa kohdeyrityksen tämänhetkinen tietoturva on. Tämän lisäksi tarkoituksena oli saatujen tulosten perusteella kehittää tarvittavia toimenpiteitä tietoturvatason nostamiseksi. Lisäksi työhömme sisältyy kohdeyritykselle tehtävä koulutusvideo. Tämän myötä myös tietoturvakoulutuksen perusteita käsitellään opinnäytetyössämme.

Jokaiselle tämän opinnäytetyön tekijälle jaettiin näiden tehtävien perusteella oma vastuualueensa. Juha Mäentauksen osuus oli haastattelututkimuksen koostaminen ja toteuttaminen, Juhani Ruusin tietoturvan peruskäsitteet ja perehtyminen toimenpiteisiin tietoturvatason parantamiseksi, ja Riina Välimaa loi yritykselle koulutusvideon tietoturvasta. Jokainen oli kuitenkin mukana kaikissa työvaiheissa vastuualueista riippumatta, ja kirjallinen osuus toteutettiin yhdessä mahdollisimman yhtenäisen lopputuloksen saamiseksi.

Työn alussa avataan olennaisimmat teoreettiset tietoturvan ja riskienhallinnan perusperiaatteet, minkä jälkeen siirrytään laadullisen tutkimuksen teoriaan sekä haastattelututkimuksen koostamiseen. Haastattelututkimuksen kysymysten koostamisessa olennaisena pohjana toimii aiemman tietoturvakartoituksen ja auditoinnin myötä saadut tiedot yrityksen sen hetkisestä tilasta. Lisäksi haluttiin selvittää, miten yritykselle luotu tietoturvapolitiikka on vaikuttanut organisaation toimintaan.

Haastattelututkimuksesta saatujen tulosten perusteella laadittiin yritykselle tietoturvatasoa edelleen kohottavia toimenpiteitä. Toimenpiteitä on pohjustettu asiaan kuuluvalla teoriatiedolla sekä esitelty käytännön tason menetelmiä.

Koska yrityksellä ei ollut mitään tietoturvaperehdytystä työntekijöilleen, koostimme heille tietoturvakoulutusvideon. Videon avulla yrityksen työntekijät oppivat yksinkertaisimmat tavat suojata tietokonettaan sekä ympäristöään suurimmilta tietoturvauhilta. Tämän myötä jokainen työntekijä voi sopivalla ajalla katsella videon ja oppia sen pohjalta. Tämän vuoksi ei tarvitse järjestää varsinaisia koulutuspäiviä, jotka yrityksen johdon mielestä ovat usein hankalasti järjestettävissä, että jokainen pääsisi paikalle.

2 PROJEKTIN TAUSTAT

Aluksi avaamme taustaa aiemmin tehdyistä projekteista kohdeyritykselle helpottaaksemme kokonaisuuden hahmottamista. Opintojemme edetessä työskentelimme usean kurssin yhteydessä kohdeyrityksen tietoturvan parissa syksyn 2014 ja syksyn 2015 välisenä aikana. Yhteistyö lähti liikkeelle tietoturvariskikartoituksesta. Tämän kartoituksen tarkoituksena oli herätellä yritystä tietoturvan tärkeydestä ja sen merkityksestä nykyaikaiselle liiketoiminnalle. Kartoitus oli yritykselle ensimmäinen, mikä näkyi kartoituksesta saaduista tuloksistakin. Ongelmia oli hyvin monella osa-alueella ja tietämys tietoturvasta todella heikkoa. Kartoitus toteutettiin haastattelemalla yrityksen johtoa sekä teettämällä kyselytutkimus yrityksen henkilöstölle. Kysely lähetettiin jokaiselle henkilöstön jäsenelle ja vastausprosentti oli äärimmäisen hyvä. Haastattelun ja kyselytutkimuksen vastausten pohjalta laadimme yritykselle raportin, jossa esitimme tulokset ja annoimme vinkkejä ilmenneiden epäkohtien kanssa toimintaan jatkoa ajatellen.

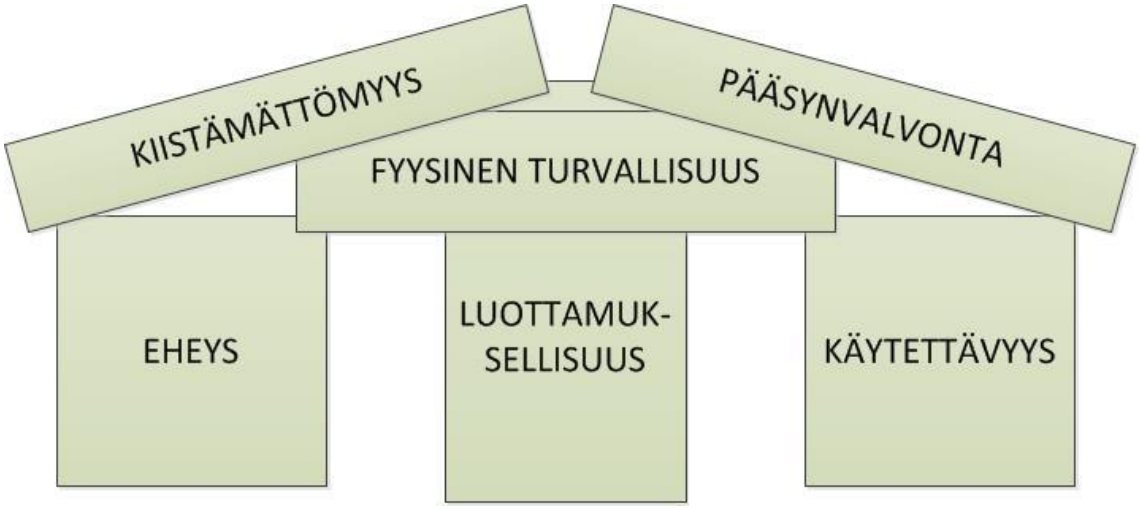
Tietoturvariskikartoitusta seurasi kohdeyrityksen tietoturva-auditointi. Auditointi tähtäsi tietoturvan syvempään tutkimiseen, tähtäimenä tietoturvapolitiikan luominen. Tietoturvapolitiikka helpottaa yrityksen toimintaa tietoturvan osalta, kun yhteiset toimintamallit siihen liittyen ovat tiedossa. Aiemmin yrityksellä ei ollut minkäänlaista ohjeistusta tietoturvallisesta toiminnasta.

3 TIETOTURVAN JA RISKIENHALLINNAN PERUSTEITA

Yritysten toiminta on päivä päivältä riippuvaisempi verkossa olevista tiedoista ja tietojärjestelmistä. Tästä syystä tietoturvasta huolehtimisesta on tullut tärkeä osa organisaatioiden päivittäistä toimintaa. Tietoturvallisuus on pieniä tekoja yritysten päivittäisessä toiminnassa. Hyvin toteutettu tietoturvallisuus ei ole erillinen osa yritystoimintaa, vaan kuuluu organisaatiokulttuuriin. Tavoitteena on, että kaikki ymmärtävät tietoturvallisuuden tärkeyden ja työskentelevät sen saavuttamiseksi ja ylläpitämiseksi. Tietoturvallisuuteen kuuluvat hyvin suunnitellut ja toteutetut tekniset ja hallinnolliset toimet. Hyvän tietoturvallisuuden saavuttamiseen ja sen ylläpitoon vaaditaan määrätietoista toimintaa ja johtamista. Tietoturva tulisi nähdä kilpailuetuna, joka realisoituu liiketoiminnan jatkuvuuden parantumisella sekä mahdollisuuksina voittaa tarjouskilpailuja, joissa on mukana tietoturvavaatimuksia. (Laaksonen ym. 2006, 17–18.) Tässä luvussa esitellään tietoturvan keskeisimmät asiat, kuten tietoturvallisuuden määritelmät ja osa-alueet.

3.1 Tietoturvallisuuden määritelmät

Klassinen tiedon arvoon perustuva määritelmä koostuu kolmesta osatekijästä, jotka ovat luottamuksellisuus, käytettävyys ja eheys. Klassinen määritelmä on lyhyt ja tiivis ja sisältää tärkeimmät osat, joista tulee huolehtia ennen muita tietoturvallisuuden osatekijöitä. (Hakala ym. 2006, 4–5.)



Kuvio 1. Tietoturvallisuuden osatekijät. (Hakala ym. 2006, 6)

Luottamuksellisuudella tarkoitetaan sitä, että tietojärjestelmässä olevat tiedot ovat vain niiden käsissä, joilla on niihin pääsyyn oikeus. Jotta luottamuksellisuuteen päästäisiin, tulee tietojärjestelmien laitteet ja tietovarastot suojata käyttäjätunnuksin ja salasanoin. Erityisen arvokkaat ja arkaluontoiset tiedot on syytä suojata salakirjoitusmenetelmillä. (Hakala ym. 2006, 4.)

Käytettävyys merkitsee järjestelmän toimivuutta ja toimivuusastetta. Käytännössä tietojen saatavuuden pitäisi olla riittävän nopeaa, ja tietojen tulee olla saatavilla tietojärjestelmästä käyttäjän haluamassa muodossa, kuten yhteenvetona tai valmiina raporttina. Riittävästä nopeudesta pidetään huolta siten, että tieto- ja tietoliikennejärjestelmien laitteet ovat riittävän tehokkaita, ja käytettävät ohjelmistot soveltuvat järjestelmään tallennettujen tietojen käsittelyyn mahdollisimman hyvin. (Hakala ym. 2006, 4–5.)

Eheydellä tarkoitetaan datan muuttumattomuutta ilman asianmukaisia oikeuksia. Eheyden toteutuessa esimerkiksi hyökkäyksessä tapahtuva muutos tulisi ainakin havaita. Eheyteen pyritään ohjelmointi- sekä laitteistoteknisillä ratkaisuilla. Ohjelmointiteknisellä ratkaisulla sovelluksiin sisällytetään erilaisia syötteen tarkistuksia tai varmistussummia. Laitteistoteknisillä ratkaisuilla pyritään estämään virheet käyttämällä virheenkorjaavia muisteja tai väyliä. (Hakala ym. 2006, 4–5.)

Nykyisin klassista tiedon arvoon perustuvaa määritelmää ei pidetä kuitenkaan tarpeeksi kattavana, sillä siinä ei huomioida riittävästi tiedon tuottajan tai omistajan identiteettiä eikä laitteistojen tai tieto- ja tietoliikennejärjestelmien arvoa. Tästä syystä määritelmää on laajennettu kahdella osatekijällä, jotka ovat kiistämättömyys ja pääsynvalvonta. (Hakala ym. 2006, 5.)

Kiistämättömyyden toteutuessa tietojärjestelmä tunnistaa ja tallentaa luotettavasti järjestelmää käyttävän henkilön tiedot. Henkilö ei voi siis menestyksellisesti kiistää tekoa, jonka hän on tehnyt. Kiistämättömyys voidaan saavuttaa käyttämällä erilaisia tunnistusmenetelmiä. Yleisimpiä tarkoitukseen kehitettyjä tunnistusmenetelmiä ovat älykortit tai muut pienet mukana kuljetettavat laitteet, joihin on tallennettu käyttäjän henkilötiedot sekä käyttölupa. Muita käytettyjä tunnistusmenetelmiä ovat esimerkiksi sormenjälki- tai silmäntunnistuslaitteet. (Hakala ym. 2006, 5.)

Pääsynvalvonta sisältää niitä menetelmiä, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä. Yritykselle on tärkeää estää ulkopuolisia henkilöitä tai omaa henkilöstöään käyttämästä yrityksen laitteita tai verkkoa omiin tarkoituksiinsa. Luvattomat järjestelmän käyttäjät heikentävät käytettävyyttä kuormittamalla tietoliikenneverkkoa sekä laitteita.

Luvaton käyttö saattaa myös altistaa yrityksen tietojärjestelmät haittaohjelmille. Tämä puolestaan johtaa ongelmiin eheys- ja luottamuksellisuus-osatekijöiden kohdalla. Pääsynvalvontaan tulee kiinnittää erityistä huomiota, jos yrityksessä käytetään langattomia verkkoja. (Hakala ym. 2006, 5–6.)

3.2 Riskienhallinta

Tietoturvariskien tunnistaminen ja niihin varautuminen kuuluu jokaisen yrityksen toimintaan. Kaikkia uhkia vastaan ei ole järkevää tai mahdollista varautua, mutta riskit tulee tiedostaa. Tietoturvariskien arviointi tehdään yrityksessä asetettujen tavoitteiden ja strategioiden mukaan. Tietoturvatoimenpiteet tulee perustaa kattavaan riskikartoitukseen. Yrityksessä on huolehdittava siitä, että tietoturvariskejä arvioidaan säännönmukaisesti yhtenä osana yrityksen muuta riskienhallintaa ja toiminnansuunnittelua. Alan jatkuvasta kehittymisestä johtuen tietoriskien arviointia tulisi suorittaa säännöllisesti vallitsevan lainsäädännön ja toimintaympäristön vaatimusten mukaan. (Andreasson & Koivisto 2013, 39.)

3.2.1 Riskikartoitus

Riskikartoitus toteutetaan aivoriihessä, jonka alkuvaiheessa muistellaan jo realisoituneita riskejä, jotka ovat johtaneet tietojen menettämiseen, vuotamiseen tai vahingoittumiseen. Tämän jälkeen pohditaan todennäköisiä ja odotettavissa olevia riskejä. Riskikartoitusta tehtäessä hyvä lähestymistapa on kerätä mieleen tulevia asioita miellekarttaan (mind map). Miellekarttatekniikassa ei pyritä heti alussa tarkkaan jäsenneltyyn rakenteeseen, vaan tarkoituksena on purkaa ihmisten mieliin painuneita tietoja ja näkemyksiä, joita voidaan käyttää hyväksi riskienhallintasuunnitelmassa. Kun miellekarttaan on listattu historia ja nykytilanne, voidaan siirtyä tarkastelemaan tulevaisuutta. (Hakala ym. 2006, 29.)

Riskien ja uhkakuvien löydyttyä voidaan alkaa arvioida riskien todennäköisyyttä ja vaikutuksia yrityksen toimintaan. Vaikutuksia tarkastellaan pääsääntöisesti yrityksen taloudellisten ja toiminnallisten seuraamusten näkökulmasta. Riskin realisoitumistodennäköisyyttä ja vaikutuksia voidaan luokitella karkeasti kolmiportaisella (pieni, kohtalainen ja suuri) asteikolla tai tarkemmalla, 10-portaisella asteikolla. Luokittelun voi aloittaa ensin karkeasti ja sitä voidaan suunnitelman edetessä tarkentaa. (Hakala ym. 2006, 29.)

3.2.2 Riskien minimointi ja vahinkoihin varautuminen

Kun uhkatekijät ja riskit on löydetty ja niiden merkittävyys yrityksen toiminnan takaamiseksi on selvitetty, voidaan siirtyä etsimään keinoja niiden välttämiseksi. Miellekarttaan kerätyistä riskeistä valitaan ne riskit ja uhkatekijät, jotka vaativat suojautumista, ja niihin aletaan miettiä teknisiä ja toiminnallisia ratkaisuja. Ratkaisuja tulisi arvioida ainakin seuraavista näkökulmista:

- Pitääkö ratkaisuun pääsemiseksi hankkia uutta osaamista?
- Mitä ratkaisu kustantaa välittömästi ja välillisesti?
- Onko valitulla ratkaisulla vaikutuksia muihin tietojärjestelmiin?
- Pitääkö jo olemassa olevia toimintatapoja muuttaa?

Löydettyjä ratkaisuja verrataan keskenään käyttäen yksinkertaista kolmiportaista asteikkoa: vähän, kohtalaisesti tai paljon. Mitä useampaan kysymykseen saadaan vastaukseksi ”vähän”, sitä parempana ratkaisua voidaan pitää sekä taloudellisesti että toiminnallisesti. (Hakala ym. 2006, 31.)

3.2.3 Vahingoista toipuminen

Vaikka tavoitteena on, että riskit eivät pääse realisoitumaan, voi vahinkoja ja onnettomuuksia tapahtua varotoimista huolimatta. Kaikkiin riskeihin, joihin on päätetty varautua, tulee sisällyttää myös toipumissuunnitelma vahinkojen minimoimiseksi. Toipumissuunnitelma kirjataan myös miellekarttaan kunkin kyseessä olevan riskin yhteyteen. (Hakala ym. 2006, 31.)

3.3 Käyttäjäoikeuksien hallinta

Tässä luvussa käsitellään käyttäjäoikeuksien hallintaa yleisellä tasolla.

3.3.1 Identiteettien ja käyttövaltuuksien hallinta

Identiteettien ja käyttövaltuuksien hallinnalla tarkoitetaan toimintaprosesseja, välineitä ja sääntöjä, joita käytetään tietojärjestelmien asianmukaiseen hallinnointiin (Andreasson &

Koivisto 2013, 106). Päällimmäisenä tavoitteena on estää järjestelmän luvaton ja sallia luvallinen käyttö.

Identiteetillä tarkoitetaan kohdetta kuvailevien ominaisuuksien eli attribuuttien kokoelmaa. Tietotekniikassa kohteella tarkoitetaan tietojärjestelmän käyttäjää, ja sen attribuutteja voivat olla esimerkiksi käyttäjätunnus, nimi sekä valtuus jonkin palvelun käyttämiseen. Käyttäjän identiteetti on siis tosielämän vastine tietojärjestelmässä olevalle tietueelle. Esimerkiksi käyttäjätunnuksen *jodoe* tiedetään kuuluvan tosielämässä John Doe -nimiselle henkilölle. Myös muilla kuin henkilöillä voi olla identiteetti. Yrityksen attribuutteja voivat olla kotipaikka, nimi ja Y-tunnus, ja verkkoon yhteydessä olevalla tietokoneella niitä voivat olla IP-osoite, domain-nimi ja julkinen avain. Identiteetin- ja pääsynhallinnan ongelmat keskittyvät kuitenkin useimmiten ihmisten identiteettiin, sillä organisaatioiden toiminta perustuu loppujen lopuksi niiden organisaatiossa työskentelevien ihmisten toimintaan, jotka tarvitsevat käyttövaltuuksia tietojärjestelmiin. (Linden 2012, 10–11.)

3.3.2 Roolipohjainen käyttäjäoikeuksien hallinta

Roolipohjaista käyttövaltuuksien hallintaa pidetään yleensä hyvänä ratkaisuna. Tätä menetelmää käyttämällä määritellään ensin käyttäjäroolit ja toiminnot, jotka kullakin roolilla on käytettävissään. Lopuksi määritellään jokaiselle käyttäjälle rooli sen mukaan, millaisia oikeuksia hän toimissaan tarvitsee. (Andreasson & Koivisto 2013, 106.) Roolipohjaisen käyttövaltuuksien hallinnan erityisenä hyötynä on vähentää hallinnallisia kustannuksia, kun pääkäyttäjän ei tarvitse syöttää samoja tietoja jokaiselle käyttäjälle erikseen (Bertino & Takahashi 2011, 154).

4 AUDITOINNIN JÄLKEISEN TILANTEEN KARTOITTAMINEN

Opinnäytetyömme tähtää kohdeyrityksen tietoturvatason parantamiseen. Jotta tähän voitaisiin ryhtyä, on selvitettävä, missä tilassa yrityksen tietoturva on auditoinnin ja tietoturvapolitiikan luomisen jälkeen. Tilanteen kartoittamiseksi päätimme haastatella yrityksen johtoa, sillä muun henkilökunnan kuormittaminen kyselyllä ei välttämättä antaisi tarkoitusta palvelevaa materiaalia. Lisäksi johtoportaan käsitys asiasta tulee olemaan työmme kannalta tärkein, ja he osaavat oletettavasti parhaiten informoida meitä siitä, mihin kaikkeen auditoinnin jälkeen ryhdyttiin.

4.1 Laadullinen tutkimus

Käsitteenä laadullinen tutkimus ei ole yksiselitteinen, vaan riippuu usein tulkintatavasta. Toisin kuin kvantitatiivinen eli määrällinen tutkimus, laadullinen tutkimus ei perustu tilastollisiin menetelmiin, joissa tutkitaan laskennallisesti mitattavaa tietoa (Pitkäranta 2014, 9). Tavoitteena laadullisessa tutkimuksessa on ymmärtää, selittää, tulkita ja usein myös mallintaa ja soveltaa jotain tiettyä tutkittavaa ilmiötä (Pitkäranta 2014, 33). ”Laadullinen tutkimus painottuu usein tulevaisuuteen. Sen avulla parannetaan, kehitetään tai uudistetaan tutkittavaa kohdetta” (Pitkäranta 2014, 9). Tämän työn tapauksessa kohde on yrityksen tietoturva. Työssä on tarkoitus tutkia tietoturvaan vaikuttavia tekijöitä, ja tutkimuksen perusteella analysoida, miten näitä tekijöitä muuttamalla saada tietoturvan taso tämänhetkistä paremmaksi.

Laadullista tutkimusta on lähestyttävä isona kokonaisuutena. Jo alkuvaiheessa on pohdittava myöhemmin tulevaa kerätyn aineiston analysointia ja sitä, miten saada parhaiten tarkoitusta palvelevaa aineistoa. (Pitkäranta 2014, 9.)

Aineiston riittävyyttä arvioimme litteroidun haastattelun informaation laadun sekä jo aiemmin kerättyjen yritystä käsittelevien tietojen pohjalta. Haastattelimme vain yhtä henkilöä. Hän edustaa yrityksen johtoa ja oli saanut kysymykset haastattelua varten etukäteen. Näin ollen vastaukset olivat sisällöltään erittäin selkeitä ja havainnollistivat tämän hetkistä tilannetta siten, ettemme kokeneet muiden henkilöiden haastattelemista tarpeelliseksi.

4.2 Haastattelu tutkimusmenetelmänä

Haastattelu on tiedonhankinnan perusmuotoja. Joustavana menetelmänä se soveltuu monenlaisiin tarkoituksiin. Sillä voidaan saada syvällistä tietoa, joka on meidän kannaltamme äärimmäisen hyvin tarkoitukseen sopivaa. Haastattelu koetaan yleensä metodina, jonka tutkimuksen osapuolet tuntevat miellyttäväksi. (Hirsjärvi & Hurme 2001, 11.) Onnistuneimpaan lopputulokseen pääsemme parhaiten, mikäli haastateltava saa kertoa mahdollisimman omin sanoin tilanteesta ja tuoda lisäksi esille sellaisiakin asioita, joita ei välttämättä osata kysyä.

Haastattelua, jossa kysymyksien vastauksia ei ole sidottu vastausvaihtoehtoihin, vaan haastateltava saa vastata omin sanoin, kutsutaan puolistrukturoiduksi haastatteluksi (Hirsjärvi & Hurme 2001, 47). Tätä haastattelumuotoa kutsutaan myös teemahaastatteluksi. Haastattelurunko on mietittävä tarkkaan, jotta keskustelua voidaan ohjata oikeaan suuntaa, mutta kun kohdataan tärkeäksi tai hyödylliseksi havaittu aihe, on siihen mahdollisuus tarttua mahdollisimman monipuolisesti.

Päätehtävänämme on kuitenkin löytää tietoturvan kannalta isoimmat edelleen olemassa olevat ongelmat ja epäkohdat yrityksen tämänhetkisessä toimintamallissa ja menettelytavoissa. Omista ongelmista on aina vaikea keskustella, ja vielä hankalammaksi tilanteen tekee se, että niitä kaikkia ei välttämättä edelleenkään tiedosteta. Tästä syystä vapaasti vastattava, keskustelunomainen haastattelu lienee tilanteena helpompi haastateltavalle ja tarjonnee rehellisempiä ja informatiivisempia vastauksia haastattelijalle kuin tenttaava kaavamainen haastattelu.

Teemahaastattelussa etukäteen valittavat teemat perustuvat jo tiedettyyn tietoon tutkimuksen kohteesta eli niin sanottuun viitekehykseen (Tuomi & Sarajärvi 2009, 75). Näin ollen koostamamme haastattelun teemat ovat rakentuneet aiemman kartoituksen sekä muun kohdeyritykselle tehdyn työn aikana kertyneestä tiedosta. Aiempi tietämys auttaa selvittämään, ovatko asiat muuttuneet parempaan suuntaan ja mikäli ovat, onko muutosten vaikutus tietoturvatasoon riittävä.

4.3 Haastattelun perustelu ja valmistelu

Opintojemme aikana yritykseen tekemämme riskikartoituksen yhteydessä paljastui useita epäkohtia tietoturvassa. Havaintomme tietoturvaa uhkaavista tekijöistä sai toivotun, silmiä avaavan reaktion yrityksessä. Tämän johdosta yritykselle luotiin tietoturvapolitiikka helpottamaan organisaation tietojen turvaamista. Politiikasta ei kuitenkaan ole apua, mikäli sitä ei noudateta. Tilanteen parantamisen kannalta tulee tietää, mikä tilanne on nyt.

Vaikka aiemmasta kartoituksesta ei vielä ole merkittävän pitkä aika, ei työ ole menossa hukkaan. Kartoitus tulisi joka tapauksessa uusia säännöllisin väliajoin ja lisäksi aina, kun tietoturvan toteuttamisessa tapahtuu muutoksia (ISO 17799 2006, 40). Kun tietoturvapolitiikan luomisen jälkeinen tilanne on kartoitettu, on tarkoituksenamme keskittyä suurimpiin laiminlyönteihin ja epäkohtiin sekä keskeisimpiin asioihin, joihin tietoturvapolitiikan pohjalta olisi tullut ryhtyä. Politiikan luomisen jälkeen emme ole olleet yhteydessä yritykseen ennen opinnäytetyöprosessin aloittamista.

4.4 Haastattelun kulku

Pohtiessamme haastattelun rakennetta ja kysymyksiä, joilla haastattelua tultaisiin ohjaamaan, päädyimme keskittymään viimekertaisessa kartoituksessa havaittuihin epäkohtiin. Koostimme kysymyksiksi osittain samoja asioita käsitteleviä kysymyksiä kuin aiemmassa kartoituksessa, mutta lisäsimme syvemmälle aiheeseen meneviä kysymyksiä Kimmo Rouskun Tutti-työkalusta. Tutti-työkalu on tietoturvan itsearviointityökalu. Työkalussa on sekä pika-arvio että laaja-arviointi, joka käsittelee tietoturvaa todella yksityiskohtaisesti (Rousku 2012). Syvemmälle aiheeseen menevillä kysymyksillä haluamme kartoittaa aiemmin havaittuja epäkohtia joille on jo suoritettu jonkinlaisia parannustoimenpiteitä. Vaikka toimenpiteitä olisikin tehty, ne eivät välttämättä ole riittäviä. Tällä tavoin selviää, ovatko toimenpiteet olleet tarpeeksi laajoja, ja onko tietoturvan tasoa nostettu riittävälle tasolle.

Haastattelun jaamme viiteen kokonaisuuteen. Tämä helpottaa haastattelun jälkeistä kysymysten analysointia sekä tulosten esittämästä ja läpikäymistä yrityksen kanssa. Lisäksi itse haastattelutilanteessa viisi kokonaisuutta toimivat muistilistana ja tarpeellisena

keskustelua ohjaavana kiintopisteenä (Hirsjärvi & Hurme 2006, 66). Ne tulevat myös helpottamaan mahdollisen vapaan keskustelun syntymistä kunkin kokonaisuuden osalta, kun tiedetään, missä aihealueessa liikutaan.

4.5 Haastattelun purku

Seuraava osio sisältää haastattelun purkamisen. Kokonaisuuden selkeyttämiseksi pidimme tärkeänä, että haastattelu on sisällytetty opinnäytetyöhön. Haastattelu puretaan teema-alue kerrallaan. Ennen kysymyksiä perustellaan teema-alueen valintaa, sen sisältämiä kysymyksiä ja sitä, mitä kysymyksillä on haluttu saada selville. Perustelua seuraavat itse kysymykset, joiden yhteydessä on aina suorina lainauksina vastaukset yrityksen johdon edustajalta, joka tässä tapauksessa on yrityksen hallintojohtaja, jonka vastuualueisiin kuuluu muun muassa tietoturvallisuus. Haastattelua seuraavassa osiossa analysoimme tilannetta ja esitämme toimenpide-ehdotukset.

4.5.1 Tietoturvapolitiikan käsittely

Ensimmäinen kysymysosio keskittyy selvittämään, kuinka paljon aiemmin tekemäämme tietoturvapolitiikkaan on perehdytty. Tietoturvapolitiikan tavoitteena on johdon tarjoama tuki ja ohjaus liiketoimintatavoitteiden ja asianmukaisten lakien mukaisesti (ISO 17799 2006, 28). Päällimmäisenä ajatuksena tässä osiossa on saada selville ajatuksia, joita tietoturvapolitiikka herätti, sekä otettiinko se heti tarkasteluun ja käsittelyyn. Lisäksi on erittäin tärkeää tietää, kuinka hyvin henkilöstö on tietoturvapolitiikkaan perehtynyt. Koko organisaation tulisi olla sitoutunut politiikan noudattamiseen.

Koetteko, että tietoturvapolitiikasta on ollut teille hyötyä?

”Suuri hyöty. Yritys on ollut aina ”pienehkö perheyhtiö”, tietoturva on asia, johon ei olla hirveästi paneuduttu. On vain tehty ja tehty. Tällä hetkellä tekemänne ja jo aiemmin tehty työ on avannut suuresti silmiä, että tietoturva on muutakin kuin tietokoneen suojaaminen salasanalla. Tämä on antanut pohjaa aiheen todelliselle laajuudelle. Ajankohta on myöskin siinä mielessä hyvä, että asiaan tullaan panostamaan lähitulevaisuudessa, kun organisaatio on nyt kohta vuoden ollut ison organisaation osa, jonka johdosta vaatimukset asian suhteen ovat kasvaneet.”

Käytiinkö tietoturvapolitiikkaa läpi henkilöstön kanssa?

”Tietoturvapolitiikka käytiin johtoryhmässä läpi, todettiin hyväksi asiaksi ja päätettiin, että viedään asia eteenpäin, kun isommat fuusioon liittyvät kokonaisuudet saadaan toteutettua. Tulevien muutosten jälkeen näin saadaan koko uudelle yhtenäiselle organisaatiolle luotua yhteiset pelisäännöt kerralla. Näin ollen asia tullaan viemään eteenpäin tulevan syksyn aikana.”

Onko tietoturvapolitiikka henkilöstön saatavilla?

”Ei tällä hetkellä, myös tämä on odottamassa ensi syksyä. Kun fuusioon liittyvät toimet saadaan suoritettua, otetaan tietoturva työn alle. Tällöin myös tietoturvapolitiikka tullaan käsittelemään henkilöstön kanssa ja tuomaan henkilöstön saataville.”

Onko yrityksen johto sitoutunut suomaan resursseja tietoturvalle ja tietoturvapolitiikalle (ollaanko valmiita käyttämään resursseja tietoturvan parantamiseen esim. koulutuksen muodossa)?

”Asian tärkeys nähdään ja tämän myötä resursseja on mahdollista suoda.”

4.5.2 Tietoturvakulttuuri sekä -vastuut

Toinen kysymysosio käsittelee kohteessa vallitsevaa tietoturvakulttuuria, tietoturvaan liittyvää vastuuta sekä sen tuntemista. Aikaisemmassa kyselyssä kävi ilmi, että tietoturva on yrityksen henkilöstölle melko uusi käsite, eikä sen vaikutusta työskentelyyn osattu hahmottaa. Kysymyksillä pyritään kartoittamaan sekä yrityksen tämänhetkistä suhtautumista tietoturvaan käsitteenä että sen tuomaa vastuuta jokapäiväisessä työskentelyssä. Lisäksi koimme erittäin tarpeelliseksi ottaa puheeksi EU:n uuden tietosuojauudistuksen.

Onko organisaatioonne muodostunut oikeanlainen tietoturva-asenne sekä hyvä tietoturvakulttuuri? (Rousku 2012)

”Aiemmin tehdyn kartoituksen yhteydessä henkilöstöllä teetetty kysely oli varsin hyvä herätys. Tämä herätti ihmisiä ajattelemaan uudestaan ja eri tavalla tätä asiaa. Esim. yksinkertainen asia: Tämän myötä ovet ovat nykyään lukittuna, jolloin kukaan ulkopuolinen ei pääse liikkumaan yrityksen tiloissa ja näin ollen pääse työntekijän koneelle tai käsiksi pöydällä oleviin asiakirjoihin. Edelleen ollaan tietenkin varsin alkutekijöissä tällä saralla, mutta pieni ajatuksen siemen asiasta on jokaisella.”

Tunteeko henkilöstö tietoturvan merkittävyyden nykyaikaisessa työympäristössä?

”Tiettyyn rajaan asti varmasti, mutta koko laajuutta ei silti pystytä vielä käsittämään. Silmät aukesivat tietoturvan merkityksellisyydestä aiemmin tehdyn riskikartoituksen yhteydessä, kun koko henkilöstölle teetettiin kysely."

Kuka on viime kädessä vastuullinen henkilö tietoturvan saralla?

”Viime kädessä minä.”

Tunteeko henkilöstö omat vastuunsa tietoturvan osalta päivittäisessä työskentelyssä?

”Hyvin kevyellä tasolla, perusasiat ovat hallussa varmasti. Mutta laajemmalla mittapuulla, mitä kaikkea tähän liittyy ja mitä tämä koskee, ei välttämättä löydy riittävää ymmärrystä.”

Tunteeko yritys lakisääteisesti sitä koskevat vastuut tietoturvan/tietosuojan osalta?

”Jos ajatellaan henkilötietoja ja niiden suojaamista, ovat asiat hyvin hallussa ja vaatimuksista ollaan kartalla. Ainakin minun näkökulmasta, kun viime kädessä olen asiasta vastuussa. Vaikka tässä on varmasti ohjeistamista muulle organisaatiolle, henkilöt, jotka päivittäin ovat näiden asioiden – siis henkilötietojen – kanssa tekemisissä, tietävät vastuunsa.”

EU:n tietosuojauudistuksen myötä uusi direktiivi velvoittaa yrityksissä tietosuojavastaavan nimeämiseen. Onko yrityksessä perehdytty asiaan?

”Tämä oli täysin uusi asia yritykselle, joten äärimmäisen tärkeää, että asia tuli tietoon.”

4.5.3 Tietoturva päivittäisessä työssä ja päätöksen teossa

Hyvä tietoturva edellyttää tarkkuutta ja valintoja päivittäisessä työskentelyssä jokaiselta organisaation jäseneltä. Tietoturvan yhteydessä puhutaankin niin sanotusta 80/20-säännöstä, jonka mukaan tietoturvassa 80 prosenttia on psykologiaa ja vain 20 prosenttia tekniikkaa (Järvinen, 2012. 24). Useissa vahinkotapauksissa onkin kyseessä inhimillinen virhe tai huolimattomuus.

Tietoturva on lisäksi otettava huomioon myös päätöksenteossa. Tietoturvalle tulisi suoda resursseja esimerkiksi laitehankintoja tai koulutuksia varten, sillä näin pystytään pitämään sekä laitteisto että henkilöstön tietotaito tietoturvan osalta ajan tasalla. Kysymyksillä halusimme selvittää organisaation käytäntöjä ja menettelytapoja erinäisissä arkisissa tilanteissa nyt, kun tietoturva on havaittu merkitykselliseksi tekijäksi.

Onko yritys kohdannut tilanteita, jossa tietoturva on joutunut uhatuksi/ollut uhattuna?

”Ei ainakaan olla tietoisia asiasta. Mikäli näin on käynyt, on tekijä onnistunut täysin.”

Onko tullut tilanteita, jossa henkilöstö on huomannut tietoturvaa vaarantavan puutteen/ongelman?

”Ei toistaiseksi ole.”

Päätöksiä tehdessä, esimerkiksi laitteisto- tai järjestelmähankintojen yhteydessä, vaikuttaako tietoturva päätöksiin/pohditaanko asiaa myös sen kannalta?

”Tällä hetkellä painopiste on enimmäkseen toiminnallisuudessa. Eli ei voida sanoa, että tietoturva olisi ainakaan se ensimmäinen kriteeri päätöksen teossa.”

Onko tietoturvaa laiminlyöty siten, että tästä on aiheutunut toimenpiteitä?

”Ei toistaiseksi.”

Yrityksellä oli aiemmin ulkoistettuja palveluita IT:n osalta, onko näiden osapuolten kanssa kiinnitetty enemmän huomiota tietoturvaan/keskusteltu muuten aiheesta?

”Asioista on totta kai keskusteltu. Tällä hetkellä ulkoistuksia on kaksi. Viime syksynä toiminnanohjausjärjestelmä päivitettiin ja se siirtyi samalla pilveen. Tämä tarkoittaa, että samassa vastuu esim. tietojen varmuuskopioinnista siirtyi palveluntarjoajalle ja päivitykset hoituvat automaattisesti. Lisäksi yrityksellä on käytössään Apple-tuki. Heidän kanssaan asiasta on keskusteltu ja asia ymmärrettiin todella hyvin.”

Perehdytetäänkö uudet työntekijät myös tietoturvan ja tietoturvapolitiikan osalta?

”Uusia henkilöitä on tullut, mutta perehdytystä tämän osalta ei ole tehty. Firmaan tulee kuitenkin henkilöstöpäällikkö, jonka yksi uusista tulevista tehtävistä tulee olemaan uuden työntekijän perehdyttäminen myös tietoturvan osalta.”

4.5.4 Luotettavuus, eheys ja saatavuus

Nykyaikana yrityksen omistamat tiedot ovat lähes missä tahansa yrityksessä avainroolissa. Monen yrityksen toiminta saattaisi loppua kokonaan, mikäli tiedoille kävisi jotain sellaista, ettei niihin pääsisi enää käsiksi. Alkutilanteessa ensimmäisen kartoituksen yhteydessä havaitsimme, että tietojen säilytyksessä ja niiden kanssa menettelyssä oli selkeitä puutteita. Koimmekin nyt ensiarvoisen tärkeäksi selvittää, mikä tilanne on ollut tietoturvapolitiikan luomisen jälkeen, kun asia on tuotu yritykselle ilmi. Halusimme myös selvittää ja näin myös havainnollistaa yritykselle, ovatko he arvioineet tiedon merkitystä omalle liiketoiminnalleen.

Säilytetäänkö yrityksen tietoja muualla kuin yrityksen omissa tiloissa?

”Ulkoistetun palvelun myötä kyllä.”

Testataanko varmuuskopioita?

”Tämä on hyvä kysymys. Asiasta ei ole tietoa. Tämä pitää selvittää, sillä tällainen asia ei saa jäädä roikkumaan.”

Onko säilytettävä tieto vain sitä tarvitsevien käyttäjien saatavissa?

”Suurimpaan osaan kaikki pääsevät käsiksi ja näin pitääkin olla. Mutta on myös tiedostoja jotka ovat kohdennettuja vain tietyille ihmisille. Esim. johtokunta pääsee vain heidän pöytäkirjoihinsa käsiksi.”

Onko tietojen tärkeyttä ja/tai merkitystä liike-/ydintoiminnalle arvioitu?

”Lähes kaikki yrityksen toiminta nojaa tietoihin ja niiden käyttöön. Mikäli tietoihin ei pääsisi käsiksi, ei yrityksen toiminta voisi käytännössä enää jatkua.”

Pääseekö yrityksen tietoihin käsiksi muualta kuin yrityksen tiloista, esimerkiksi etäyhteydellä kotoa käsin? Vaaditaanko etätyöskentelyyn esim. VPN-yhteyttä?

”Tietoihin pääsee käsiksi muualtakin, esimerkiksi kotoa etätöitä ajatellen. VPN-yhteys on kuitenkin vaadittu tätä varten.”

Kerätäänkö ja käsitelläänkö verkoista, laitteista ja järjestelmistä lokitietoja?

”Tästä asiasta ei ole täyttä varmuutta. Mikäli lokeja kerätään, en tiedä käytetäänkö niitä varsinaisesti. Toistaiseksi ei ole ainakaan ollut tarvetta tutkia lokeja esim. väärinkäytösten takia.”

4.5.5 Laitteistot ja järjestelmät

Tietoturva on pääosin kiinni käyttäjien toiminnasta, mutta laitteistot ja järjestelmät näyttelevät silti suurta roolia asianmukaisen toiminnan ohella. Laitteisto- ja järjestelmäturvallisuuden osa-alueeseen sisältyy laitteiden ja järjestelmien tarkoituksenmukainen mitoitus, toiminnan testaus, varautuminen ajan tasalla pitämiseen sekä järjestelyt huollon kannalta (Hakala ym. 2006, 12).

Aiemmin tehdyn kartoituksen aikana selvisi, että kohdeyrityksellä oli epäselvyyksiä laitteidensa ajan tasalla pitämisessä, automaattisissa tarkastuksissa ja päivityksissä. Valtaosa maailmalla tapahtuvista tietomurroista ja haittaohjelmatartunnoista olisi voitu välttää, tai ainakin tietomurtautujan onnistumista olisi voitu vaikeuttaa, mikäli ajantasaisia päivityksiä ei olisi laiminlyöty (Andreasson ym. 2014, 34). Katsoimme merkitykselliseksi kiinnittää tämänkertaisessa kartoituksessa huomiota siihen, ovatko nämä perustason asiat edelleen riskialttiissa tilassa.

Pidetäänkö yrityksessä laiterekisteriä?

”Asia on parhaillaan tekeillä. Vastaavista tehtävistä huolehtimiseen on palkattu uusi henkilö, joka tulee huolehtimaan, että asia pysyy ajan tasalla.”

Onko palomuurilaitteisto ajan tasalla (ei vanhempi kuin 5 vuotta)?

”Laitteisto on ajan tasalla.”

Onko yrityksellä käytössä automaattiset päivitykset?

”Toiminnanohjausjärjestelmässä ja omalla palvelimella kyllä. Tietokoneissa tämä on parhaillaan työn alla.”

Tarkastetaanko laitteistot säännöllisesti/automaattisesti virusten varalta?

”Tietääkseni kyllä, säännöllisesti ja usein.”

Huolehtiiko organisaatio siitä, että organisaation tietojärjestelmissä ei ole tunnettuja tietoturvahaavoittuvuuksia? (Rousku 2012)

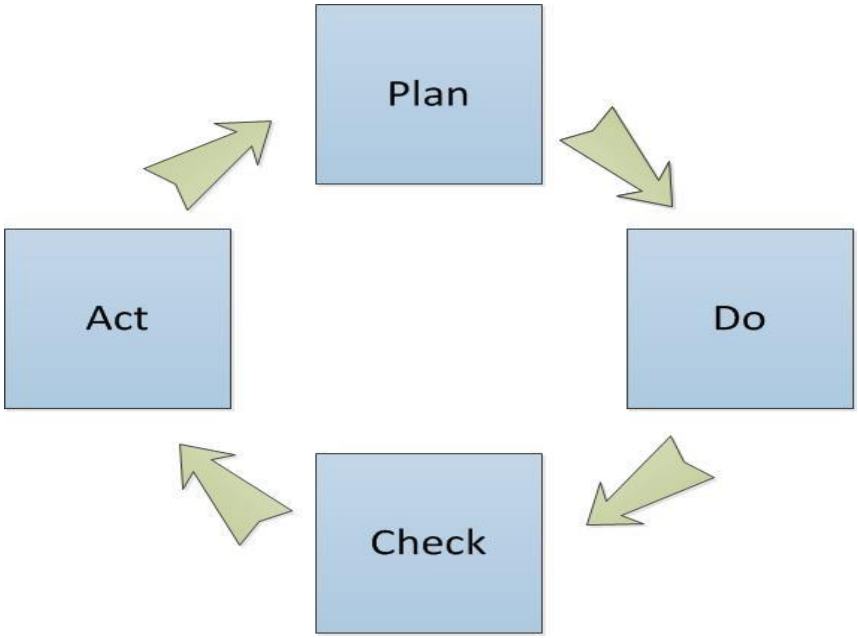
”Tämä on kunnossa.”

5 TILANTEEN ANALYSOINTI JA PARANNUSTOIMENPITEITÄ

Haastelu onnistui hyvin. Haastateltava oli tutustunut kysymyksiin etukäteen huolellisesti, minkä ansiosta haastattelutilanne oli sujuva ja vastaukset erittäin kattavia. Mistään aihealueesta ei varsinaisesti syntynyt kysymyksien ulkopuolista vapaata keskustelua. Tämä ei kuitenkaan tuota jatkon kannalta ongelmia, sillä jo monipuolisten vastausten puolesta aineistoa syntyi riittävästi. Seuraavassa osiossa käsitellään yrityksen tilannetta kunkin osa-alueen pohjalta ja esitetään korjausehdotuksia.

5.1 Tietoturvapolitiikan käsittely

On ensiarvoisen tärkeää, että tietoturvapolitiikka on koettu positiiviseksi asiaksi. Kuten selvisi, sitä on käyty läpi johtoryhmän kanssa, ja tietoturvapolitiikka tullaan tuomaan koko yrityksen tasolle suunnitellusti lähitulevaisuudessa. Asiaa ei saa niin sanotusti jättää roikkumaan vain suunnittelutasolle, jotta yrityksen koko henkilöstö saadaan noudattamaan samoja vakiintuneita tietoturvakäytäntöjä ja sääntöjä. On tärkeää, että prosessina tietoturva tullaan pitämään jatkuvassa Tietoturvastandardi ISO 27001:n mukaisessa PDCA-syklissä (Kuvio 2.). Sykli edellyttää aktiivisuutta ja tähtää toiminnan jatkuvaan kehittämiseen.



Kuvio 2. PDCA-mallin mukainen sykli

On positiivista, että yrityksen johto on valmis suomaan resursseja tietoturvallisuudelle, sillä tämä on iso osa toimivaa tietoturvajohtamista. Se ilmenee riittävien resurssien varaamisena, strategian ja politiikan luomisena sekä mahdollistamalla työntekijöiden osallistumisen tietoturvaa koskeviin asioihin. (Porvari 2013, 88). Näin tietoturva prosessina kulkee koko organisaation läpi, ylhäältä alas. Koko organisaation laajuisen tietoturvatyön pohjalle vaaditaan johdon tuki, millä pidetään huolta, että työn tekemisen edellytykset täyttyvät (Valtionvarainministeriö 2011).

5.2 Tietoturvakulttuuri sekä -vastuut

Haastattelun myötä ilmeni, kuinka paljon yrityksen tietoturvan osalta oli tapahtunut ensimmäisen kartoituksen ja tämän hetken välisenä aikana. Käytännön toimien lisäksi huomasimme, että yritykseen oli syntynyt selkeää tietoturva-ajattelua, jota ei aiemmin välttämättä pystynyt havaitsemaan lainkaan. Emme osanneet odottaa näin nopeaa reagointia. Hyvin paljon pieniä perusasioita on jo korjaantunut, mikä kertoo siitä, että onnistuimme herättämään yrityksen tietoisuuden tämän tärkeän aiheen osalta.

Tietoturvan perusasioiden hallitseminen on henkilöstölle minimivaatimus. Henkilöstön tietoturvaosaaminen sekä tietoisuus omista vastuista todennäköisesti kehittyvät luomamme koulutusvideon sekä myöhemmin henkilöstön käyttöön annettavan tietoturvapolitiikan sisäistämisen myötä.

Yrityksen tietoisuus heitä sitovista lakisääteisistä vastuista vaikutti olevan melko hyvällä tasolla etenkin tietyissä osissa organisaatiota. Kuitenkin pian voimaan tuleva EU:n tietosuojauudistus oli täysin uusi asia yritykselle. Oli todella tärkeää, että tämä asia tuli ilmi, sillä uudistus tulee koskemaan myös kohdeyritystämme. Tästä syystä käsittelemme uudistusta seuraavaksi.

5.3 EU:n tietosuojauudistus

EU:n tietosuojauudistuksen tavoitteena on luoda Euroopan unionille vahva, ajanmukainen, yhtenäinen ja kattava tietosuojakehys. Tavoitteena on myös parantaa luottamusta verkkoasiointiin ja täten edistää EU:n digitaalista sisämarkkinoiden kehittämistä. Asetus tulee voimaan aikaisintaan keväällä 2018, ja se korvaa vuonna 1995 annetun henkilötietodirektiivin. Asetuksella päivitetään ja nykyaikaistetaan tietosuojadirektiivin periaatteet. Tietosuojauudistus pitää sisällään muun muassa henkilötietojen käsittelyä koskevia periaatteita ja arkaluontoisten tietojen käsittelyä. (Tietosuojavaltuutetun toimisto 2015.)

Asetus koskee kaikenlaista henkilötietojen käsittelyä EU:n jäsenvaltioissa. Uusi asetus on tärkeä, sillä se yhdenmukaistaa eurooppalaista tietosuojasääntelyä, joka tällä hetkellä muodostuu 28 jäsenvaltion epäyhtenäisestä sääntelystä. Yhdenmukainen henkilötietolainsäädäntö EU:ssa tukee valtioiden rajat ylittävää kaupankäyntiä, ja kansalaisen on helpompi luottaa esimerkiksi verkkokauppoihin tietäessään, että hänen henkilötietojaan käsitellään asianmukaisesti. (Tietosuojavaltuutetun toimisto 2015.)

Asetuksen voimaantullessa yrityksillä on velvollisuus nimittää tietosuojavastaava ja ilmoittaa tietoturvaloukkauksista viranomaisille ja käyttäjille viivytyksettä. Tietosuojavastaava voi olla oma työntekijä tai esimerkiksi ulkopuolinen palveluntarjoaja. Yrityksen vastuulla on myös selvittää henkilötietojen keruuseen liittyvät riskit ja osoittaa viranomaisille, että lain vaatimuksia noudatetaan. (Hartikainen 2016.)

Tietosuoja-asetuksen noudattaminen on tärkeää jo mahdollisten seuraamusten takia, sillä törkeästä laiminlyönnistä voi joutua maksamaan sakkoa pahimmillaan 20 miljoonaa euroa tai neljä prosenttia yrityksen globaalista liikevaihdosta. (Hartikainen 2016.)

Tietosuojavastaavan tehtävänä on:

- Toimia asiantuntija-apuna rekisterinpidosta vastuussa oleville henkilöille tietosuojakysymyksissä
- Osallistua tietoturva- ja tietosuojariskien hallintaan
- Osallistua tietosuojavaatimuksien määrittelyyn uusia hankintoja ja projekteja tehdessä
- Toimia tarvittaessa yhteistyössä valvontaviranomaisten kanssa
- Toimia raportoijana yrityksen johdolle koskien tietosuojan tilaa ja kehittämistarpeita.
- Ilmoittaa yrityksen tiedotuskanavan kautta tietosuoja-asioista ja ohjeistaa niistä

(Andreasson ym. 2014, 19.)

Kohdeyrityksen tapauksessa tietosuojavastaavaksi sopisi parhaiten hallintojohtaja, joka vastaa tällä hetkellä tietoturvasta ja on jo perehtynyt henkilötietojen suojaamiseen sekä käsittelyyn. Vastuun määrä tehtävän myötä kasvaa kuitenkin valtavasti, mikä saattaa kuormittaa toisen työnkuvan jo omaavaa henkilöä suuresti. Mikäli koetaan tarpeelliseksi ja resurssit sen mahdollistavat, voisi tehtävään hallintojohtajan mukaan ajatella myös uutta työntekijää tai vaihtoehtoisesti jo aiemmin mainittua tehtävän ulkoistamista.

5.4 Tietoturva päivittäisessä työssä ja päätöksenteossa

Toistaiseksi yritys ei ole kohdannut sellaisia tilanteita päivittäisessä työskentelyssä, joissa tietoturva olisi joutunut uhatuksi tai henkilöstö olisi havainnut tietoturvaa vaarantavia virheitä tai puutteita. Tämä on tietenkin positiivinen asia. On kuitenkin otettava huomioon, että henkilöstön tietoturvaosaaminen on vasta perustavalla tasolla, mikä ei mahdollista välttämättä kaikkien uhkien havaitsemista. Tietoturvakoulutuksen ja henkilöstön kasvavan osaamisen myötä virheitä tullaan mahdollisesti jatkossa havaitsemaan enemmän. Lisäksi on otettava huomioon tietoturvaosaamisen kasvaessa, että laiminlyönneistä johtuvat, tietoturvapolitiikassakin mainittavat seuraamukset, ovat asiaankuuluvia ja oikeudenmukaisia.

Tietoturva ei ole hallintojohtajan mukaan hankintapäätöksiä tehtäessä tärkeimpiä valintakriteereitä. Yrityksen olisi kuitenkin tärkeää ottaa jatkossa tietoturva yhdeksi merkittäväksi kriteeriksi. Esimerkiksi järjestelmä- tai laitehankinnoissa tietoturvasta säästäminen saattaa koitua erittäin kalliiksi.

Yrityksen päivittäisessä työskentelyssä myös ulkoistukset ovat tärkeässä roolissa, koska toiminnanohjausjärjestelmän ylläpito on kolmannen osapuolen vastuulla. Tietoturvan läpikäyminen ulkoistuksia tehtäessä on jokaisessa yrityksessä tärkeä asia. Myös kohdeyrityksessä näin oli asianmukaisesti tehty, minkä ansiosta molemmat osapuolet ovat tietoisia vastuista sekä tarpeista.

5.5 Luotettavuus, eheys ja saatavuus

Kuten haastattelussa kävi ilmi, kohdeyrityksemme liiketoiminta nojaa vahvasti omistamiinsa tietoihin ja niiden käyttöön. Jo tästäkin syystä tietoja tulisi varjella huolella ja ymmärtää niiden merkityksellisyys, sillä ilman pääsyä niihin ei yrityksen toiminta voisi käytännössä enää jatkua.

Huomiota vaativa asia yrityksen toiminnassa on puutteellinen menettely lokitietojen kanssa. Oli epäselvää, kerätäänkö lokitietoja ylipäätään ja mikäli kerätään, ei niitä kuulemma varsinaisesti hyödynnetä. Lokeja hyväksi käyttäen voidaan selvittää käyttäjien toimintaa tietojärjestelmässä ja lupaa käyttää tietoja. Lokien ollessa todisteena on niihin pääsy rajattava käsittelyä, tuhoamista tai muuttamista varten vain tähän oikeutetuille henkilöille, kuten tietoturvapäällikölle tai -vastaavalle. (Andreasson ym. 2015, 138–139.)

5.5.1 Varmuuskopiointi

Aiemmin yrityksen ongelmana oli varmuuskopiointi ja -kopioiden säilytys. Tiedot sijaitsivat vain yrityksen omissa tiloissa, eikä niitä esimerkiksi testattu säännöllisesti. Tilanne on nyt huomattavasti parempi, sillä tiedot sijaitsevat ulkoistuksen myötä myös kolmannen osapuolen tiloissa. Varmuuskopioiden testauksen kanssa esiintyy kuitenkin epätietoisuutta, mitä olisi hyvä hälventää ensitilassa.

Varmuuskopioinnin perusperiaatteena on tietokoneen levyillä olevien tietojen varmentaminen. Varmuuskopiointi on yksinkertaisimmillaan tiedostojen kopiointia tietokoneesta USB-tikulle, mutta yritysmaailmassa tarvitaan usein huomattavasti monimutkaisempia

menetelmiä. Valitettavan usein varmuuskopioinnin tärkeyteen havahdutaan vasta vahingon jo satuttua, eli kun tiedostopalvelin on jo hajonnut esimerkiksi vesivahingon, tulipalon tai ylijännitepiikin seurauksena, tai kun tietokoneen käyttäjä on poistanut tahattomasti hakemistollisen tiedostoja. Käyttöönottovaiheessa varmuuskopiointiin kuluu yrityksen resursseja niin laitehankintoina kuin työtunteina, mutta tämän jälkeen toimenpide tapahtuu lähes huomaamattomasti ja automaattisesti.

Varmuuskopioinnin tärkeys realisoituu parhaiten, kun ajattelee sitä, mitä kaikkea yritys voi menettää tietojen kadotessa. Mahdollisesti konkreettisin ja valitettavin menetys on asiakkaat. Asiakkaan luottamus yritystä kohtaan kärsii hänen kuullessaan tapahtumasta, jossa yritys on menettänyt tietoa piittaamattomuuden seurauksena. Lisäksi tiedon levitessä tämä vaikuttaa siihen, miltä yritys näyttää kilpailijoiden silmissä, jolloin niille annetaan mahdollisuus käyttää tätä yritystä vastaan. Pahimmassa tapauksessa tietokannan tuhoutuessa yritys voi myös kirjaimellisemmin kadottaa asiakkaansa, jos asiakkaasta ei löydy merkintöjä tietokannan ulkopuolelta. Varmuuskopioinnin tärkeyttä ajateltaessa ei tule myöskään unohtaa henkilökunnan työmoraalin heikentymistä, kun heidän mahdollisesti päivien tai viikkojen ajan tekemänsä työ menee hukkaan tietojen kadotessa lopullisesti. (Preston 2007, 9–10.)

Optimaalisinta tietenkin olisi, jos yritys voisi ottaa kopiot kaikista tiedostoistaan joka yö. Tämä ei kuitenkaan ole käytännössä mahdollista tietojärjestelmien suurien kokojen takia. Nyrkkisääntönä voidaan pitää sitä, että täydellinen varmistus otetaan kerran viikossa ja edelliseen täydelliseen varmuuskopioon lisättävät varmuuskopioinnit suoritetaan päivittäin (Koivuniemi 2009). Täydellinen varmuuskopiointi tarkoittaa sitä, että tietokoneen levy kopioidaan kokonaisuudessaan. Tästä syntynyttä suurta tiedostoa kutsutaan levykuvaksi. Varmuuskopiointiaikatauluja suunniteltaessa voidaan käyttää eri varmuuskopiointitasoja, jotka määrittelevät, milloin mitäkin tiedostoja varmistetaan. (Preston 2007, 28.)

Taulukko 1. Varmuuskopiointitasot (Preston 2007, 28)

Taso 0	Täydellinen varmuuskopio
Taso 1	Varmuuskopio, joka varmistaa kaikki muutokset, jotka ovat tapahtuneet edellisen tason 0 varmistuksen jälkeen.
Tasot 2–9	Jokainen taso varmuuskopioi muutokset, jotka ovat tapahtuneet seuraavaksi alemmalla tasolla.

Tasoja 0–9 käyttämällä saadaan riittävän kattava aikataulutus varmistuksille. Täydellisen tason 0 varmuuskopion otto on hyvä ajoittaa sunnuntaille, jolloin tietojärjestelmän käyttö on minimissä. Tämän jälkeen seuraavien tasojen varmistukset ajastetaan otettaviksi seuraavina päivinä yksi kerrallaan.

Taulukko 2. Varmuuskopiointiaikataulu (Preston 2007, 31).

Sunnuntai	Maanantai	Tiistai	Keskiviikko	Torstai	Perjantai	Lauantai
Taso 0	Taso 1	Taso 2	Taso 3	Taso 4	Taso 5	Taso 6

Yhdysvaltalaisyritys Imation Corporationin tekemän tutkimuksen mukaan ainoastaan 32 prosenttia yrityksistä testaa ja arvioi säännöllisesti varmuuskopiointijärjestelmänsä toimivuuden vähintään kerran vuosineljänneksessä, joka on suositeltu vähimmäisvaatimus. Suositeltavaa olisi kuitenkin tarkistaa varmistusten toimivuus kerran kuukaudessa. (Koivuniemi 2009.)

5.5.2 Tietojen luokittelu

Tällä hetkellä osa yrityksen tiedoista on jo joissain määrin luokiteltua. Koimme kuitenkin tärkeäksi kertoa tietojen luokittelun perusasioista. Yrityksen tulee luokitella käsittelemänsä tiedot yhdenmukaisella tavalla ja opastaa työntekijät noudattamaan oikeaa tietojenkäsittelytapaa eri tasoilla (Rousku 2014, 156). Helpoin luokittelutapa on jakaa tiedot salaisiin ja julkisiin dokumentteihin. Useimmiten tapa osoittautuu kuitenkin liian karkeaksi, joten käytännöllisimmäksi tavaksi valikoituu kolmen tai neljän luokan käyttö. Monipuolinen jaotteluperiaate saadaan jakamalla tiedot erittäin salaisiin, salaisiin, luottamuksellisiin ja julkisiin tietoihin. (Raggad 2010, 6–8.)

Tietoturvauhkien jatkuva kehittyminen ohjaa yrityksiä siihen, että erittäin salaiseksi luokiteltua tietoa tulisi käsitellä ainoastaan ympäristössä, josta ei ole pääsyä internetiin. Ympäristöön tuotaisiin tietoa ulkopuolelta vain tarkasti harkituilla ja valikoiduilla menetelmillä. Menetelmänä voisi käyttää esimerkiksi vain tähän tarkoitukseen käytettävää salattua USB-tikkua. (Rousku 2014, 156–157.)

Seuraavaksi korkeimman eli salaiseksi luokitellun tiedon käsittely saisi tapahtua internetverkkoon liitetyillä laitteilla, mutta tietoa käsiteltäessä verkkoon ei tulisi olla suoraa yhteyttä. Yhteyden terminointi voi tapahtua esimerkiksi käyttämällä SSH-pääte- tai virtualisoitua istuntoa siten, että salaista tietoa käsittelevän henkilön työasema ei ole suoraan internetissä. Menetelmää käyttämällä mahdollisesta haittaohjelmasta koituva uhka kohdistuisi ainoastaan terminoituun pääteistuntoon eikä käyttäjän työasemaan ja siellä pidettäviin salaisiin tietoihin. Salaiseksi luokiteltuja asiakirjoja ei saisi myöskään käsitellä älypuhelimilla tai tableteilla ilman erillisiä ratkaisuja. (Rousku 2014, 157.)

Kolmannen tason eli luottamukselliseksi luokitellun tiedon käsittely sallitaan normaalisti verkkoon kiinteällä tai langattomalla yhteydellä olevalla laitteella. Tässä tapauksessa riittää päätelaitteiston tietoturvallisuudesta huolehtiminen tietoturvaohjelmistoilla kuten haittaohjelmantorjunnalla ja palomuurilla (Rousku 2014, 157). Kohdeyrityksessämme myös VPN-yhteys on vaadittu etätyöskennellessä.

Alin, eli julkinen taso käsittää informaatiota jota yritys voi jakaa esimerkiksi verkkosivuillaan tai yritystä koskevassa mainonnassa. (Raggad 2010, 8.)

5.6 Laitteistot ja järjestelmät

Kohdeyrityksessä on ollut huomautettavaa useassa osa-alueessa. Kuitenkin tarkasteltaessa laitteistoja ja järjestelmiä tilanne on nyt hyvin kelvollinen aiempaan verrattuna. Päivitykset ja tarkastukset tapahtuvat automaattisesti ja laitteet ovat tarpeeksi uusia. Kun laitteet ovat ajan tasalla, pienenee tietoturva-aukkojen todennäköisyys näissä merkittävästi.

Huomautimme laiterekisterin puuttumisesta aiemmin tehdyn auditoinnin yhteydessä. Tilanteen parantamiseksi on kohdeyrityksessä nyt palkattu henkilö, jonka vastuulla kyseisen rekisterin luominen ja käyttöönotto on. Laiterekisteri on hyödyllinen ainoastaan sen ollessa ajan tasalla, minkä vuoksi laiterekisterin ylläpidon on oltava jatkuvaa ja säännöllistä. Tällä tavoin tiedetään, mitä laitteita kunkin henkilöstön jäsenellä on käytössään ja ettei tuntemattomia laitteita loju kohdeyrityksen tiloissa.

6 TIETOTURVAKOULUTUS

Tietoturvakoulutus on tänä päivänä suuressa roolissa yrityksissä. Jotta yrityksen tietoturvallisuus voidaan taata, tulee jokaisen työntekijän noudattaa annettuja ohjeita. Yksi suurimmista tietoturvariskeistä ovatkin juuri työntekijät itse. Huono tai puuttuva koulutus voi johtaa pahoihin tietoturvavuotoihin tai -hyökkäyksiin. Kun tietoturvakoulutus on säännöllistä, tietoturva on yrityksessä vakaampaa, koska työntekijät ovat jatkuvasti ajan tasalla tietoturva-asioista ja esimerkiksi uusista uhkista. Vankkaa työntekoa ja työntekijöiden turvallisuutta tukee hyvä tietoturvatietoisuus.

”Tietoturvakoulutusta tarvitaan siihen, että voidaan lisätä tietoisuutta ja muuttaa vääriä toimintamalleja ja -tapoja. Pelkällä ohjeistuksella ei enää nykyisin pärjää, vaan koulutusta tarvitaan sen lisäksi. Yrityksen riskien hallinnasta iso osa on nimenomaan saada ne toimintaan kohdistuvat suurimmat riskit pois, mikä taas vaatii sitä, että henkilökunta tiedostaa uhkat ja riskit ja osaa toimia oikein”, sanoo Tieturin osastopäällikkö Ismo Kantola. (Kirves 2004.)

6.1 Tietoturvakoulutuksen teoria

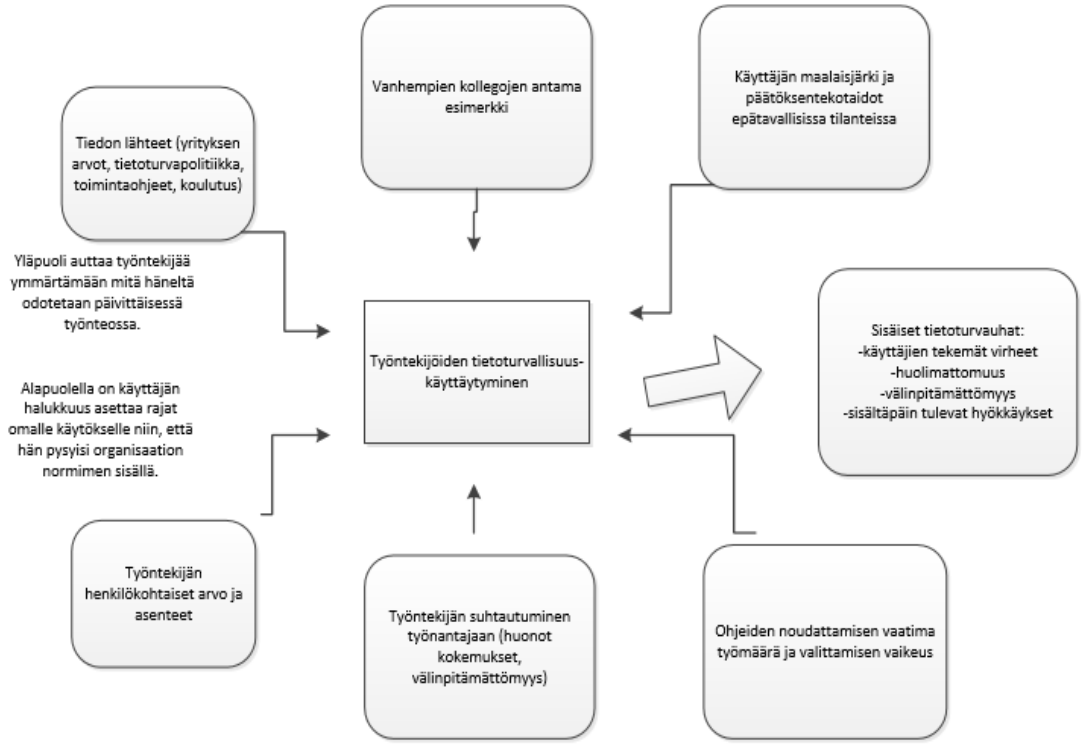
Tietoturvaosaamiseen ja sen kouluttamiseen vaikuttavat monet asiat. Myönteiset ajatukset tietoturvasta lähtevät organisaation ylimmästä portaasta. Johdon asenne tietoturvaosaamista ja -kouluttamista kohtaan vaikuttaa suuresti siihen, millä mallilla organisaation tietoturvallisuus on. Kun yritys käyttää resurssejaan parempaan tietoturvamateriaaliin ja niiden pohjalta pidettäviin koulutuksiin, työntekijät osaavat varautua erilaisiin riskeihin. Johdon tulisi myös varmistaa, että jokainen työntekijä osallistuu koulutuksiin tai lukee mahdolliset materiaalit heti työhön tullessaan sekä aina tiedon päivittyessä.

Jotta materiaalit ja koulutus saisivat työntekijöiden täyden kiinnostuksen, tulisi työntekijöiden ymmärtää tietoturvariskit, jotka vaikuttavat heidän työhönsä. Myös sen sisäistäminen, miten näiden riskien toteutumista voitaisiin ehkäistä, on merkittävää. (Laaksonen ym. 2006, 258.)

Kun jokainen työntekijä on ymmärtänyt omaan työhönsä liittyvät riskit, on koulutuksessa hyvä käydä läpi ainakin seuraavat asiat:

- Peruskäsitteet

- Tietoturvan tavoitteet
- Tietokoneen, internetin sekä sähköpostin käyttö
- Tietoturvan vastuuhenkilöt
- Etätyö
- Miten toimia ongelmatilanteissa
- Tietoturvan laiminlyönnin seuraamukset



Kuvio 3. Yrityksen tietoturvakäsikirja (Laaksonen ym. 2006, 249).

Kuvio 3 esittää työntekijöiden työkäyttäytymistä. Kuvion mukaan henkilöstön tietoturvakäyttäytymiseen liittyy organisaation näkökulmasta kolme asiaa, jotka ovat kuvattuna kuvion ylemmässä osiossa. Yrityksen arvot, työntekijöiden kokemukset työnantajasta ja toimintaohjeet toimivat tiedonlähteinä työntekijöille ja auttavat heitä ymmärtämään yrityksen henkilöstöön kohdistamia odotuksia. Tietojenkäsittelyn ja tietoturvariskien hallinta

vaatii organisaation luonteen ja kulttuurin ymmärtämistä sekä näkemystä siitä, miten erilaiset toimintatavat voivat vaikuttaa henkilöstön käyttäytymiseen. (Laaksonen ym. 2006, 248–249.)

Jotta yrityksessä voitaisiin muuttaa henkilöstön omaksumia vääränlaisia toimintatapoja, tietoturvakoulutuksen tulisi pitää sisällään myös eettistä koulutusta paitsi tietoturvan tärkeyden tiedostamiseksi myös asenteiden muuttamiseksi. (Nykänen 2011, 21–22.)

Tietoturvakoulutuksesta voi vastata oman yrityksen tietoturvavastaava, tai koulutusta varten voi hankkia ulkopuolisen tietoturva-asiantuntijan. On kuitenkin tärkeää, että asiantuntijalta löytyy myös koulutusosaamista, sillä pedagogisen osaamisen puute voi estää tärkeän asian ymmärrettäväksi tekemisen. (Mattord & Whitman 2010, 197.)

Yksinkertainen tapa aloittaa koulutus on kirjoittaa ohjelehtinen siitä, kuinka toimia tietoturvauhan alla ja kuinka estää uhat. Teimme yritykselle tietoturvakartoituksen jatkeeksi henkilöstön tietoturvaohjeen, jossa käytimme pohjana Valtiovarainministeriön tekemää tietoturvaohjetta. Siinä kerrotaan tietoturvallisuuden ohjeet pähkinänkuoressa sekä ohjataan henkilöstöä käyttämään tietokoneitaan tietoturvallisesti (ks. 6.3 Tietoturvaohjeistus).

6.2 Koulutusvideo

Koska yrityksellä ei ollut ennestään mitään tietoturvaperehdytysmateriaaleja, päädyimme tekemään myös koulutusvideon. Video kertoo tärkeimmät tiedot tietoturvasta, sen uhista ja uhkien estämisestä. Usein pelkkä tekstivihkonen ei innosta työntekijää kiinnostumaan asiasta. Yksi suurimmista tietoturvauhista ovat työntekijät itse, jos heitä ei ole koulutettu oikein, ja sen vuoksi videon tarkoituksena on hauskalla ja tehokkaalla tavalla opettaa työntekijöitä varautumaan suurimpiin tietoturvauhkiin. Yrityksen johtoa haastateltuamme oivalsimme, että video olisi paras tapa saada jokaisen työntekijän huomio, sillä he voivat katsoa videon milloin tahansa, kun heille sopii. Myös uuden työntekijän saavuttua tietoturvaperehdytys pidetään tietoturvakoulutusvideon avulla. Video on noin kymmenen minuuttia pitkä.

Video alkaa peruskäsitteiden läpikäymisellä. Perusteissa käydään läpi, mitä tietoturvallisuudella tarkoitetaan ja miksi se on tärkeää. Heti videon alussa on hyvä tehdä selväksi, kuinka tärkeästä asiasta puhutaan, jotta työntekijän kiinnostus saadaan pysymään yllä koko videon ajan. Jokaisen työntekijän tulisi ymmärtää, kuinka paljon tietoturva vaikuttaa

hänen työhönsä joka päivä. Tämä ymmärretään usein aivan liian myöhään, jolloin ei ole enää mitään tehtävissä. Monet uhat ovat kuitenkin yksinkertaisilla asioilla estettävissä.

Seuraavana aiheena ovat työhön liittyvät tiedot. Jokaisen työntekijän, jolla on pääsy salassa pidettävään tietoon, tulee olla erityisen varovainen näiden dokumenttien kanssa. Dokumentit tulee merkata merkinnällä siitä, ketkä saavat dokumenttia lukea. Työntekijän tulee ottaa huomioon aineistoa tallentaessaan mihin ja miten sitä tallentaa, ja kuinka sitä voi turvallisesti lähettää eteenpäin. Tiedon hävittämisessä tulee käyttää niitä varten tarkoitettuja silppureita ja tietoturvasäiliöitä.

Omien tietojen ja yksityisyyden sekoittaminen työhön on helppoa, mutta ei kuitenkaan sallittavaa. Henkilökohtaiseen viestintään tulisi pääsääntöisesti käyttää omia yksityisiä sähköposteja eikä työsähköpostia. Kun työntekijä käyttää internetiä selailuun, siitä tallentuu yksityiskohtaista lokitietoa. Lokeja on työnantajan helppo tutkia, ja niitä voidaan valvoa, kuten aiemmin todettiin.

Oman tietokoneen käyttöä tulisi myös valvoa tarkasti. Videolla tästä opetetaan muun muassa kuinka tulee estää muiden henkilöiden pääsy omalle koneelle, ja kuka saa asentaa mitäkin ohjelmia koneelle. On myös tärkeää aina muistaa tallentaa tiedostoja useasti ja oikeisiin paikkoihin.

Fyysinen tietoturva jää usein unohduksiin. Monet eivät edes tiedä, mitä vaaroja oman yrityksen toimitiloissa voi olla. Tästä videolla kerrotaan tärkeimmät tilanteet. Työntekijän tulisi aina huomata työpisteelleen palattuaan, jos jotakin on muuttunut sinä aikana, kun on itse ollut muualla. On tärkeää muistaa piilottaa tärkeät tiedot siksi aikaa, kun on poissa työpisteeltään, ja paperit, joissa on yritykseen tai asiakkaaseen liittyvää tietoa, tulisi kääntää ylösalaisin. Näin ohikulkija ei pysty nopealla vilauksella näkemään mitään tietoja. Vieraat tulee aina saattaa ulos asti heidän lähtiessään eikä jättää heitä yksin kävelemään toimistoon.

Sosiaalinen media on suuressa suosiossa nykyään. Monet yritykset ovat Facebookissa ja Twitterissä ja työntekijät itse LinkedInissä. Sosiaalisessa mediassa kytee yhtä paljon tietoturvauhkia kuin muualla internetissä. Koulutusvideolla kerrotaan, mitä eroa on sillä, käyttääkö sosiaalista mediaa työntekijänä vai yksityishenkilönä. Kun internetiin laittaa jotain, ei voi olla varma, saako sitä koskaan sieltä pois. Käyttäjän tulee olla erittäin tarkka, mitä julkaisee itsestään tai yrityksestään.

Ongelmatilanteissa ohjeistetaan työntekijöitä ottamaan yhteyttä tietoturvavastaavaan, joka nimetään videolla. Työntekijällä on velvollisuus ilmoittaa kaikista poikkeuksista eteenpäin. Jos esimerkiksi kadottaa työssä käytettävän muistitikun tai kulkukortin, tulee siitä välittömästi kertoa tietoturvavastaavalle. Jos työntekijällä on hyviä kehitysideoita, kehotetaan häntä ehdottamaan ideaansa.

Lopuksi videolla kerrotaan, mistä saa lisätietoa tietoturvasta, jos aihe kiinnostaa enemmän. Muistutamme myös, että ongelmatilanteissa on aina käännyttävä välittömästi tietoturvavastaavan puoleen, minkä ansiosta monet uhat voidaan saada taltutettua ennen kuin niistä koituu suurempaa haittaa. Tietoturva lähtee työntekijöistä itsestään.

6.3 Tietoturvaohjeistus

Teimme yritykselle paperisen ohjeistuksen, joka tulisi olla helposti löydettävissä ja kaikkien ulottuvissa. Ohjeistuksen pohjana käytettiin Valtiovarainministeriön tekemää tietoturvaohjetta, jota vain hieman muutimme yrityksen tarpeiden mukaiseksi. Ohje on julkinen, ja sitä saa käyttää sellaisenaan yrityksen tietoturvaohjeistuksena. Ohjeistus löytyy opinnäytetyön liitteestä.

Tietoturvaohjeistus tehtiin työntekijöiden avuksi. Jos heille tulee ongelmia tietoturvan kanssa tai kysymyksiä tietoturvasta, he löytävät vastaukset helpoiten ohjeistuksesta. Ohjeistus tullaan myös antamaan uusille työntekijöille osana tietoturvaperehdytystä.

7 POHDINTA

Opinnäytetyöhön ryhtyminen oli mielekästä, sillä työssä pääsi entistä syvemmälle kohdeyrityksen tietoturva-asioihin. Koska opinnäytetyö oli osana pidempiaikaista yhteistyötä, oli myös ilo nähdä oman työmme tuottaneen tuloksia. Toivomme, että yritys jatkaa tilanteensa kehittämistä tietoturvan osalta yhtä suurella innokkuudella kuin yhteistyömme aikana.

Mielestämme työnjako ja opinnäytetyön rajaaminen onnistuivat hyvin, ja teoria- ja empiriaosat tukevat vahvasti toisiaan. Organisaation johdolta saatu tieto tietoturvapolitiikan jälkeisestä tietoturvatasosta oli todella kattavaa ja palveli tarkoitusta erittäin hyvin. Todella suurena yllätyksenä tuli se, kuinka pienessä ajassa organisaatiossa oli saatu parannettua tilannetta vajaan kahden vuoden takaisesta lähtötilanteesta**.**

Tiedonhankinta toteutettiin haastatteluna yrityksen johdon edustajan, hallintojohtajan, haastatteluna. Haastattelun kysymykset toimitettiin haastattelua varten etukäteen, jolloin haastatteluun valmistautuminen oli helpompaa ja näin ollen mahdollisimman paljon hyödyksi molemmille osapuolille.

Vaikka tietoturvan taso on lähtötilanteesta parantunut valtavasti, löytyi kuitenkin osa-alueita, joissa on edelleen parantamisen varaa. Pystyimme kuitenkin mielestämme tarjoamaan tilannetta parantavia toimenpide-ehdotuksia yritykselle, ja toivomme yrityksen kiinnittävän huomiota niihin.

Tulevaisuutta ajatellen etenkin uusien työntekijöiden perehdyttäminen tietoturvan osalta tulee varmasti helpottumaan luomamme perehdyttämisvideon avulla. Tämä säästää resursseja, kun henkilöstö voi perehtyä videoon tarvittaessa milloin tahansa ja tarpeen vaatiessa uudelleen, eikä organisaation tarvitse järjestää erillistä henkilöstön yhteen kokoavaa koulutustilaisuutta.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Andreasson, A.; Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Tallinna: Tietosanoma Oy

Andreasson, A.; Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 1. Riika: Tietosanoma Oy

Andreasson, A.; Koivisto, J. & Ylipartanen, A. 2014. Tietosuojavastaavan käsikirja 2. Tallinna: Tietosanoma Oy

Bertino, E. & Takahashi, K. 2011. Identity Management: Concepts, Technologies and Systems. Norwood: Artech House.

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

Hartikainen, J. 2016. Sakonuhka patistaa ryhtiliikkeeseen tietoturvassa. Kauppalehti 17.3.2016. Viitattu 28.3.2016 http://www.kauppalehti.fi/uutiset/sakonuhka-patistaa-ryhtiliikkeeseen-tietoturvassa/Tvg47xD3

Hartikainen, J. 2016. Tietosuojauudistuksesta versoo uutta liiketoimintaa. Kauppalehti 17.3.2016. Viitattu 21.3.2016 http://www.kauppalehti.fi/uutiset/tietosuojauudistuksesta-versoo-uutta-liiketoimintaa/nY4QsyuV

Hirsjärvi, S. & Hurme, H. 2001. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Järvinen, P. 2012. Arjen tietoturva – Vinkit & Ratkaisut. Jyväskylä: Docendo

Kirves, A. 2004. Mitä on tietoturvakoulutus, osa 1. Digitoday. Viitattu 27.4.2016 http://www.digitoday.fi/tietoturva/2004/01/13/mita-on-tietoturvakoulutus-osa-1/20046591/66

Koivuniemi, J. 2009. Imation: Vain 32 prosenttia yrityksistä testaa varmuuskopioinnin toimivuuden. Visionist 20.3.2009. Viitattu: 26.4.2016. https://visionist.fi/2009/03/20/imation-vain-32-prosenttia-yrityksista-testaa-varmuuskopioinnin-toimivuuden/

Laaksonen, M.; Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Mattord, H. & Whitman, M. 2010. Management of Information Security. Boston, MA: Course Technology Cengage Learning

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Tampere: Oulun Yliopisto, luonnontieteiden tiedekunta, tietojenkäsittelytieteiden laitos

Pitkäranta, A. 2014. Laadullinen tutkimus opinnäytetyönä. E-Oppi.

Porvari, P. 2013. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Helsinki: Unigrafia Oy.

Poutanen, P. 2009. Työpaikan tietoturvakoulutuksen suunnittelu, järjestäminen ja koulutusmateriaalin luonti. Opinnäytetyö. Opettajakoulun kehittämishanke. Tampere: Tampereen ammatillinen opettajakorkeakoulu. Viitattu 13.3.2016. https://www.theseus.fi/bitstream/handle/10024/8099/Poutanen.Pekka.pdf?sequence=2

Preston, C. 2007. Backup & Recovery - Inexpensive Backup Solutions for Open Systems. Sebastopol: O'Reilly

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press

Rousku, K. 2012. TUTTI v 2012 - TietotUrvallisuuden iTsearvioinTiväIne 3. osa. Tivi. Viitattu 11.5.2016 http://www.tivi.fi/blogit/2012-10-22/TUTTI-v-2012---TietotUrvallisuuden-iTsearvioin-Tiv%C3%A4lIne-3.-osa-3195686.html

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

SFS ISO/IEC 17799:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardoimisliitto SFS

SFS ry 2016. ISO 31000 Riskienhallinta. Viitattu 16.2.2016 http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_31000_riskienhallinta

Tietosuojavaltuutetun toimisto. Viitattu 21.3.1016 http://www.tietosuoja.fi/fi/index/lait/euntietosuojauudistus.html

Tuomi, J. & Sarajärvi, A. 2009. Laadullinen tutkimus ja sisällönanalyysi. Vantaa: Hansaprint Oy

VAHTI 2/2011 Johdon tietoturvaopas. Viitattu 20.4.2016 https://www.vahtiohje.fi/c/document_library/get_file?uuid=6068ca18-6214-4244-8ce6-dffe952e3e8e&groupId=10128&groupId=10229

VAHTI 4/2013 Henkilöstön tietoturvaohje. Viitattu 16.4.2016 https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10128&groupId=10229

Vallasvuo, K. 2012. Henkilöstön tietoturvakoulutuksen toteuttaminen valtionhallinnossa. Opinnäytetyö. Turvallisuusalan koulutusohjelma. Leppävaara: Laurea ammattikorkeakoulu. Viitattu 15.3.2016. https://www.theseus.fi/bitstream/handle/10024/53165/ONT_Vallasvuo_Kaisa.pdf?sequence=1

Yrityksen tietoturvaohjeistus

Tiedottaminen ja koulutus

• Seuraa tietoturvallisuuteen liittyviä organisaatiosi tiedotteita, tutustu ohjeisiin ja osallistu tietoturvakoulutukseen.

Tilojen turvallisuus

• Ohjaa kulkuoikeudetta olevat henkilöt ulos.

• Älä jätä tietokonettasi tai muita tärkeitä tiedonlähteitä vartioimatta neuvottelutiloihin.

• Älä jätä vieraita neuvottelu- tai työtiloihin yksin kokouksen tai tapaamisen jälkeen. Saata vieraat ulos asti.

Päätelaitteet

Kannettavia tietokoneita, pöytäkoneita, älypuhelimia, tabletteja jne., joita voidaan kutsua päätelaitteeksi, käytetään nykyään yhä useammin maksu- ja tunnistautumisvälineinä. Suojele niitä myös sen mukaisesti – kuten lompakkoasi.

• Älä anna ulkopuolisen henkilön käyttää päätelaitettasi.

• Varmista, että päätelaitteillasi, esimerkiksi puhelimessasi, on automaattiset lukitukset sekä salasana, jonka vain sinä tiedät.

• Lukitse tietokoneesi ruutu aina, kun poistut koneelta.

Tietoaineistojen käsittely

• Ole erityisen varovainen työskennellessäsi julkisissa tiloissa ja huomioi, että joku voi nähdä syöttämiäsi tunnuksia tai muita tietoja huomaamattasi tai salakuunnella keskusteluitasi.

• Julkista tietoa voi välittää internetin kautta yleisellä salaamattomalla sähköpostilla. Salassa pidettävän viestin välittämisessä internetin kautta on aina hyödynnettävä turvasähköpostia.

• Älä anna ulkopuolisten nähdä tietokoneesi näyttöruutua, kun käsittelet salassa pidettävää tietoa. Peitä myös näppäimistö, kun syötät käyttäjätunnuksia ja salasanoja, varsinkin yleisellä paikalla. Pyri käyttämään tietokoneesi näytöllä tietoturvakalvoa.

Tunnukset ja salasanat

Pankkiautomaatillakin suojaat tunnuslukusi tarkkaillen, ettei kukaan kurki olkapääsi yli. Noudata vastaavaa varovaisuutta työpaikallasi ja erityistä varovaisuutta julkisilla paikoilla.

• Älä luovuta henkilökohtaisia käyttäjätunnuksiasi tai salasanojasi toisen henkilön käyttöön.

• Käytä eri salasanaa eri palveluissa — työkäyttöön liittyviä tunnuksia tai salasanoja ei saa koskaan käyttää vapaa-ajan palveluissa.

• Pidä salasanasi mahdollisimman vahvana tekemällä siitä pitkä ja vaikea. Käyttämällä numeroita, isoja ja pieniä kirjaimia, ja pitämällä salasanan yli 8 kirjaimen pituisena, salasanasta saa vahvan. Se tulee olla helppo muistaa, mutta vaikea arvata.

• Vaihda salasana vähintään puolen vuoden välein tai silloin, kun epäilet sen paljastuneen.

Työvälineiden ja internetin käyttö

• Käytä työhösi liittyviä tietoaineistoja ja organisaatiosi antamia työvälineitä vain työtehtäviesi hoitamiseen.

• Ole varovainen — valitse tarvittaessa ”Peruuta”, jos www-sivu ei vaikuta luotettavalta ja sivusto suosittelee tai edellyttää tiedoston lataamista tietokoneellesi.

• Älä asenna ohjelmia tai tee niiden asetusmuutoksia, ellei se kuulu työtehtäviisi.

• Käytä vain organisaatiosi tietohallinnon hyväksymiä muistitikkuja tai muita lisälaitteita.

• Salaamaton muistitikku soveltuu vain julkisen tiedon siirtämiseen.

• Salatulla muistitikulla voit siirtää salassa pidettäviä tietoaineistoja vain organisaatiosi tietoaineistojen käsittelyohjeistuksen mukaisesti.

• Jos löydät tuntemattoman muistitikun, älä liitä sitä päätelaitteeseesi. Muistitikkujen kautta on helppo levittää viruksia tietokoneellesi.

Huomioithan, että työpöydälläsi olevat kuvakkeet, kansiot ja tiedostot eivät kuulu varmuuskopioinnin piiriin.

Sosiaalinen media

Muista, että aina kun käytät työorganisaatiosi laitetta, toimit organisaatiosi edustajana tietoverkossa.

• Huomioi, että palvelun ylläpitäjät pääsevät käsiksi kaikkeen palvelussa käsiteltävään tietoon, myös kahdenvälisiin keskusteluihin. Internetverkkoon päätynyttä tietoa voi olla mahdotonta poistaa jälkikäteen.

• Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä palveluissa tai järjestelmissä. Tämä koskee myös sosiaalisen median käyttöä.

• Käytä työsähköpostia vain työtehtäviesi hoitamiseen. Vapaa-ajan tehtäviin käytä omaa vapaa-ajan sähköpostiasi, älä työsähköpostiasi.

• Tiedätkö, mitä tietoa sinusta on kertynyt sosiaalisen median palveluihin? Hae tietoja nimelläsi ja tutki mitä löytyy. Tarvittaessa säädä palveluiden yksityisyydensuoja-asetuksia kovemmiksi.

Havaitsitko ongelman?

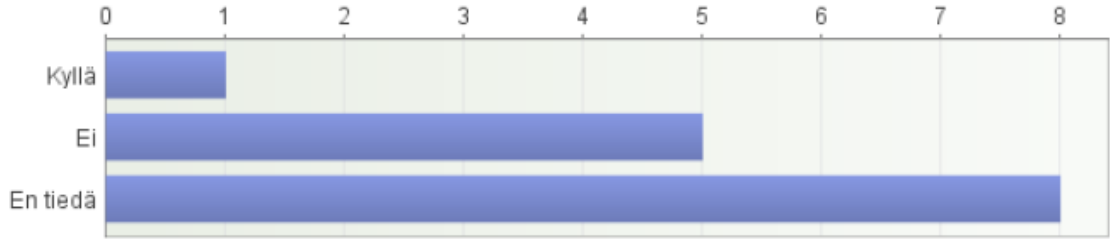
• Jos huomaat tietoturvaongelman, velvollisuutesi on kertoa siitä eteenpäin välittömästi. Älä luota siihen, että joku muu ilmoittaa ongelmasta tai korjaa sen.

• Ilmoita tietoturvallisuuteen liittyvistä ongelmista, uhkista tai suojauspuutteista organisaatiosi tietoturvavastaavalle tai esimiehellesi. Heidän velvollisuutensa on aloittaa toimenpiteet.

Auditoinnin yhteydessä tehty kysely kohdeyrityksen henkilöstölle

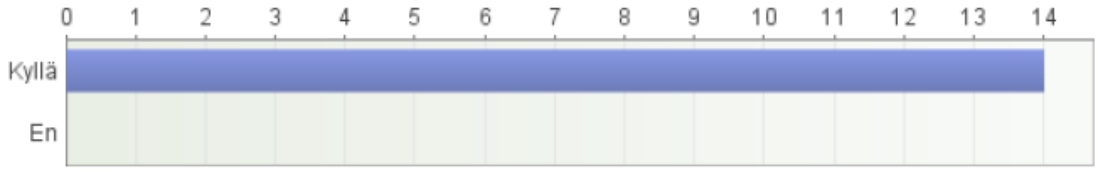
1. Onko yrityksessänne olemassa tietoturvaohjeistusta?

Vastaajien määrä: 14



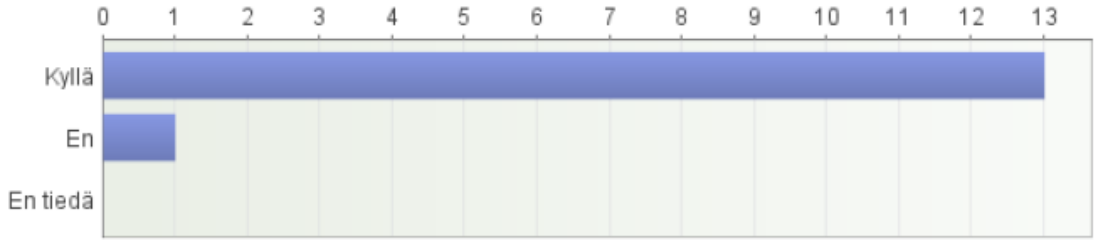
2. Tiedätkö keneen otat yhteyttä ongelmatilanteessa? (Esimerkiksi havaitessasi tietokone-/tietoturvaongelman)

Vastaajien määrä: 14



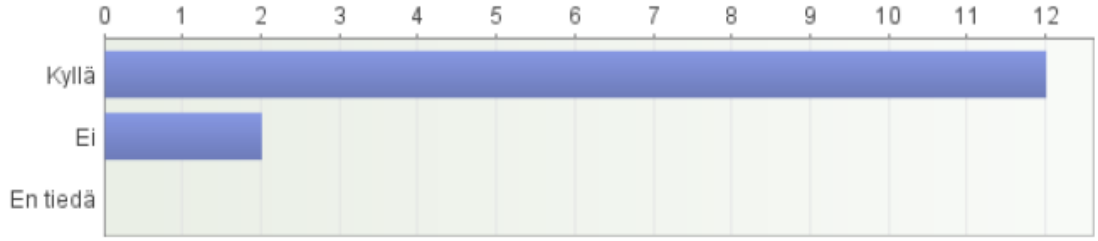
3. Käytätkö monimutkaisia salasanoja (pienet ja isot kirjaimet, numerot, erikoismerkit/pidempi salalause)?

Vastaajien määrä: 14



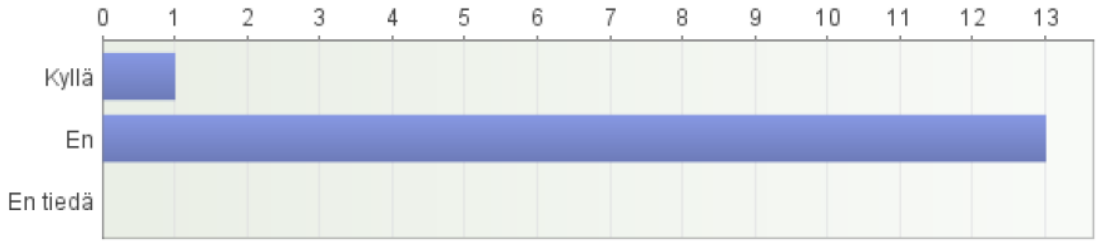
4. Onko salasanasi vähintään kahdeksan merkkiä pitkä?

Vastaajien määrä: 14



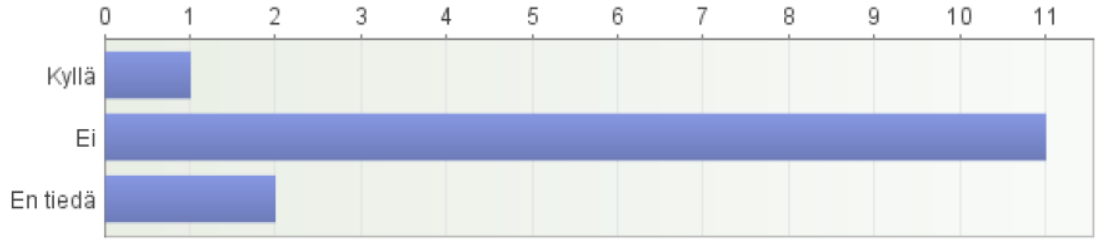
5. Vaihdatko salasanasi säännöllisesti?

Vastaajien määrä: 14



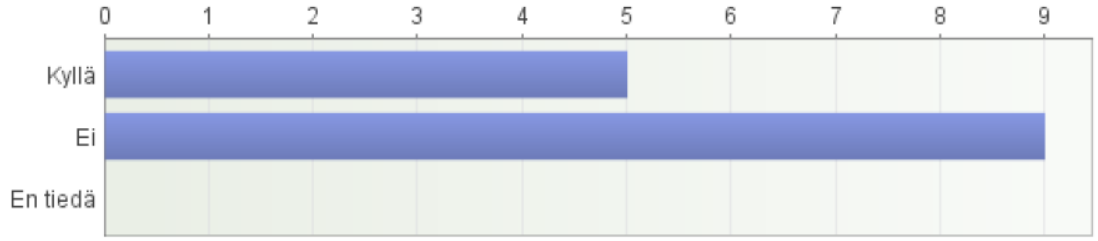
6. Vanhentuuko salasanasi tietyn ajan jälkeen?

Vastaajien määrä: 14



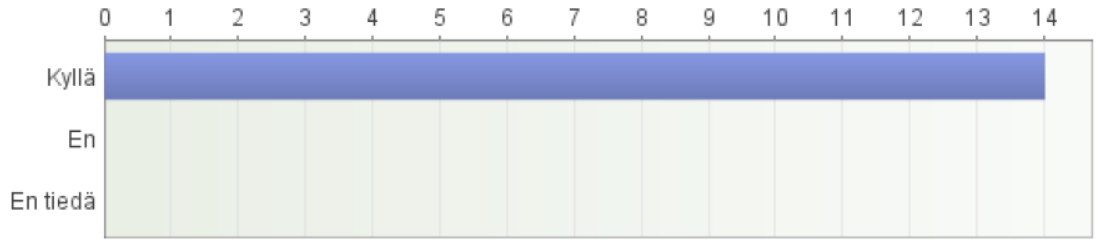
7. Onko sinulla tapana lukita tietokone (esim. salansasuojattu näytönsäästäjä) aina kun poistut koneen luota?

Vastaajien määrä: 14



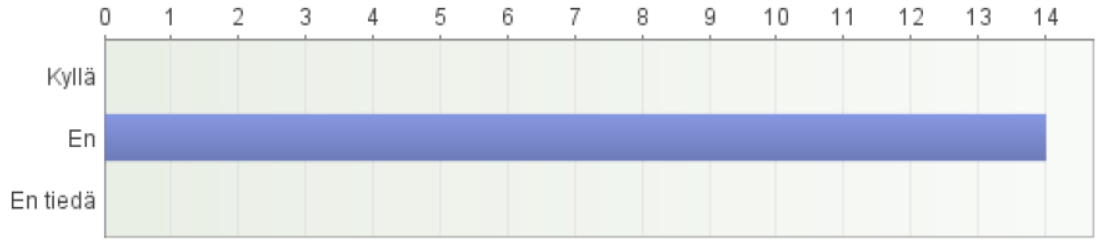
8. Käytätkö eri järjestelmissä eri salasanaa?

Vastaajien määrä: 14



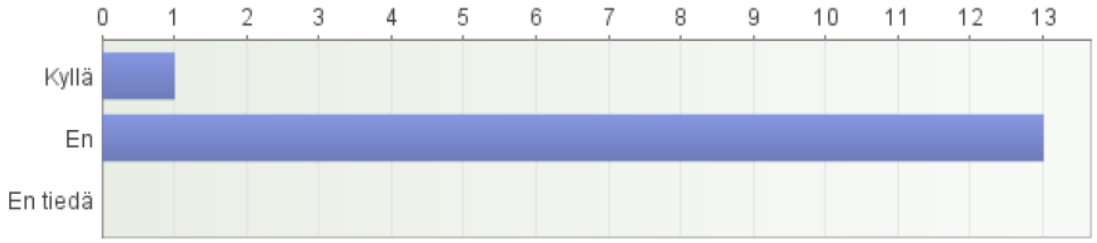
9. Säilytätkö yritystä koskevaa tietoa esim. kotitetokoneella tai muilla ei yrityksen laitteilla?

Vastaajien määrä: 14



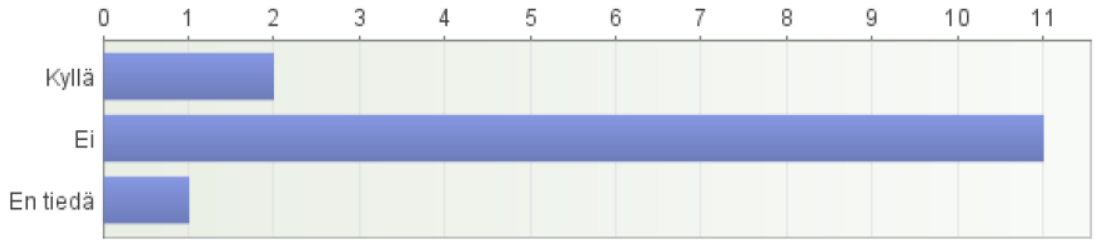
10. Säilytätkö yritystä koskevaa tietoa pilvipalvelussa? (Esimerkiksi OneDrive, DropBox, Box...)

Vastaajien määrä: 14



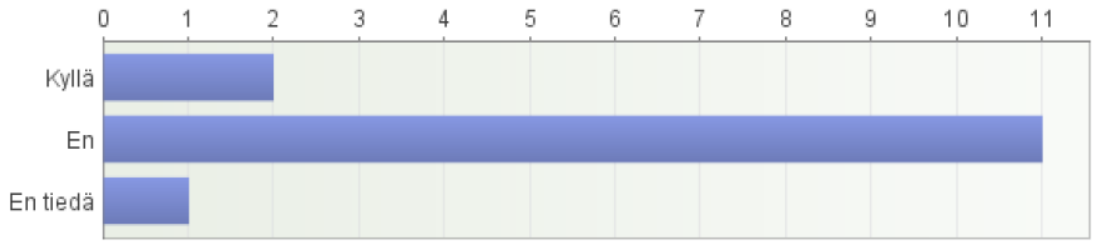
11. Onko omalla laitteellasi (esim. USB-tikku, ulkoinen kovalevy...) oleva yritystä koskeva tieto salattu?

Vastaajien määrä: 14



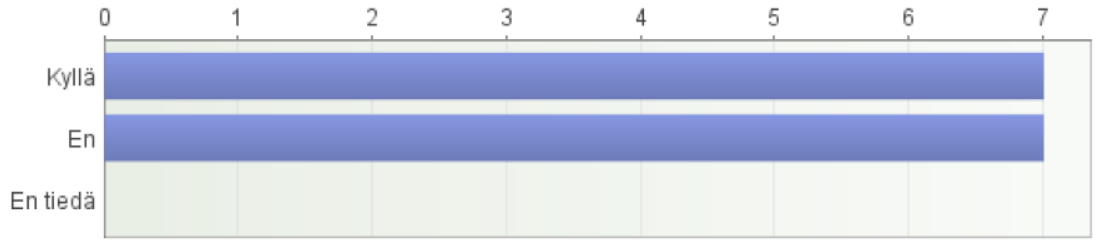
12. Kirjoitatko kynällä tjms. USB-muistitikulle/ulkoiselle kovalevylle mitä dataa se sisältää?

Vastaajien määrä: 14



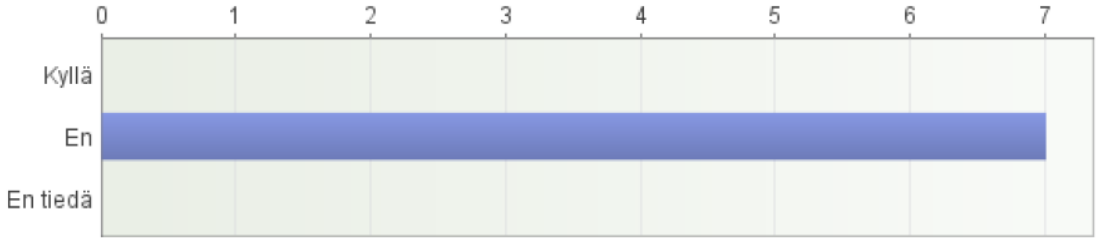
13. Otatko tiedostoista varmuuskopioita?

Vastaajien määrä: 14



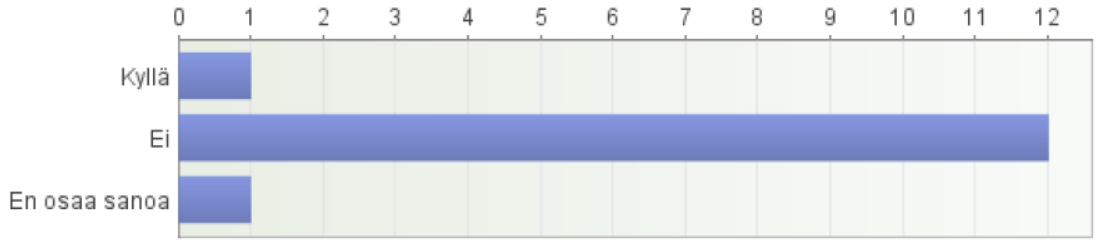
14. Mikäli vastasit edelliseen kysymykseen kyllä: Otatko varmuuskopiot useampaan kuin yhteen paikkaan?

Vastaajien määrä: 7



15. Haittaavatko tietoturvallisuus-vaatimukset päivittäistä työtäsi?

Vastaajien määrä: 14



16. Koetko tietoturvan tärkeäksi asiaksi päivittäisessä työssäsi?

Vastaajien määrä: 14