Opinnäytetyö

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2014

Jukka Uusi-Pohjola

LAKEUDEN ETAPPI OY:N TIETOTURVAKARTOITUS JA TIETOTURVALLISUUDEN PARANNUSEHDOTUKSET

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2014 | 46 sivua

Jarkko Paavola

Jukka Uusi-Pohjola

LAKEUDEN ETAPPI OY:N TIETOTURVAKARTOITUS JA TIETOTURVALLISUUDEN PARANNUSEHDOTUKSET

Tämän opinnäytetyön tavoitteena on tuottaa Lakeuden Etappi Oy:lle tietoa sen nykyisestä tietoturvan tasosta ja antaa ehdotuksia tietoturvan parantamiseen.

Tietojen säilyttäminen sähköisessä muodossa on nykyään monelle yritykselle arkipäivää. Tietomurrot ja teollisuusvakoilu ovat kuitenkin yritystoiminnalle suuri riski ja yrityksen tulisi tehdä asianmukaiset toimenpiteet pitääkseen tärkeät tietonsa turvassa.

Tutkimuksessa käytetyllä kyselyllä selvitetään esimerkiksi yrityksen hallinnolliseen tietoturvaan, fyysiseen turvallisuuteen ja pääsynhallintaan liittyviä kysymyksiä. Kyselyllä kartoitetaan yrityksen tämän hetkinen tilanne, minkä jälkeen kysymyksistä tehdään päätelmät ja tarvittaessa annetaan parannusehdotuksia.

Tutkimus on toteutettu kyselytutkimuksena, johon vastasi 15 yrityksen henkilöstöön kuuluvaa henkilöä.

ASIASANAT:

tietoturva, tietoturvallisuus, tietoturvakartoitus, organisaatio, yritys

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2014| 46 sivua

Jarkko Paavola

Jukka Uusi-Pohjola

INFORMATION SECURITY SURVEY FOR LAKEUDEN ETAPPI LTD. AND SUGGESTIONS FOR MAKING INFORMATION SECURITY BETTER

The purpose of this study is to produce information for Lakeuden Etappi ltd. about its current level of information security and to give suggestions how to make it better.

Storing information in its electronic form is very common for companies nowadays. However, data breaching and industrial espionage are very serious threat to these companies and they should make the appropriate procedures to keep their vital information safe.

In the study I have used a quantative survey investigating corporate administerial security, physical security and access control. The survey was issued to 15 company workers. Suggestions to improve the information security of the company were created according to the answers provided by the workers.

The significance of this survey is to help the company realize that information security is an important aspect of business and that it is important to keep it up-to-date.

KEYWORDS:

information security, data security, security survey, organization, business

SISÄLTÖ

LIITTEET

1 JOHDANTO

Yrityksen tietoturvasta huolehtiminen on tärkeää, sillä onnistuneella tietoturvalla varmistetaan yrityksen liiketoiminnan jatkuminen ja pidetään toiminta luotettavana. Tämän opinnäytetyön toimeksiantaja on Lakeuden Etappi Oy, jolle tehtiin tietoturvakartoitus. Osa opinnäytetyöstä on salattu, koska tiedot sisältävät yrityksen liiketoiminnan ja turvallisuuden kannalta arkaa materiaalia.

Tietoturvakartoituksen tarkoituksena oli havainnoida yrityksessä olevia tietoturvaongelmia ja riskejä. Tietoturvakartoitusta varten kerättiin tietoa kyselylomakkeen avulla ja tietojen perusteella yritykselle koottiin kattava tietoturvaraportti. Tämä 31-sivuinen raportti on salattu, koska se sisältää yksitysikohtiasta tietoa yrityksen tietoturvasta. Raportti kertoi yrityksen sen hetkisestä tietoturvan tasosta ja esitti myös korjaavia toimeenpiteitä ongelmien korjaamiseksi ja riskien ehkäisyyn.

Tutkimuksen muina tavoitteina oli tuoda yrityksen henkilökunnalle tietoisuutta tietoturvasta ja sen moninaisuudesta. Myös oma henkilökohtainen tietoturvatietoisuuteni ja ammattitaidon lisääntyminen olivat opinnäytetyöprosessin tavoitteita.

Opinnäytetyön teoriaosuudessa selvitetään tietoturvaa ja sen periaatteita, sekä kyselylomakkeen aihealueita. Lähteinä on käytetty alan kirjallisuutta ja sähköisiä materiaaleja.

2 YRITYKSEN TIETOTURVA

Tässä luvussa esitellään toimeksiantajayritystä, yritysturvallisuuden osa-alueita ja tietoturvaa. Luvussa käsitellään myös tietoturvan heikointa lenkkiä ja sosiaalista manipulointia.

2.1 Lakeuden Etappi Oy

Lakeuden Etappi Oy on vuonna 1997 perustettu jätehuoltoyritys. Se vastaa käytännön jätehuollon järjestämisestä yhdeksän omistajakuntansa alueella Etelä-Pohjanmaalla. Nämä omistajakunnat ovat Alavus, Ilmajoki, Jalasjärvi, Kihniö, Kuortane, Kurikka, Lapua, Seinäjoki ja Ähtäri. Yhtiön toimialueella on noin 130 000 asukasta. Etapin tavoitteena on tarjota toimivaa jätepalvelua asiakkaiden ja ympäristön hyväksi. Yhtiön tehtäviin kuuluuvat jätteenkuljetus ja -käsittely sekä tiedotus ja neuvonta jätehuoltoasioissa. (Lakeuden Etappi 2014, 7.)

Yhtiön arvoja ovat asiakaslähtöisyys, asiantuntemus, tehokkuus, yhteistyö, ympäristövastuu ja työhyvinvointi. (Lakeuden Etappi 2014, 7).

Asiakaspalvelu on myös tärkeä osa yrityksen toimintaa, ja yhä enenevissä määrin asiakaspalvelu on siirtymässä sähköiseen muotoon. Esimerkiksi vuosien 2012 ja 2013 välisenä aikana sähköposteilla tapahtuvat yhteydenotot lisääntyivät (2041 kpl → 2109kpl). Tietoturvan rooli korostuu sähköisen asiakaspalvelun edelleen lisääntyessä. Yrityksessä työskentelee 42 henkilöä. Yrityksen liikevaihto oli 22,1 miljoonaa euroa vuonna 2013. (Lakeuden Etappi 2014, 5, 6, 16.)

2.2 Yritysturvallisuuden osa-alueet

Keskeinen edellytys yritysturvallisuuden määrittämiselle on uhkien tunnistaminen. Yrityksien tulisi tehdä kokonaisvaltainen peruskartoitus hyödyntämällä esimerkiksi haavoittuvuusanalyysiä. Turvallisuusanalyysejä käytetään uhkien tunnistamiseen, niiden merkityksen arviointiin ja niihin varautumiseen. Riskien todennäköisyyksiä ja muutoksia tulisi seurata jatkuvasti. (Elinkeinoelämän keskusliitto 2014.)

Yritysturvallisuus jaetaan kymmeneen osa-alueeseen:

- **Tuotannon ja toiminnan turvallisuus**
  Tavoitteena häiriötön tuotanto ja toiminta. Häiriön jälkeen nopea toipuminen.

- **Työturvallisuus**
  Turvallinen työnteko ja työntekijöiden hyvinvointi

- **Ympäristöturvallisuus**
  Vastuun ottaminen ympäristöstä ja henkilöstön tietoisuuden lisääminen

- **Henkilöturvallisuus**
  Työntekijöiden suojaaminen rikoksilta ja onnettomuuksilta, liiketoiminnan suojaaminen estämällä rikollisten soluttautuminen yritykseen.

- **Kiinteistö- ja toimitilaturvallisuus**
  Yrityksen toimitilojen suojaaminen. Tarkoituksena estää yritykselle arvokkaan tiedon tai materiaalin anastaminen.

- **Ulkomaantoimintojen turvallisuus**
  Henkilöstön turvallisuustason takaaminen heidän ollessaan ulkomailla.

- **Valmiussuunnittelu**
  Lakisääteisten valmiustoiminnan mukaisten velvoitteiden toteuttaminen.

- **Rikosturvallisuus**
  Rikosten ennaltaehkäisy ja rikosten selvittäminen

- **Pelastustoiminta**
  Onnettomuuksien ennaltaehkäisy ja onnettomuustilanteissa toimiminen

- **Tietoturvallisuus**
  Yrityksen tiedon luottamuksellisuuden, käytettävyyden ja eheyden takaaminen. (Heijaste ym. 2008, 28-30.)

Yritykselle teettämäni tietoturvakartoitus keskittyy ensisijaisesti tietoturvallisuus-osa-alueeseen. Raportti sivuaa kuitenkin muitakin osa-alueita, kuten tuotannon ja toiminnan turvallisuutta, henkilöturvallisuutta, kiinteistö- ja toimitilaturvallisuutta sekä rikosturvallisuutta.

2.3 Tietoturva

Tietoturvallisuus on tiedon perusominaisuuksien eli eheyden, luottamuksellisuuden ja käytettävyyden turvaamista. Tietoturvallisuus on pieniä tekoja osana jokapäiväistä toimintaa. Hyvä tietoturvallisuus on osa yrityskulttuuria, jolloin jokainen ymmärtää tietoturvan merkityksen ja työskentelee sen saavuttamiseksi ja ylläpitämiseksi. Yrityksessä tietoturvalla pyritään suojaamaan tärkeät tiedot ulkopuolisilta henkilöiltä. Tietoturvalla tarkoitetaan siis toimenpiteitä, joilla taataan yrityksen tietojen koskemattomuus. (Laaksonen ym. 2006, 17. Suomen Internetopas 2014.)

Suomen internetoppaassa todetaan: ”Tietoturvalle asetettuja tavoitteita ovat tiedon luottamuksellisuus, eheys, kiistämättömyys, pääsynvalvonta, saatavuus ja tarkastettavuus. Jotta tiedot olisivat **luottamuksellisia**, tulisi niiden olla vain niihin oikeutettujen henkilöiden käytössä.” Jokaisella tiedolla ja dokumentilla tulisi olla turvaluokitus, missä määritellään sitä käsittelevät henkilöt. Näillä henkilöillä on oikeus tiedon käytön lisäksi myös esimerkiksi sen säilytykseen ja tuhoamiseen. (Suomen Internetopas 2014.)

Tiedon **eheys** tarkoittaa, että tieto pysyy muuttumattomana sen luomisen, käsittelyn ja siirron ajan. **Kiistämättömyys** tarkoittaa tiedon siirtoon ja käsittelyyn osallistuneiden henkilöiden tunnistamisen valvontaa. **Pääsynvalvonnalla** valvotaan ja rajoitetaan käyttäjien tietoon käsiksi pääsyä. **Saatavuudella** tarkoitetaan, että henkilöillä joilla on oikeus tietoon, tulisi olla myös tiedon saaminen helppoa ja viiveetöntä. **Tarkastettavuus** tarkoittaa, että tuloksena saadun tiedon oikeellisuus on kyettävä osoittamaan ja tieto on kyettävä tarkastamaan. (Suomen Internetopas 2014.)

Tietoturvaa ei tulisi nähdä välttämättömänä pahana, jonka tarkoitus on kiusata työntekijöitä. Tietoturva tulisi nähdä kilpailuetuna, joka realisoituu liiketoiminnan jatkuvuuden parantumisena. (Laaksonen ym. 2006, 18.)

Organisaation työntekijöiden tulee huolehtia omalta osaltaan tietoturvallisuuden tavoitteiden saavuttamisesta. Jokaisen työntekijän tulisi toimia työsopimuksen ja muiden sopimusten ja ohjeiden mukaisesti. Henkilöstölle kuuluvia tietoturvaan liittyviä tehtäviä ovat esimerkiksi

- tiedon luokittelu ja käsittely ohjeiden mukaisesti
- luokitellun tiedon käsittely, siirtäminen ja säilyttäminen ohjeiden mukaisesti
- omista salasanoista huolehtiminen
- ohjeiden noudattaminen
- heikkouksien ja puutteiden raportointi
  (Laaksonen ym. 2006, 137.)

Suojautumismenetelmät jaetaan kolmeen eri ryhmään: Tekniseen, fyysiseen ja hallinnolliseen (Suomen Internetopas 2014).

Tekninen tietoturva keskittyy käytössä olevien laitteiden ja ohjelmistojen tietoturvaan. Teknistä tietoturvaa tulisi miettiä jo laitteistoja ja ohjelmistoja hankittaessa. (Suomen Internetopas 2014.)

Fyysinen tietoturva keskittyy laitteiden fyysiseen suojaamiseen. Esimerkiksi laitteiden sijoittaminen suojakoteloon tai kaappiin tai kokonaan omaan huoneeseensa, joka on suljettu lukolla. (Suomen Internetopas 2014.)

Hallinnollinen tietoturva koskee yrityksen työntekijöiden ja organisaation jäsenten riittävää tietoturvaosaamista (Suomen Internetopas 2014).

2.4 Tietoturvan heikoin lenkki

Moni yritys ja yksityinen henkilö luulee, että tietoturvasta huolehtimiseen riitäisi yksi kaiken kattavan tietoturvalaitteiston tai sovelluksen hankinta. Nämä voivat estää joitain tietoturvariskien muotoja, mutta todellisuudessa suurinta riskitekijää ei mikään laitteisto pysty estämään. Kyseessä on suurin yksittäinen uhka tietoturvalle eli ihminen itse. Yrityksessä se voi olla esimerkiksi passiivisena toimijana yrityksen työntekijä tai aktiivisena teollisuusvakoilija. (Airola 2013; Valve 2014.)

Erilaiset haittaohjelmat eivät yleensä tule laitteisiin itsestään, vaan ne tulevat joko ihmisen toiminnan kautta suoraan laitteeseen tai esimerkiksi ihmisen käyttämän massamuistilaitteen mukana. Kyseessä ei tietenkään tarvitse olla tahallinen

laitteiston saastuttaminen, vaan yleensä tällaisen tilanteen aiheuttaa henkilön tietämättömyys ja varomattomuus. Helpoin ja kustannustehokkain tapa tällaisten tilanteiden välttämiseksi on henkilöiden koulutus ja valistaminen tietoturvan eri riskeistä. Jos yritys saa työntekijänsä valveutuneiksi tietoturvasta, on yritys turvassa tietoturvan suurimmalta yksittäiseltä riskitekijältä. (Airola 2013, Valve 2014.)

Henkilö, joka haluaisi saada tietoonsa yrityksen salattuja tietoja, voisi yrittää hakkeroinitaitojaan yrityksen tehokasta ja kallista tietoturvaratkaisua vastaan. Se todennäköisesti ei olisi kuitenkaan järkevää, koska hän saattaisi saada nämä tiedot muullakin keinolla, esimerkiksi kysymällä suoraan oikealta henkilöltä. Tämä on sosiaalista manipulointia, tietoturvan vaarallisin uhka ja vaarallisin keino. (US-Cert 2009.)

Sosiaalisella manipuloinnilla tarkoitetaan toimintaa, jolla yritetään saada henkilö paljastamaan salattuja tietoja tai antamaan niihin pääsy. Sosiaalinen manipulointi on huijausyritys, jossa hyökkääjä yrittää saada uhrin luottamaan itseensä niin paljon, että hän pystyy tätä valhein saatua luottamusta hyödyntämään omiin tarkoituksiinsa. Esimerkki sosiaalisesta manipuloinnista voisi olla, että hyökkääjä haluaa saada tietoonsa henkilön työpaikalla käyttämän salasanan. Hän ottaa selville henkilön työpuhelinnumeron, soittaa esiintyen teknisenä tukena ja vaatii salasanaa. Yrityksessä jossa tietoturvaohjeistusta ei ole annettu, työntekijä todennäköisesti antaisi salasanansa hyökkääjän tietoon. (US-Cert 2009.)

3 KYSELYN TOTEUTUS

Tietoturvakartoitus toteutettiin käyttämällä kyselylomaketta. Tässä luvussa käsitellään kyselylomakkeen luomiseen, kysymyksien valintaan, kyselyn lähettämiseen ja tulosten analysointiin liittyviä asioita. Luvussa käsitellään myös kyselystä saatua palautetta.

3.1 Kyselylomakkeen luominen

Kyselyn suunnitteluvaiheessa huomioitiin, että vastaajilla ei olisi tietoturvaosaamista tai tietoteknisen alan asiantuntemusta. Kyselystä tuli siis tehdä mahdollisimman yksinkertainen ja helppolukuinen, mutta samalla sen pitäisi pystyä tuottamaan sellaista tietoa, että laadukkaan raportin laatiminen olisi mahdollista. Kyselyyn tuli lopulta 54 kysymystä. Mukaan on tarkoituksella laitettu vaikeampiakin kysymyksiä, joilla mitattiin edistyneempää tietoturva-asioiden hallintaa. Suurimpaan osaan kysymyksistä annettiin vastausvaihtoehdoiksi ”Kyllä”, ”Ei” ja ”En osaa sanoa”. Muutamassa kohdassa oli kysymyskohtaiset vastausvaihtoehdot ja kahdessa viimeisessä kysymyksessä avoin vastausmahdollisuus.

Kysely toteutettiin käyttämällä Webropol–kysely- ja -analysointisovellusta. Ensimmäiseksi valittiin sovelluksessa valmiista olevista graafisista kyselypohjista malli. Tämän jälkeen kysymykset kirjoitettiin yksitellen ja valittiin jokaiseen kysymykseen sopiva kysymystyyppi. Vaihtoehtoja oli useita erilaisia, esimerkiksi monivalintoja, positiomatriiseja ja avoimia tekstikenttiä. Kyselyssä käytettiin pääasiassa tavallista valinta-vaihtoehtoa, jossa annetaan vastausvaihtoehdoksi useampi vaihtoehto, mutta vastauksia voi olla vain yksi. Kyselyn lopussa olevat palautekysymykset olivat ainoat, joissa oli avoin tekstikenttä vastaajalle.

3.2 Kyselylomakkeen kysymykset

Kyselyn kysymykset rakennettiin Standardized Information Gathering (SIG) version 6 pohjalta (Shared Assessments 2010). SIG on standardoitu tiedonkeruumenetelmä kyselylomakkeen muodossa ja sen on laatinut Santa Fe Group -yritys. SIG-kyselylomakkeessa kysymykset oli lajiteltu eri aihealueiden mukaan. Tätä jaottelua on osittain hyödynnetty toimeksiantajalle laaditussa lomakkeessa. Osa kyselyn

kysymyksistä käännettiin suoraan SIG-lomakkeesta ja osa uudelleenmuotoiltiin yrityksen tarkoitukseen sopivimmiksi. SIG-lomakkeen alkuperäiskieli oli englanti, joten sen hyödyntäminen vaati kääntämistä suomen kielelle.

Kysely sisälsi 54 kysymystä, jotka oli jaettu viitteellisesti kuuteen eri ryhmään:

1. Hallinnollinen tietoturva (12)
2. Fyysinen turvallisuus (4)
3. Pääsynhallinta (16)
4. Varmuuskopiointi ja laitteet (10)
5. Virustorjunta, palomuuri, päivitykset ja langaton lähiverkko (10)
6. Palaute (2)

Hallinnolliseen tietoturvaan liittyviä kysymyksiä olivat esimerkiksi kysymykset yrityksen koosta, tietoturvaohjeistuksen olemassaolosta, ulkopuolisten tahojen kanssa tehdyistä sopimuksista ja yrityksen tietoturvakoulutuskäytännöistä.

Fyysiseen turvallisuuteen liittyviä kysymyksiä kyselyssä olivat esimerkiksi fyysisen turvallisuuden suunnitelman olemassaolosta ja laitteistojen huoltotoimikäytännöistä.

Pääsynhallintaan liittyviä kysymyksiä olivat esimerkiksi salasanojen monimutkaisuus, käyttämättömien tilien poistotoimenpiteet, järjestelmien käyttöoikeudet ja etäkäyttö.

Varmuuskopiointiin ja laitteisiin liittyviä kysymyksiä olivat esimerkiksi massamuistilaitteiden käyttöön liittyvät toimenpiteet, järjestelmien varmuuskopioinnit ja käytöstä poistettavien laitteiden menettely.

3.3 Kyselyn lähetys

Kysymykset lähetettiin 17 ennaltamäärätylle henkilölle, jotka yritys valitsi. Yrityksen talouspäällikkö ilmoitti henkilöstölle kyselystä etukäteen, jotta kysely otettaisiin vakavemmin ja siihen vastaaminen nähtäisiin tärkeänä. Kyselyn vastausaika oli ensisijaisesti kaksi viikkoa, jonka jälkeen lähetettiin muistutusviesti kaikille niille, jotka eivät kyselyyn olleet vastanneet. Kokonaisvastausajaksi muodostui kokonainen kuukausi ja tänä aikana kysymykseen vastasi 15 henkilöä, kun kysely lähetettiin yhteensä 17:lle. Kyselyn vastausprosentti oli siten 88,2%.

Vastaajat listattiin sähköpostiosoitteen perusteella Webropoliin. Tämän jälkeen kaikille oli mahdollista lähettää massaviesti, jossa ohjeistettiin kyselyyn liittyvistä

asioista. Samassa viestissä oli myös jokaiselle vastaajalle henkilökohtainen vastauslinkki, jonka avulla Webropol ylläpiti tietoa kyselyyn vastaajista. Tämän ominaisuuden avulla muistutusviestien lähetys vain niille, jotka eivät olleet vastanneet kyselyyn, oli äärimmäisen helppoa. Saman ominaisuuden ansiosta Webropol havaitsi, jos vastaaja oli avannut vastauslinkin, mutta ei kuitenkaan ollut täyttänyt kyselyä.

3.4 Tulosten analysointi

Webropol antoi kysymysten analysointiin useita vaihtoehtoja. Jokaiseen kysymykseen oli mahdollista saada tilastoarvoina keskiarvo, keskiarvon luottamusväli ja mediaani. Kysymyksen vastausmäärän näki halutessaan myös prosentteina. Webropolin avulla vastaukset voitiin esittää numeraalisesti ja prosentuaalisesti. Tulokset oli mahdollista esittää visuaalisesti siirtämällä ne erilaisiin kuvaajiin. Selkeimmäksi vastausten esitystavaksi koettiin piirakkamallinen kuvaaja, jossa vastausmäärä oltiin kuvattu myös prosentteina. Tämän avulla oli helpointa nähdä, mikä oli yleisin vastaus eri kysymyksissä.

3.5 Palaute kyselystä

Kyselylomakkeen lopuksi vastaajilla oli mahdollisuus antaa palautetta kyselystä. Palautteissa kysyttiin, opettiko kyselyn tekeminen vastaajalle uusia asioita turvallisuudesta tai minkälaisia ajatuksia se vastaajassa herätti. Avointa palautetta oli myös mahdollista antaa.

Suuri osa vastaajista moitti omaa tieoturvatietoisuuttaan ja muutama vastaaja mainitsi kysymysten olleen haastavia. Pääasiallinen viesti palautteista oli kuitenkin, että kysely koettiin hyödylliseksi. Samalla mainittiin, että koulutusta tulisi saada lisää. Vastaajien halu muutokseen nykyisestä oli selkeä. Omaa tietoturvatietoisuutta haluttiin lisätä ja samalla haluttiin tietoa yrityksen yhteisistä tietoturva-asioista.

4 RAPORTIN KOOSTAMINEN YRITYKSELLE

Kyselyn vastausten perusteella koostettiin toimeksiantajalle raportti. Raportti koostui johdannosta, kyselyn vastausten läpikäymisestä ja suositelluista toimenpiteistä sekä muistilistasta.

4.1 Yritykselle suunnattu johdanto

Raportin johdannossa esiteltiin raportin tarkoitus ja rakenne. Johdannossa muistutettiin myös, että kyselystä saatujen vastausten todenmukaisuus ei välttämättä ole absoluuttinen, koska tiedot on kasattu usean ihmisen henkilökohtaisten näkemyksien ja kokemuksien perusteella. Tämän takia raportissa esitettävät tiedot tulisi käydä yrityksen tietoturvasta vastaavan henkilön kanssa tarkasti läpi. Johdannossa kerrottiin myös, että raportissa esitetyt parannusehdotukset tulisi käydä tietoturvavastaavan kanssa läpi siten, että yritykselle kriittisimmät epäkohdat korjataan tarvittaessa ensimmäisenä.

4.2 Kyselyn vastaukset ja suositellut toimenpiteet

Kyselystä saadut vastaukset esitettiin aluksi siten, että kerrottiin yksinkertaisesti jokaisen kysymyksen vastaus ja vastausprosentti. Tällä tavoin oli mahdollista nähdä heti, jos joku vastausten perusteella muodostuneista väitteistä ei pitänyt paikkansa. Esimerkiksi: ”Yrityksessä on tietokoneita, 85%” näkee, että suurin osa vastaajista oli sitä mieltä, että yrityksessä on tietokoneita. Jos tämä ei pitäisi paikkansa, niin yritys tietäisi heti ryhtyä vastaukseen liittyviin toimenpiteisiin.

Pelkistetyn tulosten esittelyn jälkeen vastaukset avattiin vielä sanallisesti tarkasti kuvaillen. Vastausten erotessa toisistaan huomattavasti esitettiin erilaisia selityksiä siihen, mistä tämä voisi johtua. Tämän jälkeen suositeltiin jatkotoimenpiteitä esille nousseisiin ongelmakohtiin.

Vastaukset oli mahdollista nähdä myös raportin liitteenä olevista kuvioista, joissa on prosentteina piirakkakuvaajaan esitetty jokainen kyselyn kysymys ja vastaus. Liitteenä oli myös koottu yhteen vastaajien antama avoin palaute kyselystä ja siitä, opettiko se heille jotain uutta tietoturvasta.

4.3 Muistilista

Raportin loppuun tehtiin vielä muistilista, josta toimeksiantaja näkee helposti kaikki yrityksessä esille nousseet tietoturvaongelmat. Raportin laajuus aiheuttaa sen, että ilmenneitä ongelmia esitetään raportin eri vaiheissa. Toimeksiantaja joutuisi itse tekemään jonkinlaisen yhteenvedon niistä, joten tämä valmiiksi tehty muistilista nopeuttaa ja helpottaa toimeksiantajan työtä. Toimeksiantaja voi keskittyä raportissa esitettyjen epäkohtien korjaamiseen sen sijaan, että resursseja menisi liikaa asioiden poimiseen raportista.

5 POHDINTA

Opinnäytetyön tekeminen opetti, miten yrityksessä näin mittavan projektin toteuttaminen onnistuu. Toimeksiantaja yritys oli koko prosessin ajan kiinnostunut ja sitoutunut projektiin, jolloin opinnäytetyöntekijä pystyi keskittymään pelkästään itse työn tekemiseen.

Jälkikäteen mietittynä asioita, joita olisi voinut toisella tapaa tehdä, tulee mieleen kyselylomakkeen luomisen vaikeudet ja erityisesti vastausvaihtoehdot. ”Kyllä” ja ”Ei” olivat selkeitä vastauksia, mutta vaihtoehto ”En osaa sanoa” jätti liian paljon arvailun varaa. Koskaan ei tiennyt, valitsiko vastaaja ”En osaa sanoa” vaihtoehdon sen takia, että ei ymmärtänyt kysymystä vai ymmärsikö hän kysymyksen, mutta ei todellisuudessa osannut sanoa kuinka asia oli. Tässä tapauksessa toimivin ratkaisu olisi lisätä neljäs vastausvaihtoehto ”En ymmärrä kysymystä”. Tällöin saisi paremman kuvan myös liian vaikeista kysymyksistä, jos neljäs vastausvaihtoehto saisi suurimman vastausmäärän kysymyksessä.

Yrityksen tulisi noudattaa raportissa annettuja parannusehdotuksia. Tämän jälkeen kyselyn voisi uusia kalenterivuoden jälkeen ja tällä tavoin selvittää, miten henkilöstö näkee parannuksien vaikutukset. Kyselyjen tuloksia voitaisiin verrata ja tämän jälkeen tehdä johtopäätökset parannuksien toimivuudesta.

LÄHTEET

Airola E-M. Anders Inno blogi. 2013. Tietämättömyys altistaa yrityksen tietoturvariskeille. Viitattu 29.9.2014. http://www.andersinno.fi/fi/blogi/198/tietamattomyys-altistaa-yrityksen-tietoturvariskeille/

Elinkeinoelämän Keskusliitto. 2014 Yritysturvallisuus. Viitattu 23.9.2014. http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/

Heijaste, J-M; Korkiamäki, J; Laukkala, H; Mustonen, J; Peltonen, J. & Vesterinen, P. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin Kamari Oy.

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

Lakeuden Etappi Oy. 2014. Vuosikertomus. Viitattu 12.9.2014 http://www.etappi.com/files/2513/9885/0343/Etappi_vuosikertomus_2013.html

Shared Assessments 2010. Standardized Information Gathering Questionnaire. Viitattu 23.9 2014. http://listserv.educause.edu/cgi-bin/SIGv6.2

Suomen Internetopas 2014. Tietoturva. Viitattu 23.9.2014 http://www.internetopas.com/yleistietoa/tietoturva/

US-Cert. 2009. Security Tip (ST04-014) Viitattu. 29.9.2014. https://www.us-cert.gov/ncas/tips/ST0

Valve, M. Taloudessa. 2014. Tietoturvariskit – it –tekniikkaa vai henkilöstöasiaa. Viitattu 29.9.2014. http://taloudessa.fi/2014/06/04/tietoturvariskit-it-tekniikkaa-vai-henkilostoasiaa/

LIITTEET

LIITE 1 LAKEUDEN ETAPPI OY:N TIETOTURVAKARTOITUS (SALATTU)