Lauri Tammelin

Tietoturvallisuuden hallintajärjestelmän auditointi

Metropolia Ammattikorkeakoulu

Bachelor of Engineering

Information Technology -tutkinto-ohjelma

Insinöörityö

1.6.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Lauri Tammelin Tietoturvallisuuden hallintajärjestelmän auditointi 24 sivua 1.6.2018
Tutkinto	Bachelor of Engineering
Tutkinto-ohjelma	Information Technology
Ohjaajat	Yliopettaja Markku Nuutinen

Insinöörityön tavoitteena oli kartoittaa kohdeyrityksen tietoturvallisuuden hallintajärjestelmän nykyinen tila. Tavoitteena oli myös selvittää tarvittavat toimenpiteet ISO 27002 -standardin mukaisen sertifioinnin saavuttamiseksi. Insinöörityö tehtiin yrityksen sisäisiä resursseja hyödyntäen.

Työssä tutustuttiin aluksi tietoturvallisuuden perusperiaatteisiin, minkä jälkeen perehdyttiin ISO 27000 -standardiperheeseen. Tämän jälkeen perehdyttiin kohdeyrityksen tietoteknisiin järjestelmiin ja sen nykyiseen tietoturvallisuuden hallintajärjestelmään sekä kartoitettiin, kuinka hyvin se toteuttaa ISO 27001- ja ISO 27002 -standardit.

Nykyisen tietoturvallisuuden hallintajärjestelmän dokumentoinnin puutteellisuuden perusteella päätettiin luoda kyselypohja ISO 27002 -standardin pohjalta. Kyselypohjan tavoitteena oli kartoittaa kohdeyrityksen nykyisiä tietoturvallisuuskäytäntöjä. Kysely käytiin läpi yrityksen tietoturvasta vastaavien henkilöiden kanssa.

Kyselyn vastauksia analysoimalla pystyttiin luomaan yritykselle kehityssuunnitelma tietoturvallisuuden parantamiseksi. Kehityssuunnitelman lopullinen tavoite oli yrityksen haluaman ISO 27002 -standardin mukaisen sertifioinnin saavuttaminen.

Insinöörityössä luotu kyselypohja oli hyvä aloituskohta tietoturvallisuuden hallintajärjestelmän kehittämiseen. Kyselypohja antoi hyvän kokonaiskuvan yrityksen tietoturvallisuuden nykytilasta. Kysymykset kuitenkin osoittautuivat liian yleisluontoisiksi ja vaikeaselkoisiksi. Insinöörityön löydösten pohjalta yritys ryhtyi konkreettisiin toimiin tietoturvallisuuden parantamiseksi.

Avainsanat	ISO 27001, ISO 27002, tietoturvallisuuden hallintajärjestelmä, CIA

Author Title Number of Pages Date	Lauri Tammelin Information security management system audit 24 pages 1 June 2018
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Instructors	Markku Nuutinen, Principal Lecturer

The aim of the thesis was to find out the current state of the information security management system of the target company and to identify the necessary measures to achieve ISO 27002 certification. The thesis was made using the company's internal resources.

The first part of the thesis introduced the basic principles of information security, after which an introduction was made to the ISO 27000 standard family. Subsequently, the target company and its IT systems were introduced. Next, the target company's current information security management system was examined and mapped out to see how well it is currently implementing ISO 27001 and ISO 27002 standards.

Based on the lack of documentation on the current information security management system, it was decided to create a questionnaire based on the ISO 27002 standard. The purpose of the questionnaire was to map out the target company's existing information security practices. The survey was conducted with those responsible for the company’s information security.

By analyzing the answers to the questionnaire a plan of action was created for the company to improve their information security. The goal of the action plan was for the company to achieve the ISO 27002 certification.

The questionnaire created in the thesis was a good starting point for developing an information security management system. The survey provided a good overview of the company's current security situation. However, the questions turned out to be too generic and difficult to understand. Based on the findings of the bachelor's thesis, the company took concrete steps to improve information security.

Keywords	ISO 27001, ISO 27002, information security management system, CIA

Sisällys

1 Johdanto

Insinöörityön tarkoituksena on kartoittaa kohdeyrityksen tietoturvallisuuden nykyinen hallintajärjestelmä ja selvittää, kuinka hyvin tietoturvallisuus käytännössä toteutetaan. Nykytilanteen pohjalta yritykselle annetaan parannusehdotuksia. Työssä keskitytään tietoteknisiin ratkaisuihin kohdeyrityksen toiveesta. ISO 27000 -standardiperheen pohjalta luodaan kyselypohja, jonka avulla kartoitetaan yrityksen nykyinen tilanne. Kyselyn tavoitteena on paljastaa suurimmat puutteet tietoturvan hallintajärjestelmässä.

Insinöörityöraportissa tutustutaan ensin tietoturvallisuuteen käsitteenä ja avataan sen keskeisimpiä termejä sekä esitellään CIA-malli. Sen jälkeen tutustutaan tietoturvallisuuden hallintajärjestelmän standardiperheeseen ISO/IEC 27000, johon kohdeyrityksen nykyistä järjestelmää verrataan myöhemmin kyselyn pohjalta.

Neljännessä luvussa esitellään kohdeyritys ja sen liiketoiminta. Luvussa kartoitetaan myös yrityksen tietojärjestelmät ja tutustutaan nykyiseen tietoturvallisuuden hallintajärjestelmään. Sen jälkeen katsotaan, kuinka hyvin yrityksen nykyinen tietoturvallisuuden hallintajärjestelmä toteuttaa standardin. Työssä luodaan myös kyselypohja. Sen avulla nykyistä järjestelmää voidaan arvioida ja kehittää, ja lopuksi käydään läpi vastuuhenkilöiden kanssa pidetyn palaverin tulokset. Palaverissa käytettiin pohjana työssä luotua kyselypohjaa, jonka avulla tunnistettiin kriittisimmät puutteet nykyisessä tietoturvallisuuden hallintajärjestelmässä.

2 Tietoturvan perusperiaatteet

Tietoturvan peruspilariksi on vuosien saatossa vakiintunut CIA-malli. Mallin nimi tulee sanoista Confidentiality (luottamuksellisuus), Integrity (eheys) ja Availability (saatavuus). Malli koostuu kolmesta perusperiaatteesta, joiden avulla voidaan arvioida minkä tahansa järjestelmän tai organisaation tietoturvan tasoa. Periaatteet ovat luottamuksellisuus, eheys ja saatavuus. Mallia voidaan myös laajentaa kehittyvän teknologian, kasvavien vaatimusten ja uhkien takia. Tässä työssä kuitenkin keskitytään vain perusmuotoiseen malliin. Tarpeen mukaan mallin ulkopuolisia konsepteja tarkastellaan ISO 27001 -standardin mukaisesti. [1]

Tietoturvallisuudessa luottamuksellisuudella tarkoitetaan, että tietoon eivät pääse käsiksi tahot, joilla ei ole siihen lupaa. Taho tässä tapauksessa voi olla esimerkiksi henkilö, ohjelma tai prosessi. Luottamuksellisuus voidaan toteuttaa esimerkiksi suojaamalla järjestelmä luvattomalta käytöltä salasanalla tai salaamalla tietoliikenne siten, että kolmas osapuoli ei pääse siihen käsiksi tietoa siirrettäessä. [1]

Eheydellä tarkoitetaan sitä, että tieto ei voi muuttua hallitsemattomasti. Toisin sanoen tietoa ei tule olla mahdollista muuttaa ilman asianmukaista lupaa ja toisaalta tieto ei saa muuttua ilman, että siitä jää jonkinlainen jälki. Käytännössä tämä tarkoittaa, että tiedon muuttamista pitää kontrolloida jollakin pääsynhallintamekanismilla. Käyttäjä on tunnistettava ja muutoksista tulee jäädä merkintä järjestelmään. Eheyteen kuuluu myös mekanismi tiedon muuttumisen havaitsemiseen esimerkiksi laitteiden vikaantuessa tai tiedonsiirto-ongelmissa. Yksi tällainen mekanismi on esimerkiksi tarkistussumma tai –koodi, joka on tiedosta laskettava uniikki tiiviste. Tiivistettä tarkastelemalla voidaan varmistaa tiedon muuttumattomuus. [1]

Saatavuuden tarkoituksena on tasapainottaa edelliset periaatteet käytettävyyden suhteen ja toisaalta taata pääsy järjestelmiin myös ongelmatilanteissa. Käytännössä tämä tarkoittaa, että edellisten kohtien järjestelmä tulee suunnitella saatavuus huomioon ottaen. Toisin sanoen tiedon turvaamismekanismit eivät saa kohtuuttomasti haitata tiedon hyödyntämistä, sillä tieto, johon ei pääse käsiksi, on hyödytöntä. Esimerkiksi sähköpostin käytön kieltäminen voisi olla tietoturvallisesti perusteltua, mutta se ei kuitenkaan liiketaloudellisesti ole järkevää. Saatavuuden toinen puoli käsittää järjestelmän suojaamisen

sellaisilta vikatiloilta, jotka estävät tiedon hyödyntämisen. Tällainen on esimerkiksi palvelunestohyökkäyksiin ja sähkökatkoihin varautuminen. [1]

Tässä työssä CIA-mallin lisäksi tarkasteluun otetaan mukaan käyttäjien tunnistaminen eli autentikaatio, joka on tärkeä osa ISO 27001 -standardia. Käyttäjien tunnistamisella tarkoitetaan sellaista mekanismia, jolla pyritään varmistamaan käyttäjien identiteetti. Perusesimerkki tunnistautumisesta on käyttäjätunnus-salasanayhdistelmä, joka on yksi yksinkertaisimmista menetelmistä käyttäjän tunnistamiseen. Vahvempaa tunnistamista varten on myös vahvempia mekanismeja, kuten esimerkiksi kaksivaiheinen tunnistautuminen [2].

3 ISO 27000 -standardiperhe

ISO 27000 -standardiperhe kehitettiin täyttämään yrityksen tarve luoda kokonaisvaltainen ja yhdenmukainen tietoturvallisuuden hallintajärjestelmä. Sitä edeltävissä standardeissa oli sivuttu aihetta, mutta standardit eivät ole yksinomaan käsitelleet tietoturvallisuuden hallintajärjestelmää. Vaikka aluksi standardin käyttöönotto ei levinnyt laajalle, varsinkaan pienissä ja keskisuurissa yrityksissä, vuonna 2016 sertifikaatti oli jo yli 33 000 organisaatiolla. Kasvu vuoteen 2015 verrattuna oli 5 000 sertifikaattia. [3; 4]

Vaikka ISO 27001 -sertifikaatti ei välttämättä näy suoraan yhtiön rahallisessa arvossa, monet asiakkaat ja yhteystyökumppanit haluavat, että se tai jokin sen kaltainen järjestelmä on käytössä [5]. Kohdeyrityksessäkin alkuperäinen tarve ottaa käyttöön tietoturvallisuuden hallintajärjestelmä lähti asiakkaan toiveesta. Lisäksi standardin tarkoituksena ei ole tuottaa suoraan rahallista lisäarvoa, vaan ennaltaehkäistä yrityksen toimintaa haittaavia tietoturvaongelmia.

Standardiperhe esittelee mallin, jota voidaan noudattaa tietoturvan hallintajärjestelmän luomisessa ja käytössä. Standardi noudattaa alan asiantuntijoiden näkemyksiä alan viimeisimmästä kehityksestä. Toteuttamalla standardin mukaisen tietoturvallisuuden hallintajärjestelmän ja noudattamalla sitä organisaatiot täyttävät CIA-mallin mukaiset tietoturvallisuuden perusedellytykset. [6]

Standardiperheessä määritellään seitsemän tietoturvajärjestelmän luomiseen kuuluvaa eri osa-aluetta [7]. Osa-alueet ovat seuraavat:

1. **Organisaation toimintaympäristö**
   Tällä tarkoitetaan yrityksen ja sidosryhmien toimintaympäristön kartoittamista. Käytännössä tämä tarkoittaa sitä, että selvitetään mitä tahoja tietoturvallisuuden hallintajärjestelmä koskee ja millaisia vaatimuksia tahot puolestaan asettavat järjestelmälle.

2. **Johtajuus**
   Johto luo yritykselle sopivan tietoturvapolitiikan, sitoutuu sen noudattamiseen ja mahdollistaa sen toteutumisen määräämällä siihen riittävät resurssit ja henkilöstön. Johdon tehtävä on myös varmistaa järjestelmän ajantasaisuus.

3. **Suunnittelu**
   Suunnittelussa kartoitetaan tietoturvaan liittyvät riskit sekä niiden toteutumisen todennäköisyydet. Lisäksi luodaan toimintasuunnitelma tunnistettujen uhkien toteutumisen varalta. Suunnittelussa arvioidaan myös tietoturvatavoitteiden toteutumisedellytykset sekä tavoitteiden realistisuus.

4. **Tukitoiminnot**
   Tukitoiminnoissa määritellään tietoturvallisuuden hallintajärjestelmän ylläpitoon tarvittavat henkilöstöresurssit. Tarkoituksena on varmistaa henkilöstön pätevyys ja tietoisuus tietoturvallisuuden suhteen. Tukitoimintoihin liittyy myös viestintäsuunnitelma tietoturvallisuuden hallintajärjestelmästä sekä sen varmistaminen, että tieto on asianmukaisesti dokumentoitu.

5. **Toiminta**
   Toiminnalla tarkoitetaan, että organisaatiolla on toimintasuunnitelma, jonka noudattamiseen se on sitoutunut. Lisäksi organisaatiolla tulee olla mekanismit suunnitelman toteutumisen seurantaan. Suunnitelma ja sen seuranta koskevat myös ulkoistettuja prosesseja.

6. **Suorituskyvyn arviointi**
   Suorituskyvyn arvioinnissa määritetään seurattavat mittarit ja niistä saatavien tulosten analysoinnista ja arvioinnista vastaavat tahot. Arviointiin sisältyy myös

tasaisin väliajoin tapahtuva sisäinen auditointi sekä sitoutuminen tulosten asianmukaiseen käsittelyyn. Osana arviointia on myös määräajoin suoritettava johdon katselmus koko tietoturvallisuuden hallintajärjestelmään.

7. **Parantaminen**
   Organisaatio sitoutuu käsittelemään tietoturvapoikkeamat ja toteuttamaan niihin liittyvät vaadittavat toimenpiteet. Tähän liittyy myös jatkuva tietoturvallisuuden hallintajärjestelmän parantaminen.

ISO 27001 -standardissa määritellään yleisluontoisesti tietojärjestelmän toteuttamiseen, ylläpitämiseen ja kehittämiseen liittyvät vaatimukset. Standardi sisältää myös tietoturvariskien arviointia ja hallinnointia koskevat vaatimukset. Tässä standardissa ei käsitellä vielä yksityiskohtaisesti esimerkiksi teknisiä ratkaisuja. [7]

ISO 27002 -standardi on tarkoitettu ohjeistukseksi ISO 27001 -standardin mukaisen tietoturvallisuuden hallintajärjestelmän toteuttamiseksi. Toisin kuin ISO 27001 tämä standardi on tarkoitettu käytettäväksi organisaatio- tai toimialakohtaisten tietoturvallisuuden hallintaohjeiden kehittämisessä. Lisäksi siinä otetaan huomioon organisaatiota tai toimialaa koskevat tietoturvallisuuteen liittyvät riski- ja toimintaympäristöt. [8]

ISO 27003 -standardissa tarkennetaan ISO 27001 -standardissa jo määriteltyjä vaatimuksia kuitenkaan lisäämättä uusia kohtia määritelmään. Se antaa vaatimuksia, suosituksia ja ehdotuksia tietoturvan hallintajärjestelmän toteuttamiselle. Standardin rakenne on sama kuin ISO 27001 -standardi, mutta se avaa lisää jokaisen kohdan vaatimuksia. [9]

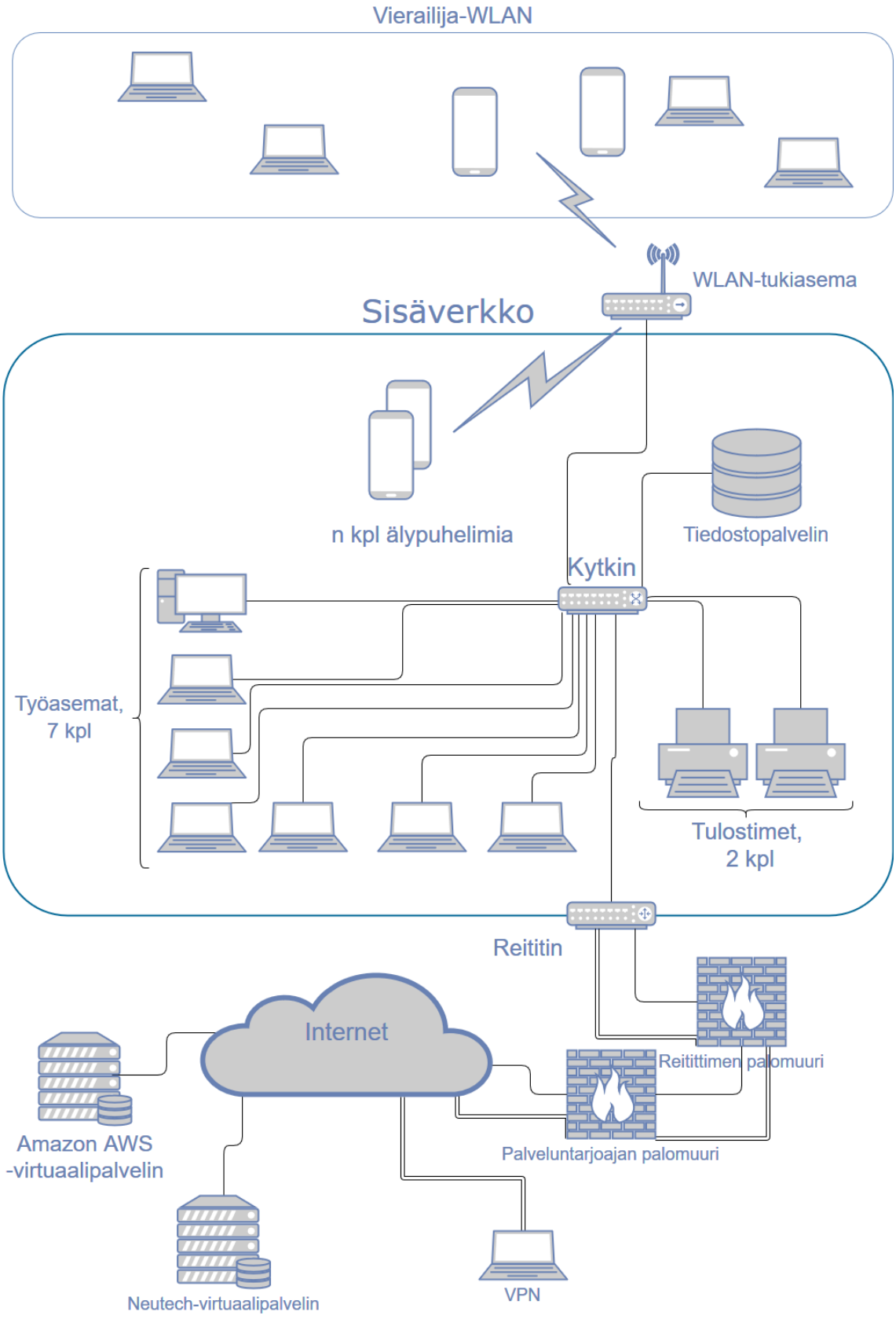
ISO 27004 -standardi tarjoaa työkalut ISO 27001 -standardin mukaisuuden arviointiin. Tässäkään standardissa ei anneta uusia vaatimuksia vaan keskitytään arvioimaan edellä määriteltyjen vaatimusten toteutumista. Kyseessä on siis tietoturvallisuuden tason seuranta- ja mittausstandardi. Standardin mukainen auditoinnin läpäiseminen oikeuttaa organisaation ISO 27001 -tason sertifikaattiin. [10]

ISO 27005 -standardissa keskitytään tietoturvariskien hallintaan. Kuten muutkin standardiperheen standardit tämäkin, syventää ISO 27001 -standardissa esitettyjä vaatimuksia, lisäämättä kuitenkaan mitään uusia kohtia. Se ei kuitenkaan ota kantaa riskienhallinnan yksityiskohtaiseen määrittelyyn, vaan se jää jokaisen organisaation määriteltäväksi. [11]

4 Kohdeyritys

4.1 Tietojärjestelmät

Kuvassa 1 on esitetty kohdeyrityksen tietoliikenneverkko ja siihen liitetyt laitteet. Verkko koostuu toimiston sisäverkosta, joka on toteutettu yhdellä reitittimellä, kytkimellä ja Wireless Local Area Network (WLAN)-tukiasemalla. Langalliseen sisäverkkoon on liitetty työasemat, tulostimet ja yksi tiedostopalvelin. Langattomaan sisäverkkoon on liitetty pääasiassa työntekijöiden älypuhelimet ja tarpeen mukaan kannettavia tietokoneita. Toimistolla on myös langaton vierailijaverkko, joka on erotettu sisäverkosta. Tämä verkko on tarkoitettu ulkopuolisten vierailijoiden käyttöön. Vierailijaverkkoon on liitetty myös joitakin sellaisia laitteita, joita ei ole haluttu sisäverkon puolelle.



Kuva 1. Kohdeyrityksen tietoliikenneverkko.

Internetin ja sisäverkon välillä on reitittimen sisäänrakennettu palomuuri ja palveluntarjoajan palomuuri. Palveluntarjoajan palomuuri on tarkoitettu pääasiassa tarkkailemaan ulospäin lähtevää liikennettä. Tarkoituksena on havaita, jos asiakasyrityksen verkko on saastunut. Lisähinnasta palveluntarjoajalta on saatavilla myös täysivertainen palomuuripalvelu. Palveluntarjoajan yhteys on varmennettu kahden eri teleoperaattorin liittymällä.

Yrityksellä on kaksi verkkosivu- ja tietokantapalvelinta. Palvelimet on sijoitettu Neutechin ja Amazonin pilvipalveluihin. Kaikki asiakkaisiin liittyvä tieto on tallennettu näille palvelimille. Näin tietojen varmistus on ulkoistettu.

Internetin kautta on mahdollista muodostaa Virtual Private Network (VPN)-yhteys yrityksen sisäverkkoon. Tämä on tarkoitettu etätyöskentelyyn, ja etäyhteyden kautta on mahdollista päästä toimiston tiedostopalvelimelle.

4.2 Nykyinen tietoturvan hallintajärjestelmä

Yrityksellä on laadittuna laadunhallinta- ja yleinen tietosuojasuunnitelma, jonka tavoitteena on ollut täyttää ISO 27001- ja ISO 27002 -standardien vaatimukset. Näiden lisäksi suunnitelmassa on otettu huomioon EU:n tietosuoja-asetus General Data Protection Regulation (GDPR) ja ISO 9001 -laadunhallintajärjestelmä. Tässä työssä keskitytään ISO 27001- ja ISO 27002 -standardien täyttymiseen, joiden osalta suunnitelma on havaittu puutteelliseksi. [12]

Pääpiirteissään nykyisessä suunnitelmassa määritellään seuraavanlaiset asiat:

- **Tiedon suojaaminen ja laadunhallinta**
  Yrityksen johto on sitoutunut GDPR-asetuksen mukaiseen tiedon suojaamisen ja suojauksen kehittämiseen. Laitteiston laadunhallinta on pääasiassa ulkoistettu ISO 9001 -standardia noudattavalle alihankkijalle.

- **Organisaatio ja vastuut tiedon suojaamisessa**
  Päävastuu on toimitusjohtajalla, ja jokainen työntekijä on tietoinen omaan työhönsä liittyvistä tiedonsuojaamisperiaatteista. Tasaisin välein koko henkilökuntaa koskevissa palavereissa käsitellään tähän liittyviä asioita.

- **Laitteiston laadunhallinta**
  Laitteiston laatu varmistetaan testaamalla se ennen käyttöönottoa ja asiakkaille luovutusta.

- **Suojattavan tiedon luokittelu ja suojausmenettely**
  Suojattava tieto on luokiteltu seuraavasti: Kriittiseen tietoon kuuluvat esimerkiksi laitteiden lähdekoodi ja asiakastiedot. Ei-kriittiseen tietoon kuuluu kaikki muu tieto, jota ei ole määritelty kriittiseksi, kuten henkilötiedot ja anonyymi tieto eli tieto, josta on poistettu yksilöivät tiedot.

- **Pääsynhallinta**
  Pääsy tietoon on rajoitettu työtehtävän perusteella. Tekninen henkilökunta on rajattu käsittelemään vain teknistä tietoa, kun taas hallinto ja myynti käsittelevät asiakastietoa.

- **Omaisuudenhallinta ja kulunvalvonta**
  Palvelimet on sijoitettu palvelinsaleihin palveluntarjoajien tiloissa, jotka täyttävät Viestintäviraston 54 A/2012M -määräyksen mukaiset vaatimukset. Yrityksen toimitilat ovat kulunvalvonnan piirissä.

- **Tiedon luottamuksellisuus**
  Siirrettävä tieto on suojattu salaamalla, ja järjestelmiin suoritetaan tunkeutumistestausta kahdesti vuodessa.

- **Tiedon pääsynhallinta**
  Tieto on suojattu salasanalla, joka on vain käyttäjän tiedossa. Tiedon käytöstä jää aina jälki.

- **Säilytettävä tieto**
  Yritys kerää ajodataa, joka on lähtökohtaisesti henkilökohtaista tietoa. Jos siitä

poistetaan käyttäjän tunnistava tieto, siitä tulee anonyymia tietoa. Tiedon säilytysaika sovitaan asiakaskohtaisesti.

- **Tietojärjestelmien hankinta, kehitys ja hallinta**
  Järjestelmät ja ohjelmat pidetään ajan tasalla, millä varmistetaan kriittisen tiedon turvallisuus. Kaikille työntekijöiden työasemille on asennettu tietoturvaohjelmisto.

- **Poikkeamien hallinta**
  Käytössä on järjestelmä, jossa määritellään poikkeaman havaitseminen, ratkaiseminen ja tiedottaminen. Kiireellisyydestä riippuen poikkeamat käsitellään heti tai viikoittaisissa palavereissa. Samassa järjestelmässä käsitellään myös asiakkaalta tuleva palaute.

- **Jatkuva parantaminen**
  Kaikki yritykselle olennainen tieto varmuuskopioidaan tasaisin aikavälein. Kaikissa uusissa projekteissa ja kehityshankkeissa huomioidaan myös tietoturva-asiat. Parantaminen liitetään myös asiakaskumppanuuksiin.

- **Vaatimustenmukaisuus**
  Yritys noudattaa ISO 27001- ja ISO 27002 -standardeja, henkilötietolakia (213/1999) ja EU:n GDPR -tietosuoja-asetusta.

5 Tietoturvakartoitus

Tässä luvussa selvitetään, kuinka hyvin kohdeyritys toteuttaa ISO 27001 -standardin asettamat vaatimukset tietoturvallisuuden hallintajärjestelmälle. Kartoituksen tavoitteena on löytää nykyisen hallintajärjestelmän puutteet ja määrittää toimenpiteet standardinmukaisuuden saavuttamiseksi.

5.1 Nykyinen tietoturvajärjestelmä ja ISO 27001 -standardi

Ensimmäinen vastaan tullut ongelma liittyy siihen, miten yrityksen tietoturvadokumentaatio on jäsennelty. Tällä hetkellä tietoturvadokumentaatio on liitetty osaksi yrityksen laadunhallinta- ja tietosuojasuunnitelmaa. Tämä hankaloittaa kaikkiin kolmeen osa-alueeseen liittyvän tiedon löytämistä ja hallintaa. Ensimmäinen askel tietoturvallisuuden hallintajärjestelmän parantamiseksi olisi kaikkien kolmen osa-alueen erottaminen omiin dokumentteihinsa.

Seuraavaksi käydään läpi ISO 27001 -standardin mukaiset kohdat ja tarkastellaan, kuinka hyvin ne nykyisessä suunnitelmassa toteutuvat.

1. **Organisaation toimintaympäristö**
   Nykyisestä suunnitelmasta puuttuu kokonaan selkeä kohta, jossa määritellään hallintajärjestelmän toimintaympäristö ja siihen liittyvät sidosryhmät. Tämän vuoksi suunnitelmasta puuttuu myös selkeä rajaus järjestelmän soveltamisalueesta.

2. **Johtajuus**
   Johto on sitoutettu tietoturvallisuuden hallintajärjestelmään, mutta itse tietoturvapolitiikka on puutteellinen. Tietoturvapolitiikka on määritelty laadunhallinta- ja tietosuojasuunnitelmassa, mutta selkeät tietoturvatavoitteet ovat määrittelemättä. Suunnitelmasta puuttuvat kokonaan myös tietoturvallisuuteen liittyvät roolit, vastuut ja valtuudet.

3. **Suunnittelu**
   Suunnitelmassa on määritelty mekanismi poikkeamien käsittelyyn, mutta siihen ei sisälly ohjeita ennalta kartoitettujen riskien käsittelyyn. Toisin sanoen suunnitelmasta puuttuu täysin tietoturvariskien arviointi ja käsittely sekä tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu.

4. **Tukitoiminnot**
   Kuten aiemmin jo mainittiin, suunnitelmasta puuttuu vastuuhenkilöiden määrittely, joten tässä mainittu vastuuhenkilöiden tarvittava pätevyys ja tietoisuus on määrittelemättä. Suunnitelmassa ei ole myöskään otettu kantaa tietoturvajärjestelmään liittyvään viestintään.

5. **Toiminta**

   Koska riskienhallintaa ei ole määritelty suunnitelmassa, ei riskeihin liittyvää toimintaakaan ole voitu määritellä.

6. **Suorituskyvyn arviointi**

   Suunnitelmassa ei ole erikseen määritelty mittareita suorituskyvyn arviointiin. Sisäistä auditointia ei ole virallisesti määritelty, mutta sitä tapahtuu epäsäännöllisin väliajoin. Tarkastelun seurauksena on havaittu suunnitelman olevan puutteellinen, minkä seurauksena tätä insinöörityötä on alun perin ryhdytty tekemään.

7. **Parantaminen**

   Suunnitelmassa on määritelty poikkeamien hallinta ja käsittely. Yritys on myös sitoutunut jatkuvaan tietoturvallisuuden hallintajärjestelmän parantamiseen, mikä on johtanut tämän insinöörityön tilaamiseen.

5.2 Nykyinen tietoturvajärjestelmä ja ISO 27002 -standardi

Tarkastelussa havaittiin, että nykyinen suunnitelma ei noudata standardin mukaista rakennetta käytännössä ollenkaan. Tämän takia standardin vertaileminen kohta kohdalta ei ole tarkoituksenmukaista, sillä käytännössä suurimpaan osaan kohdista voidaan todeta, että suunnitelma ei noudata standardia. Käytännöllisin ratkaisu onkin siis aloittaa uuden suunnitelman tekeminen puhtaalta pöydältä, käyttäen standardin rakennetta pohjana.

6 Kyselypohja järjestelmäauditointia varten

Tietoturvakartoituksen pohjana järkevin ratkaisu on käyttää kyselypohjaa, joka perustuu ISO 27002 -standardiin ja huomio ISO 27001 -standardin vaatimukset. Sen sijaan, että olisi käytetty valmista pohjaa päädyttiin, tekemään kysely itse, mikä mahdollisti perusteellisen tutustumisen standardiin kyselyä tehdessä. Kyselypohjasta oli tarkoitus tehdä

sellainen, että sen avulla voidaan luoda, arvioida ja päivittää tietoturvallisuuden hallintajärjestelmä kohdeyritykselle. Kyselystä jätettiin pois kohdat, jotka eivät kuulu kohdeyritykselle, kuten kiinteistön vuokranantajan vastuulla olevat asiat. Standardissa olevia päällekkäisiä kohtia myös karsittiin soveltamisen käytännöllistämiseksi.

Insinöörityön osana laadittu kyselypohjan rakenne koostuu ISO 27002 -standardin 14 osa-alueesta. Kyselyn ensimmäisessä osa-alueessa selvitetään tietoturvapolitiikka. Tämän perusteella luodaan julkinen dokumentti, jossa määritellään yrityksen tietoturvan peruspilarit [13]. Kohdissa 2-14 käydään läpi kohdeyrityksen sisäisen tietoturvallisuuden eri osa-alueet ja käytännöt. Tietoturvallisuuskäytännöt muodostavat yrityksen sisäiseen käyttöön tarkoitetun tietoturvallisuuden hallintajärjestelmän.

1. Tietoturvapolitiikka

    a. Mikä on yrityksen tietoturvapolitiikan päämäärä?

        Tässä kohdassa pyritään vastaamaan seuraaviin kysymyksiin:

        - Mikä on tietoturvallisuuden tarkoitus, kuten yrityksen tietojärjestelmien käytettävyys ja turvallisuus?
        - Mitä tahoja tietoturvapolitiikka koskee?
        - Miten tietoturvallisuus on määritelty? Luottamuksellisuus, eheys ja saatavuus?
        - Miten tietoturvallisuutta seurataan? Erilaiset seurantamekanismit?
        - Missä tietoturvallisuuspolitiikka otetaan huomioon? Sopimukset, hankinnat yms.?
        - Miten asiakastietoja käsitellään? GDPR:n huomioiminen?

    b. Miten tietoturvapolitiikassa on jaettu vastuut ja organisointi?

        Tässä kohdassa pyritään vastaamaan seuraaviin kysymyksiin:

        - Onko tietoturvapolittikassa eritelty eri osa-alueita?
        - Onko jokaiselle osa-alueille määritelty vastuuhenkilö?

c. Mitä erilaisia prosesseja on olemassa tietoturvapoikkeamien käsittelyyn?

- Esimerkkejä prosessista ovat riskien arviointi, tietojen luokittelu ja käsittely, henkilötietojen käsittely, tietoverkon käyttö, tietoturvakoulutus, valvonta ja seuranta ja tietoturvapoikkeamien käsittely, tietoturvarikkomukset ja viestintä henkilöstölle ja kumppaneille.

2. Tietoturvallisuuden organisointi

a. Mitkä ovat yrityksessä suojattavat kohteet?

- Esimerkiksi yrityskiinteistö, yrityksen maine, työasemat, tietokanta ja lähdekoodi.

b. Edellisessä määriteltyjen kohteiden suojausprosessit?

- Esimerkiksi kiinteistössä kulunvalvonta ja tietokannassa varmuuskopiointi.

c. Kuka tai ketkä vastaavat kustakin suojattavasta kohteesta ja sen suojausprosessista?

d. Kenellä on oikeus ja minkä tasoinen valtuutus kuhunkin suojattavaan kohteeseen?

e. Onko nimetyillä henkilöillä riittävä pätevyys tehtäväänsä ja mahdollisuudet pitää osaamisensa ajan tasalla?

f. Kuka vastaa asiakassuhteissa tietoturvasta?

g. Miten tietoturvan vastuualueet on eriytetty?

h. Kenen vastuulla on viranomaisyhteistyö?

i. Mikä on mobiililaitteita koskeva politiikka?

- Hankkiiko yritys työpuhelimet, ja onko niiden käytössä mitään rajoituksia?

j. Mikä on etätyötä koskeva politiikka?

- Miten etäyhteys on toteutettu? VPN?

- Mihin etäyhteydellä pääsee?

- Fyysinen turvallisuus? Kuka saa käyttää etäyhteydellä varustettua laitetta?

3. Henkilöstöturvallisuus

    a. Mitä tulee ottaa huomioon ennen palkkaamista?

        - Ansioluettelon ja koulutuksen oikeellisuuden varmistaminen?
        - Henkilöllisyyden varmistaminen?
        - Tehtävään vaaditut tarkistukset? Rikosrekisteri?

    b. Miten tietoturvallisuus tulee ottaa huomioon työsopimuksessa?

        - Salassapito- tai vaitiolosopimus?
        - Tekijänoikeus?
        - Vastuu tiedonkäsittelystä?
        - Rangaistustoimenpiteet?

    c. Miten varmistetaan tietoturvallisuus työsuhteen aikana?

        - Miten johto on sitoutunut ja sitouttaa muut tietoturvallisuuteen?
        - Miten varmistetaan, että työntekijät pystyvät hoitamaan vastuualueensa? Esim. opastus, koulutus, työkalut?

    d. Mitä tulee ottaa huomioon työsuhteen päättyessä tai muuttuessa?

        - Muuttuvatko vastuut työsuhteen muuttuessa?
        - Salassapito- tai vaitiolosopimus työsuhteen loppuessa?

4. Suojattavan omaisuuden hallinta

    a. Mitä kaikkea suojattavaa tietoa yrityksellä on?

    b. Kuka omistaa suojattavan omaisuuden?

    c. Miten tai mihin suojattavaa omaisuutta saa käyttää?

d. Mitä on määrätty suojattavan omaisuuden palauttamisesta?

    - Esim. työsuhteen päättyessä?

e. Onko tieto luokiteltu ja suojattu sen luokan vaatimalla tavalla?

    - Kuinka paljon haittaa tiedon paljastamisesta koituu yritykselle?

f. Onko tieto merkitty luokittelun mukaan?

    - Salassa pidettävä tieto?

g. Kuka saa käsitellä suojattavaa tietoa?

h. Saako siirrettäviä tietovälineitä käyttää? Mihin tarkoitukseen?

i. Tietovälineiden asianmukainen hävittäminen?

    - Vanhan työaseman kiintolevyn oikeanlainen tyhjentäminen?

j. Fyysisten tietovälineiden siirtäminen?

    - Asiakirjojen lähettäminen postissa?

5. Pääsynhallinta

    a. Minkälaista pääsynhallintapolitiikkaa yritys noudattaa?

        - Miten pääsy eri järjestelmiin ja tietoon on rajattu?

        - Kuka päättää pääsynhallinnasta?

        - Jääkö käytöstä merkintä?

        - Onko pääsynhallinnan periaate ”kaikki on kiellettyä, ellei sitä erikseen sallita”?

    b. Miten pääsy verkkoihin ja verkkopalveluihin on hallinnoitu?

        - Onko pääsyä verkkoihin ja verkkopalveluihin rajattu?

        - Millä tavalla rajaus on toteutettu?

- Seurataanko käyttöä?

c. Miten pääsyoikeuksia hallinnoidaan?

- Kuka käyttäjiä hallinnoi ja miten?
- Yksilöidäänkö käyttäjät?
- Miten varmistetaan käyttäjälistan ajanmukaisuus?

d. Kenelle ja millä perusteilla annetaan ylläpito-oikeudet?

e. Miten hallinnoidaan käyttäjätunnusten jakamista ja salassapitoa?

f. Arvioidaanko käyttäjäoikeuksia tasaisin väliajoin?

g. Miten käyttäjät on velvoitettu pitämään tunnistautumistiedot salassa ja käyttämään riittävän turvallisia tunnistautumistietoja?

h. Noudattaako pääsynhallinta vähäisimmän tarpeen periaatetta?

- Annetaanko pääsyoikeus vähimmäistarpeen mukaan, esim. vain lukuoikeus, kun ei ole tarvetta muokata tietoa.

i. Onko kirjautumismekanismit mietitty tapauskohtaisesti eli suhteutettuna järjestelmän kriittisyyteen?

j. Onko käytössä salasanojen hallintajärjestelmä, joka velvoittaa käyttäjät käyttämään turvallisia salasanoja?

- Riittävän vahva salasana?
- Salasana vaihdettava tasaisin väliajoin?

k. Onko ohjelmien asentamista rajoitettu tietokoneelle?

- Erityisesti ohjelmat, joilla voi kiertää järjestelmän hallintakeinoja?

l. Onko ohjelmiston lähdekoodi suojattu pääsynhallinnalla?

6. Salaus

a. Onko salaus toteutettu yrityksessä ja miten?

b. Kuka on vastuussa salauksen toteuttamisesta?

c. Salainen viestintä? Digitaalinen allekirjoitus?

7. Fyysinen turvallisuus ja ympäristön turvallisuus?

   a. Onko määritelty fyysisiä turva-alueita?

      - Alue, jonne vain asianmukaiset henkilöt pääsevät?

   b. Kulunvalvonta?

   c. Miten laitteet on suojattu fyysiseltä pääsyltä?

   d. Miten laitteet on suojattu eri häiriötilanteilta?

   e. Miten laitteet on suojattu, kun ne viedään toimitilojen ulkopuolelle?

      - Työasemien salaus?

   f. Miten ilman valvontaa jäävät laitteet on suojattu?

      - Työasemien turvaaminen?

      - Palvelinhuoneen lukitseminen?

8. Käyttöturvallisuus

   a. Onko toimintaohjeet dokumentoitu asianmukaisesti?

      - Järjestelmien asentaminen?

      - Varmuuskopiointi?

      - Järjestelmien uudelleenkäynnistysmenettelyt?

   b. Onko muutoksenhallintaprosesseja määritelty?

      - Onko huomioitu, miten suuret muutokset yrityksen toiminnassa vaikuttavat tietoturvallisuuteen? Esimerkiksi uuden järjestelmän käyttöönotto.

   c. Seurataanko resurssien käyttöä ja varmistetaanko järjestelmien suoritus-kyky?

d. Onko kehitys-, testaus- ja tuotantoympäristöt erotettu toisistaan?

e. Onko haittaohjelmilta suojauduttu?

    - Onko ohjelmien asentamista rajoitettu?
    - Virustorjunta? Palomuuri?
    - Ohjelmistopäivitykset?

f. Harjoitetaanko varmuuskopiointia?

    - Kuinka laajasti? Kuinka usein?

g. Kerätäänkö tapahtumalokia, josta selviävät mahdollisuuksien mukaan käyttäjien suorittamat toiminnot, tapahtuneet poikkeamat, virheet ja tietoturvatapahtumat?

h. Onko lokitiedot suojattu asianmukaisesti?

i. Onko määritelty prosessi tuotantokäytössä olevien ohjelmistojen asentamiseen?

j. Seurataanko haavoittuvuustiedotteita?

k. Onko olemassa tietojärjestelmien auditointiprosessia, ja miten se on toteutettu?

    - Ohjelmiston ajantasaisuus ja eheys?

9. Viestintäturvallisuus

a. Kuka vastaa verkkolaitteiden valvonnasta ja hallinnasta?

b. Miten verkkoa hallitaan ja valvotaan?

c. Miten on huomioitu julkisessa verkossa liikkuvan tiedon turvallisuus?

d. Miten käyttäjäryhmät on erotettu verkossa?

e. Mitä tiedonsiirtoa koskevia menettelyjä on määritelty?

f. Minkälaisia tiedonsiirtosopimuksia on tehty ulkopuolisten kanssa?

- Miten vastuut on jaettu?

g. Miten sähköinen viestintä on suojattu?

- Sähköposti, Slack?

h. Mitä salassapito- ja vaitiolositoumuksien piiriin kuuluu?

10. Järjestelmien hankkiminen, kehittäminen ja ylläpito

a. Minkälaisia tietoturvavaatimuksia liittyy uusien järjestelmien hankintaan?

b. Miten julkiset sovelluspalvelut on suojattu julkisessa verkossa?

- Laitteiden suojaus? Yksityinen APN?

- Verkkosivujen suojaus?

c. Miten sovelluspalvelutapahtumat on suojattu?

- Datan kulkeminen laitteelta palvelimelle ja siitä asiakkaalle?

d. Kuinka tietoturvallisuuden kehittäminen on huomioitu tietojärjestelmien elinkaaressa?

- Kehitysympäristön turvallisuus?

e. Onko ohjeistusta uuden järjestelmän turvallisen suunniteluun?

f. Onko määritelty turvallinen kehitysympäristö?

g. Seurataanko ulkoisen kehityksen turvallisuutta?

h. Testataanko järjestelmän turvallisuutta?

i. Tehdäänkö järjestelmälle hyväksymistestausta?

- Uuden version, päivityksen tai kokonaan uuden järjestelmän testaus?

j. Käytetäänkö testauksessa luottamuksellista tietoa?

- Jos käytetään, miten se on suojattu?

11. Suhteet toimittajiin

    a. Miten toimittajien pääsynhallinta on toteutettu?

    b. Kuinka on varmistettu toimittajien käyttämän tiedon luottamuksellisuus?

    c. Onko toimittajasopimuksissa määritelty toimittajia koskevat tietoturvallisuusvelvoitteet?

    d. Onko ulkoistettujen palveluiden jatkuvuus huomioitu?

    e. Auditoidaanko toimittajien tuottamia palveluita?

12. Tietoturvahäiriöiden hallinta

    a. Kuka vastaa tietoturvahäiriöiden hallinnasta?

    b. Minkälainen prosessi häiriöiden käsittelyä varten on luotu?

    c. Miten häiriöistä ja tapahtumista raportoidaan ja kenelle?

        - Miten raportit on luokiteltu?

    d. Onko käytäntö tietoturvapuutteiden raportointiin?

    e. Minkälainen menettely on tietoturvahäiriöihin vastaamiseen?

        - Miten on varmistettu, että häiriöstä opitaan?

13. Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

    a. Miten tietoturvallisuuden jatkuvuus on suunniteltu ja toteutettu ja miten sen toteutumista seurataan?

    b. Onko vikasietoisuus otettu huomioon tietojenkäsittelypalvelussa? Miten?

14. Vaatimustenmukaisuus

    a. Miten on varmistettu kaikkien tietoturvallisuuteen liittyvien lakien, asetusten, säännösten ja sopimusten velvoitteiden ja turvallisuusvaatimusten noudattaminen?

    b. Miten on varmistettu tekijänoikeuslakien noudattaminen?

c. Miten tietosuoja ja henkilötietojen suojaaminen on toteutettu?

    - GDPR?

d. Miten tietoturvallisuuden hallintajärjestelmä katselmoidaan?

    - Tekeekö ulkopuolinen taho auditoinnin sisäisen katselmoinnin lisäksi?

7 Parannussuunnitelma

Kohdeyrityksessä pidettiin palaveri, jossa käytiin läpi työssä laadittu ja luvussa 6 esitelty kyselylomake. Palaveriin osallistuivat henkilöt, jotka ovat vastuussa tietoturvallisuudesta. Kuten luvussa 5 todettiin, kohdeyrityksen suurin tietoturvallisuuteen liittyvä puute on dokumentoinnin vajavaisuus. Tämän lisäksi kyselyä läpikäydessä havaittiin puutteita vastuuhenkilöiden ja -roolien tunnistamisessa tietoturvallisuuden eri osa-alueilla. Nykyisestä dokumentoinnista puuttuivat kokonaan suojattavan omaisuuden ja suodattavan tiedon määrittelyt, joten myöskään niitä ei ole luokiteltu. Luokittelun puuttumisen myötä tiedon suojaus voi olla riittämätön, koska suojaustasojakaan ei ole määritelty. Vaikka kunnollinen dokumentaatio puuttuikin, tunnistettiin kyselystä myös monia asioita, jotka toteutuvat. Niitä ei ole kuitenkaan kirjattu mihinkään.

Kohdeyrityksen toiveesta parannussuunnitelmassa keskitytään tietoteknisiin ongelmiin ja niiden ratkaisuihin. Suurimmat kohdatut puutteet olivat käyttäjien yksilöinti, pääsyoikeuksien rajoittaminen ja päivittäminen, asennettavien ohjelmien hallinta niin työpuhelimissa kuin työasemissa, riittävän salauksen käyttö, lokitiedostojen keräys ja vanhojen työvälineiden hävittäminen.

Käyttäjien yksilöinti, pääsyoikeuksien rajoittaminen ja päivittäminen ovat kaikki osa samaa ongelmaa eli riittämätöntä käyttäjienhallintaa. Tämän ratkaisemiseksi on erilaisia valmiita ratkaisuja riippuen alustasta. Suurin ongelma käyttäjienhallinnassa liittyy yrityksen tuotteeseen liittyvään kirjautumisjärjestelmään. Järjestelmässä on tuki käyttäjien yksilöintiä varten ja pääsynhallintaan, mutta kyselyä tehdessä huomattiin, että se ei ole

käytössä läheskään riittävässä mitassa. Tiedostopalvelimella on käytössä Samba -tiedostojenjako-ohjelmisto, joka tukee palvelimen Unix-tiedostojen käyttäjäryhmiä ja oikeuksia. Palvelimella on sama ongelma kuin yrityksen omassa järjestelmässä, eli teknologia on olemassa, mutta sitä ei vain hyödynnetä riittävästi. Käyttäjät yksilöidään, mutta kaikilla on täydet valtuudet koko järjestelmään. Suureksi tietoturvaongelmaksi havaittiin myös, että vanhoja käyttäjätunnuksia ei käydä systemaattisesti läpi tasaisin väliajoin. Jos käyttäjätunnuksia ja pääsyoikeuksia ei poisteta tarvittaessa, voi järjestelmään päästä käyttäjä, jolla ei pitäisi enää olla oikeuksia.

Toinen tunnistettu mahdollinen tietoturvallisuuspuute on se, että ohjelmistojen asentamista työasemille ja työpuhelimiin ei rajoiteta. Yrityksen koon vuoksi tämä ei ole välttämätöntä, mutta jonkinlainen ohjeistus sallittavista ohjelmista olisi tarpeellinen. Jos kuitenkin päädytään rajoittamaan asennettavia ohjelmistoja, siihen on erilaisia ohjelmistoratkaisuja. Nykyaikaisissa älypuhelimissa tällainen ominaisuus on lähes poikkeuksetta. Työpöytäkäyttöjärjestelmistä on myös valmiita ratkaisuja, mutta keskitetyt ratkaisut voivat vaatia lisäinvestointeja.

Salauksen osalta perustavanlaatuisin puute on puuttuva tiedon luokittelu. Toissijaiset puutteet ovat älypuhelinten ja työasemien salaamattomuus ja salaamaton viestintä. Esimerkiksi sähköpostissa välitetään tietoa, joka tulisi pitää salassa. Älypuhelimissa on sisäänrakennettu salausominaisuus, mutta sen käyttöön ei ole velvoitettu. Työasemien puolella salaus voidaan toteuttaa käyttöjärjestelmissä valmiina olevilla ominaisuuksilla tai kolmannen osapuolen ohjelmistoilla.

Lokitiedostojen keräyksessä parannettavaa olisi kerättävän tiedon määrässä. Tämän voi ratkaista laskemalla tiedonkeräyskynnystä. Lokitiedot voisi myös kerätä keskitetysti, jolloin niiden seuranta olisi helpompaa.

Vanhan tiedon hävittämisessä olisi parannettavaa käytettyjen kiintolevyjen ja asiakirjojen käsittelyssä. Vanhoja kiintolevyjä ei hävitetä asianmukaisesti, vaan tällä hetkellä ne ovat kerättynä hyllyyn muun elektroniikkajätteen kanssa. Kaikkia vanhoja asiakirjoja ei hävitetä asianmukaisesti. Kiintolevyt voisi itse tuhota fyysisesti tehden niille tallennetusta tiedosta käyttökelvotonta. Vanhat asiakirjat tulisi silputa järjestelmällisesti. Vaihtoehtoisesti molemmat voisi toimittaa ulkopuoliselle yritykselle, joka on erikoistunut tiedon hävittämiseen.

Edellä mainituista toimenpiteistä tärkeimmät toteutettavat toimenpiteet olisivat keskitetty käyttäjienhallinta ja puhelimien ja työasemien salaus. Lisäksi suositeltavaa olisi parantaa vanhan tiedon asianmukaista hävittämistä.

8 Yhteenveto

Insinöörityön tarkoituksena oli kartoittaa kohdeyrityksen tietoturvallisuuden taso. Työssä tutustuttiin ensin lyhyesti tietoturvallisuuden perusteisiin. Kohdeyrityksen toiveesta tutustuttiin ISO 27000 -standardiperheeseen, jonka pohjalta kartoitus tehtiin. Työssä päädyttiin tekemään kyselypohja ISO 27002 -standardin perusteella. Itse tehty kysely mahdollisti standardeihin tutustumisen ja olennaisilta osin soveltamisen kohdeyrityksen tarpeisiin.

Kyselylomake toimi hyvin, kun pyrittiin kartoittamaan yrityksen tietoturvapuutteet. Kuitenkin kyselylomaketta käytettäessä paljastui, että se on liian suppea, jotta sen avulla olisi mahdollista luoda tietoturvallisuuden hallintajärjestelmä. Jo olemassa olevan hallintajärjestelmän päivittämiseen sen sijaan kysely voisi toimia. Tämä selviää käytännössä, kun kohdeyrityksessä palataan asiaan puolen vuoden päästä. Kyselyä täyttäessä havaittiin, että kysymykset olivat liian suurpiirteisiä eikä niitä ollut selitetty riittävästi niin, että henkilö, joka ei ole tutustunut standardiin, ymmärtäisi kysymyksen perimmäisen ajatuksen.

Seuraava askel on tunnistettujen puutteiden korjaaminen. Puutteiden korjaamisen jälkeen kannattaa vasta keskittyä standardinmukaisen dokumentaation ja täysimittaisen tietoturvallisuuden hallintajärjestelmän luomiseen. Kun kaikki edellä mainitut on tehty, voidaan haluttaessa hakea ISO 27001 -standardin sertifikaattia.

Lähteet

1 Stallings, W. 2011. Cryptohraphy and Network Security Principles and Practice. Fifth Edition. New York: Prentice Hall.

2 Google 2-step verification. 2018. Verkkoaineisto. Google Inc. https://www.google.com/landing/2step/#tab=how-it-works. Luettu 29.3.2018

3 ISO Survey 2016. 2017. International Organization for Standardization.

4 Barlette, Yves & Fomin, Vladislav. 2008. Exploring the Suitability of IS Security Management Standards for SMEs. Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). Hawaii: Waikoloa.

5 Hsu, C., Wang, T. & Lu, A. 2016. The Impact of ISO 27001 Certification on Firm Performance. 49th Hawaii International Conference on System Sciences (HICSS). Hawaii: Koloa

6 SFS-EN ISO/IEC 27000:2017 Informaatioteknologia. 2017. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardisoimisliitto.

7 SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. 2017. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto.

8 SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. 2017. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen Standardisoimisliitto.

9 SFS-ISO/IEC 27003:2017 Information technology. 2017. Security techniques. Information security management systems. Guidance. Helsinki: Suomen Standardisoimisliitto.

10 SFS-ISO/IEC 27004:2016 Informaatioteknologia. 2016. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Helsinki: Suomen Standardisoimisliitto.

11 SFS-ISO/IEC 27005:2011 Informaatioteknologia. 2011. Turvallisuus. Tietoturvariskien Hallinta. Helsinki: Suomen Standardisoimisliitto.

12 Target Companys Quality policy and General Data Protection.

13 Tietoturvapolitiikka. 2013. Verkkoaineisto. Kesko Oyj. https://www.kesko.fi/yritys/politiikat-ja-periaatteet/tietoturvapolitiikka/. Luettu 19.4.2018.