Jani Rintala

VAHTI-ohjeistuksen käyttö yrityksen tietoturvan kehittämisessä

Tietojenkäsittelyn koulutusohjelma

2020

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VAHTI-ohjeistuksen käyttö yrityksen tietoturvan kehittämisessä

Rintala, Jani
Satakunnan Ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2020
Sivumäärä: 34
Liitteitä: 0

Asiasanat: Tietoturva, ISO, Katakri, VAHTI, Tietoturvapolitiikka, Riskienhallinta

---

Työn tarkoitus on tutkia nykyisiä yrityksissä käytettyjä standardeja, tietoturvallisuudenhallintajärjestelmiä, tietoturvaa ja sen osa-alueita sekä hieman tietoturvapolitiikkaa ja riskienhallintaa.

Hyvällä tietoturvalla pystytäänkin ennaltaehkäisemään yritykseen mahdollisesti kohdistuvia uhkatekijöitä, joita ovat vaikkapa tiedon kalastelu, huijausviestit, mahdolliset virukset sekä ehkä jopa tärkeimpänä tekijänä yrityksen oma henkilöstö.

Työn aikana laajensin paljon omaa tietämystäni alan standardeista, hallintajärjestelmistä ja tietoturvasta yleisesti. Aion jatkaa aiheeseen perehtymistä ja tietopankkini laajentamista.

Using Vahti-guidance in developing company security policy

Rintala, Jani
Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
May 2020
Number of pages:34
Appendices:0

Keywords: Security, ISO, Katakri, VAHTI, Information policy, Risk management

---

Goal of this thesis was to examine standards, information security management systems, infomation security, risk management and how they are used in a company.

With good information security, we can prevent possible incoming threats for the company, which could be something like, information fishing, scam emails, viruses, and maybe even most important factor, it's own employees.

During this thesis, I expanded my knowledge in this branch of industry. Now I know a lot more about, risk management, infomation security overall, information security management systems and standards used in the business. Im going to keep developing my knowledge with information security and moving forward with it.

SISÄLLYS.

LYHENNELUETTELO

IEC - International Electrotechnical Commission on kansainvälinen sähköalan standardointiorganisaatio.
ISMS - Tietoturvan johtamisjärjestelmä
ISO - International Organization for Standardization eli ISO on kansainvälinen standardisoimisjärjestö.
Katakri - Katakri on viranomaisten auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata viranomaisen salassa pidettävää tietoa.
SFS - Suomen Standardisoimisliitto SFS ry on standardisoinnin keskusjärjestö
VAHTI - Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

1 JOHDANTO

Tietoturvallisuus on yksi tärkein osa organisaation liiketoimintaa, jos yrityksen tietoturva ei ole kunnossa saattaa koko yritys olla vaarassa. Toiminnan kannalta on erittäin tärkeää, että yritys pystyy tunnistamaan omat tietoturvariskinsä ja hallitsemaan tietojärjestelmiinsä mahdollisesti kohdistuvat uhkat. Täydellistä tietoturvallista ympäristöä ei tietenkään voida ikinä saavuttaa, on liikaa muuttujia, jotka aiheuttavat vaaratekijöitä, kuten esim. palveluntarjoajat, teknologiatoimittajat sekä ehkä suurimpana vaikuttajan yrityksen oma henkilöstö.

Tässä opinnäytetyössä pyrin perehtymään yrityksen omaan tietoturvaan sekä tietosuojaan. Aiheena on Vahti henkilöstön tietoturvaohje (4/2013) ja sen peilaus yrityksen nykyiseen tietoturva ohjeistukseen. VAHTI on Valtiovarainministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä, joka kehittää VAHTI-ohjeistusta, tämä sisältää kaikki tietoturvan osa-alueet. Koska tietoturvallisuus on aiheena kovin laaja, on työ vain pintaraapaisu mitä tietoturva pitää sisällään. Työn jälkeen oppimieni asioiden perusteella tulen myös täydentämään yrityksen omaa tietoturvaohjetta, soveltaen vahdin omia ohjeistuksia.

Opinnäytetyö tehdään It-alalla toimivalle yritykselle.

Työn alussa tulen käsittelemään tietoturvastandardien osiota, jotka pitää sisällään VAHTI-ohjeistuksen, ISO-standardit sekä Katakri-auditointityökalun. Tämän jälkeen avaan yleisesti asioita tietoturvasta, sen hallintajärjestelmistä, tietoturvapolitiikasta sekä hieman riskienhallinnasta.

2 TIETOTURVASTANDARDIT

2.1 VAHTI

Valtiovarainministeriö yhteensovittaa sekä ohjaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä.
Vahti eli ministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä, on asetettu hallinnon tietoturvallisuuden ohjaukseen, kehitykseen sekä koordinaatioon.
VAHTIn tehtävä on käsitellä kaikki merkitykselliset valtionhallinnon tieto- ja kyberturvallisuuden linjaukset sekä näiden tietoturvatoimenpiteiden ohjausasiat. Vahti tukee tällä toiminnalla valtioneuvostoa sekä valtiovarainministeriöitä hallinnon tietoturvallisuuteen liittyvissä päätöksenteoissa ja niiden valmisteluissa.

”VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toiminmtojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä editää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.” (Valtiovarainministeriö 2009.)

Valtioneuvosto on tehnyt 26.11.2009 periaatepäätöksen, joka korostaa VAHTIn asemaa ja tehtäviä hallinnon tietoturvallisuuden ohjaamisen, kehityksen ja koordinaation ytimenä. Tämän päätöksen mukaan hallinnonalat kohdistavat varoja ja resursseja tietoturvan kehitykseen sekä VAHTIssa koordinoitavaan yhteistyöhön. (Valtiovarainministeriö 2009.)

VAHTIn avulla parannetaankin valtion tietoturvaa ja työn vaikutus on nähtävissä hallinnon ohessa myös yrityksissä sekä kansainvälisesti. Tuloksena on jopa kansainvälisesti verrattuna merkittäväksi katsottu yleinen tietoturvallisuusohjeistus. (Valtiovarainministeriö 2009.)

2.2 Katakri

Katakri on tietoturvallisuuden auditointityökalu viranomaisille, jota voidaan hyödyntää arvioitaessa kohdeyrityksen kykyä suojata viranomaisten salassa pidettävää tietoa. Katakri sisältää kansallisten säännösten ja kansainvälisiin velvoitteisiin perustuvat vähittäisvaatimukset. Tietoturvallisuudelle Katakri ei yksinään aseta mitään ehdottomia vaatimuksia, vaan siihen kuuluvat vaatimukset perustuvat nykyiseen lainsäädäntöön sekä Suomea sitoviin kansainvälisiin tietoturvallisuusvelvotteisiin. (Puolustusministeriö, 2019)

Katakrin rakenne:
Katakrissa esiintyvät vaatimukset on jaoteltu kolmeen eri osioon. Turvallisuusjohtamiseen, Fyysiseen turvallisuuteen ja tekniseen tietoturvallisuuteen. Turvallisuusjohtamisen osa-alueessa on pyritty varmistumaan siitä, että yrityksellä on riittävät turvallisuusjohtamisen valmiudet ja kyvykkyys. Tässä osa-alueessa on kuvattu oma perustasonsa, jonka vaatimukset on kohdeyrityksen täytettävä.
Fyysisen turvallisuuden osa-alueeseen kuuluu salassapidettävän tiedon fyysistä käyttöympäristöä koskevat turvallisuusvaatimukset. Yrityksen tilat pystytään salaisten tietojen käsittely- ja säilytystarpeen mukaan jakaa kolmeen eri osa-alueeseen: eli hallinnolliseen alueeseen, turva-alueeseen ja vielä tekniseen turva-alueeseen. Teknisen tietoturvan osa-alueessa kuvataan nimenomaan tekniselle tietojenkäsittely-ympäristölle määritetyt turvallisuusvaatimukset. (Puolustusministeriö, 2019)

Tarkemmin osa-alueista:
Turvallisuusjohtaminen: tämä alue kattaa henkilöstöturvallisuuden ja hallinnollisen turvallisuuden, sekä sisältää menetelmät, joilla turvallisuus ja sen hallinta luodaan osaksi koko yrityksen toimintaa. Asetetuilla vaatimuksilla pyritään siihen, että yritykselle saadaan toimiva turvallisuuden hallintajärjestelmä ja siihen riittävät menettelyt sen varmistamiseksi, että viranomaisten salassa pidettäviä tietoja käsitellään henkilös-

tön toimesta asianmukaisesti. Aiheeseen liittyvät prosessit tulee käsitellä kokonaisuuksina sekä turvallisuuden hallintamenettelyt on suhteutettava riskienarviointiin perustuvaan suojattavaan tietoon ja kohdeyrityksen toimintaan.

Fyysisen tietoturvan osassa on oleellista varmistaa, että salassa pidettävä tieto on hyvin suojassa oikeudettomalta paljastumiselta. Tarkoitus on pyrkiä estämään tunkeutuminen salaa tai väkisin sekä ehkäistä, estää ja havaita mahdolliset luvattomat toimet ja mahdollistaa henkilöstön luokitus ja pääsy salattuihin tietoihin sen perusteella, mikä vaadittava tiedonsaantitarve on.

”Fyysisen turvallisuuden perusta on suunnittelussa. Tilojen ja rakennusten suunnittelussa ja käytössä on syytä ottaa huomioon seuraavat seikat:
1) Missä tiloissa suojattavia tietoja käsitellään ja minkä suojaustason tiedoista on kyse.
2) Missä ympäristössä ja rakennuksen osassa suojattavia tietoja käsitellään.
3) Rakennuksen tai tilan turvajärjestelyt ja rakenteet.
4) Salassa pidettävien tietojen suojaaminen tilassa (luominen, vastaanottaminen, käyttäminen, säilyttäminen ja hävittäminen).
5) Millä tietojenkäsittelyvälineillä ja järjestelmillä tietoja tilassa käsitellään.
6) Tietojen määrä; suojattavien tietojen kasautuminen saattaa edellyttää tiukempien turvallisuusvaatimusten soveltamista (esimerkiksi suuri määrä suojaustason IV tietoa saattaa muodostaa suojaustason III kokonaisuuden).
7) Tietoja käsitellään muuten kuin satunnaisesti sellaisissa tiloissa, joiden turvallisuus on käsiteltävän tiedon suojaustason huomioon ottaen riittävä.
8) Suunnittelu- ja ylläpito-organisaation kanssa on sovittu rakennuksen turvallisuusdokumentaation luottamuksellisuudesta.” (Puolustusministeriö, 2019)

Katakrin käyttö: Tätä auditointityökalua voidaan käyttää, kun arvioidaan esimerkiksi organisaation turvallisuusjärjestelyjen toteutumista yrityksen turvallisuusselvityksessä sekä viranomaisien tietojärjestelmien turvallisuuden arvioinneissa. Voidaan myös hyödyntää organisaatioiden, yhteisöjen ja viranomaisten muissa tuvallisuustöissä sekä

niiden kehityksessä. Katakrin käytöllä pyritään varmistumaan siitä, että kohdeyrityksellä on riittoisat turvallisuusjärjestelyt viranomaisten salassapidettävien tietojen oikeudettoman paljastumisen ehkäisyyn kaikissa mahdollisissa ympäristöissä, joissa tietoa käsitellään.

Hyödyntämällä turvallisuusjärjestelyjen suunnittelua sekä toteutusta, pyritään varmistumaan uhkiin nähden hyvästä turvallisuustasosta. Yrityksen on pystyttävä osoittamaan turvallisuusjärjestelyiden riittävyys luotettavalla tavalla. Riittävyyden arvioinnin on pohjauduttava järjestelmälliseen riskienarviointiin. Turvallisuusriskien hallinnalla pyritään toteuttamaan turvatoimien yhdistelmä, millä aikaansaadaan sopiva tasapaino käyttäjien kustannuksien, vaatimuksien sekä turvallisuuteen kohdistuvien jäännösriskien välillä. (Puolustusministeriö, 2019)

Katakria ei ole luotu käytettäväksi sellaisenaan julkisen hankinnan turvallisuusvaatimuksena. Julkisessa hankinnassa on tarkat turvallisuusvaatimukset määritettävä erikseen, huomioiden hankintaan liittyvät riskit sekä eritystarpeet. ”Yksittäiseen hankkeeseen voi sisältyä muitakin kuin Katakriin koottuja salassa pidettävän tiedon käsittelyä ja suojaamista koskevia vaatimuksia. Näiden vaatimusten toteutumista ei arvioida Katakrin avulla, vaan kohdeorganisaatio sitoutuu noudattamaan niitä sopimusperusteisesti.” (Puolustusministeriö, 2019)

2.3 ISO Standard

International Organization for Standardization (ISO) ja International Elechtrotechnical Commission (IEC) muodostavat yhdessä globaalin standardeihin erikoistuneen järjestelmän. Yhdessä nämä järjestöt ovat laatineet standardin ISO/IEC 27000:2016 ja se on hyväksytty eurooppalaiseksi tietoturvastandardiksi.

Standardien tehtävänä on yhteisten toimitapojen laatiminen, helpottaa viranomaisten, elinkeinoelämän ja kuluttajien arkipäiväistä elämää, sekä auttaa kaikentyyppisiä ja kokoisia yrityksiä tai organisaatioita, hyödyntämään tätä tietoturvallisuuden hallinnointijärjestelmää. Standardisoinnilla pyritään lisäämään tuotteiden yhteensopivuutta ja turvallisuutta, helpottamaan kotimaisia sekä kansainvälisiä kauppoja, sekä suojellaan ympäristöä ja kuluttajia. (ISO/IEC 27000:2017.)

Standardit julkaistaan asiakirjoina, joita kuka tahansa peruskäyttäjä voi hankkia käyttöönsä. Näiden standardien käyttö ja hyödyntäminen on maksutonta, mutta hankinta maksaa. Tällä keinolla rahoitetaan suuri osa SFS:n ja sen toimialayhteisöjen standardisointityöstä. (ISO/IEC 27000:2017.)

Tietoturvastandardeilla voi olla suuri merkitys organisaatioiden ja yritysten välisen liiketoiminnan ja kumppanuuden kannalta. Mikäli organisaatio noudattaa tiettyä standardia omassa toiminnassaan, on mahdollista, että potentiaaliselta yhteistyökumppanilta vaaditaan samanlaista laatutasoa tietoturvallisuuden osalta. (ISO/IEC 27000:2017.)

2.3.1 27001

Soveltamisala: Tämä kansainvälinen standardi määrittelee vaatimukset, jotka koskevat muodollisen tietoturvallisuuden hallintajärjestelmän luomisen, toteuttamisen, käyttämisen, seurannan, katselmoinnin, ylläpidon ja parantamisen ottaen huomioon yrityksen liiketoimintariskit. Tässä standardissa määritellään yksittäisen organisaation tai siihen kuuluvien osioiden yksilöllisten tarpeiden mukaan mukautettujen hallintakeinojen toteuttamista koskevat vaatimukset. (SFS-EN ISO/IEC 27000:2020:en)

Tarkoitus: Tässä standardissa ISO/IEC 27001 esitetään vaatimukset tietoturvallisuuden hallintajärjestelmän käyttöä sekä luomista varten. Tämän tietoturvallisuuden hallintajärjestelmän avulla yritys pystyy suojaamaan tieto-omaisuuttaan. Lisäksi esitellään joukko hallintakeinoja, joilla pystytään hallitsemaan sekä lieventämään tieto-omaisuuteen liittyvät riskit. Yritykset jotka käyttävät tätä tietoturvallisuuden hallintajärjestelmää, voivat hankkia järjestelmän vaatimustenmukaisuuden auditoinnin ja sertifioinnin. (SFS-EN ISO/IEC 27000:2020:en)

2.3.2 27002

ISO/IEC 27002 -standardi on tietoturvallisuuden hallintaa koskeva menettelyohje. Standardissa tietoa pidetään erittäin tärkeänä suojattavana kohteena muiden liiketoiminnallisten kohteiden tavoin, minkä vuoksi tietoa on suojattava asianmukaisesti. Standardin mukaan systemaattisessa ja toistuvassa turvallisuusriskien arvioinnissa on otettava huomioon erilaiset muutokset, kuten muutokset suojattavissa kohteissa. (SFS-EN ISO/IEC 27000:2020:en)

2.3.3 27003

ISO/IEC 27003 -standardissa keskitytään tietoturvallisuuden hallintajärjestelmän rakentamiseen. Standardin tarkoituksena on tuoda esille seikat, jotka auttavat järjestelmän suunnittelussa ja toimeenpanemisessa. Suojattavien kohteiden tunnistamis- ja luokittelutarve otetaan standardissa esille osana tarvittavan vaatimustason määrittelyä. Standardin tehtäväohjeistuksessa neuvotaan keräämään seuraavaa tietoa; prosessien

yksilöidyt nimet, prosessien kuvaukset, prosessien kriittisyys organisaatiolle, prosessien omistajat, input- ja output -liittymäprosessit, prosesseja tukevat tietotojärjestelmät sekä tietoaineistot turvallisuustarpeiden mukaisesti luokiteltuina. Nämä tiedot ovat syötteenä tietoturvallisuuden rakentamisen seuraavalle vaiheelle, jossa arvioidaan riskit. (SFS-EN ISO/IEC 27000:2020:en)

2.3.4 27005

ISO/IEC 27005 -standardi on tietoturvallisuuden hallintajärjestelmäkontekstiin sovellettu riskienhallintastandardi. Se on luonteeltaan ohjaava ja käsittelee riskienhallinnassa huomioon otettavia näkökohtia, ottamatta kantaa varsinaisiin menetelmiin ja työkaluihin. Standardin mukaan kaikki asiaankuuluvat suojattavat kohteet on otettava huomioon riskien arvioinnissa. Standardissa suojattava kohde määritellään kaikeksi, jolla on arvoa ja mikä tämän johdosta vaatii suojausta. Lisäksi standardissa muistutetaan, että kohteiden tunnistaminen on tehtävä soveltuvalla yksityiskohtaisuuden tasolla riskien arvioimiseksi. Edelleen pidetään tärkeänä tunnistaa jokaiselle kohteelle omistaja vastuun ja tilivelvollisuuden toteamiseksi. Lisäksi omistajalla on usein paras näkemys kohteen arvosta ja vaikutuksista. (SFS-EN ISO/IEC 27000:2020:en)

3 TIETOTURVALLISUUDENHALLINTAJÄRJESTELMÄ

3.1 Yleiskuvaus

Tietoturvallisuuden hallintajärjestelmä eli ISMS koostuu toimintaperiaatteista, menettelytavoista, ohjeista ja niihin liittyvistä toiminnoista sekä resursseista, joita yritys käsittelee hallitusti suojatakseen tieto-omaisuuttaan. Tietoturvallisuuden hallintajärjestelmä on järjestelmällinen lähestymistapa yrityksen tietoturvan toteutukseen, laatimiseen, käyttöön, seurantaan, katselmointiin sekä ylläpitoon ja parannukseen liiketoimintatavoitteiden saavuttamisen vuoksi. Hallintajärjestelmä perustuukin riskien arviointiin ja yrityksen riskien hyväksyntätasoihin, jotka on suunniteltu nimenomaan tehokkaaseen riskien käsittelyyn ja hallintaan. Tieto-omaisuuden suojausvaatimuksia

analysoimalla ja suojauksen varmistamiseen soveltuvat hallintakeinot suorittamalla voidaan myös myötävaikuttaa tietoturvallisuuden hallintajärjestelmän onnistuneeseen toteutukseen. (Valtiovarainministeriö 2009; ISO/IEC 27000:2017.)

Myös seuraavat luokitellut perusperiaatteet vaikuttavat hallintajärjestelmän onnistuneeseen toteutukseen:

- tetoisuus tietoturvallisuuden tarpeesta
- tietoturvallisuuden vastuiden määrittely
- johdon sitoutuminen sekä sidosryhmien etujen huomiointi
- yhteiskunnallisten arvojen tukeminen
- riskien arviointi, jossa on määritetty asianmukaiset sekä hyväksyttävien riskitasojen saavuttamiseen vaaditut hallintakeinot
- turvallisuuden sisällytys tietojärjestelmien sekä -verkkojen olennaiseksi osaksi
- mahdollisten tietoturvahäiriöiden jatkuva ehkäisy ja havainnointi
- tietoturvallisuuden hallinnan kattavan toimintamallin varmistus
- tietoturvallisuuden jatkuva uudelleenarviointi sekä tarvittujen muutoksien tekeminen.
  (ISO/IEC 27000:2017.)

3.2 Miksi hallintajärjestelmä on tärkeä?

Koska yrityksen tieto-omaisuuteen liittyviä riskejä on käsiteltävä, tietoturvallisuuden toteuttaminen vaatii riskienhallintaa. Tämä liittyy erilaisiin riskeihin, jotka aiheutuvat niin fyysisistä kuin inhimillisistä ja teknologiaan liittyvistä uhkista ja liittyvät kaikenlaiseen tietoon, jota yrityksessä on tai yrityksessä käytetään. (ISO/IEC 27000:2017.)

Enimmäkseen organisaation tietoturvallisuuden hallintajärjestelmän suunnitteluun ja toteutukseen vaikuttavat yrityksen asetetut tavoitteet, tarpeet, turvallisuusvaatimukset,

käytettävät liiketoimintaprosessit sekä vielä yrityksen suuruus ja rakenne. Hallintajärjestelmän suunnitteluun sekä käytön on heijastettava kaikkien organisaation sidosryhmien – kuten toimittajien, asiakkaiden, liikekumppanien, osakkaiden ja muiden oleellisten ulkopuolisten tahojen etuja sekä tietoturvavaatimuksia. (ISO/IEC 27000:2017.)

Nykyisessä verkottuneessa maailmassa tieto ja siihen liittyvät prosessit, järjestelmät ja verkot muodostavat yhdessä kriittisen suojatun liiketoimintaomaisuuden. Yritykset sekä niiden tietojärjestelmät ja verkot joutuvat alttiiksi niihin kohdistuvien uhkatekijöiden vuoksi. Mahdollisia uhkia voi olla mm. tietokoneavusteinen petos, yritysvakoilu, sabotaasi, yleinen vahingonteko, tulipalo tai vesivahinko. Tietojärjestelmiin ja verkkoihin eniten vahinkoa aiheuttaa kuitenkin haittaohjelmat, tietomurrot ja palvelunestohyökkäykset, koska nämäkin ovat yleistymässä ja ne ovat entistä monitahoisempia ja kunnianhimoisempia. (ISO/IEC 27000:2017.)

Hallintajärjestelmä on myös tärkeä tekijä julkisen sekä yksityisen sektoreiden liiketoiminnassa. Hallintajärjestelmää käytetään kaikilla toimialoilla apukeinona, jonka tarkoitus on tukea sähköistä liiketoimintaa. Se on siis olennainen osa riskienhallinnan toimintoja. Nykyään nähtävä julkisten ja yksityisten verkkojen yhdistyminen ja yhteisen tieto-omaisuuden käyttö tekevät tiedon käyttöoikeuksien ja tiedon käsittelyn valvomisesta hankalaa. Tämän lisäksi tärkeää suojattavaa omaisuutta sisältävien kannettavien tallennusvälineiden leviäminen voi vaikuttaa negatiivisesti perinteisten hallintakeinojen vaikuttavuuteen. Kun yritys käyttöönottaa tämän tietoturvallisuuden hallintajärjestelmästandardisarjan, se osoittaa jo siinä liikekumppaneilleen ja muille sidosryhmille, että heillä on kyky noudattaa johdonmukaisia ja molempien osapuolien tuntemia tietoturvaperiaatteita. (ISO/IEC 27000:2017.)

Vaikka tietoturvallisuus onkin tärkeimpiä osia yrityksissä, ei sitä aina oteta riittävästi huomioon tietojärjestelmien kehityksessä ja suunnittelussa. Joskus se vain mielletään tekniseksi ratkaisuksi. Tekniset keinot kuitenkin tarjoavat vain rajallisia mahdollisuuksia optimaalisen tietoturvallisuuden saavuttamiseen, eivätkä ne aina ole kovin vaikuttavia, ellei niitä tueta tietoturvallisuuden hallintajärjestelmän puitteissa tapahtuvalla asianmukaisella hallinnoinnilla ja menettelyillä. Turvallisuusasioiden sisällytys jo en-

nestään toimivaan järjestelmään voi käydä hankalaksi ja kalliiksi. Hallintajärjestelmässä tunnistetaan käytössä olevat hallintakeinot, ja järjestelmä edellyttääkin huolellisen suunnittelun sekä yksityiskohtien huomioon ottamista. Esimerkkinä vaikka pääsynhallintamekanismit, jotka voivat olla teknisiä, fyysisiä, hallinnollisia tai näiden tapojen yhdistelmä, tarjoavat keinon varmistaa, että tieto-omaisuuteen pääsevät vain ne, joilla on valtuudet ja että pääsyä on rajoitettu liiketoiminta- sekä turvallisuusvaatimusten verukkeella. (ISO/IEC 27000:2017.)

Hallintajärjestelmän onnistunut omaksuminen on hyvin tärkeää, sillä suojataan tieto-omaisuutta ja se antaa organisaatiolle mahdollisuudet

- saavuttaa vielä parempi varmuus siitä, että tieto-omaisuus on suojattu tarpeiden mukaisesti uhkilta
- ylläpitää organisoituja ja kattavia puitteita, joiden avulla voidaan tunnistaa ja arvioida mahdolliset tietoturvariskit, valita ja suorittaa soveltuvat hallintakeinot sekä mitata ja parantaa niiden vaikuttavuutta
- jatkuva hallintaympäristön parantaminen
- täyttää pyydetyllä tavalla lakisääteiset ja viranomaisten vaatimukset.

(ISO/IEC 27000:2017)

3.3 Tietoturvallinen johtaminen

Mitä on tietoturvallinen johtaminen? Se perustuu yleensä määrätietoiseen sekä organisoituun toimintaan. Yrityksen johdosta katsottuna näkökulma on, että tietoturvallisuus on hierarkkista politiikan ja toimintaohjeiden laatimista sekä tavoitteiden asettamista ja jatkuvaa valvontaa ja toiminnan kehitystä. Sitten taas toisaalta, tietoturvallisuuden johtaminen on sitä aivan samaa johtamista kuin muidenkin toimintojen johtaminen. Eli on asetettu tavoitteet, vastuut määritetty ja osoitetaan riittävät resurssit. Loppujen lopuksi tulosta pitää verrata asetettuihin tavoitteisiin ja mietitään jatkotoimenpiteitä, joita mahdolliset poikkeamat voivat aiheuttaa. (Laaksonen 2006.)

Yrityksen tietoturvaohjelman suuruus riippuu mahdollisista uhkaavista tekijöistä sekä liiketoiminnan ja toimintaympäristön vaatimuksista, joita yrityksen johdon on jatkuvasti mietittävä laatiessaan ja katselmoidessaan tietoturvapolitiikkaa sekä sen toiminnan tavoitteita. (Laaksonen 2006.)

Tietoturvallisuuden johtamisprosessin yksiä ensimmäisiä toimenpiteitä on yrityksen liiketoiminnallisten ja tietoturvatavoitteiden yhdistäminen niin, että tietoturvallisuudelle asetettavat tavoitteet on määritelty olevan linjassa muiden tavoitteiden kanssa. (Laaksonen 2006.)

Liiketoiminnan ja tietoturvallisuuden tavoitteiden harmonisointi on kannattavaa, koska tämä vaikuttaa resurssien jakamiseen, toiminnan mittaamiseen ja seurantaan. Resursointia on mahdollista tehostaa esimerkiksi laajentamalla laatuorganisaation tehtäväkenttää sijoittumaan osittain tietoturva-asioihin sekä yhdistämällä muihin prosesseihin tietoturvallisuuden toteutumisen puolesta merkityksellisiä elementtejä ja kontrolleja. (Laaksonen 2006.)

Asioita joita kannattaa pohtia on, miten laaja johtamisjärjestelmä tietoturvallisuuden hallinnointiin on rakennettava. Ovat seuraavat.

- Millaista tietoa yritys käsittelee? Onko jonkun mahdollista hyötyä esimerkiksi taloudellisesti näistä tiedoista? Kuinka paljon tiedon tuottaminen on vaatinut panostusta taloudellisesti tai muilla keinoilla? Voidaanko tieto tuottaa nopeasti uudelleen? Ja onko siitä enää silloin hyötyä?
- Mitkä ovat mahdolliset tahot, jotka ovat kiinnostuneet yrityksen tiedoista? Miten ulkopuoliset pyrkivät tietoon käsiksi?
- Millä keinoin tieto voidaan viedä yrityksestä ulos? Millaisia tapoja tiedon havittelijat voivat käyttää?
- Miten laaja ja monimuotoinen yrityksen toiminta on ja miten monimutkainen nykyään ajossa oleva johtamisjärjestelmä on? Voidaanko tietoturvan johtaminen yhdistää nykyiseen johtamisjärjestelmään?
- Minkälainen on yrityksen ulkoinen vaatimusympäristö ja miten se mahdollisesti kehittyy tulevaisuudessa? Miten valmistaudutaan ulkopuolelta tuleviin tietoturvavaatimuksiin?

- Onko yrityksellä käsitys sitä velvoittavista yleisistä lainsäädännöistä tai erityisistä säännöstelyistä, jotka koskevat liiketoiminnan tietoturvavelvoitteita tai oikeuksia? (Laaksonen 2006.)

Koska yrityksen omistuksessa tai hallinnassa oleva tieto voi olla monella tapaa hyvin kiinnostavaa ulkopuolisille tahoille, niin mahdolliset syyt tiedon hankkimiseen tai tuhoamiseen voivat olla henkilökohtaisia, taloudellisia tai jopa poliittisia. Esimerkkinä henkilökohtaisiin syihin voisi olla yrityksen oman henkilöstön motiivit. Tilanne, jossa työntekijät ovat kokeneet, että heitä on kohdeltu väärin, voi laukaista henkilökohtaisen tarpeen yrityksen tietoon kohdistuvalle vahingonteolle. (Laaksonen 2006.)

Yleensä taloudelliset syyt ovat enemmänkin rikollisten motiiveja. Rikollisia kiinnostaa enemmän esimerkiksi yrityksen hallussa olevat henkilötiedot, jotka ovat hyvää kauppatavaraa vaikka roskapostittajille tai luottokorttiväärentäjille. Poliittiset syyt voivat olla esimerkiksi joidenkin innovaatioiden tai keksintöjen tutkimus- ja kehitystietojen varastamisessa.

Edellä mainitut tilanteet saattavat aiheuttaa uhkatilanteen tiedon luottamuksellisuuden, saatavuuden ja eheyden kannalta. Yllätykselliset tilanteet, joissa yrityksen tieto voi olla uhattuna, aiheuttavat häiriötä tai estävät yrityksen normaalia toimintaa. Tietoturvaan vaikuttavat uhat johtuvat yleensä monenlaisista eri syistä. Mahdollisesti ihminen voi aiheuttaa tahallaan häiriötä yrityksen tietojenkäsittelylle. Tietojärjestelmissä voi olla puutteita, ne voivat toimia väärin ja olla puutteellisia. Tekniset suojauskeinot eivät aina ole riittäviä tai voivat muuten vain pettää. Mahdolliset uhat on selvitettävä huolella, jotta syy voidaan korjauttaa tai ennaltaehkäistä tulevaisuuden häiriötekijät. Tähän liittyen suuressa roolissa on yrityksen jatkuvuussuunnittelu, joka on vaatinut niin normaaliajan kuin toipumissuunnitelman kautta vahvaa kriisiajan johtamista. (Laaksonen 2006.)

3.4 Fyysinen ympäristö

Fyysinen turvallisuus takaa yritykselle häiriöttömän ja turvallisen ympäristön toimia. Toimitilojen suojaus luo pohjan kaikille muille suojaustoimille, mitä tietoturvallisuuden ylläpitoon käytetään. Jos ympäristö ei ole turvallinen, ei tiedon luotettavuutta voida aukottomasti varmentaa. Yleensä kovaa suojaustasoa vaativat kohteet ovat organisaation vahvuusalueisiin liittyvät tilat, kuten tuotekehitys, atk sekä hallinnolliset tilat. Fyysisen turvallisuuden suunnitelman piiriin pitäisi kuulua aina tilat, joissa käsitellään merkityksellistä tietoa. Toimintaympäristö olisi hyvä arvioida ajoittain riskikartoitusten yhteydessä. (Laaksonen 2006.)

3.5 Tietoturvan toteutus – tietoturvaohjelma

“Tietoturvaohjelmalla tarkoitetaan niitä toimenpiteitä, joilla määrätään noudatettavista tietoturvallisuuteen liittyvistä periaatteista ja toimintalinjoista yleensä sekä tietoturvallisuuden organisoinnista.” (Laaksonen 2006.)

Tämä on kokonaisuus, joka koostuu turvallisuustoiminnan järjestelystä, henkilöstön tehtävien, vastuiden sekä ohjeistuksen, koulutuksesta ja valvonnasta. Yleensä näihin asioihin otetaan kantaa organisaation tietoturvapolitiikassa. Tietoturvaohjelman tavoite on suojata tiedon luottamuksellisuus, käytettävyys ja eheys. On myös otettava huomioon viestinnän luottamuksellisuuden, yksityisyydensuojan ja sananvapauden asettamat vaatimukset. Siksi toimenpiteiden on oltava huolella suunniteltu, ettei yritys joudu vastuuseen mahdollisesti tietoturvatoimenpiteiden seurauksena. Tavoitteet kannattaa purkaa osiin, lyhyelle ja pitkälle aikavälille sekä yhdistää yrityksen muihin tavoitteisiin. Ohjelman ei tarvitse olla laajuudeltaan suuri, mutta sen on sisällettävä keskeisimmät suuntaviivat ja linjaukset yrityksen tietoturvaan liittyville toimintatavoille. (Laaksonen 2006.)

3.6 Tietoturvan hallinnan rooli ja vastuu

Yksi tämän ohjelman avaintekijöistä on tietoturvallisuuden hallinnointiin liittyvien roolien ja vastuiden määrittelyt. Yrityksen on määritettävä hyvin tarkkaan, kehen tämä ohjelma vaikuttaa ja erityisesti ketkä siitä ovat vastuussa. Tietoturvaorganisaation vastuuhenkilöiden lisäksi on pohdittava koko henkilökunnan ja ulkopuolisten sidosryhmien roolia tietoturvallisuuden hallinnoinnin kannalta. (Laaksonen 2006.)

3.7 Mitä on tietohallinto?

Kun tietoturvaohjelmalla otetaan kantaa vastuiden jakamiseen ja toimenkuviin. Tietohallinnon tehtävä on enemmänkin keskittyä siihen, että tietojärjestelmien käytettävyys on turvattu ja liiketoimintaa säätelevät järjestelmät ja ylläpito ovat kunnossa. Näiden järjestelmien käyttäjät yleensä kuuluvat tietohallintoon. Palveluiden saatavuuteen yleensä liittyvät usein myös laatukysymykset, kuten jatkuvuudesta varmistuminen sekä sovelluksien testaaminen. Tietohallinnon osastolle jääkin tietoturvallisuuden tekninen toteutus ja sen ylläpidosta huolehtiminen, mutta hallinto ei päätä järjestelmien ja tiedon vaatimista suojauksen tasoista, koska tämä kuuluu enemmän tiedon, prosessien sekä järjestelmien omistajille. Nämä käyttäjät eivät välttämättä kuulu tietohallintoon, paitsi ehkä joidenkin yleiskäyttöisten sovelluksien kautta. Tietohallinto kerää myös lokeja erilaisista sovelluksista, aktiivilaitteista ja muista mahdollisista tietojärjestelmän osista. Lokien analysointi ei välttämättä ole tietohallinnon vastuulla, tai ainakaan sen ei pitäisi olla järjestelmän pääkäyttäjienkään vastuulla. Näillä lokitiedoilla voidaan suorittaa valvontaa ja raportoida yrityksen tilasta liikkeenjohdolle, huomioimalla kuitenkin tunnistamistietojen käsittelyyn liittyvät määräykset, jos joudutaan käsittelemään tunnistamistietoja. (Laaksonen 2006; Tupper 2011.)

Mitkä ovat tietohallinon tehtävät?

- On ylläpidettävä ajantasaiset tiedot liittyen tietoturvallisuuden tekniseen suojaukseen ja keskusteltava asiasta tietoturvasta vastaavan tahon, järjestelmän, tiedon sekä prosessien omistajien kanssa.
- Huolehditaan loogisien pääsykontrollien asianmukaisuudesta ja että ne ovat ajan tasalla yhdessä pääkäyttäjien kanssa.

- Noudatetaan käyttöoikeusmenettelytapoja.
- Varmistetaan tietojärjestelmä
- Turvataan tiedonsiirto.
- Säilytetään ja kerätään lokitiedostot.
- Testataan muutokset ennen käyttöönottoa.
  (Laaksonen 2006; Tupper 2011.)

3.8 Ulkoisista sidosryhmistä

Yrityksen johto on vastuussa ulkoisten sidosryhmien käytöstä. Jos palveluja ostetaan ulkopuolelta, on johdon osattava arvioida näiden ulkopuolisten tahojen toimijoiden pätevyys.” On myös osattava arvioida ostettavaan palveluun tai toimintaan liittyvät tietoturvariskit yhdessä palvelusta vastaavien yrityksen omien asiantuntijoiden kanssa. ” (Laaksonen 2006.)

4 TIETOTURVA JA SEN OSA-ALUEET

4.1 Tieto

Tieto on juuri se suojattava kohde, joka muiden tärkeiden liiketoiminnallisten kohteiden tavoin on hyvin tärkeä yrityksen liiketoiminnalle, siksi sitä on siis suojattava asianmukaisesti. Tietoahan voidaan säilöä monissa eri muodoissa, kuten esim. digitaalisessa muodossa (sähköisiin ja optisiin tietovälineisiin tallennetut tiedostot), fyysisessä muodossa (paperilla) sekä työntekijöiden tiedoista koostuvana aineettomana tietona.

Tietoa voidaan myös liikuttaa eri tavoin, sähköisellä tai suullisella viestinnällä tai lähettien välityksellä. Tiedon muodosta ja välityskeinoista riippumatta, on ylläpidettävä aina asianmukainen tiedon suojaus. (ISO/IEC 27000:2017)

4.2 Tietoturva

Tietoturva itsessään ei ole itseisarvo, vaan se on jotain, jolla on tarkoitus. Se tarkoitus yritysmaailmassa on liiketoiminnan tarpeiden tukeminen sekä ulkoisten että sisäisten vaatimusten täyttäminen. Yleisesti tietoturvallisuudella tarkoitetaan tiedon perusominaisuuksien eli eheyden, luottamuksellisuuden ja käytettävyyden turvaamista.
Kuitenkin tietoturva ja tietosuoja ovat kaksi eri asiaa, vaikka niillä onkin jotain yhteisiä piirteitä. Niin niiden erottaminen käytännössä ei ole aina helppoa. Tietosuojalla erityisesti suojataan ihmisen yksityisyyttä ja itsemääräämisoikeutta. (Laaksonen 2006; Opitietosuojaa.fi 2014.)

Tietoturva taasen tarjoaa erilaiset metodit tai toimintamallit tietosuojan ylläpitoon; sillä rakennetaan ikään kuin suojamuuri salassa pidettävän tiedon ympärille. Jos tämä muuri on heikko, on hyvin vaikeaa suojata tietoa, jota sillä on tarkoitus suojata. Tietoturvan kannalta on siis hyvin olennaista tietää myös tietosuojaan liittyvät lainsäädännölliset perusteet. Tietoturvallisuus koostuu pienistä teoista osana arkipäiväistä toimintaa. Hyvä tietoturvallisuus on siis osa organisaatiokulttuuria, jossa kaikki ymmärtävät tietoturvallisuuden merkittävyyden ja tekevät töitä sen saavuttamiseksi sekä ylläpitämiseksi. Tietoturvallisuus koostuu teknisistä ja hallinnollisista toimista, jotka on suunniteltava huolellisesti.
Riippumatta siitä, miten tietoturva on määritelty, hyvän tietoturvallisuustason saavuttaminen ja ylläpito vaativat organisaatiolta määrätietoista ja -muotoista johtamista sekä toimintaa. (Laaksonen 2006; Opitietosuojaa.fi 2014.)

4.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus on organisaation henkilöistä riippuvaa riskienhallintaa. Turvallisuuden perustana on sitoutunut ja pätevä henkilökunta, jolle tietoturvatehtävät ja vastuut on kuvattu selkeästi annetuissa toimenkuvissa. Lisäksi vaaditaan tietyllä tasolla määritellyt henkilöstöhallinnon prosessit ja muut prosessit, joissa on kuvattu työtehtävät niin hyvin ja tarkasti, että avainhenkilöriskien syntymiseltä voidaan välttyä. (Valtiovarainministeriö 2009.)

Tärkeitä asioita ovat työhönottoon, toimenkuvien vaadittuihin muutoksiin ja palvelussuhteen päättymiseen liittyvät prosessit ja niistä pitää tarpeen mukaan olla jokaisella osastolla käytössä sovittu toimintamalli. Riippuen tehtäviten vaativuudesta tai luottamuksellisuudesta, on selvitettävä rekrytoitavan henkilön taustat, pätevyys sekä osaaminen ennen mahdollista työhönottoa. (Valtiovarainministeriö 2009.)

”Avainhenkilöriskien hallinnassa tunnistetaan toiminnan kannalta avainhenkilöt, sekä varmistetaan heidän käytettävyytensä organisaation palveluksessa eri tilanteissa.” (Valtiovarainministeriö 2009.)
Suunnitelussa on varauduttava henkilöstön lomiin, poissaoloihin, työkiertoon ja väliaikaisiin järjestelyihin tarpeellisen hyvin sekä on valmennettava henkilöstö poikkeustilanteisiin. Vaaralliset työyhdistelmät pitää havaita ja hävittää, jotta yrityksen toimintojen suojaksi rakennettuja menetelmiä ei pysty havaitsematta ohittamaan. (Valtiovarainministeriö 2009.)

4.4 Fyysinen turvallisuus

Tarkoituksena on turvata yrityksen jatkuva toiminta ilman häiriöitä kaikissa olosuhteissa niiden erityistarpeet ja riskit huomioon ottaen. Jokainen yritys vastaa itse omasta fyysisestä suojastaan. (Valtiovarainministeriö 2009.)

Tämä tietoturvallisuuden osa-alue pitää sisällään mm. kulunvalvonnan, kameravalvonnan, muun teknisen valvonnan ja vartioinnin sekä palo-, vesi-, sähkö-, ilmastointi-

ja murtovahinkojen torjunnan. Vähittäisvaatimukset tilaturvallisuutta kasvattaville toimille ja järjestelmille määritetään turvallisuustarpeiden perusteella, jotka voivat kohdistua alueeseen, rakennuksiin, tilaryhmiin tai tilaan. Uudempien rakennuksien tai tilojen peruskorjausten yhteydessä toimitilojen suojaus on toteutettu tai sitä parannetaan turvallisuusluokituksien mukaan töiden ohessa. (Valtiovarainministeriö 2009.)

Usein silti toimitilojen hallinta sekä turvallisuusjärjestelyjen toteutus kuuluvat kiinteistöhallinnon tai rakennuksen omistajan tehtäviin. Parhaiten toiminnot ja niiden käyttämät tietotekniikan turvallisuusperiaatteet tuntee kuitenkin käyttäjäorganisaation johto, joka on vastuussa turvallisuusratkaisuihin liittyvistä päätöksistä. On myös huomioitava toimitilaturvallisuus ja sen kehittämistarpeet vuosisuunnitelmaa laatiessa. (Valtiovarainministeriö 2009.)

4.5 Käyttöturvallisuus

“Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat olosuhteet,” Tämä toteutuu huolehtimalla seuraavista asioista: toimivuuden valvonta, käyttöoikeuksien hallinta, käytön ja lokien valvonta, ohjelmistotukeen, ylläpito-, kehitys- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. Käyttöturvallisuutta on myös kaikkien tietojärjestelmien suojaaminen mahdollisilta haittaohjelmilta kuten esimerkiksi sähköpostiviruksilta tai vaikkapa verkkomadoilta. (Valtiovarainministeriö, 2009)

4.6 Ohjelmistoturvallisuus

Käyttöjärjestelmiin ja eri ohjelmistoihin suuntautuvat toimet, kuten ohjelmistojen tunnistamis, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

4.7 Tietoliikenneturvallisuus

Tietoverkon turvallisuus kannattaa ottaa huomioon jo suunnittelu vaiheessa. Myöhemmin suoritetut turvallisuuspaikkaukset eivät usein kykene korjaamaan jo ennen verkon rakentamista tehtyjä mahdollisia virheitä.
Tietoliikenneturvallisuuteen tähtäävät keinot ovat esim. laitteistojen ja siirtoyhteyksien ylläpito ja niihin kuuluva kokoonpanojen hallinta, verkkojen hallinta, pääsynvalvonta, tietoliikenteen käytön valvominen ja tarkkailu, mahdollisten ongelmien kirjaaminen ja selvitys, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaaminen sekä hyväksyntä. Ratkaisut on suunniteltava niin, että ne ovat saatavilla myös poikkeusolosuhteissa. (Valtiovarainministeriö 2009.)

5 TIETOTURVAPOLITIIKKA

Politiikkaa tulisi katselmoida ajoittain ja pohtia, onko se ajan tasalla. Jos muutokselle on tarvetta, uusi tietoturvapolitiikka määritetään johdon toimesta. ”Riskienhallinta ja tietoturvallisuuteen kuuluvat linjaukset määritetään yleensä ylimmän johdon puolelta. Liikkeenjohto laatii karkean tason tietoturvalinjaukset ja nämä esitetään yleensä tietoturvapolitiikan muodossa.” Politiikkaa, joka on perusta koko yrityksen tietoturvaohjeistukselle sekä koulutukselle, hyödyntämällä liikkeenjohto pystyy osoittamaan tukensa ja sitoutumisensa yrityksen turvallisuuden kehitykseen. Tällä luodaan selkäranka yrityksen tietoturvallisuuden formaaliselle kehitykselle. (Laaksonen 2006; Cassetto 2019.)

Mihin tietoturvapolitiikka ottaa kantaa?

- tietoturvallisuuden tavoitteet ja niihin liittyvät toimet

    - Tuodaan esiin johdon näkemys, miten tietoturvallisuus vaikuttaa yrityksen toiminnallisuuteen ja miten tietoturva-asioihin pitää suhtautua.
- tietoturvallisuuden roolit ja vastuut
    - Politiikka määrittelee tahot, jotka ovat vastuussa asetettujen tavoitteiden saavuttamisesta. Voidaan ottaa myös kantaa käyttöoikeuksien valvomiseen. On myös tärkeä määritellä linjaus, kuinka tietoturvallisuus huomioidaan sopimuksissa sekä muissa juridisissa kysymyksissä.
- tietoturvallisuuskoulutus
    - Tälle aiheelle on politiikassa määriteltävä omat vaatimuksensa. Koulutuksella henkilö pystyy ymmärtämään ja sisäistämään politiikan tavoitteet sekä toimenpiteet, joiden avulla nämä tavoitteet on saavutettu. Jos ei ole koulutusta, tietoturvallisuus saattaa jäädä toteutumatta tai toteutuu vain tekniseltä osin tietoturvallisuuden politiikan mukaan.
- tietojenkäsittelyn suojaus
    - Toimintojen suojaukseen on lukuisia keinoja, eikä tietoturvapolitiikan tarkoitus ole käytössä olevien keinojen listaus, vaan määritetään suuntaviivat, joita suojauksessa on noudatettu. Näitä voivat olla esimerkiksi päätös tietosisällön luokittelusta sekä laitteiden ja sovelluksien suojaus mahdollisilta viruksilta.
- yleiset linjaukset, liiketoimintojen jatkuvuus- ja toipumissuunnittelun toteutus
    - Seuraukset tietoturvapolitiikan laiminlyönnistä. On myös otettava huomioon kurinpitotoimenpiteet. Ohjeiden laiminlyönnin seurauksista tulee tiedottaa myös käyttäjille, että ymmärretään tekojen seuraukset.

(Laaksonen 2006; Cassetto 2019.)

Tietoturvapolitiikalle ei ole olemassa mitään yhtä mallia, eikä netistä kopioitu ole välttämättä sopiva toisen yhteisön liiketoimintaan. Yrityksen johto keskustelee edellä mainituista asioista ja laatii kirjallisen dokumentin, joka otetaan käyttöön yrityksen tietoturvapolitiikkana. (Laaksonen 2006.)

6 JATKUVUUS JA TOIPUMISSUUNNITELMAT

Jatkuvuussuunnitelman tarkoitus on turvata organisaation merkittävien liiketoimintaprosessien jatkuva toiminta normaalitilanteissa, häiriötilanteissa ja näiden jälkeisissä tilanteissa. Jatkuvuussuunnitelma on määritelty olevaksi suunnitelma siitä, miten tietojenkäsittely ja tiedonsiirto on turvattu niin, että ne voivat toimia erilaisten häiriöidenkin aikana ja niiden jälkeenkin. (Laaksonen 2006.)

Liiketoiminnan toipumissuunnitelman tarkoituksella mahdollistetaan organisaation arvokkaiden liiketoimintaprosessien nopea jatkuminen erilaisien häiriöiden aiheuttamien vahinkojen jälkeen. Suunnitelmassa kannattaa huomioida yrityksen sijainti, ympäristö, toiminnan luonne ja laajuus. On myös mietittävä tiedon siirtämistä, muokkaamista ja hävittämistä. Tulee myös laatia toimintaohjeet, kouluttaa henkilöstö sekä suunnitella toimivia organisaatiota erilaisiin tilanteisiin ja olosuhteisiin. (Laaksonen 2006.)

7 TIETOJÄRJESTELMÄN TURVALLISUUS

Tietojärjestelmän turvallisuudella tarkoitetaan toimenpiteitä, jotka on luotu järjestelmään parantamaan tietoturvaansa. On pyrittävä siihen, että tietojärjestelmät itsessään ovat jo niin turvallisia, ettei niiden tietoturvallisuus vaarannu, vaikka tietoverkon omat palomuurit eivät olisikaan toiminnassa. Jos kaikkia periaatteita noudatetaan tietoverkkojen ja järjestelmien rakennuksessa, saavutetaan tietojen suojaukseen kerroksellisuutta. Kerroksellisen suojauksen pystyttäminen tulee usein myös halvemmaksi kuin yhden tehokkaan suojauksen toteutus. Kahdella tai useammalla hieman teholtaan pienemmällä suojausmenetelmillä, saavutetaan helposti yhtä hyvä suojaustaso. (Laaksonen 2006.)

8 RISKIENHALLINTA

Yleisesti

Riskienhallinnalla pyritään mahdollistamaan organisaation menestyminen, toimintojen jatkuvuuden takaaminen ja tavoitteiden saavuttaminen. Riskienhallinta on hyvin järjestelmällistä ja tavoitteellista toimintaa, joka tukee yrityksen johtamista ja kehittymistä. Useimmiten riski sanaa käytetään uhka-sanan synonyyminä, mutta pohjimmiltaan se voi myös olla positiivinen asia ja mahdollistaa saada hyötyä jostain toimenpiteestä. Riskienhallinnan tarkoitus on havaita yrityksen menestymiseen ja tuloksellisuuteen sekä henkilöstön hyvinvointiin vaikuttavia tekijöitä.

”Riski tarkoittaa epävarmuuden vaikutusta tavoitteisiin, poikkeamaa odotetusta. Vaikutus voi olla myönteinen tai kielteinen odotettuun verrattuna.”

8.1 Riskienhallintaprosessi

Toimiva ja onnistunut riskienhallinta on aktiivista ja se reagoi tuleviin muutoksiin. Riskienhallintaa on pyrittävä toteuttamaan säännöllisesti, esim. merkittävien muutoksien yhteydessä ja sitä pitää kehittää määrätietoisesti sekä tarkoituksenmukaisesti. Riskienhallinnan on oltava osa jokaisen yksilön arkipäiväistä työtä.

Toimintaympäristön määrittelyvaiheessa suoritetaan riskien arvioinnin kannalta keskeisimmät rajaukset siihen, mitä sisällytetään riskien arviointiin ja mitkä asiat jäävät sen ulkopuolelle. Välttämätöntä on myös merkittävien riippuvuuksien tunnistaminen. Määrittelyn yhteydessä riskien arvioinnin kohde tarkentuu. Riskienhallinnan kehityksellä parannetaan myös yrityksen sietokykyä selvitä mahdollisista häiriötilanteista.

Riskien arviointiprosessi on yrityksen määrittelemä ja johdon hyväksymä menetelmä, jota riskien arvioinnissa käytetään. Prosessi sisältää seuraavat vaiheet. Tunnistaminen. Analyysi. Merkityksen arviointi.

Riskien tunnistamisella tavoitellaan sitä, että voidaan havaita ja kuvata kaikki merkittävimmät riskit ja mahdollisuudet, riskien lähteet, vaikutusalueet, tapahtumat, sekä mukaan lukien olosuhteiden muutokset ja niistä aiheutuvien syiden mahdolliset seuraukset. Henkilöillä jotka osallistuvat tunnistamiseen, on oltava tarkasteltavaan toimintoon riittävä asiantuntemus. Tunnistamisessa pitää ottaa huomioon yritykseen vaikuttavat tekijät riippumatta siitä, että onko riskien mahdollinen lähde yrityksen omassa hallinnassa. (Valtionvarainministeriö, 2017)

Riskianalyysin avulla voidaan luoda perusta päätöksille siitä, miten ja mitä riskejä nyt käsitellään. Analyysin arvioit todennäköisyydestä ja vaikutuksista perustuvat yleensä osallistujien subjektiivisiin käsityksiin, jolloin yhteisen käsityksen muodostaminen riskin tasosta voi tulla hankalaksi. Tämän takia on tärkeä kirjata ylös mahdolliset mielipiteisiin tai muihin epävarmuustekijöihin perustuvat seikat tarpeeksi selkeästi myöhemmin tapahtuvaa päätöksentekoa varten. Yleensä analyysi perustuu joko kvantitatiiviseen (eli määrälliseen, numeerisesti esitettävään) tai kvalitatiiviseen (eli laadulliseen, kuvailevaan esitykseen) tarkasteluun tai näiden yhdistelmään. (Valtionvarainministeriö, 2017)

9 YHTEENVETO

Tässä opinnäytetyössä tutkin yleisiä yritystenkin käyttämiä tietoturvastandardeja, tietoturvallisuuden hallintajärjestelmiä, tietoturvaa, sen osa-alueita sekä hieman riskienhallintaa. Luettuani paljon standardeista ja tietoturvasta yleisesti, sain laajennettua omasta mielestäni hyvin paljon tietämystäni, pystyn luomaan yritykselle tietoturvakartoituksen sekä olen hyvin perillä standardien käytöistä tietoturva yrityksissä. Vaikka tässä työssä ei perehdytty juuri yhteen asiaan, valaisi tämä suuresti mitä yrityksissä halutaan tietoturvalta. Tulevaisuudessa aion opiskella lisää aiheesta ja kehittää itseäni alan osaajaksi.

LÄHTEET

Cassetto, O. (30. 5 2019). *Exabeam*. Haettu 5. 3 2020 osoitteesta https://www.exabeam.com/information-security/information-security-policy/

Mika Laaksonen, T. N. (2006). *Yrityksen tietoturvakäsikirja, ohjeistus, toteutus ja lainsäädäntö.* Edita Publishing Oy.

Opitietosuojaa.fi. (27. 11 2014). *Tietoturva*. Haettu 5. 11 2019 osoitteesta https://opitietosuojaa.fi/fi/aloitus/tietoturva

Puolustusministeriö. (25. 2 2019). *https://www.defmin.fi/.* Noudettu osoitteesta https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Suomen Standardisoimisliitto SFS ry. (3. 3 2017). *SFS Online.* Haettu 9. 3 2020 osoitteesta https://online.sfs.fi/fi/index.html.stx

Tietosuojavaltuutetun toimisto. (14. 05 2020). *Mitä tietosuoja on?* Haettu 14. 05 2020 osoitteesta https://tietosuoja.fi/tietosuoja

Tupper, C. D. (2011). *Data Administration - an overview | ScienceDirect Topics*. Haettu 14. 1 2020 osoitteesta https://www.sciencedirect.com/topics/computer-science/data-administration

Valtionvarainministeriö. (27. 10 2017). *Ohje riskienhallintaan - Valtionvarainministeriön julkaisuja 22/2017.* Haettu 14. 05 2020 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1&isAllowed=y

Valtionvarainministeriö. (13. 2 2019). *VM - VM, VAHTI ja tietoturvallisuus*. Haettu 28. 2 2020 osoitteesta https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus

Valtionvarainministeriö. (28. 2 2020). *VM - Vahti-ohjeet.* Haettu 28. 2 2020 osoitteesta https://www.vahtiohje.fi

Valtiovarainministeriö. (9. 10 2009). Haettu 6. 2 2020 osoitteesta https://www.vahtiohje.fi/web/guest/test?p_p_id=56_INSTANCE_Rx39&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_Rx39_struts_action=%2Fjournal_co

ntent%2Fview&_56_INSTANCE_Rx39_groupId=10128&_56_INSTANCE_Rx

Valtiovarainministeriö. (10. 9 2009). *VM - Fyysinen turvallisuus*. Haettu 2. 3 2020 osoitteesta https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

Valtiovarainministeriö. (10. 9 2009). *VM - Henkilöstöturvallisuus*. Haettu 2. 3 2020 osoitteesta https://www.vahtiohje.fi/web/guest/henkilostoturvallisuus

Valtiovarainministeriö. (10. 9 2009). *VM - Käyttöturvallisuus*. Haettu 2. 3 2020 osoitteesta https://www.vahtiohje.fi/web/guest/kayttoturvallisuus

Valtiovarainministeriö. (27. 11 2013). *Vm - Tietoturvallisuus - mitä se on?* Haettu 30. 10 2018 osoitteesta Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (vahti) ohjesivusto: https://www.vahtiohje.fi/web/guest/691