Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Joona Päivelin

Oleellisimmat vaatimukset ICT-yritykselle tietoturvallisuuden toteuttamiseksi

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

8.11.2019

Tekijä(t) Otsikko Sivumäärä Aika	Joona Päivelin Oleellisimmat vaatimukset ICT-yritykselle tietoturvallisuuden toteuttamiseksi 21 sivua + 1 liitettä 8.11.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	tieto- ja viestintätekniikka
Suuntautumisvaihtoehto	Communication Networks and Applications
Ohjaaja(t)	Tapio Wikström

Insinöörityön tavoitteena on kertoa ICT-yrityksen oleellisimmat tietoturvavaatimukset ja miten ne toteutetaan.

Työssä on teoriaosuus, jossa käydään läpi tietoturvan peruskäsitteet, ja kerrotaan konkreettisia esimerkkejä miten tietoturva saadaan toteutettua.

Vaatimuksia tarkastellaan kohdeyritykselle tehdyn tietosuojatyökalun avulla. Tietosuojan työkalun pohjana on käytetty KATAKRIA.

Tuloksena saatiin yritykselle tehtyä tietoturvakalu, jolla he voivat tarkastella omaa tietoturvaansa. Teoriatietoa aiheesta saatiin myös runsaasti ja sitä saatiin hyödynnettyä Katakrin vaatimusten mukaisesti.

Avainsanat	ICT, tietoturva, KATAKRI, Tietoturvakartoitus

Author(s) Title	Joona Päivelin Essential requirements for ICT-company to implement information security
Number of Pages Date	21 pages + 1 appendices 8th of November 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Specialisation option	Communication Networks and Applications
Instructor(s)	Tapio Wikström

This thesis tells the essential security requirements for ICT company and tell how to implement them.

Thesis includes theory section which includes security core concepts and how to implement them.

Requirements are checked with audition tool which was made of using Katakri.

As result the audition tool was made to the company which they can use to review their ICT security. Theory section was filled with lots of information and it was used to review Katakri requirements.

Keywords	ICT, security, Katakri, Security mapping

Sisällys

Lyhenteet

1 Johdanto 1

2 Mitä tietoturvallisuudella tarkoitetaan? 1

3 Tietoturvallisuuden osa-alueet 3

3.1 Hallinollinen tietoturvallisuus 3
3.2 Ohjelmistoturvallisuus 5
3.3 Laitteistoturvallisuus 6
3.4 Tietoliikenneturvallisuus 6
3.5 Tietoaineistoturvallisuus 7
3.6 Käyttöturvallisuus 7
3.7 Tietosuoja 7

4 Yrityksen sisäinen tietoturvallisuus 8

4.1 Turvallisuuden johtaminen 8
4.2 Henkilöstoturvallisuus 9
4.3 Fyysinen turvallisuus 10
4.4 Jatkuvuuden ja erityistilanteiden hallinta 10
4.4.1 Jatkuvuussuunnitelma 11
4.4.2 Valmiussuunnitelma 12
4.4.3 Pelastumissuunnitelma ja toipumissuunnitelma 13

5 Tietoturvakartoitus yritykselle Katakria käyttäen 13

5.1 Katakri yleisesti 13
5.2 Turvallisuusjohtaminen 14
5.2.1 Turvallisuusjohtaminen – riskienhallinta 15
5.2.2 Henkilöstoturvallisuus 16
5.3 Fyysinen turvallisuus 17
5.4 Katakri - Tekninen tietoturvallisuus 18
5.4.1 Tietoliikenneturvallisuus 18

5.4.2 Tietojärjestelmäturvallisuus 19
5.4.3 Tietoaineistoturvallisuus 20
6 Yhteenveto 20
Lähteet 22

Liitteet

Liite 1. tietosuojantukityökalu.xlsx (salattu)

Lyhenteet

Katakri	Kansallinen turvallisuusauditointikriteeristö.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä.
SOC	Security Operations Center (turvallisuusoperaatioiden keskus).
VPN	Virtual Private Network (virtuaalinen erikoisverkko).

1 Johdanto

Insinöörityön tarkoituksena on selvittää oleellisimmat vaatimukset ICT-yritykselle tietoturvallisuuden takaamiseksi. Kohdeyritykselle tehdään tukityökalu, jolla voidaan tarkastella oleellisempia ICT-yrityksen tietoturvavaatimuksia. Pohjana työkalulle käytetään KATAKRI:a. Tukityökalua ei liitetä työhön mukaan salassapitosyistä.

Työ tehdään pääkaupunkiseudulla toimivalle keskisuurelle IT-yritykselle, joka tarjoaa tuki-, ohjelmisto- ja konesalipalveluita. Yrityksellä on kymmeniä asiakkaita Etelä-Suomessa, ja se vastaa myös useiden asiakkaiden tietoturvallisuuden hoitamisesta.

Kansallinen turvallisuusauditointikriteeristö on Suomen Puolustusministeriön tekemä auditointityökalu, jolla voidaan arvioida kohdeorganisaation tietoturvallisuutta. KATAKRI on jaettu kolmeen osa-alueeseen, jotka ovat: turvallisuusjohtaminen, fyysinen turvallisuus ja tekninen turvallisuus.

2 Mitä tietoturvallisuudella tarkoitetaan?

Tietoturvallisuus on tiedon suojelemista erilaisin keinoin. On äärimmäisen tärkeää että yritys tunnistaa riskit ja pyrkii suojaamaan arkaluontoiset tiedot.

Tietoturvallisuuden osana ovat saatavuus, luottamuksellisuus, eheys, joita voidaan täydentää vielä todennuksella, tunnistuksella ja kiistämättämyydellä.

Saatavuudella ja **käytettävyydellä** tarkoitetaan ominaisuutta, jolloin tiedetään että tiedot ovat käytettävissä, kun niitä tarvitaan. Saatavuutta voi esimerkiksi heikentää järjestelmän virheet ja tietoliikenneyhteyksien virheet. Paras käytettävyys saadaankin, kun järjestelmiä huolletaan ja ylläpidetään säännöllisesti.

Luottamuksellisuudella tarkoitetaan, että tieto on käytettävissä vain niillä henkilöillä ja järjestelmillä, joilla on siihen oikeus. Tiedon luottamuksellisuus voidaan jakaa myös eri luokkiin, kuten luottamuksellinen, salainen ja erittäin salainen. Luottamuksellisuutta ylläpidetään muun muassa suojaamalla laitteet ja käyttäjätunnukset salasanojen avulla.

Eheydellä tarkoitetaaan, että tieto ei saa muuttua esimerkiksi kyberhyökkäyksien aikana, tai tietojen muutos pitää ainakin havaita. Tietojärjestelmien virheet voivat myös aiheuttaa muutoksia tiedoissa, jolloin eheys varmistetaan ottamalla säännölliset varmuuskopiot tiedoista tasaisin väliajoin.

Kiistämättömyydellä tarkoitetaan, että todennettu ja tunnistettu henkilö ei voi kiistää tekojaan, koska ne ovat tallentuneet järjestelmään. Esimerkkinä tästä voidaan käyttää biometristä tunnistusta tai kaksivaiheista tunnistusta.

Tunnistuksella tarkoitetaan, että järjestelmä tai käyttäjä yhdistetään esimerkiksi käyttäjätunnukseen, joka voi olla myös anonyymi. Tähän ei kuitenkaan vaadita salasanaa, vaan kyse voi olla esimerkiksi työyhteisön tunnistamisesta.

Todentamisella tarkoitetaan käyttäjän todentamista, jotta hänellä on väittämänsä identiteetti. Tämä voidaan varmentaa esimerkisi salasanalla, PIN-koodilla tai biometrisella tunnisteella. (Bel Raggad 2010).

3 Tietoturvallisuuden osa-alueet

Tässä kappaleessa käsitellään tietoturvallisuuden osa-alueet, jotka ovat nähtävissä alla olevassa kuvassa.

Kuva 1. Tietoturvallisuuden osa-alueet.

3.1 Hallinollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus tähtää orgasaation tietoturvallisuuden parantamiseen hallinollisilla toimenpiteillä. Sillä pyritään varmistamaan tietoturvan johtaminen ja kehittäminen. Hallinnnolliseen tietoturvaan voidaan katsoa allaolevan taulukon asiat. Organisaation koosta riippuen myös tietoturvan laajuus otetaan huomioon. Olisi erittäin tärkeää, että yrityksen osastoilla otettaisiin huomioon tietoturva osana jokaisen työntekijän päivittäisiä toimia.

Taulukko 1. Hallinnollinen tietorturvallisuus osa-alueet (Katakri versio II)

Aihealue	**Sisältö**
Tietoturvapolitiikka	Turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt. Yrityksen johto hyväksyy ja katselmoi säännöllisesti.
Tietoturvallisuuden tavoitteet	Tavoitteiden määrittely yrityksen toiminnoille ja hierarkiatasoille. Tavoitteiden saavuttamisen mittaus ja aikataulutus.
Tietoturvallisuuden toimintaohjelma	Menetelmät ja vastuut tietoturvallisuuden tavoitteiden saavuttamiseksi.
Tietoturvallisuuden koordinointi	Turvallisuusorganisaation luonti ja vastuiden jakaminen. Resursointi, roolien tiedotus ja sitouttaminen.
Tiedon luokitus	Tiedon luokittelun luominen ja ohjeistus
Suojattavien kohteiden hallinta	Suojattavien kohteiden luetteloiminen sekä niiden omistajien ja hyväksyttävän käytön määrittäminen.
Tehtävien eriyttäminen	Tehtävien jakaminen eri ihmisille siten, ettei vaarallisia yhdistelmiä synny ja kriittiset päätökset vaativat useamman henkilön hyväksynnän.
Riskien hallinta	Sisäisten ja ulkoisten riskien tunnistus, arviointi ja kontrollit, toimenpiteiden toteuttamisen ja tehokkuuden valvominen, riskien priorisointi ja tietoturvan arviointi. Tulosten hyödyntäminen turvallisuuskoulutuksissa. Riskien hallinnan osa-alueiden läpikäynti säännöllisesti.
Jatkuvuuden hallinta	Menetelmät poikkeusten havaitsemiseksi ja korjausten tekemiseksi, korjauksista aiheutuvien riskien arvioinniksi ja toimenpiteiden vaikutusten analysointi hallittujen tietojärjestelmämuutosten varmistamiseksi. Vastuut kriisi- ja poikkeustilanteissa toimimisessa.
Tietoturvallisuuden raportointi	Turvallisuusjärjestelmän toimivuuden tarkistus säännöllisesti, seurantatarkastusten dokumentointi ja tulosten käyttö tietoturvallisuuden parantamiseen.
Tietoturvakoulutus	Tietoturvakoulutusten käytännöt, järjestys ja sisältöjen valikointi.
Järjestelmien suunnittelu, kehitys ja muutosten hallinta	Järjestelmän hankinta-, kehitys- ja ylläpitoprosessit, vaatimusten mukaisuus ja kapasiteettien hallinta sekä järjestelmän hyväksyntä.
Ulkopuolisten palveluiden hallinta	Ulkoistettujen palveluiden hallinta, tarkkailu, katselmointi ja muutosten hallinta. Turvallisuudesta huolehtiminen asiakassuhteissa ja kolmansien osapuolten sopimuksissa.
Tiedonvaihto	Tiedonvaihtoperiaatteet, -menettelytavat ja -sopimukset, fyysiset tietovälineet kuljetuksen aikana, sähköinen viestintä ja liiketoiminnan tietojärjestelmät.

Dokumentaation hallinta	Turvallisuusdokumenttien tekomenetelmät, säilytysajat ja -paikat..

Hallinnollisen tietoturvallisuuden aihealueet. [ISO/IEC 27001:fi 2006:32-34, 40, 44; Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009:8-19, 21, 28-46.]

3.2 Ohjelmistoturvallisuus

Ohjelmistojen ja lisenssien hallintaa tietojärjestelmissä pidetään ohjelmistoturvallisuutena. On tärkeää, että yrityksessä noudatetaan ohjelmistoturvallisuutta, koska esimerkiksi virusturvaohjelman lisenssin päättyminen voi aiheuttaa ison tietoturvariskin yritykselle. Luvattoman käytön ohjelmiin ja järjestelmiin voi minimoida käyttäen vahvoja salanoja ja henkilökohtaisia tunnuksia. Tärkeää on myös huolehtia, että käyttöjärjestelmät ja ohjelmat ovat ajantasalla päivityksineen. Huolto- ja ylläpitosopimukset ovat hyvä lisä yritykselle, mikäli sillä ei itse riitä resurssit ylläpitoon. Tällöin myös vastuu ohjelmistoturvasta siirtyy ylläpitöyritykselle. Joskus myös virukset voivat yllättää ja tietojärjestelmät menettää tietoja niiden seurauksena. Tämän takia kannattaa olla varmuuskopiot, mistä tiedot voidaan palauttaa entiselleen.

3.3 Laitteistoturvallisuus

Kaikkien yrityksen teknisten laitteiden suojaamista sanotaan laitteistoturvallisuudeksi. Tähän lukeutuvat muun muassa palvelimet, tulostimet, matkapuhelimet ja tietokoneet. Laiterekisteri on hyvä tapa ylläpitää turvallisuutta laitteiden keskuudessa. Tällä tavalla saadaan tieto dokumentoitua yrityksen kaikista laitteista eli siitä, milloin ne on otettu käyttöön ja poistettu käytöstä. Mikäli laite katoaa, niin laiterekisteristä saadaan tarvittavat tiedot laitteesta.

Laitteiden fyysinen sijainti kannattaa myös ottaa huomioon turvallisuudessa. Yöllä tilat on lukittu, jolloin laitteiden joutuminen vääriin käsiin on epätodennäköistä, mutta päiväsaikaan esimerkiksi ulko-ovien lähellä olevat laitteet voivat muodostaa tietoturvariskin yritykselle ulkopuolisen ottaessa ne mukaan.

Ennakoiva valmistautuminen on myös syytä ottaa huomioon laitteiden keskuudessa. Tämä varmistetaan muun muassa palvelimien osalta riittävällä sähkönsyötöllä ja ilman lämpötilan säätelyllä. Huolto ja ylläpitösopimukset kannattaa olla liiketoiminnan mukaan sillä tasolla, että avun saa mahdollisimman nopeasti eikä tuotanto pääse katkeamaan.

3.4 Tietoliikenneturvallisuus

Kaikki liikkuva data ja sitä siirtävät laitteet kuuluvat tietoliikenneturvallisuuteen, kun puhutaan sen suojaamisesta. Tavoitteena on, että tieto on suojattu parhaalla mahdollisella tavalla eikä se päädy ulkopuolisien käsiin. Suojaaminen onnistuu laitetasolla puhuttaessa esimerkisi palomuureilla, kytkimillä ja reittitimillä. On tärkeää, että laitteissa on uusimmat järjestelmäpäivitykset asennuttuina sekä pääsy niihin rajoitettu salasanoilla ulkoisten riskitekijäiden pois rajaamiseksi. Dokumentointi on tässä osaalueessakin tärkeässä roolissa, sillä se nopeuttaa tietoruvallisuuden ylläpitämistä. (Krutz & Vines, 2003)

3.5 Tietoaineistoturvallisuus

Tiedostojen, asiakirjojen sekä tietovälineiden hallintaa kutsutaan tietoainestoturvallisuudeksi. Tietoaineisto pitää olla luokiteltua sen mukaan, mihin kenelläkin tulee olla pääsy. Yksinkertaisin tapa on jakaa tieto salaisiin ja julkisiin tietoihin. Julkista informaatiota voidaan esitellä myös yrityksen ulkopuolisille tahoille, kun taas luottamuksellista ja salaista tietoa vain henkilöille, joille on annettu siihen pääsy. Mikäli tiedon jaotteleminen on vaikeaa, voi aputyökaluna käyttää VAHTI-taulukointia, jossa jokainen vaatimus on eriteltynä.

3.6 Käyttöturvallisuus

Käyttöturvallisuuteen kuuluvat tietojenkäsittelyn suojaustoimenpiteet kuten järjestelmien asianmukainen valvonta, tietolokien läpikäynti sekä salasanojen hallinointi. Tavoitteena on saada riskit minimoitua turvallisella tavalla. Etätyötä tehdessä on huolehdittava työpisteen ja tietoliikenteen asianmukaisesta turvallisuudesta ja estää tiedon pääsy ulkopuolisten käsiin. Toimistolla töitä tekevän on huolehdittava työaseman lukitsemisesta, kun poistutaan työpisteeltä.

3.7 Tietosuoja

Tietosuoja on perustuslain takaama yksityisyyden suoja. Sen tarkoitus on pitää huoli, että yritykset käsittelevät henkilötietoja lainmukaisella tavalla.

Lain mukaan henkilöllä on oikeus

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin

- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.
  [Tietosuojavaltuuteton toimisto. 2019. Verkkoaineisto. Viitattu 29.10.2019 https://tietosuoja.fi/tunne-oikeutesi.

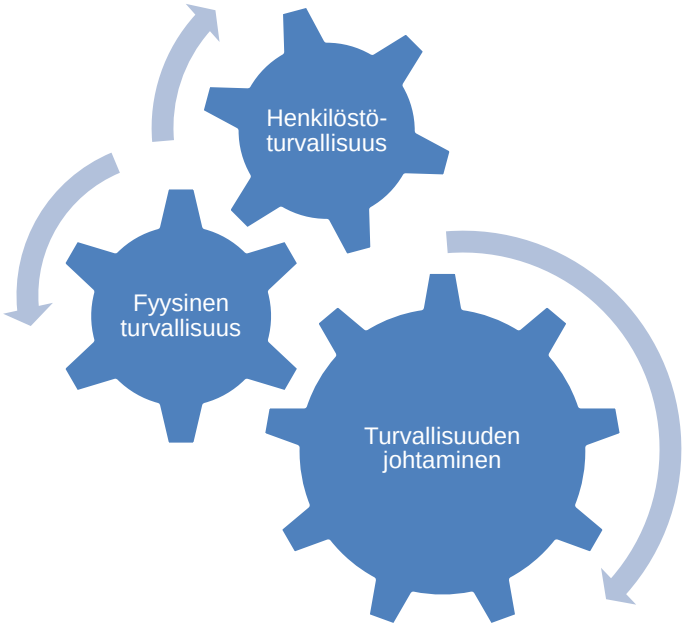
4 Yrityksen sisäinen tietoturvallisuus

4.1 Turvallisuuden johtaminen

Tietoturvallisuuteen pitää osallistua myös yrityksen johdon. Johto on pääasiassa vastuussa alaisistaan ja myös tietoturvasta sekä resurssien jakautumisesta tälle osa-alueelle.

Johdon pitää:

- selvittää toiminnan ja palvelujen tietoturvatarpeet ja vaatimukset
- arvioida ulkoiset ja sisäiset riskit
- selvittää säädöksistä ja määräyksistä johtuvat vaatimukset
- arvioida toiminnan ja tietotekniikan muutoksien vaikutukset tietoturvallisuuteen
- selvittää sidosryhmien odotukset
- edellä mainittujen perusteella määritellä tietoturvallisuuden tarpeet, periaatteet ja toteutustapa.



Kuva 2. Yrityksen sisäisen tietoturvallisuuden osa-alueet

4.2 Henkilöstoturvallisuus

Henkilöstöön liittyvää riskien hallintaa kutsutaan henkilöstätuvalisuudeksi. Tähän liittyviä aiheita ovat muun muassa valvonta, turvallisuuskoulutus, sijaisjärjestelyt, toimenkuvat ja henkilöstön soveltuvuus. Henkilöstoturvallisuuteen liittyviä uhkia ovat muun muassa puutteelliset toimintatavat, tahattomat virheet sekä tahalliset teot, joihin sisältyvät tietokantoihin tunkeutuminen ja tiedon varastaminen.

Yrityksen palkatessa uutta työntekijää voi kyseeseen tulla taustaselvitys, jolla saadaan selville edelliset työnantajat ja suosittelijat. Mikäli haetaan työntekijää kriittisiin tehtäviin turvaselvityksen tilaaminen suojelupoliisilta voi tulla tarpeeseen.

Työsuhteen päättyessä pitää huolehtia että lähtevän henkilön haltuun ei jää yritykseä koskevia tietoja ja tunnuksia, joita hän voisi hyödyntää uudessa työpaikassa. Käyttöoikeudet ja tunnukset on poistettava ja henkilöstölle ilmoitettava työsuhteen päättymisestä.

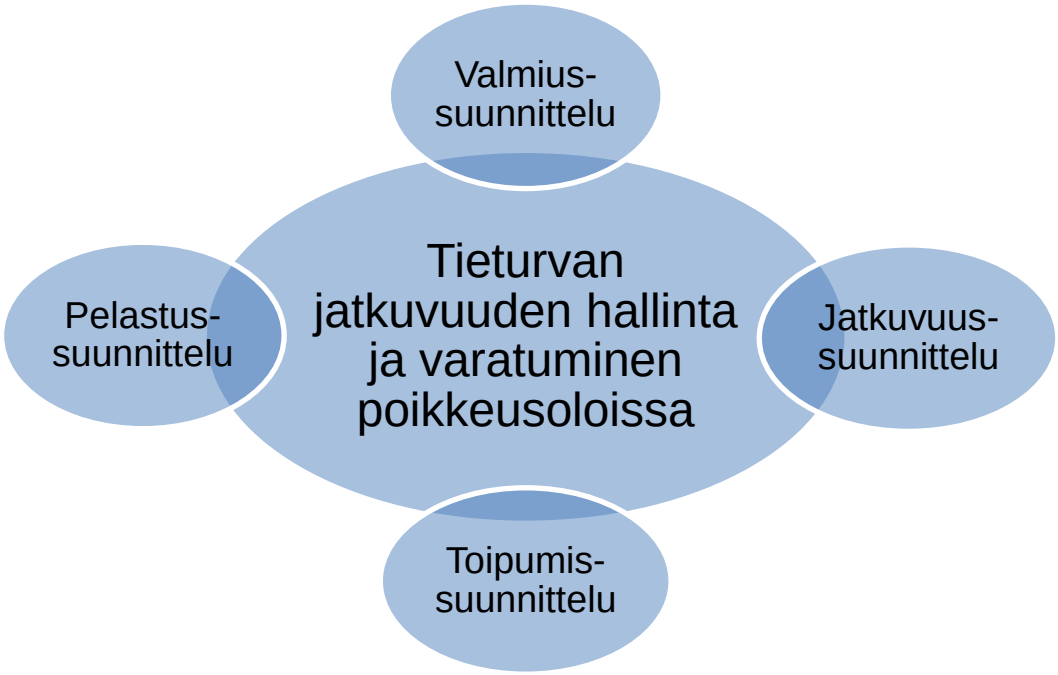
4.3 Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluu estää muun muassa palo-, vesi-, sähkö-, ilmastointi ja murtovahingot. Tämän lisäksi siihen kuuluvat kulunvalvonta, vartiointi ja tekninen valvonta. Fyysisessä turvallisuudessa pitää muistaa, että kohteet vaativat erilaisen tärkeysluokituksen sen sisältämän tiedon ja tavaran suhteen. Palvelinhuoneessa pitää olla tarkempi kulunvalvontaselvitys kuin keittiössä, ja niin edespäin. Organisaation koko ja toimiala vaikuttavat myös, kuinka tarkasti fyysinen turvallisuus pitää ottaa huomioon. (Miettinen 1999).

4.4 Jatkuvuuden ja erityistilanteiden hallinta

Valtakunnallisesti vaikeutuneet toimintaolosuhteet voivat aiheuttaa poikkeusoloja, jotka on määriltelty puolustus- sekä valmiuslaissa.

Toimintakyvyn säilyttäminen suunnitellusti poikkeus- ja häiriötilanteiden aikana on turvattava. Tilanteet voivat aiheuttaa vahinkoa organisaatiolle ja ne ovat yleensä äkillisiä. Tietojärjestelmät on tunnistettava keskeisyyden kannalta ja häiriötilanteet voivat aiheuttaa resurssien ohjaustarvetta.



Kuva 3. Jatkuvuuden ja erityistilanteiden hallinta.

4.4.1 Jatkuvuussuunnitelma

Tärkeimpiä huomioitavia seikkoja selvitettäessä palvelujen ja sitä tukevan tietotekniikan jatkuvuuden varmistamista ovat:

- keskeisten toimintojen ja palvelujen määrittely
- keskeisille toiminnoille välttämättömän tietojenkäsittelyn määrittely
- tilannearviot vakaviin keskeytyksiin johtavista tapahtumista
- keskeytysten vaikutukset tuotantoon, palveluihin, asiakkaisiin ja toimituksiin
- toimintojen tietojenkäsittelyriippuvuudet
- muiden tahojen välilliset riippuvuudet palvelujen keskeytymisestä
- kriittisiksi muodostuvat keskeytysajat
- kausiluonteiset kriittiset ajankohdat
- arviot keskeytystilanteessa syntyvistä taloudellisista menetyksistä sovelluksittain
- tietotekniikan käytön rajoittuessa ylläpidettävien sovellusten ja varmistamistoimenpiteiden prioriteetit.

4.4.2 Valmiussuunnitelma

Valmiussuunnitelmassa varmistetaan tai korvataan etukäteen sovittu ja organisaation päättämä toiminta.

Keskeisiä seikkoja selvitettäessä palvelujen ja sitä tukevan tietotekniikan suunnittelua poikkeusoloihin ovat:

• ajantasaiset uhkakuvat
• poikkeusolojen vaikutus toimintaan
• ulkomaisten tietoliikenneyhteyksien lamaantuminen tai katkeaminen laitteiden ja varaosien saanti
• organisaation kannalta tärkeiden reserviläisten ja muiden henkilöiden henkilövaraukset (VAP)
• tietojenkäsittelyn merkitys organisaatiolle ja asiakkaille poikkeusoloissa
• organisaation toiminnan, tuotannon tai palvelun merkitys kansalaisten ja yhteiskunnan toimeentulolle eri tilanteissa
• valtiovallan asettamat poikkeusolojen tuotantovaatimukset ja sen edellyttämä tietojenkäsittelyn ylläpito
• tietotekniikan käytön supistaminen ja riippuvuuksien vähentäminen sekä turvallisuustoimenpiteet. (Vahti-ylläpito 2009).

4.4.3 Pelastumissuunnitelma ja toipumissuunnitelma

Pelastussuunnitelma on laadittava mikäli, organisaation toimitiloissa samaan aikaan olevien henkilöiden määrä ylittää tietyn rajan tai mikäli konesalitilat on varustettu paloilmoittimella ja sammutuslaitteistolla. Vastuuhenkilöt on koulutettava pelastustoimintaan ja, suunnitelma on pidettävä ajantasalla.

Toipumissuunnitelmat ovat järjestelmäkohtaisia. Niiden avulla poikkeustiloista valmistaudutaan palautumaan normaaliin toimintaan. Suunnitelmassa kuvataan, mitkä toimenpiteet tulee tehdä, että palaudutaan tuotantojärjestelmien palveluihin riskittä.

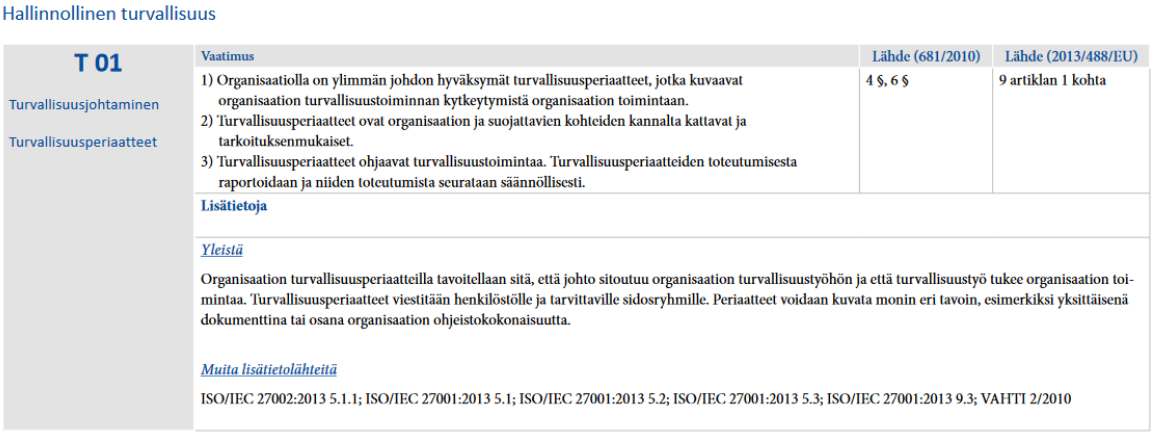
5 Tietoturvakartoitus yritykselle Katakria käyttäen

5.1 Katakri yleisesti

Kansallinen turvallisuusauditointikriteeristö on Suomen Puolustusministeriön tekemä auditointityökalu, jolla voidaan arvioida kohdeorganisaation tietoturvallisuutta. Katakri on jaettu kolmeen osa-alueeseen turvallisuusjohtamiseen, fyysiseen turvallisuuteen ja tekniseen turvallisuuteen.

Katakri ei aseta itse tietoturvallisuudelle ehdottomia vaatimuksia, vaan ne perustuvat kansainvälisiin tietoturvallisuusvelvoitteisiin ja voimassa olevaan lainsäädäntöön. Katakrin käytöllä pyritään varmistamaan, että kohdeyrityksellä on kaikissa ympäristöissä, joita käsitellään riittävät turvallisuusjärjestelyt. (Puolustusministeriö. 2011. Kansallinen turvallisuus auditointikriteeristö Versio II.)

Yritykselle tehty tietoturvakartoitus jätetään arkaluontoisuuden takia salattuna pois tästä työstä.



Hallinnollinen turvallisuus

T 01	Vaatimus	Lähde (681/2010)	Lähde (2013/488/EU)
Turvallisuusjohtaminen Turvallisuusperiaatteet	1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan ja niiden toteutumista seurataan säännöllisesti.	4 §, 6 §	9 artiklan 1 kohta

Lisätietoja

Yleistä

Organisaation turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa. Turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana organisaation ohjeistokokonaisuutta.

Muita lisätietolähteitä

ISO/IEC 27002:2013 5.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; ISO/IEC 27001:2013 9.3; VAHTI 2/2010

Kuva 4. Katakrin T01 kohdan rakenne turvallisuusjohtamisesta

5.2 Turvallisuusjohtaminen

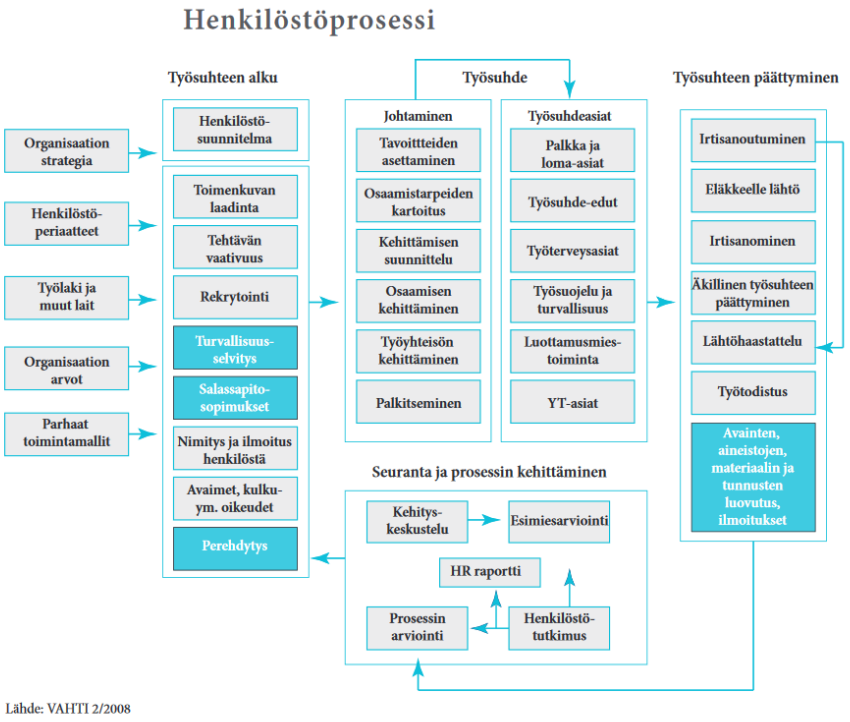
Turvallisuusjohtaminen osa-alueena kattaa henkilöstöturvallisuuden ja hallinnollisen turvallisuuden. Näissä osioissa käsitellään menetelmiä, joilla turvallisuus ja sen hallinta saadaan osaksi koko organisaation toimintaa. Turvallisuusjohtamisen perusperiaatteisiin kuuluu, että johto sitoutuu organisaation turvallisuustyöhön, sekä turvallisuusperiaatteet kerrotaan henkilöstölle.

Esimerkkinä Katakrin kohta ” T06 Turvallisuusjohtaminen 1) Organisaatiolla on menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn 2) Organisaatio on määrittänyt henkilöt/tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa.” Kohdeyrityksessä seuraavat on otettu huomioon perustamalla SOC-tiimi (Security Operations Center). Tämän tiimin vastuuna on varmistaa, että organisaatio kykenee toimimaan tehokkaasti tilanteissa, joissa tietoturva on uhattana, minimoidaan vahingot ja palautetaan tilanne normaaliksi.

5.2.1 Turvallisuusjohtaminen – riskienhallinta

Riskienhallinta on prosessi, jota sovelletaan koko organisaation toiminnassa. Sen tavoitteena on hallita ja tunnistaa vaarantavia tekijöitä organisaatiolle ja pitää riskit rajoissa, jotta toiminta ja tavoitteet eivät ole uhattuna. Turvallisuusjärjestelyiden monitasoisuus tulee huomioida osana riskienhallintaa, sillä täydellistä suojausta ei pystytä aina rakentamaan. Hyvän riskienhallinnan tunnistaa suunnitelmallisuudesta, järjestelmällisyydestä, tietoisuudesta ja ennakoivuudesta.

5.2.2 Henkilöstoturvallisuus



Kuva 5. henkilöstöprosessi Katakrin mukaan.

Henkilöstoturvallisuus on hyvällä tasolla, mikäli henkilöstö on sitoutunut tietoturvavastuisiin ja heillä on selkeä toimenkuva. Tehtävistä riippuen ennen työhöntuloa olisi selvitettävä rekrytoitavan tausta, sopivuus ja osaaminen. Työsuhteen päättyessä tulee huolehtia pääsyoikeuksien poistamisesta ja mahdollisuuksien mukaan salassapitovelvollisuudesta koskien työtehtävää.

Esimerkkinä Katakrin henkilöstöturvallisuusosiosta: ”T11 Turvallisuuskoulutus ja -tietoisuus kohdat 2) Henkilöstölle annetaan ohjeet ja koulutusta salassapidettävien tietojen asianmukaisesta käsittelystä. 3) Salassa pidettävien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneet henkilöt dokumentoidaan.” Kohdeyrityksessä nämä ylläolevat kohdat on huomioitu pitämällä henkilöstölle säännöllisin väliajoin tietoturvakoulutusta sertifioiduilta kumppaneilta.

5.3 Fyysinen turvallisuus

Fyysinen turvallisuus on Katakrissa tarkasteltuna viranomaisten salassa pidettävän tietoaineston näkökulmasta. Turvatoimet määritellään riskinhallintaprosessien perusteella ja niihin kuuluvat esimerkiksi ehkäiseminen, estäminen ja havaitseminen luvattomille toimille. Fyysinen turvallisuus jaetaan vielä kolmeen osa-alueeseen, jotka ovat hallinnollinen alue, turva-alue ja tekninen turva-alue.

Tilojen ja laitteiden suojauksessa tulee ottaa huomioon rakenteelliset suojaratkaisut, turvajärjestelmät ja -laitteet sekä rakennuksen turvallisuus. Käytännössä tämä toteutetaan siten, että rakennuksen ulkokuori muodostaa ensimmäisen tason. Kulkua tiloihin valvotaan ja hallitaan. Sisemmissä tiloissa estetään tunkeutuminen arkaluontoisiin tiloihin. Ikkunat ja muut aukot otetaan myös suunnittelussa huomioon.

Luvattoman pääsyn estäminen haluttuihin tilohin onnistuu kätevästi kuvallisilla henkilökorteilla. Kulkuoikeuksista tehdään dokumentti ja sitä päivitetään säännöllisin väliajoin. Vierailijoiden pitää liikkua organisaatioon kuuluvan henkilön kanssa ja hänellä pitää olla henkilökortti näkyvillä.

Kassakaapit, kulunvalvontajärjestelmät ja valvontajärjestelmät pitää olla hyväksyttyjen standardien ja vähimmäisvaatimusten mukaisia sekä niitä pitää testata ja pitää käyttäkuntoisena. Euroopan talousalueella hyväksytyt standardien vaatimukset on täytettävä ja tuotteet pitää olla sertifioituja.

Tietojen salakuuntelua ja salakatselua vastaan suojaudutaan asianmukaisin keinoin. Tämä onnistuu muun muassa käyttämällä kannettavissa tietokoneissa näyttösuojia, tilan ikkunoiden näköpiirin peittämistä sälekaihtimilla tai verhoilla ja salassapidettävän tiedon keskustelun välttämistä yleisissä tiloissa, mistä ääni voi kantautua sivullisten korviin. (Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille).

Esimerkkinä Katakrin fyysinen turvallisuus kohdat: ”F02 Tekninen turva-alue 20) Alueella on murtohälytysjärjestelmä 21) Alue pidetään lukittuna silloin, kun se ei ole käytössä ja vartioituna silloin, kun se on käytössä. 22) Avaimia valvotaan.” Kohdeyrityksessä seuraavat on otettu huomioon pitämällä tilat lukittuina ja liikkuminen tiloihin onnistuu elektronisilla kulkutunnisteilla. Murtohälytysjärjestelmä on otettu 24/7 kattavana palveluna ulkoiselta turvallisuusyritykseltä, joka hoitaa samalla konesalipalveluiden hälytyspalvelut.

5.4 Katakri - Tekninen tietoturvallisuus

Teknisen tietoturvallisuuden osiossa Katakrissa kuvataan vaatimukset, jolla pyritään varmistamaan salassa pidettävän tiedon riittävyys sähköisessä käyttöympäristössä. Vaatimukset on jaettu tietoliikenne-, tietojärjestelmä-, tietoaineisto- ja käyttöturvallisuuden osioihin.

5.4.1 Tietoliikenneturvallisuus

Tietojenkäsittely-ympäristöjen suojattu yhteenliittäminen ja verkon rakenteellinen turvallisuus hoidetaan erottamalla ne muusta verkosta sekä käyttämällä palomuuriratkaisua. Tietoliikenneverkko jaetaan erillisille alueille ja pääsyä niihin säädellään. Verkkohyökkäyksiin varaudutaan yleisimpien keinojen avulla ja poistetaan tarpeettomat protokollat käytöstä.

Verkkorakenne pitää dokumentoida semmoisella tarkkuudella, että viranomainen voi tarkistaa siitä hyväksytyn rakenteen. Asetusten ja päivitysten pitää olla tarkastusten alla vähintään vuosittain tai ympäristöstä riippuen jopa useammin. Langattomien verkkojen rajapintaa tulee käsitellä kuin julkista verkkoa ja liikenne tulee salata.

Esimerkkinä Katakrin kohta: ”I03 Tietoliikenneturvallisuus 3) Verkon ja siihen liittyvien suodatus- ja valvontajärjestelmien dokumentaatiota ylläpidetään sen elinkaaren aika erottamattomana osana muutosten ja asetusten hallintaprosessia.” Kohdeyrityksessä tämä on otettu huomioon pitämällä omaa

wiki-pohjaista alustaa, mihin dokumentoidaan verkon tiedot. Erityistä lisäturvaa saadaan pitämällä wiki vain sisäverkossa ja ulkoverkosta vain VPN:llä saavutettavissa olevalla ratkaisulla.

5.4.2 Tietojärjestelmäturvallisuus

Tietojärjestelmäturvallisuus on Katakrissa erittäin laaja osio, joten tähän kerätään tiivistetysti pääkohtia.

Pääsyoikeuksien hallinta pitää olla hallittua sekä vastuuhenkilöiden takana. Käyttäjistä pitää olla asianmukaiset listat ja dokumentaatiot tehtynä ja oikeudet tarkastetaan säännöllisin väliajoin. Käyttäjät pitää tunnistaa ja todentaa, mikä käytönnössä onnistuu salasanalla, joka on tarpeeksi vahva.

Verkon aktiivilaitteisiin pitää olla oletussalasanat vaihdettuna, tarpeelliset turvapäivitykset asennettuna ja tarpeelliset verkkopalvelut vain päällä. Työasemien ja palvelimien turvapäivitykset on asennettuina ja salasanat ovat salasanapoliitikan mukaan vahvoja. Ulkoiset käytettävät ohjelmat kuten web-selaimet, PDF-lukijat ja sähköpostiojelmistot ovat turvallisesti konfiguroituja.

Haittaohjelmasuojaus asennetaan kaikkiin järjestelmiin, joihin on mahdollista tulla tartuntoja. Ohjelmien pitää päivittyä useasti ja tuottaa lokitietojen lisäksi myös hälytyksiä uhkista. Torjuntaohjelmistot voidaan jättää asentamatta ympäristöihin, jotka ovat täyisin eristyksissä muusta verkosta.

Verkkoliikenteen seuraaminen pitää olla käytössä ja liikennemäärät, protokollat ja yhteydet tiedossa. Pitää olla keino saada tietoon normaaliin liikenteeseen poikkeavat tapahtumat kuten palvelunestohyökkäykset.

Esimerkkinä Katakrin kohdat: ”I09 1) Haittaohjelmantorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, jotka ovat alttiita haittaohjelmatartuntoille. 2) Torjuntaohjelmistot ovat toimintakykyisiä ja käynnissä.” Kohdeyrityksessä nämä on huomioitu asentamalla jokaiseen

työasemaan virustorjunta, joka päivittää itsensä uusimmilla tietoturvapäivityksellä heti, kun ne ovat saatavilla.

5.4.3 Tietoaineistoturvallisuus

Salassa pidettävien tietojen välitys fyysisesti suojattujen alueiden välillä pitää olla salattua viranomaisten hyväksymällä menetelmällä. Tämä tarkoittaa, että puhelimen, faksin, pikaviestimien ja sähköpostin tiedonsiirto pitää hoitaa asianmukaisella tavalla, ettei tietoa pääse ulkopuolisten käsiin. USB-muititikut ja CD-levyt pitää olla salattuja ja niitä lähettäessä eteenpäin pitää aineisto sulkea suljettavaan kirjekuoreen tai vastaavaan. Organisaation sisäiseen postinkäsittelyketjuun kuuluu vain hyväksyttyä henkilöstöä. Tietojen hävittäminen on käsiteltävä sähköisten/ei sähköisten -aineistojen osalta niin, ettei hävitettyjä tietoja pystytä kokoamaan uudelleen osittain tai kokonaan.

Esimerkkinä Katakrin osiot: ”I19 1) Ei sähköisten aineistojen hävittäminen on järjestelty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelle kokonaan tai osittain & I20 3) Tietojenkäsittely-ympäristön turvallisuusasiakirjoja kehitetään sen elinkaaren aikana erottomattomana osana muutosten ja asetusten hallintaprosessia.” Nämä toteutetaan kohdeyrityksessä hävittämällä vanhat IT-laitteet SER-kierrätyksellä tietoturvallisesti kaikki kovalevyt ensin poistaen ja tyhjentäen. Turvallisuusasiakirjoja kehitetään aina erikseen vain niille kuuluvien henkilöiden kesken.

6 Yhteenveto

Lopputyön tavoitteena oli kertoa tietoturvasta yleisesti ja tehdä tietoturvakartoitus kohdeyritykselle. Oikeanlaisten tietojen etsiminen Internetistä ja kirjoista oli aikaanvievää työtä, mutta palkitsevaa, kun vihdoin löysi etsimänsä. Tietoturvasta löytyi jo jonkun verran kokemusta työelämästä, mutta tätä työtä tehdessä tietoturvaosaaminen kasvoi myös huomattavasti. Lopputyön tietosuojatyökalun salaaminen piti ottaa huomioon työtä tehdessä, ja se hankaloitti jonkin verran

kirjallisen osien kirjoittamista, koska itse konkreettinen työ jäi lähes kokonaan salattuna pois. Yritys sai arvokasta tietoa omasta tietoturvastaan tukityökalun avulla, ja pystyy sitä kehittämään sen avulla jatkossakin.

Lähteet

1 Puolustusministeriö. 2011. Kansallinen turvallisuus auditointikriteeristö Versio II. Viitattu 29.10.2019. Verkkoaineisto https://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf.

2 Verkkojulkaisu 2006. Viitattu 29.10.2019 ISO/IEC 27001:fi 2006, 29–31, 48–62; ISF 2007, 40–50).

3 Miettinen, Juha 1999. Tietoturvallisuuden johtaminen. Näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

4 Krutz, Ronald L. & Vines, Russel Dean 2003. Tietoturvasertifikaatti – CISSP. Helsin-ki: Edita Publishing Oy.

5. Vahti-ylläpito 2009 Luettu 29.10.2019 Verkkoaineisto https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus.

6 Tietosuojavaltuuteton toimisto. 2019. Verkkoaineisto. Viitattu 29.10.2019 https://tietosuoja.fi/tunne-oikeutesi.

7 Vahti-ylläpito 2009 Luettu 29.10.2019 Verkkoaineisto https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=102298.

8 Bel Raggad 2010. Information Security Management: Concepts and Practice.

9 Vahti-ylläpito. 2009. Luettu 29.10.2019 Verkkoaineisto https://www.vahtiohje.fi/web/guest/jatkuvuuden-ja-erityistilanteiden-hallinta?p_p_id=56.

10 Puolustusministeriö. 2015. Katakri 2015 Tietoturvallisuuden auditointityökalu viranomaisille. Verkkojulkaisu. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf.

1. Tietosuojan tukityökalu.xlsx