

**MÄÄRÄYKSEN 47 PERUSTELUT JA
SOVELTAMINEN**

**TELEYRITYSTEN TIETOTURVALLISUUDEN
HALLINNASTA**

MPS 47

SISÄLLYS

SISÄLLYS	1
1 LAINSÄÄDÄNTÖ	2
1.1 MÄÄRÄYKSEN LAINSÄÄDÄNTÖPERUSTA.....	2
1.2 MUUT ASIAAN LIITTYVÄT SÄÄNNÖKSET.....	2
2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA	2
2.1 MÄÄRÄYKSEN TARKOITUS	2
2.2 KESKEISET MUUTOKSET JA MUUTOSHISTORIA.....	3
2.3 MÄÄRITELMÄT.....	3
3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET	6
3.1 1 § SOVELTAMISALA	6
3.2 2 § TIETOTURVALLISUUDEN ORGANISOINTI	7
3.3 3 § TIETOTURVALLISUUDEN OHJAUSASIAKIRJAT.....	8
3.4 4 § RISKIEN HALLINTA	10
3.5 5 § TIETOTURVATOIMENPITEET.....	21
3.6 6 § TIETOTURVALLISUUDEN HALLINNAN SEURANTA.....	23
4 VIITELUETTELO	24
5 LIITTEET	25
5.1 YKSINKERTAISTETTU ESIMERKKI RISKIEN ARVIOINNISTA	25

1 LAINSÄÄDÄNTÖ

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle kokonaiskuva siitä, mihin säädöksiin määräys perustuu. Lisäksi luvussa listataan aihepiiriin liittyvä muu oleellinen säädäntö.

1.1 Määräyksen lainsäädäntöperusta

Viestintäviraston määräysehdotus perustuu sähköisen viestinnän tietosuojalain (SVTsL) [1] 19 ja 20 §:iin.

Viestintävirasto voi SVTsL:n 19 §:n 4 momentin nojalla antaa teleyritykselle tarkempia määräyksiä pykälän 1 - 3 momentissa tarkoitettusta palvelun tietoturvasta. Pykälän 1 momentin mukaan teleyrityksen ja lisäarvopalvelun tarjoajan on huolehdittava palvelujensa tietoturvasta. Pykälän 3 momentin mukaan teleyritys vastaa tilaajille ja käyttäjille 1 momentissa tarkoitettusta tietoturvasta myös sellaisen kolmannen osapuolen osalta, joka kokonaan tai osittain toteuttaa verkko- tai viestintäpalvelun.

1.2 Muut asiaan liittyvät säännökset

Tässä kappaleessa kuvataan Viestintäviraston antamat tämän määräyksen aihepiiriin liittyvät muut määräykset. Kappaleen tarkoituksena on antaa määräyksen käyttäjälle parempi mahdollisuus viestintäverkkoja ja -palveluita koskevien velvoitteiden kokonaiskuvan hahmottamiseen.

Määräys 54 Viestintäverkkojen ja -palvelujen varmistamisesta [2]. Määräyksen tarkoituksena on viestintäverkkojen ja -palvelujen toimintavarmuuden, tietosuojan ja tietoturvan takaaminen normaalioloissa, normaaliolojen häiriötilanteissa ja poikkeusoloissa. Tästä syystä määräys asettaa teleyrityksille minimivelvoitteet muun muassa viestintäverkkojen ja -palvelujen toteutuksessa käytettyjen laitteiden tehonsyötön varmistukselle, laitteiden fyysiselle suojaamiselle sekä laitteiden ja yhteyksien varmistamiselle.

2 MÄÄRÄYKSEN TARKOITUS JA MUUTOSHISTORIA

Tämän luvun tarkoituksena on antaa määräyksen käyttäjälle tieto määräyksen tavoitteista ja tarkoituksesta. Luvussa käsitellään myös merkittävimmät muutokset määräystä edeltäneisiin velvoitteisiin ja suosituksiin.

2.1 Määräyksen tarkoitus

Tietoturvan hallintaa on kuvattu kattavasti muun muassa ISO 27001 (Information Security Management - Specification With Guidance for Use) standardissa [3]. Tämän standardin kattava noudattaminen voi olla liian raskasta erityisesti pienille teleyrityksille Suomessa.

Määräyksessä kuvataan ne vähimmäisvaatimukset tietoturvan hallinnoinnille, jotka jokaisen teleyrityksen tulee toteuttaa toiminnassaan. Vaatimuksilla pyritään turvaamaan teleyrityksen harjoittaman teletoiminnan perustietoturvaso, joka toimii pohjana viestintäverkkojen ja -

palveluiden tietoturvallisuuden varmistamiseksi. Vaatimuksissa keskitytään erityisesti tietoturvallisuuden hallinnan jatkuvaan kehittämiseen, suunnitteluun, toteuttamiseen ja arviointiin. Määräyksellä pyritään myös pienentämään tietoturvariskien aiheuttamia vahingollisia vaikutuksia teletoiminnalle.

2.2 Keskeiset muutokset ja muutoshistoria

Määräyksen edellisen version voimaantulon jälkeen Viestintävirasto on antanut palvelukohtaisia määräyksiä, kuten sähköpostipalvelun (M11) [4] ja internet-yhteyspalvelun (M13) [5] osalta. Palvelukohtaisissa määräyksissä asetetut veloitteet ovat olleet jossain määrin päällekkäisiä tämän määräyksen edellisessä versiossa asetettujen veloitteiden kanssa. Päällekkäisyydet on pyritty poistamaan määräysmuutoksella. Samalla on pyritty myös tarkentamaan tietoturvallisuuden hallinnointiin liittyviä vaatimuksia muun muassa riskien hallinnan osalta.

2.3 Määritelmät

Tässä kappaleessa kuvataan määräyksessä käytetyt määritelmät.

2.3.1 Teletoiminta

Teletoiminta määritellään viestintämarkkina-alaissa. Lain mukaan teletoiminnalla tarkoitetaan verkkopalvelua tai viestintäpalvelua. Yleisellä teletoiminnalla tarkoitetaan verkkopalvelun tai viestintäpalvelun tarjoamista käyttäjäpiirille, jota ei ole etukäteen rajattu.

Verkkopalvelulla viestintämarkkina-alaissa tarkoitetaan verkkoyrityksen tarjoamaa palvelua ja viestintäpalvelulla palveluyrityksen tarjoamaa palvelua. Verkkoyrityksellä tarkoitetaan yritystä, joka tarjoaa omistamaansa tai muulla perusteella hallussaan olevaa viestintäverkkoa käytettäväksi viestien siirtoon, jakeluun tai tarjolla pitoon. Palveluyrityksellä taas tarkoitetaan yritystä, joka siirtää viestejä hallussaan olevassa tai verkkoyritykseltä käyttöönsä saamassa viestintäverkossa taikka jakelee tai pitää tarjolla viestejä joukkoviestintäverkossa.

Tyypillisiä verkko- ja viestintäpalveluja ovat esimerkiksi puhelinpalvelut, laajakaistapalvelut, sähköpostipalvelut ja joukkoviestintäpalvelut.

2.3.2 Tietoturva

Tietoturva määritellään sähköisen viestinnän tietosuojalaissa. Lain mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

2.3.3 Tietoturvariski

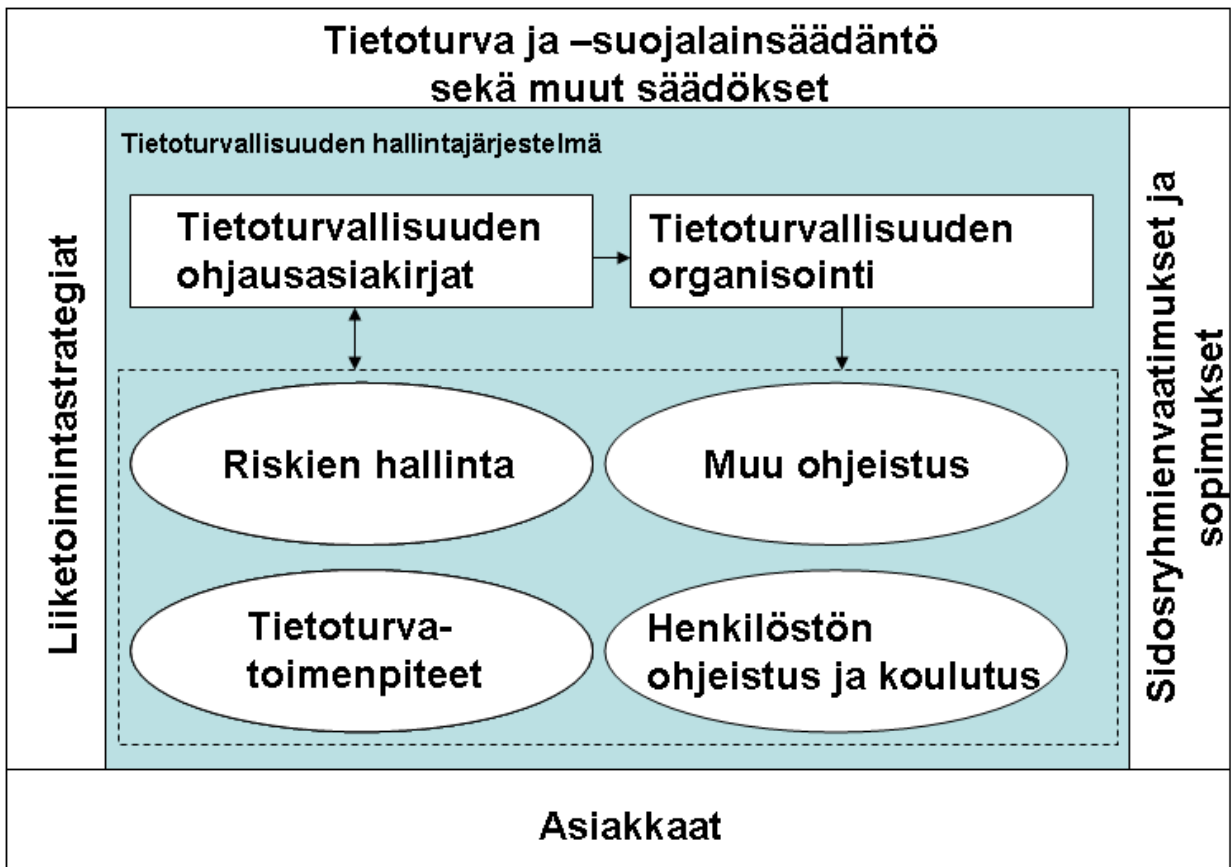
Tietoturvariskeillä tarkoitetaan tässä määräyksessä sellaista tahatonta tai tahallista tekijää, joka vaarantaa teletoiminnan luottamuksellisuutta, eheyttä tai käytettävyyttä. Tietoturvariskin erottaa tietoturvauhasta sillä, että sen todennäköisyyttä ja vaikutuksia on arvioitu.

Tietoturvariskit voivat aiheutua esimerkiksi:

- inhimillisistä virheistä,
- henkilöstölle annettujen ohjeiden puutteista tai noudattamatta jättämisestä,
- varkauksista,
- kapasiteettivajeista,
- laitteiden rikkoutumisista,
- sovellusvirheistä,
- haittaohjelmien leviämisestä,
- tietoliikennehäiriöistä,
- ilkeistä,
- tulipalosta ja
- alihankkijan tai kumppanuusverkostoon kuuluvan toimijan virheistä ja laiminlyönneistä.

2.3.4 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan tässä määräyksessä teleyrityksen johtamisjärjestelmän osaa, joka perustuu riskien arviointiin ja hallintaan. Teleyritykseltä edellytetään oman toimintaympäristön tuntemusta ja sen erityispiirteiden huomioonottamista oman tietoturvallisuuden hallintajärjestelmän kehityksessä. Hallintajärjestelmän vaatimukset tulevat liiketoimintastrategian lisäksi yleensä tietoturva ja -suojalainsäädännöstä, Viestintäviraston antamista määräyksistä, muista säädöksistä sekä asiakkaiden ja sidosryhmien vaatimuksista ja sopimuksista.



Teleyrityksen tietoturvasta huolehtimisen vaatimukset tulevat tietoturva ja -suojalainsäädännöstä, sekä muista säädöksistä esimerkiksi:

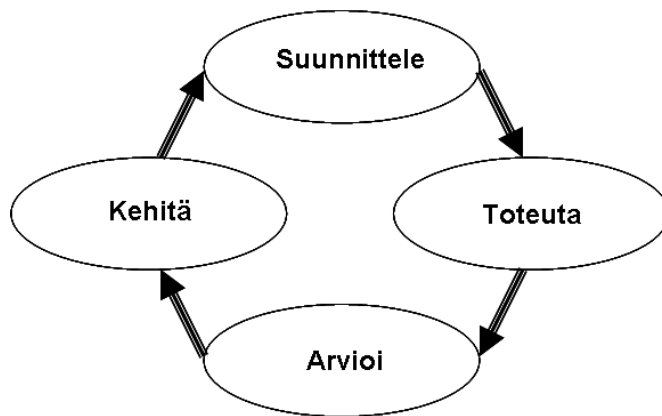
- viestintämarkkinalaki,
- sähköisen viestinnän tietosuojalaki ja
- viestintäviraston määräys 47/2009 M.

Teleyrityksen toimintaan saattaa kohdistua myös muita vaatimuksia tietoturvan osalta, kuten esimerkiksi:

- asiakkaiden vaatimukset,
- ISO 27000 standardiperhe,
- PCI DSS,
- HIPAA,
- SOX,
- EuroSOX,
- VAHTI-ohjeet ja
- muiden maiden lainsäädäntö.

Hallintajärjestelmän tarkoituksena on toimia tietoturvallisuuden kehittämisen, suunnittelun, toteutuksen ja arvioinnin tukena.

Tietoturvallisuuden hallintajärjestelmää kuvataan yleisesti esitettynä nelivaiheisena prosessina:

**Suunnitteluvaihe:**

Suunnitteluvaiheessa luodaan politiikat, määritellään tavoitteet ja kohteet sekä tarvittavat toiminnot tietoturvallisuuden osalta.

Toteutusvaihe:

Toteutusvaiheessa sovelletaan tietoturvapoliitikoita, -kontroleja ja -toimintoja.

Arviointivaihe:

Arviointivaiheessa mitataan toimenpiteiden vaikutuksia suunnitteluvaiheessa määriteltyihin tavoitteisiin, politiikkoihin ja käytännön kokemuksiin.

Kehitysvaihe:

Kehitysvaiheessa kehitetään tietoturvallisuuden hallintajärjestelmää arviointivaiheen tulosten pohjalta. Kehityskohteita voivat olla esimerkiksi tietoturvapoliitikat ja tietoturvatoiminnot.

3 PYKÄLÄKOHTAISET PERUSTELUT JA SOVELTAMISOHJEET

Tässä luvussa käydään läpi pykäläkohtaisesti pykälän perustelut sekä sen soveltamissuosituksukset.

3.1 1 § Soveltamisala

Tätä määräystä sovelletaan teleyritysten yleisten verkko- ja viestintäpalvelujen toteuttamiseen liittyvään toimintaan. Määräyksen soveltamisala kattaa esimerkiksi internetyhteyspalveluiden, sähköpostipalveluiden ja viestintämarkkinalain mukaisten puhepalveluiden tarjonnan. Määräystä sovelletaan myös merkitykseltään vähäiseen teletoimintaan [6].

Tätä lakia ei sovelleta viranomaistoimintaan viestintämarkkinalaissa tarkoitetussa viranomaisverkossa tai muussa yleiseen järjestykseen ja turvallisuuteen, maanpuolustukseen, pelastustehtäviin, väestönsuojeluun tai maaliikenteen, meriliikenteen, raideliikenteen taikka ilmailiikenteen turvallisuuteen liittyvien tarpeiden vuoksi rakennetussa viestintäverkossa. Määräystä ei

myöskään sovelleta viestintäverkkojen tai -palveluiden väliaikaiseen tarjontaan. Väliaikaisuudella tarkoitetaan pituudeltaan enintään kahden kuukauden pituisia yhtenäisiä jaksoja.

Määräyksen soveltamisala rajoittuu teletoimintaan, eikä kata sellaisia toimintoja, joilla ei ole suoranaista vaikutusta viestintäpalveluiden ja -verkkojen toimintaan eikä loppukäyttäjien tietosuojaan tai -turvaan.

3.2 2 § Tietoturvallisuuden organisointi

Perustelut:

Tietojen, tietojärjestelmien ja toimintaedellytysten turvaaminen edellyttää tietoturvatointojen tehokasta organisointia yrityksessä. Perusedellytyksenä on, että tietoturvatointojen vastuut ja velvollisuudet on määritelty.

Soveltaminen:

Tietoturvallisuuden hallintajärjestelmään tulee sisällyttää ylimmän johdon näkemys siitä, miten tietoturvallisuuden vastuut jakautuvat organisaatiossa. Tietoturvallisuuden vastuut ja velvollisuudet voivat olla sekä hallinnollisia vastuita että operatiivisia vastuita. Tietoturvastuita on syytä tarkistaa erityisesti silloin kun organisaatiossa tapahtuu muutoksia. Kysymyksessä voi olla esimerkiksi henkilöstössä tapahtunut muutos tai yritysjärjestelyn toimintaympäristöön aiheuttama muutos.

Tietoturvallisuuden vastuut voivat olla jaoteltuina ryhmiin. Hallinnollisen vastuun osalta voidaan esimerkkinä mainita tietoturvallisuusryhmä. Operatiivisista ryhmistä esimerkkejä ovat taas abuse- ja cert/csirt -ryhmät.

Esimerkkejä hallinnollisista tietoturvallisuusvastuista ovat tietoturvallisuuden hallintajärjestelmän ja ohjausasiakirjojen kehittäminen, yrityksen tietoturvallisuustilannetta kuvaavan seurantajärjestelmän ylläpitäminen, tietoturvallisuusasioiden huomioiminen riskienhallinnassa ja jatkuvuussuunnittelussa, asiaan kuuluvien tietojärjestelmien ylläpitäminen ja kehittämien sekä tietoturvallisuustoimintojen ja -investointien oikeasuhtainen resursointi ja tietoturvallisuusasioiden huomioiminen erityisesti avaintoimintojen henkilökunnan koulutuksessa.

Koska nämä vastuut koskettavat useita yrityksen johtamisjärjestelmän osa-alueita, on suositeltavaa ohjata ja valvoa tietoturvallisuusvastuiden toteutumista koordinoitulla tavalla. Toimivan koordinoinnin merkitys on sitä tärkeämpi, mitä laajemmin tietoturvallisuusvastuut on yrityksen organisaatiossa hajautettu. Yrityksen koosta riippuen tietoturvallisuusasioiden kehittäminen ja seuranta tulee olla vastuutettu yhdelle tai useammalle tietoturvallisuusvastaavalle. Tietoturvallisuusasioita tulee käsitellä osana normaalia johdon raportointia.

Tietoturvaloukkaustapausten koordinoitua ensivasteen toiminnasta ja ilmoitusyhteyspisteen ylläpidosta käytetään joissakin yhteyksissä nimityksiä CERT (Computer Emergency Response Team) - tai CSIRT (Computer Security Incident Response Team)-toiminta. Internet-palveluiden tarjonnan yhteydessä asiakkaiden ja ulkoisten sidosryhmien tietoturvaloukkaustapauksiin liittyvien tapausten yhteys- ja palvelupisteeksi tarkoitettua toimintoa on puolestaan perinteisesti kutsuttu Abuse-toiminnoksi.

Yksittäisiin telepalveluihin liittyvistä tietoturvaloukkausten käsittelyvalmiuksista määrätään tarvittaessa erikseen. Teleyrityksellä on kuitenkin aina oltava perusvalmius omaan toimintaansa kohdistuvien ja merkittävällä tavalla asiakkaisiin vaikuttavien tietoturvaloukkausten ja -riskien hallinnoimiseksi.

Hallinnollisilla vastuilla voidaan esimerkiksi tarkoittaa vastuuta:

- tietoturvapoliitikan suunnittelusta,
- henkilöstön tietoturvakoulutuksen suunnittelusta,
- teleyrityksen oman tietoturvatason seuraamisesta,
- riskien hallinnan suunnittelusta ja organisoinnista ja
- tietoturvaa parantavien hankkeiden käsittelystä ja suunnittelusta.

3.3 3 § Tietoturvallisuuden ohjausasiakirjat

Perustelut:

Tietoturva on osa teleyrityksen tarjoaman teletoiminnan laatua. Tietoturvallisuuden ohjausasiakirjat ovat tietoturvallisuuden perusdokumentteja, joilla organisaation johto osoittaa tietoturvallisuuden tahtotilan ja yleiset periaatteet. Dokumentit luovat perustan järjestelmälliselle tietoturvakehitykselle ja tietoturvan hallinnalle, sekä auttavat tietoturvaluusinvestointien kohdentamisessa.

Soveltaminen:

Teleyrityksen on suunniteltava tietoturvallisuuden ohjausasiakirjat omien riskiensä ja tarpeidensa mukaan. Esimerkiksi teleyrityksen tietoturvaryhmä tai muu riittävän laaja edustus organisaatiosta valmistelee asiakirjat johdon hyväksymistä varten. Asiakirjat valmistellut toimija voi myös huolehtia niiden julkaisemisesta ja tarkoituksenmukaisesta tiedottamisesta kaikille organisaation työntekijöille. Ohjausasiakirjojen tulee olla helposti kaikkien työntekijöiden saatavilla, esimerkiksi organisaation intranet-sivujen kautta. Lisäksi asiakirjojen tulee olla osana uuden henkilön perehdytysohjelmaa. Teleyrityksen on huolehdittava, että asiakirjoissa esitetyt tietoturvallisuuden pääperiaatteiden noudattamista valvotaan.

Tietoturvallisuuden ohjausasiakirjoista tulee ilmetä seuraavat asiat teleyrityksen teletoimintana pidettävän toiminnan osalta:

- tietoturvatavoitteet,
- vastuut tietoturvasta huolehtimiselle,
- tietoturvallisuusorganisaatio ja
- keinot organisaation oman tietoturvallisuuden ylläpitämiseksi ja kehittämiseksi esimerkiksi sisäisten auditointien osalta.

Teleyrityksellä on oltava kirjallisesti dokumentoituna se, miten seuraavat erityysoa-alueet on käytännössä huomioitu ja toteutettu niiltä osin, kuin ne ovat soveltuvia teleyrityksen omaan teletoimintaan:

- Henkilöstöturvallisuus
 - Henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet.
 - Henkilöstön tietoturvaosaaminen ja sen kehittäminen.
 - Avainhenkilöriskien kartoitus mahdollisine taustatarkastuksineen.
 - Teletoiminnan kannalta vaarallisten vastuu- ja tehtäväkokonaisuuksien estäminen.
 - Ohjeet työsuhteen päättyessä noudatettavasta menettelystä.
- Laitteisto-, ja ohjelmistoturvallisuus
 - Riittävä dokumentaatio havaitun haavoittuvuuden korjauksen kohdentamiseksi.
 - Varaosien saanti.
 - Yleinen järjestelmien muutosten hallintaprosessi.
- Tietoliikenneturvallisuus
 - Tietoliikenneturvallisuutta koskevia vaatimuksia käsitellään tarkemmin palvelukohtaisissa määräyksissä, kuten sähköpostipalvelujen tietoturvasta ja toimivuudesta (M11)[4] ja internet-yhteyspalvelujen tietoturvasta ja toimivuudesta annetuissa määräyksissä (M13)[5].
- Tietoaineistoturvallisuus
 - Tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistaminen: Miten tiedot luokitellaan ja miten henkilöstö ohjeistetaan tietojen käsittelystä.
- Käyttöturvallisuus
 - Käyttöoikeusrekisterin ylläpitovastuut: käyttöoikeuksien jakaminen, muuttaminen ja poistaminen.
 - Käyttöoikeuksien kasaantumisen estäminen.
 - Asiaankuulumattomien pääsyn estäminen viestintäpalveluiden toteuttamiseen liittyviin hallinta- ja konfiguraatietietoihin sekä teleyrityksen asiakkaiden veloitus-, tilaaja- ja lokitietoihin.
- Tietoturvaloukkauksiin ja väärinkäyttöihin puuttuminen
 - Toimintavastuut tietoturvallisuuden kannalta merkittävien tapahtumien havaitsemiseen ja niihin puuttumiseen.
 - Toimintaohjeet ja prosessit tietoturvaongelmista toipumiseksi.
 - Vakavuuden arviointi.
 - Viranomaisilmoitukset.
 - Poikkeamista tiedottaminen.

- o Poikkeaman jälkeinen toiminta.
- o Henkilöstön väärinkäytökset ja ohjeistuksen vastaiset toimet.

Fyysisen turvallisuuden osalta on tarkemmin säädetty määräyksessä Viestintävirasto M54. Tietoturvaloukkausten sekä vika ja häiriötilanteiden ilmiottamisvelvollisuudesta yleisessä teletoiminnassa on säädetty määräyksessä Viestintävirasto M9 [7].

Teleyrityksen tulee lisäksi määritellä riittävän yksityiskohtaiset ohjeet tietoturvallisuuden kannalta olennaisten yksittäisten käytäntöjen osalta. Käytännössä tämä tarkoittaa tarkan ohjeistuksen määrittelemistä muun muassa tunnistamistietojen käsittelystä teletoiminnassa.

Alihankinta- / toimintojen ulkoistamissopimuksissa tulee huolehtia siitä että tietoturva-asteiden rajat on määritelty riittävän tarkasti teleyrityksen ja alihankkijan välillä. Kokonaisvastuu palveluiden tietoturvallisuudesta kuuluu kuitenkin aina teleyritykselle, riippumatta siitä onko toimintoja ulkoistettu vai hoidetaanko ne itse.

Alihankintasopimukseen on syytä sisällyttää viittaukset teletoimintaa koskeviin velvoittaviin säädöksiin ja sanktiot säädösten rikkomisesta.

Huoltovarmuuskeskus on julkaissut suosituksia [8], joihin voidaan viitata sopimuksissa toiminnan jatkuvuuden hallinnan osalta. Nämä suositukset käsittelevät:

- johtamista,
- toiminnan ohjausta,
- henkilöstöä ja henkilöresurssien hallintaa,
- kumppanuuksia ja
- toiminnan jatkuvuuden hallinnan arviointia.

3.4 4 § Riskien hallinta

Perustelut:

Tietoturvallisuuden hallintajärjestelmän yksi tärkeimmistä komponenteista on tehokas riskienhallinta. Sillä tarkoitetaan yleensä yrityksen liiketoimintaan liittyvien merkittävien riskien tunnistamista, tunnistamisen jälkeistä riskien arviointia ja hallitsemistoimenpiteitä sekä toimenpiteiden toteuttamisen valvontaa. Hallintajärjestelmän päätehtävänä on suojella organisaatiota ja sen kykyä suorittaa sille annettuja tehtäviä normaali-, normaaliolojen häiriö- ja poikkeusoloissa taloudelliset seikat huomioon ottaen. Riskienhallinta voi olla osa yrityksen valmius- tai jatkuvuussuunnittelua.

Teleyritysten varautumisvelvollisuudesta säädetään Viestintämarkkinalain 90 §:ssä ja 128 §:ssä [9].

Viestintämarkkinalain 90 §:ssä on asetettu teleyrityksille velvollisuus varautua poikkeusoloihin. Teleyrityksen on valmiussuunnittelulla ja poikkeusoloihin varautumisella huolehdittava siitä, että sen toiminta jatkuu mahdollisimman häiriöttömästi myös valmiuslaissa [10] tarkoitetuissa poikkeusoloissa sekä normaaliolojen häiriötilanteissa.

Viestintämarkkinalain 128 §:n mukaan yleiset viestintäverkot ja -palvelut sekä niihin liitettävät viestintäverkot ja -palvelut on suunniteltava, rakennettava ja ylläpidettävä siten, että ne toimivat mahdollisimman luotettavasti myös valmiuslain tarkoittamissa poikkeusoloissa ja normaaliolojen häiriötilanteissa ja että pääsy hätäpalveluihin on turvattu myös verkon häiriötilanteissa mahdollisimman luotettavasti.

Riskien hallinnan tavoitteena on muun muassa:

- nopeuttaa teletoiminnan tietoturvaongelmista toipumista,
- vähentää teletoiminnan tietoturvaongelmista aiheutuneita kustannuksia ja vahinkoja,
- kohdentaa teletoiminnan tietoturvallisuutta parantavia investointeja,
- teletoiminnan laadun ja tuottavuuden parantaminen,
- teletoimintaan kohdistuvien riskien hallinnan taloudellinen optimointi ja
- teletoimintaan kohdistuvien riskien toteutumisen ennaltaehkäisy.

Riskien hallinnan vaatimuksilla pyritään varmistamaan se, että teleyritys on tietoinen riskien toteutumisen aiheuttamista seurauksista ja ovatko riskiä pienentävät toimenpiteet riittäviä.

Soveltaminen:

Riskien hallinnasta on laadittu mm. seuraavia standardeja ja julkaisuja:

- ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security. [11],
- ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management [12],
- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology [13],
- Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools [14],
- COSO ERM (Enterprise Risk Management - Integrated Framework (2004)) [15],
- BS 31100:2008, Risk management. Code of practice [16],
- ISO 31000 Risk management -- Principles and guidelines [17],
- The Institute of Risk Management (IRM), Risk Management Standard [18] ja
- PK-RH:n Pk-yrityksien riskien hallinta [19].

Tässä määräyksessä ei aseteta velvoitetta tietyn standardin noudattamiselle. Riskienhallintamallit vaihtelevat yhtiöittäin, eikä yhtä jokaiselle sopivaa mallia ole olemassa. Keskeistä on sitoa

riskienhallintajärjestelmän tavoitteet yhtiön toiminnallisiin tavoitteisiin ja pitää huolta yhtiön johdon tuesta.

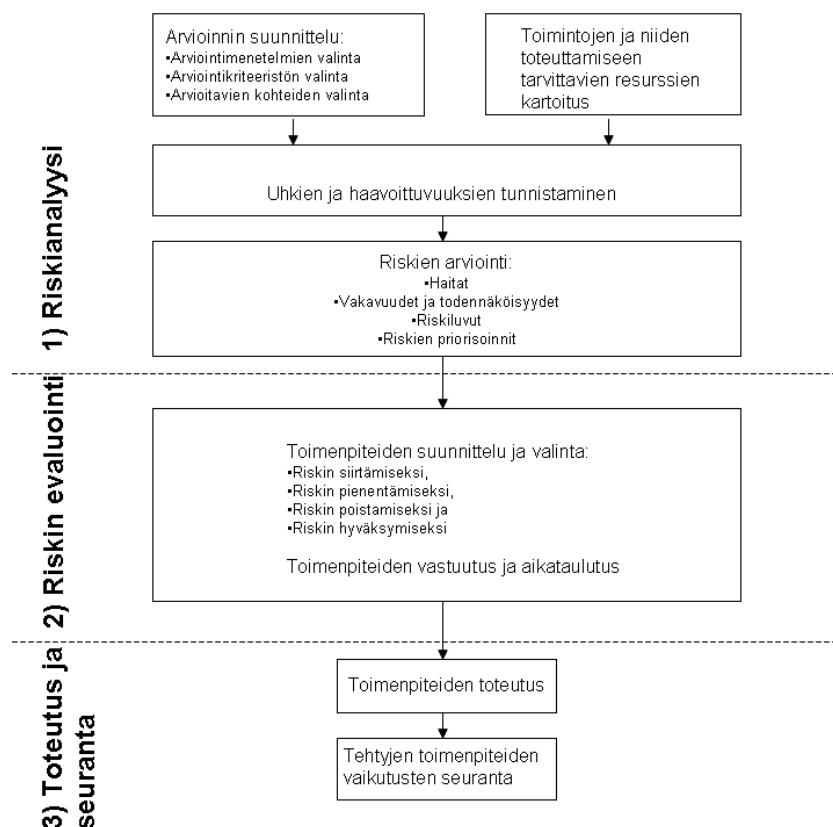
Minimivaatimuksena riskien hallinnan osalta voidaan pitää, että:

- Teleyritys on luokitellut teletoiminnan kannalta tärkeimmät ja kriittisimmät toiminnot, prosessit ja järjestelmät.
- Teletoimintaan liittyvät tietoturvallisuus riskit on kartoitettu.
- Teleyritys seuraa säännöllisesti omaan teletoimintaansa liittyvää tietoturvallisuuden tasoa. Tietoturvallisuuden tasoa voidaan seurata esimerkiksi pistokokeiden, tietoturvallisuustarkastusten ja tietoturvallisuusauditointien avulla.

Viestintäverkkojen ja -palveluiden toimivuuden osalta tärkeysluokittelusta on määrätty Viestintäviraston määräyksessä 54/2008 M. Teleyritykset voivat käyttää määräyksen 54 perusteella tehtyä tärkeysluokittelua loppukäyttäjän kokeman palvelun käytettävyyteen liittyvien riskien kartoituksen osalta.

Teletoimintaan liittyvät tietoturvallisuusriskit on kartoitettava teletoiminnan kannalta tärkeimpien ja kriittisimpien toimintojen, prosessien ja järjestelmien osalta ja toimenpiteet havaittujen riskien pienentämiseksi, poistamiseksi ja siirtämiseksi on dokumentoitava.

Riskien hallinta voidaan karkeasti jakaa kolmeen eri vaiheeseen:



3.4.1 Riskianalyysi

Riskianalyysillä tarkoitetaan niitä järjestelmällisiä toimenpiteitä, joilla pyritään tunnistamaan teletoiminnan toteuttamista vaarantavia tietoturvallisuuden uhkia ja haavoittuvuuksia, sekä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Riskianalyysi on suunniteltava, toteutettava ja dokumentoitava laadukkaasti. Riskianalyysi tulisi tehdä kohteelle ennalta määrättyyn tavoitetasoon nähden. Tällä tarkoitetaan esimerkiksi Viestintäviraston määräyksessä tai asiakassopimuksessa asetettua vaatimusta viestintäpalvelun käytettävyydelle. Riskianalyysillä haetaan erityisesti niitä uhkia jotka vaarantavat kohteelle asetetun tavoitteen täyttymisen.

Riskianalyysi koostuu viidestä osa-alueesta, jotka ovat:

- arvioinnin suunnittelu,
- teletoimintaa vaarantavien tietoturva-uhkien tunnistaminen,
- alttiina olevien järjestelmien ja toimintojen tunnistaminen,
- riskien vakavuuksien ja todennäköisyyksien arviointi ja
- riskien priorisointi.

Riskianalyysin vastaa seuraaviin kysymyksiin tilannetta tarkasteltavassa kohteessa:

- mitä kaikkea voi tapahtua? (Uhat),
- miksi uhka voi toteutua? (Haavoittuvuudet),
- mikä on uhan toteutumisen todennäköisyys ja mitkä sen toteutumisesta aiheutuvat seuraukset teletoiminnan kannalta? (Todennäköisyys ja vakavuus),
- miten suuri on aiheutuva riski? (Riskiluku) ja
- mitkä ovat suurimmat riskit (Priorisointi)?

Riskianalyysin keskeisimpinä tavoitteina on:

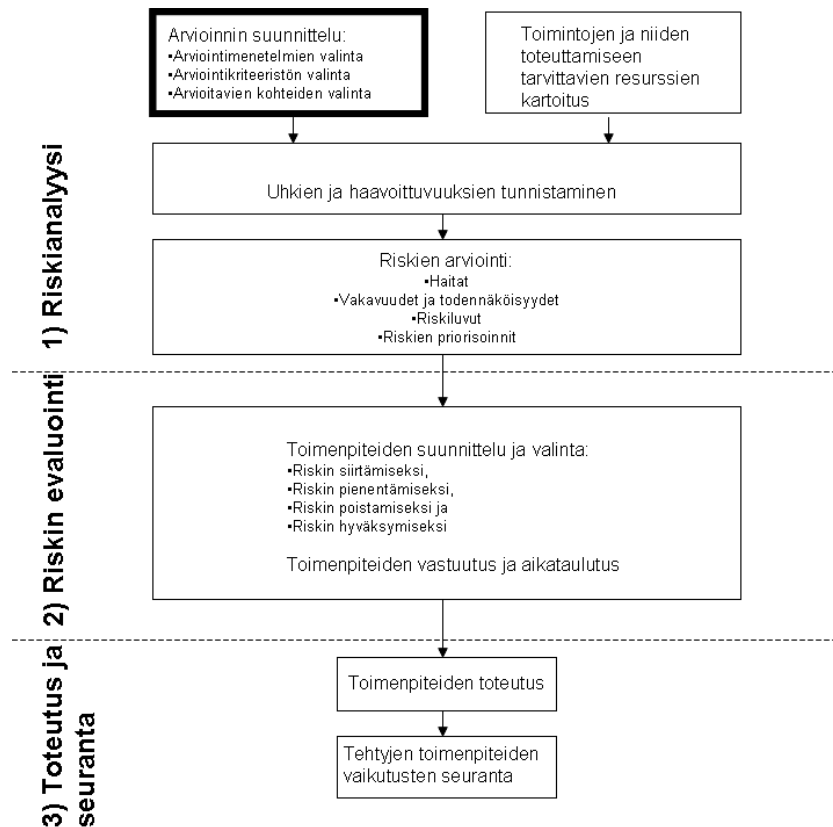
- tukea tietoturvallisuusjohtamista ja investointien kohdentamista,
- tietoturvallisuuden parantaminen ja
- tunnistaa teletoimintaan vaikuttavat tietoturvallisuusriskit ja niiden vakavuudet.

Riskianalyysin tavoitteista johtuen riskianalyysin tekijöiden olisi syytä tuntea hyvin riskianalyysin kohteen toiminta, toiminnan tavoitteet ja siihen kohdistuvat vaatimukset.

3.4.1.1 Riskien arvioinnin suunnittelu

Tietoturvariskien arviointi on tärkeä osa teletoiminnan tietoturvallisuuden järjestelmällistä kehittämistä. Arvioinnin avulla selvitetään teletoiminnan kannalta tärkeät toiminnot, tiedot ja järjestelmät.

Pohja hyvälle riskianalyysille luodaan jo riskianalyysin suunnittelu- ja valmisteluvaiheessa, jolloin tunnistetaan arvioitavan kohteen toiminnalliset tavoitteet, rajataan analyysin ulkopuolelle jäävät osa-alueet ja valitaan parhaiten soveltuva analyysimenetelmä. Perusteellisella suunnittelulla ja valmistelulla voidaan varmistaa riskien arviointiin varattujen resurssien tehokas käyttö, riskianalyysin tavoitteiden täyttyminen sekä parhaan mahdollisen toiminnallisen hyödyn saavuttaminen.



Riskiarvoinnin suunnittelun tulee sisältää käytettävät riskien arviointimenetelmät, riskien arvioinnin kriteerit ja arvioinnin tavoitteet sekä aihealueet joihin arviointi kohdistuu. Esimerkiksi henkilöriskien arviointiin parhaiten soveltuvat menetelmät eivät välttämättä ole samoja kuin mitä tulee soveltaa tietojärjestelmien riskien arviointiin.

Ennen arvioinnin aloittamista tulee selvittää arvioinnin tarkoitus, kohteen toiminnalliset tavoitteet, arvioinnin toteutustapa ja aikataulu. Riskien arvioinnin tavoitteet voidaan sitoa esimerkiksi arviointien määrään, aikatauluun tai arvioinnin tuottamien parannustoimenpiteiden määrään.

Arvioinnin suunnittelussa on syytä ottaa huomioon teletoiminnan laajuus ja organisaation mahdollisuudet. Esimerkiksi jos teleyrityksen liiketoimintana on tarjota ainoastaan pienimuotoista sähköpostipalvelua, voi riskien arviointimenetelmät olla hyvinkin pelkistettyjä. Minimivaatimus

riskien arvioinnin suunnittelun kannalta on kuitenkin se, että pelkistetykin arviointimenetelmät on dokumentoitu.

Riskien arvioinnissa kannattaa hyödyntää esimerkiksi aiempia tietoturvaluustarkasteluja, "läheltä piti" tilanteista saatavilla olevaa tietoa ja muuta tietoturvaluuteen liittyvää aineistoa.

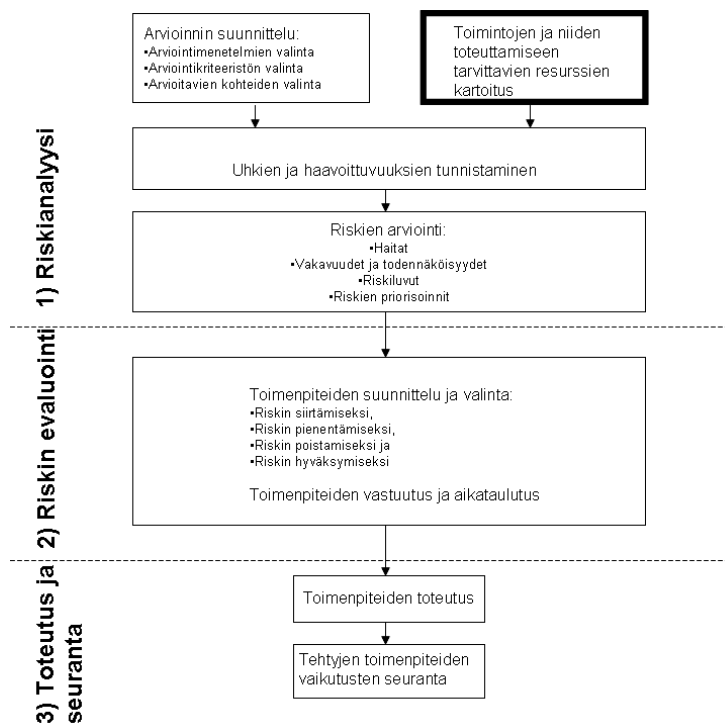
Teleyrityksen tulee varmistaa, että arviointiin osallistuvilla henkilöillä on riittävä tietämys käytettävästä riskien arviointimenetelmästä.

Suunnitteluvaiheessa tulee sopia myös riskien arvioinnin kirjaamisesta, tallentamisesta ja arvioinnin tulosten käsittelystä.

3.4.1.2 Toimintojen ja niiden toteuttamiseen tarvittavien resurssien kartoitus

Järjestelmien ja toimintojen tunnistamisen perusedellytys on, että teletoiminnan kannalta keskeisten järjestelmien ja toimintojen kartoitus on tehty ainakin seuraavilta osa-alueilta:

- laitetilat,
- laitteistot ja ohjelmistot,
- tietoliikenneyhteydet,
- tietoaineistot ja
- järjestelmien ylläpito- ja tukihenkilöt.



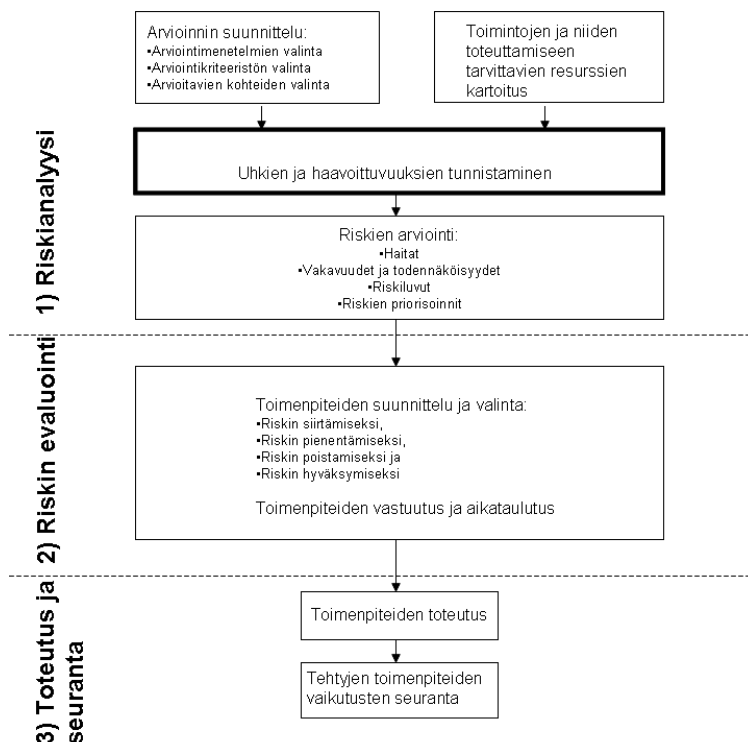
Teleyritykset voivat käyttää määräyksen 54 perusteella tehtyä tärkeysluokittelua loppukäyttäjän kokeman palvelun käytettävyyteen liittyvien riskien kartoitukseen. Määräyksessä 47 edellytetään

lisäksi teleyritysten kartoittavan riskejä tietoaaineistoturvallisuuden näkökulmasta arkaluontoisia tietoja käsittelevissä järjestelmissä. Tällaisia järjestelmiä ovat esimerkiksi laskutus-, telekuuntelu- ja televalvontajärjestelmät.

Kartoitus parantaa teleyrityksen mahdollisuuksia arvioida tietojärjestelmien ja käsiteltävien tietojen kriittisyyttä, arkaluontoisuutta ja tarvittavaa resursointia. Lisäksi kartoitus helpottaa tietoturvallisuutta parantavien toimenpiteiden kohdentamista.

3.4.1.3 Uhkien tunnistaminen

Uhkalla tarkoitetaan tässä yhteydessä teletoimintaan vaarantavaa tilannetta, jonka todennäköisyyttä tai vakavuutta ei ole arvioitu. Uhkien määrittely riippuu valittavasta riskianalysikohteesta ja rajauksesta. Uhkien määrittelyssä tulee hyödyntää riskianalyysin kohteeseen tehtyjen tietoturvallisuusauditointien tuloksia sekä aikaisemmin realisoituneita riskejä tai tietoturvapoikkeamia. Tietoturvallisuusauditoinnit voidaan toteuttaa joko talon sisäisinä auditointeina tai ne voidaan ostaa palveluna ulkopuoliselta toimittajalta. Auditointeja olisi suositeltavaa tehdä kohteen kriittisyydestä riippuen 6kk - 2 vuoden välein ja aina silloin kun arvioitavassa kohteessa tapahtuu merkittäviä muutoksia.



Uhkan toteutumiseen liittyy aina jokin haavoittuvuus eli alttius teletoimintaa uhkaavalle tekijälle. Haavoittuvuudet voivat olla joko teknisiä tai ei teknisiä, ja ne voivat liittyä esimerkiksi:

- laitteistoihin ja ohjelmistoihin,
- prosesseihin ja

- henkilöstöön.

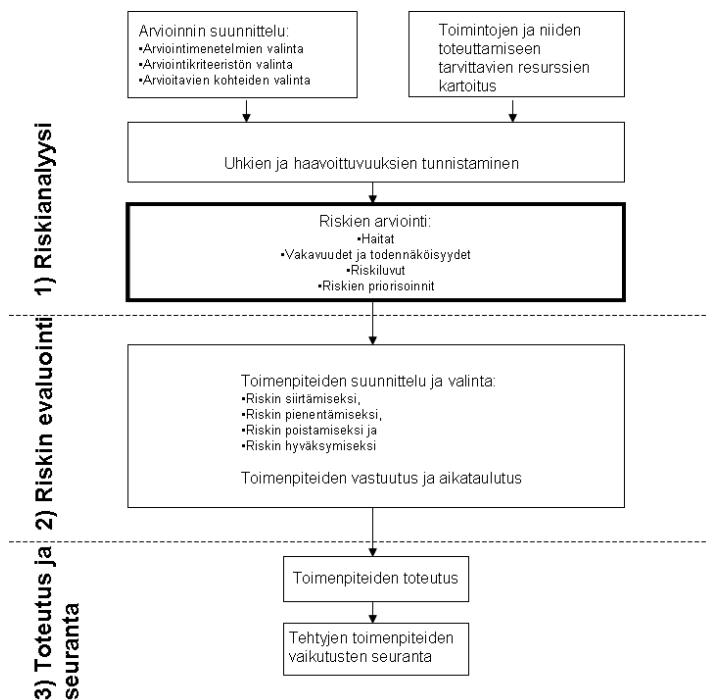
Laitteistoihin ja ohjelmistoihin liittyvällä uhalla tarkoitetaan esimerkiksi sitä, että jokin häiriöohjelma estää ko. laitteen tai ohjelmiston toiminnan.

Prosesseihin liittyvillä uhalla voidaan tarkoittaa esimerkiksi edellä mainitun häiriöohjelmatarjunnan selviämisen viivästymistä. Haavoittuvuutena voi olla esimerkiksi sovittujen toimintatapojen puuttuminen.

Henkilöstöön liittyvä uhka voi olla, että jokin palvelu jää ilman vastuuhenkilöä. Tähän liittyvä haavoittuvuus on esimerkiksi vastuuhenkilön sairaus tai irtisanoutuminen.

3.4.1.4 Riskien arviointi

Riskien arvioinnilla tarkoitetaan tunnistetun uhan vakavuuden ja sen toteutumisen todennäköisyyden arviointia.



Vakavuus:

Vakavuudella tarkoitetaan uhan toteutumisen seurauksia sille toiminnolle johon uhka kohdistuu. Vakavuus saattaa kasvaa ajan myötä jolloin palvelun hetkellisen toimimattomuuden vakavuus voi olla pienempi kuin, että palvelu on toimimaton pidemmän aikaa.

Todennäköisyys:

Todennäköisyydellä tarkoitetaan uhan toteutumisen todennäköisyyttä.

Todennäköisyyttä arvioitaessa tulee ottaa huomioon jo tehdyt toimenpiteet uhan toteutumisen ehkäisemiseksi.

Vakavuutta ja todennäköisyyttä voidaan kuvata esimerkiksi luvuin asteikolla 0-3, jossa luku 0 tarkoittaa ei vaikutusta tai todennäköisyyttä ja luku 3 tarkoittaa erittäin merkittävää vaikutusta tai toteutumisen todennäköisyyttä.

Riskiluku:

Riskejä kuvataan yleensä riskiluvulla, joka voidaan muodostaa esimerkiksi uhan vakavuuden ja uhan todennäköisyyden kertolaskun tuloksena. Riskiluvun perusteella voidaan riskit tärkeysluokitella uhan todennäköisyyden ja vakavuuden perusteella.

Riskien luokittelu:

Analysoidut riskit voidaan priorisoida esimerkiksi riskiluvun perusteella. Riskien priorisointi niiden liiketoiminnalle aiheuttamien vaikutusten kannalta on erityisesti suurimmissa yrityksissä yleisesti käytetty menetelmä. Pääasia on kuitenkin se, että havaitut riskit on luokiteltu jollain tavoin käytössä olevien resurssien kohdistamiseksi vakavimpiin riskeihin.

Riskien luokittelu toimii suosituksena, joka tukee päätöksen tekoa korjaavia toimenpiteitä suunniteltaessa ja kohdennettaessa. Riskien luokittelu voi yksinkertaisimmillaan esimerkiksi seuraavanlainen uhan todennäköisyyden ja vakavuuden asteikon ollessa 0-3:

riskiluku	suositus
[0-1]	Merkityksetön riski. Ei edellytä toimenpiteitä.
[2]	Hyväksyttävä riski. Päätös riskin hyväksymisestä on dokumentoitava.
[3-4]	Kohtalainen riski: Riski voidaan hyväksyä väliaikaisesti. Suositellaan ryhtymistä toimenpiteisiin riskin pienentämiseksi käytettävissä olevien resurssien puitteissa.
[6]	Merkittävä riski: Suositellaan ryhtymistä toimenpiteisiin mahdollisimman pian riskin pienentämiseksi.
[9]	Sietämätön riski: Suositellaan ryhtymistä välittömiin toimenpiteisiin riskin pienentämiseksi.

Dokumentointi:

Dokumentoinnin tulee sisältää sellaiset tiedot, joiden perusteella voidaan jälkikäteen arvioida riskien hallinnan toteutumista ja riskikartoituksen ja toimenpiteiden riittävyyttä. Dokumentoinnin tulee sisältää ainakin seuraavat asiat:

- riskianalyysi
 - Riskianalyysin tavoitteet.
 - Riskianalyysin rajaukset.
 - Riskianalyysin tuotokset.
 - Riskianalyysin loppuraportti.
- riskien evaluointi
 - Lista suurimmista riskeistä.
 - Lista kriittisimmistä puutteista.

3.4.2 Riskin evaluointi

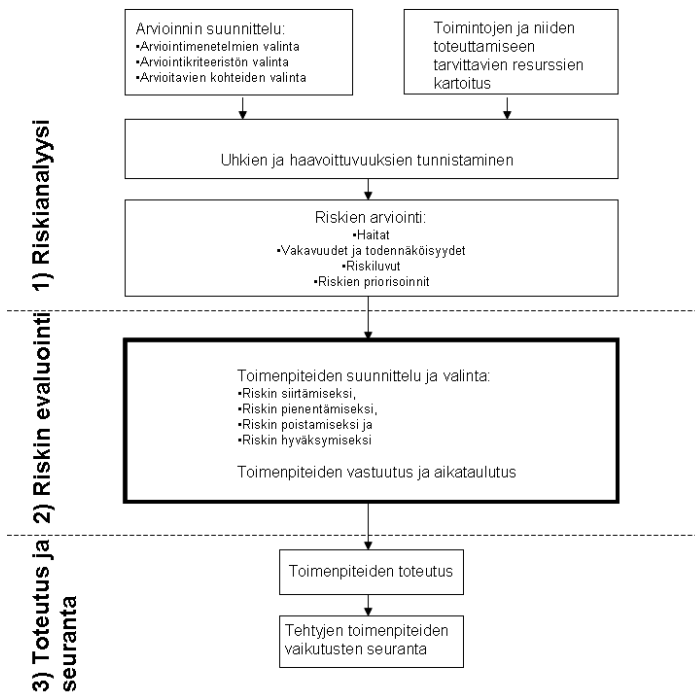
Riskin evaluoinnissa nostetaan esiin keskeisimmät kehittämistarpeet riskien arvioinnin tulosten pohjalta. Tästä riskien arvioinnin yhteenvedosta käy ilmi muun muassa:

- suurimmat riskit,
- kriittisimmät puutteet ja
- lisäselvitysten kohteet.

3.4.2.1 Toimenpiteiden suunnittelu ja valinta

Riskianalyysin pohjautuvien tietoturvatoinenpiteiden valinnassa on syytä ottaa huomioon velvoittavien säädösten asettamat vaatimukset, ratkaisujen kustannukset, henkilöresurssit, yrityksen riskinottohalukkuus ja riskin toteutumisesta aiheutuvat tappiot. Näillä tarkoitetaan toimenpiteitä:

- riskin siirtämiseksi,
- riskin pienentämiseksi,
- riskin välttämiseksi,
- riskin hyväksymiseksi,
- riskien ennaltaehkäisemiseksi ja
- riskin havainnoinnin parantamiseksi.



Jos merkittävää riskiä ei voida kokonaan poistaa, tulee teleyrityksen tehdä toipumissuunnitelma riskin toteutumisen varalle.

Riskien siirtämisellä tarkoitetaan riskin toteutumisesta aiheutuvien kustannusten siirtämistä kolmannelle osapuolelle esimerkiksi vakuutuksilla tai sopimuksilla. Riskin toteutuessa kokonaisvastuu teletoiminnan tietoturvasta säilyy joka tapauksessa teleyrityksellä.

Riskien pienentämisellä tarkoitetaan vahinkojen ennaltaehkäisyä ja riskin jakamista.

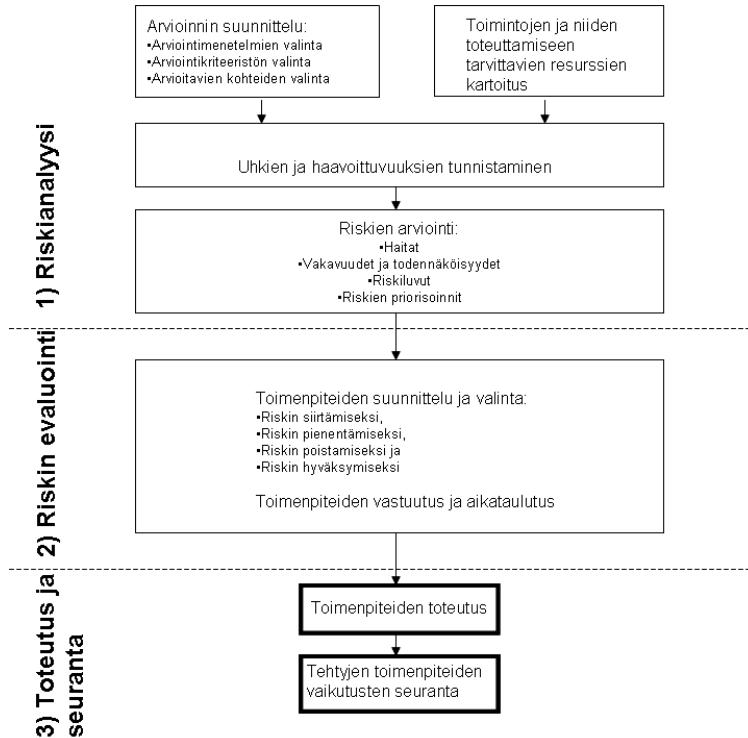
Riskin välttämällä pyritään pääsemään eroon liian suuren riskin omaavasta tuotteesta, palvelusta, sopimuskumppanista tai toiminnasta.

Vaikutuksiltaan vähäiset riskit voidaan usein hyväksyä, jos riskit eivät ole lainsäädännön ja määräysten vastaisia. Usean vähäisen riskin toteutuminen samanaikaisesti voi kuitenkin muuttaa tilannetta merkittävästi esimerkiksi teletoiminnan laadun suhteen. Tehtäessä päätöksiä riskien hyväksymisestä on otettava tapauskohtaisesti huomioon kenen kannalta ja missä olosuhteissa riski on hyväksyttävissä, sekä riskin toteutumisesta aiheutuvat seuraamukset ja kustannukset.

Toiminnon tai palvelun omistajan tulee huolehtia siitä, että riskit tulevat hyväksytyiksi. Päätös riskien hyväksymisestä tapahtuu yrityksen päätäntävaltuuksien mukaisesti.

3.4.2.2 Toimenpiteiden vastuutus ja aikataulutus

Tämä osio liittyy määräyksen 5 §:ään ja se käsitellään tässä dokumentissa kappaleessa 3.5 Tietoturvatoinenpiteet.



3.5 5 § Tietoturvatoinenpiteet

Soveltaminen:

Valituille tietoturvaa parantaville toimenpiteille tulee laatia suunnitelma, jossa on määritelty muun muassa vastuuhenkilöt päätetyille toimenpiteille ja toteutuksille sekä aikataulu niiden seurannalle.

Tietoturvaa parantavia toimenpiteitä riskin siirtämisen osalta ovat esimerkiksi:

- tietyn tuotteen, protokollan tai menetelmän välttäminen,
- epämääräisten sopimuskumppaneiden välttäminen ja
- liian suuren riskin omaavasta toiminnasta luopuminen.

Tietoturvaa parantavia toimenpiteitä riskien pienentämisen osalta ovat esimerkiksi:

- henkilöstön koulutus tietoturvallisuuden osalta,
- toimintaohjeet,
- tietoturvallisuutta parantavien tuotteiden käyttöönottoaminen,
- varajärjestelmät,
- säännölliset tietoturvapäivitykset,
- ajantasaiset varmuuskopiot,
- dokumentaation turvaluokitukset ja
- kulunvalvonta.

Riskien ennalta havainnointia voidaan parantaa esimerkiksi suorittamalla kohteille säännöllisiä auditointeja, ottamalla riskienhallinta mukaan tuotekehitykseen mahdollisimman aikaisessa vaiheessa, henkilöstön tietoturvaluustietoisuuden lisääminen ja ongelmatilanteista raportoinnin ohjeistaminen.

Riskejä voidaan ennaltaehkäistä henkilöriskien osalta esimerkiksi varahenkilöjärjestelyin ja tietojärjestelmien osalta varajärjestelmillä.

Teleyrityksen tulee määritellä yksityiskohtaiset ja riittävät ohjeet tietoturvaluuden kannalta olennaisten yksittäisten käytäntöjen osalta. Nämä ohjeet voivat koskea esimerkiksi seuraavia osa-alueita:

- vierailijakäytännöt,
- kulkuoikeuksien hallinnointi,
- teletoimintaan käytettyjen järjestelmien etäkäyttö ja
- arkaluontoisten tietoaaineistojen käsittely (esim. tunnistamis-, laskutus- ja asiakastiedot).

3.5.1 Tietoaaineistoturvaluus

Teleyrityksessä on oltava käytössä teletoiminnan kannalta tärkeiden tietoaaineistojen käsittelyohje. Käsittelyohjeen tulee kattaa muun muassa seuraavat asiat:

- yleiset periaatteet tietoaaineiston turvaluokan ja luottamuksellisuuden arvioimiseksi ja tietoaaineistojen salassa pysymiseksi,
- käsittely- ja muutosoikeudet tietoaaineiston lukuoikeuksien jakamisesta, muutosoikeuksista sekä näiden oikeuksien jakamisesta,
- luottamuksellisuusluokan määrittäminen,
- tiedon tai asiakirjan julkisuus: esimerkiksi asiasta puhumisesta julkisesti,
- asiakirjan ominaisuudet: paperi, leima ja muut merkinnät
- säilytys ja salaaminen
- tulostaminen ja kopiointi
- vastaanottaminen, jakaminen, lähettäminen ja kuljettaminen,
- tietojen ja asiakirjan käsittelyn dokumentoiminen ja
- asiakirjan arkistointi, käsittely tai käsittelyoikeuksien päättyminen, tietojen ja asiakirjan hävittäminen.

Kaikelle turvaluokitellulle tietoaaineistolle on erikseen määriteltävä käyttäjä- tai käyttäjäryhmäkohtaiset käsittelyoikeudet. Samalla on huolehdittava siitä, että asiaan kuulumattomat eivät pääse käsiksi turvaluokiteltuihin tietoaaineistoihin. Turvaluokiteltujen tietoaaineistojen on kuitenkin oltava niiden käsittelyyn oikeutettujen käytettävissä.

Teleyritysten tietoaaineistojen käsittelyohje voi pohjautua soveltuvin osin esimerkiksi Valtionvarainministeriön valmistelemaan valtioneuvoston tietoaaineistojen käsittelyn tietoturvaluusohjeeseen[20].

Teleyrityksen on huolehdittava, että viestintäverkkojen ja viestintäpalvelujen käytettävyyden kannalta olennaisista tietoaineistoista on ajan tasalla olevat varmuuskopiot, jotka säilytetään lukituissa tiloissa ja erillään kyseisistä laitteista. Varmuuskopiot on voitava ottaa käyttöön alkuperäisen tietoaineiston vaurioituessa esimerkiksi ohjelmistovian, laitevian tai laitetilassa tapahtuneen onnettomuuden jälkeen. Tällaisia tietoaineistoja ovat esimerkiksi käyttäjätiedot ja konfiguraatitiedot.

3.5.2 Väärinkäyttöihin ja tietoturvaluusongelmiin puuttuminen

Teleyrityksellä tulee olla kyky reagoida tietoturvaloukkauksiin ja tietoturvauhkiin, jotka vaikuttavat toisaalta yrityksen kyvyn tuottaa palveluita teleyrityksroolissa sekä toisaalta oleellisella tavalla vaarantavat teleyrityksen asiakkaiden tietoturvaa.

Verkko- ja viestintäpalveluiden väärinkäyttöihin ja tietoturvaluusongelmiin puuttuminen tulee olla organisoitua ja sisältää ainakin seuraavia toimintoja:

- Ohjeiden ja prosessien valmistelu väärinkäytösten ja tietoturvaluusongelmiin puuttumisesta.
- Väärinkäytöksistä ja tietoturvaongelmista raportointi.
- Vastuut ja toiminnot väärinkäytöksien ja tietoturvaongelmien tutkimiselle, esitutkintaan saattamiselle ja niiden vakavuuksien arvioimiselle.
- Vastuut ja toiminnot vahinkojen rajoittamiselle, väärinkäytöksen tai tietoturvaluusongelman poistamiselle, sekä ylemmän johdon tiedottamiselle.
- Viranomaisilmoitukset.
- Vastuut ja toiminnot väärinkäytöksestä tai tietoturvaluusongelmasta toipumiselle.
- Toiminnot tapahtuman uusiutumisen estämiselle.

3.6 6 § Tietoturvaluisuuden hallinnan seuranta

Perustelut:

Uudet tekniikat ja palvelut tuovat mukanaan uusia haasteita viestintäpalveluiden ja -verkkojen tietoturvan osalta. Tietoturvaluisuuden hallinta onkin jatkuvaa, muutoksiin reagoivaa ja osa yrityksen normaalia toimintaa viestintäpalveluiden ja -verkkojen suunnittelusta ylläpitämis-vaiheeseen.

Soveltaminen:

Organisaation johdon on huolehdittava riittävästä resursseista tietoturvaluisuuden hallintajärjestelmän suunnitteluun, toteutukseen, arvioimiseen ja ylläpitämiseen.

Tietoturvaluisuuden hallintajärjestelmää tulee ylläpitää säännöllisesti ja päivittää tarvittaessa. Muutostarpeita tulee tarkastella kerran vuodessa ja aina tarpeen vaatiessa. Tarvetta hallintajärjestelmän muutoksille voi tulla esimerkiksi organisaatiomuutosten tai yrityksen strategiamuutosten yhteydessä.

4 VIITELUETTELO

- [1] Sähköisen viestinnän tietosuojalaki (516/2004 muutoksineen, SVTsL), ajantasainen versio
<http://www.finlex.fi/fi/laki/ajantasa/2004/20040516>
- [2] M54 Määräys viestintäverkkojen ja -palvelujen varmistamisesta
<http://www.ficora.fi/attachments/suomiry/5vB4GW4xt/Viestintavirasto542008M.pdf>
- [3] Information Security Management - Specification With Guidance for Use
<http://www.iso.org/iso/home.htm>
- [4] M11, Määräys sähköpostipalvelujen tietoturvasta ja toimivuudesta
<http://www.ficora.fi/attachments/suomiry/5AWLwAxxQ/Viestintavirasto11A2008M.pdf>
- [5] M13, Määräys Internet-yhteyspalvelujen tietoturvasta ja toimivuudesta
<http://www.ficora.fi/attachments/suomiry/5AWLt8K4m/Viestintavirasto13A2008M.pdf>
- [6] Valtioneuvoston asetus (N:o 675) merkitykseltään vähäisestä teletoiminnasta
<http://www.finlex.fi/fi/laki/kokoelma/2003/20030106.pdf>
- [7] M9, Määräys Tietoturvaloukkausten sekä vika- ja häiriötilanteiden ilmoittamisvelvollisuudesta yleisessä teletoiminnassa
<http://www.ficora.fi/attachments/suomiry/5hw8uQW3c/Viestintavirasto09C2009M.pdf>
- [8] Huoltovarmuuskeskus: Sopimukseen perustuva varautuminen tietoyhteiskuntasektorilla
http://www.huoltovarmuus.fi/documents/3/SOPIVA_julkaisu.pdf
- [9] Viestintämarkkinalaki (93/2003), ajantasainen versio
<http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>
- [10] Valmiuslaki (1080/1991) ajantasainen versio:
[http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search\[type\]=pika&search\[pika\]=valmiuslaki](http://www.finlex.fi/fi/laki/ajantasa/1991/19911080?search[type]=pika&search[pika]=valmiuslaki)
- [11] ISO/IEC TR 13335-3, Information technology - Guidelines for the management of IT Security - Techniques for the management of IT Security
<http://www.iso.org/iso/home.htm>
- [12] ISO/IEC 27005:2009 Information technology - Security techniques - Information security risk management
<http://www.iso.org/iso/home.htm>
- [13] NIST Special Publication 800-30, Risk Management guide for Information Technology Systems, Recommendation of the National Institute of Standards and Technology
<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>
- [14] Enisa: Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools
http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf
- [15] COSO ERM (Enterprise Risk Management - Integrated Framework (2004))
<http://www.coso.org/-ERM.htm>
- [16] BS 31100:2008, Risk management. Code of practice.
<http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030191339>
- [17] ISO 31000 Risk management -- Principles and guidelines
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170
- [18] The Institute of Risk Management (IRM), Risk Management Standard
<http://www.theirm.org/publications/PUstandard.html>

[19] PK-RH:n pk-yrityksen riskienhallinta
www.pk-rh.fi/riskilajit/tietoriskit/tietoriskit

[20] Valtiovarainministeriö: Tietoaineistojen käsittelyn tietoturvallisuusohje
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

5 LIITTEET

5.1 Yksinkertaistettu esimerkki riskien arvioinnista

Tässä yksinkertaistetussa ja rajatussa esimerkissä kuvataan pienen sähköpostipalvelua tarjoavan teleyrityksen riskien hallinta prosessia kappaleessa 3.4 esitetyn mallin pohjalta. Esimerkissä käytetyllä yrityksellä on sähköpostipalvelussa noin 750 asiakasta. Esimerkissä sähköpostipalvelun riskienarviointia on kuvattu vain yhden riskin osalta. Tyypillisesti sähköpostipalveluun kohdistuu monia muitakin riskejä, jotka tulee myös arvioida.

5.1.1.1 Riskianalyysi

Riskianalyysin tavoitteet:

Riskien arvioinnissa pyritään selvittämään sähköpostipalvelun liiketoimintavaikutukset tilanteelle, jossa osaavaa ylläpitohenkilöstöä ei ole saatavilla. Arvioinnissa huomioidaan myös tilanteen taloudellinen vaikutus. Arviointi pohjautuu nykyisten vastuuhenkilöiden ja esimiehen haastatteluihin.

Riskianalyysin rajaukset:

Riskianalyysin kohteena on teleyrityksen asiakkaille tarjottava sähköpostipalvelu, joka muodostaa noin kolmasosan yrityksen kassavirrasta. Tässä analyysissä keskitytään sähköpostipalvelun ylläpitoon. Ylläpidon tehtävänä on varmistaa sähköpostijärjestelmän häiriötön toiminta kaikissa tilanteissa. Henkilöstön saatavuus ja osaaminen ovat edellytyksiä sähköpostijärjestelmän ylläpidolle ja kehittämiselle.

Riskianalyysin tuotokset:

Arviointimenetelmänä käytetään ns. potentiaalisten ongelmien analyysiä.

Arviointikriteeristönä käytetään uhan vakavuuden arvioinnissa asteikkoa 0-3, jossa luku:

- 0 tarkoittaa, ettei uhalla ole merkitystä yrityksen liiketoimintaan,
- 1 tarkoittaa, että uhalla on vähäinen merkitys yrityksen liiketoimintaan,
- 2 tarkoittaa, että uhan merkitys yrityksen liiketoimintaan on merkittävä ja
- 3 tarkoittaa, että uhalla on erittäin merkittävä vaikutus yrityksen liiketoimintaan.

Uhan toteutumisen todennäköisyyttä arvioitaessa käytetään vastaavaa asteikkoa.

Riskit priorisoidaan ns. riskiluvun eli uhan toteutumisen todennäköisyyden ja uhan vakavuuden kertolaskun tulona. Riskiluvun asteikko on 0 - 9, jossa luvut:

- 0-1 tarkoittavat merkityksetöntä riskiä,
- 2 tarkoittaa hyväksyttävää riskiä,
- 3-4 kohtalaista riskiä,
- 6 merkittävää riskiä ja
- 9 sietämätöntä riskiä.

Sähköpostipalvelun ylläpito on nykyisin vastuutettu kahdelle henkilölle, joista toisen määräaikainen työsopimus päättyy kolmen kuukauden kuluttua ja henkilö on ilmoittanut muuttavansa opiskelemaan ulkomaille työsopimuksen päättymisen jälkeen.

Keskeinen uhka on järjestelmän toiminnan häiriintyminen esimerkiksi roskapostimäärän yllättävästä kasvusta johtuen. Toiminnan häiriintyminen näkyy loppuasiakkaille sähköpostiviestien perillemenon viivästymisenä, joka pitkeytyessään voi aiheuttaa merkittävää taloudellista tappiota yritykselle. Pitkeytyminen on todennäköistä, jos osaavaa ylläpitohenkilöstöä ei ole saatavilla.

Haavoittuvuudet:

- Määräaikaisen työntekijän työsuhde päättyy kolmen kuukauden kuluttua.
- Ainoan ylläpitäjän sairastuminen tai muu poissaolo.

Uhan vakavuus: Sähköpostipalvelu muodostaa noin kolmasosan yrityksen kassavirrasta. Sähköpostipalvelun toimivuuden merkitys yrityksen liiketoiminnalle on erittäin merkittävä ja siksi uhan vakavuusluvuksi annetaan arvo 3.

Uhan todennäköisyys: Todennäköisyyttä nostattaa tuleva kesälomakausi, jolloin nykyinen ylläpitäjä viettää kesälomaa heinäkuussa kolme viikkoa. Merkittäviä vikoja sähköpostijärjestelmässä on havaittu noin kerran kuukaudessa. Edellä kuvatuilla perusteilla uhan todennäköisyysluvulle annettiin arvoksi 2.

Riskiluku: uhan vakavuus * uhan toteutumisen todennäköisyys = $3 * 2 = 6$.

Riskianalyysin loppuraportti:

Riskianalyysin perusteella sähköpostipalvelun ylläpidosta löydettiin yksi merkittävä riski, jota suositellaan pienennettäväksi mahdollisimman pian.

Vaikutukseltaan ylläpito henkilöstön saatavuuden estyminen ei ole lyhytkestoisena välttämättä merkittävä, jos poissaoloaikana ei tapahdu toimintahäiriöitä. Poissaolon pidentyessä vaikutukset kasvavat merkittävästi. Vastaavasti myös häiriötilanteiden todennäköisyys kasvaa. Koska sähköpostijärjestelmää ei saada toimintakuntoon ilman ylläpito henkilöstön erityisosaamista, palvelun toimintaan vaikuttavan häiriötilanteen kanssa samanaikaisesti sattuva ylläpito henkilöstön poissaolo aiheuttaa merkittävää taloudellista tappiota ja vaikuttaa yrityksen julkisuuskuvaan negatiivisesti,.

Tässä arviossa ylläpito henkilöstön saatavuuden estyminen häiriötilanteen aikana aiheuttaa merkittävän riskin pohjautuen riskin realisoidumisen vaikutukseen ja toteutumismahdollisuuteen. Riski liittyy selkeästi yrityksen ydintoimintaan.

5.1.1.2 Riskin arviointi

Toimenpiteet:

Sähköpostipalvelun toimivuus on kirjattu yhtiön tärkeisiin liiketoiminnallisiin tavoitteisiin. Jotta liiketoiminnalliset tavoitteet täyttyvät, edellyttää arvioitu riski toimenpiteitä riskin pienentämiseksi. Pienentämistoimenpiteenä sähköpostijärjestelmälle nimetään toinen ylläpito henkilö hyvissä ajoin ennen vanhan työntekijän poislähtöä, jotta vältetään tilanne, jossa ylläpitotyö olisi vain yhden henkilön varassa. Ylläpito henkilöstölle laaditaan koulutussuunnitelma tarvittavan osaamisen varmistamiseksi myös tulevaisuudessa.

Vastuu ja aikataulu:

Toimenpiteistä vastaa ylläpito henkilöstön lähin esimies, joka käynnistää tarvittavan yrityksen sisäisen rekrytointiprosessin välittömästi.

5.1.1.3 Toteutus ja seuranta

Ylläpitohenkilöstön lähin esimies raportoi sovittujen toimenpiteiden suorittamisesta ja raportoi tilanteen edistymisestä omalle esimiehelleen.

Toimenpiteiden vaikutusten seuranta:

Ylläpitohenkilöstön resursseja ja osaamista seurataan jatkossa osana sähköpostipalveluympäristön vuosittaista riskianalyysiä ja osana päivittäistä esimiestyötä.