VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOTEKNIIKKA

Mikko Orrenmaa

YRITYKSEN TIETOJÄRJESTELMIEN RISKIANALYYSI

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten Vaasassa 30.11.2011

Työn valvoja	Prof. Jouni Lampinen
Työn ohjaaja	KTM Peter Jansson

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Mikko Orrenmaa
Diplomityön nimi: Yrityksen tietojärjestelmien riskianalyysi
Valvojan nimi: Prof. Jouni Lampinen
Ohjaajan nimi: KTM Peter Jansson
Tutkinto: Diplomi-insinööri
Koulutusohjelma: Tieto- ja tietoliikennetekniikan koulutusohjelma
Suunta: Ohjelmistotekniikka
Opintojen aloitusvuosi: 2005
Diplomityön valmistumisvuosi: 2011 **Sivumäärä:** 126

TIIVISTELMÄ:

Tämän työn tavoitteena on havainnoida ja analysoida erään yrityksen sisäisistä IT-palveluista vastaavan osaston toimintaa ja selvittää millaisia riskejä on olemassa liittyen osaston henkilökuntaan ja osaston ylläpitämiin tietojärjestelmiin. Työssä keskitytään kolmeen riskejä sisältävään osaan: henkilöstöturvallisuuteen, laitteistoturvallisuuteen ja ohjelmistoturvallisuuteen.

Työssä määritellään aluksi riskit joita halutaan tutkia. Määrittelyn jälkeen tutkitaan millaisia riskejä löytyy henkilöstön ja tietojärjestelmien toiminnassa, miten riskit ilmenevät, miten todennäköistä riskien toteutuminen on ja miten vakavia riskit ovat. Työn lopussa on tarkoitus keskittyä riskien esiintymistiheyteen, niiden vakavuuksien analysointiin ja korjaustoimenpiteisiin. Analysoimalla henkilöstön ja tietojärjestelmien toiminnassa ilmenneitä riskejä pyritään luomaan tietoa osaston toiminnan ja tietojärjestelmien suunnittelun, -käyttöönoton, -operoinnin, -käytöstäpoiston ja -toiminnan kehittämisen tueksi esittämällä toiminnassa ilmenneet ongelmat ja niiden vakavuudet.

Tutkimus osoittaa, että ilman säännöllistä arviointia tietoturvan ja riskienhallinnan huomiointi unohtuu helposti, jolloin riskien määrä ja vakavuus kasvavat. Tutkimuksen pohjalta laaditaan ohjeistus tulevaisuudessa tehtävälle järjestelmän riskianalyysille. Tutkimuksessa havaittiin, että järjestelmien ylläpitäjillä on hyvin tiedossa suuri osa järjestelmien riskeistä, mutta niiden korjaamisen vaativan suuren työpanoksen vuoksi kaikkia korjauksia ei ole ehditty toteuttamaan. Tutkimus myös osoittaa, että järjestelmien riskianalyysiin tulisi varata säännöllisesti aikaa jolloin riskienhallinta pysyisi ajan tasalla.

AVAINSANAT: Riskianalyysi, riskienhallinta, tietoturva, tietojärjestelmä

UNIVERSITY OF VAASA
Faculty of technology
Author: Mikko Orrenmaa
Topic of the thesis: Yrityksen tietojärjestelmien riskianalyysi
Supervisor: Prof. Jouni Lampinen
Instructor: M.Sc.(econ.). Peter Jansson
Degree: Master of Science in Technology
Degree Programme: Degree Programme in Computer Science
Major of Subject: Software engineering
Year of Entering the University: 2005
Year of Completing the Thesis: 2011 **Pages:** 126

ABSTRACT:

The aim of this thesis is to observe and analyze departments operation that is responsible for target company's internal IT-services and examine what kind of risks are involved in operation of department staff and information systems. Focus of this thesis is in personnel security, hardware security and software security.

At the beginning in thesis, risks will be defined. After risk definition, risks involved to personnel security and information system security will be studied, how those appear, how big are odds that risk will appear and how severe the risks are. In the end of thesis focus will be on incidence of risks, analyze of risks and correction operations. The meaning of analyzing risks involved in operations of staff and information systems will be to produce knowledge to support departments operation and information system design, system deployment, system operation, system deprecation and system function by stating appeared risks and risks severity.

Study will point out that without regular evaluation of data security and risk management, risk observation will be forgotten. When risk observation will be forgotten amount and severity of risks will increase. Using the results of the study, layout for the future risk analysis will be made. Study points out that system administrators are well aware of risks involved system that they are administrating, but because of the large amount of work for fix the systems all the risks are not yet fixed. Study also points out that system risk analyze should be made regularly so the risk management will stay up to date.

KEYWORDS: Risk analysis, risk management, data security, information system

LYHENTEET 7

1. JOHDANTO 9

2. HENKILÖSTÖTURVALLISUUS 11

3. LAITTEISTO- JA TIETOLIIKENNETURVALLISUUS 26

4. OHJELMISTOTURVALLISUUS 43

5. HENKILÖSTÖTURVALLISUUDEN ANALYSOINTI 55

5.1. Henkilöstön toimenkuvat 56

5.2. Henkilöstön osaamisen varmistaminen 57

5.3. Avain henkilöstö 59

5.4. Työhöntuloprosessi 61

5.5. Prosessi työsuhteen päättyessä 65

5.6. Sijaisjärjestelyt 67

5.7. Työnkierto ja lomat 68

5.8. Ulkopuolinen työvoima 70

5.9. Varautuminen poikkeusoloihin 73

6. LAITTEISTOTURVALLISUUDEN ANALYSOINTI 74

6.1. Käyttöönotto 76

6.2. Huolto ja kunnossapito 78

6.3. Käytöstä poisto 80

6.4. Käytettävyys 80

6.5. Laitetyyppien erityisvaatimuksia 82

6.5.1. Palvelimet 82

6.5.2. Päätelaitteet 89

6.5.3. Levyjärjestelmät 91

6.5.4. Kaapelointi 93

6.5.5. Verkonaktiivilaitteet 94

6.6. Tietoliikenneverkkojen suunnittelu ja dokumentointi 98

6.7. Tietoliikenneverkkojen varmistukset ja varajärjestelyt 100

6.8. Tietoliikenneverkkojen operointi ja valvonta 101

6.9. Varautuminen poikkeusoloihin 102

7. OHJELMISTOTURVALLISUUDEN ANALYSOINTI 106

7.1. Ohjelmistot 107

7.2. Ohjelmistoasennukset 107

7.3. Päivitykset 108

7.4. Etäkäyttö 109

7.5. Eheys ja käytettävyys 110

7.6. Lisenssit 112

7.7. Versionhallinta 113

7.8. Varautuminen poikkeusoloihin 115

8. JOHTOPÄÄTÖKSET 116

LÄHDELUETTELO 119

LYHENTEET

DDoS	Distributed Denial of Service, tekniikka tietyn verkkopalvelun lamauttamiseksi siten, että palvelu ei ole käytettävissä.
DMZ	Demilitarized Zone, fyysinen tai looginen verkko joka yhdistää organisaation verkon turvattomampaan verkkoon.
DoS	Denial of Service, tekniikka tietyn verkkopalvelun lamauttamiseksi siten, että palvelu ei ole käytettävissä.
IDS	Intrusion Detection System, tietoverkkoon asennettava järjestelmä jonka tarkoitus on tunnistaa verkkoon suuntautuvat hyökkäysyritykset.
IP	Internet Protocol, protokolla joka huolehtii tietoliikennepaketin perille toimittamisesta.
ISDN	Integrated Services Digital Network, piiri kytkentäinen puhelinverkkojärjestelmä.
NAT	Network Address Translation, tekniikka jolla voidaan käyttää useaa sisäistä IP-osoitetta yhden ulkoisen IP-soiteen avulla.
PUA	Potentiaalisten Uhkien Analyysi, uhkien tunnistus menetelmä.
RADIUS	Remote Authentication Dial In User Service, radius palvelin toimii autentikointipalvelimena.
RAID	Redundant Array of Independent Disks, tekniikka jota käyttämällä yhdistetään erillisiä kiintolevyjä yhdeksi loogiseksi levyksi.
SET	Secure Electronic Transaction, Tekninen määrittely turvallisiin luottokorttiostoksiin avoimessa tietoverkossa.
SSL	Secure Socket Layer, tietoliikenteen salaus protokolla.
SSH-2	Secure Shell, tietoliikenteen salaus protokolla.
S/HTTP	Secure Hypertext Transfer Protocol, schema web yhteyksien salaukseen.

UPS	Uninterruptible Power Supply, järjestelmä tai laite jonka tehtävä on taata tasainen virransyöttö lyhyissä katkoksissa ja syöttöjännitteen epätasaisuuksissa.
VAHTI	VAHTI, valtionhallinnon tietoturvallisuuden johtoryhmä.
VPN	Virtual Private Network, tapa jolla kaksi tai useampia tietoverkkoja voidaan yhdistää julkisen verkon yli näennäisesti yksityiseksi verkoksi.
xDSL	Digital Subscriber Line, digitaalinen tilaajayhteys eli tietoliikenneyhteys.

1. JOHDANTO

Tämän tutkimuksen tavoitteena on tunnistaa yrityksen IT-palveluita tarjoavan osaston toimintaan ja laitteistoon liittyviä riskejä. Tunnistetut riskit arvioidaan niiden mahdollisen esiintymistodennäköisyyden ja vakavuuden perusteella. Arvioinnin jälkeen suunnitellaan jatkokehitysidea, miten riskiä pienennetään tai mahdollisesti poistetaan ja nimetään kehitysidean toteuttamiselle vastuuhenkilö. Riskien tunnistaminen edellyttää, että tiedetään: mitkä ovat todellisia uhkia, mitkä ovat toteutuneen uhkan seuraukset, millä tavoin uhka saattaa esiintyä ja kuinka todennäköisesti uhka esiintyy. Riskien hallinnassa on kuitenkin hyvä muistaa, että ympäristö muuttuu kokoajan. Muutoksesta johtuen kaikkia riskejä ei ole järkevää, eikä usein edes mahdollista huomioida

Krutz & Vines (Ronald L. Krutz & Russel Dean Vines, 2003: 15) pitävät tietoturvan tärkeimpänä osa-alueena riskienhallintaa. Riskienhallinnan tärkein tavoite on riskien pienentäminen. Riskien pienentämisellä tarkoitetaan riskien määrän vähentämistä organisaation tietoturvapolitiikassa määritellylle hyväksytylle tasolle.

Työn lopputuloksena laaditaan riskianalyysi, jonka tuloksia pyritään tulevaisuudessa pitämään tukena laitekokoonpanoja ja ohjelmistosuunnittelua koskevien päätösten tekoprosessia suunniteltaessa ja toteutettaessa. Kuten Krutz & Vines (2003: 16) osoittavat, on riskianalyysin tarkoitus arvioida uhkien aiheuttamia menetyksiä liiketoiminnassa ja tästä koituvia kustannuksia. Riskianalyysin kaksi tärkeintä tulosta ovat: riskien tunnustaminen sekä vastatoimien hyötyjen ja kustannusten välisen suhteen selvittäminen. Nämä kaksi tulosta ovat tärkeitä suunniteltaessa strategiaa riskien pienentämiseksi.

Krutz & Vines (2003: xiii) määrittelevät tietoturvan kolmeksi perusperiaatteeksi: luottamuksellisuus, eheys ja käytettävyys. Näiden perusperiaatteiden ympärille rakentuu kaikki

tietoturvan valvontamekanismit, uhat, heikkoudet ja tietoturvaprosessit. Tutkimuksen avulla pyritään löytämään osaston toiminnan kannalta tärkeät riskit luottamuksellisuudelle, eheydelle ja käytettävyydelle. Osaston tarjotessa palveluita organisaatiolle ja ulkopuolisille asiakkaille, otetaan työssä kantaa henkilöstön, laitteiston ja koko palvelun toimintaan. Luottamuksellisuudella tarkoitetaan tiedon tahallista tai tahatonta paljastumista henkilölle jolla ei ole oikeutta tietoon. Eheydellä varmistetaan, ettei valtuuttamattomat henkilöt tai prosessit pääse muokkaamaan tietoja ja että sisäiset ja ulkoiset tiedot ovat yhdenmukaisia. Käytettävyydellä tarkoitetaan tiedon ja resurssien saantia. Käytettävyys takaa, että järjestelmät toimivat kun niitä tarvitaan.

Työssä on tarkoitus analysoida potentiaalisia uhkia PUA-tekniikan avulla. Työssä käytetään kvantitatiivista tutkimusta jolloin, potentiaalisten uhkien analyysissä määritetään mitä uhkat ovat, mikä on niiden esiintymistiheys, esiintymistodennäköisyys, vaikutukset, kustannukset ja kehitysehdotukset.

Krutz & Vines (2003: 19) listaavat riskianalyysin kolmeksi tärkeimmäksi vaiheeksi: omaisuuserien arvojen määrittäminen, omaisuuseriin kohdistuvien uhkien analysoiminen ja odotettavien vuotuisten menetysten arvioiminen. Työssä keskitytään tarkimmin omaisuuseriin kohdistuvien uhkien analysointiin ja kehitysideoiden luomiseen.

Tämä työ tehtiin toimeksiantona kohde yrityksessä toimivalle, IT-palveluista vastaavalle osastolle. Osastolla on ylläpidettävänään suuri määrä verkonaktiivilaitteita ja palvelimia joiden toiminta on kriittinen osa koko yrityksen liiketoimintaa.

2. HENKILÖSTÖTURVALLISUUS

Valtionvarainministeriön ohjeessa riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa (Valtionvarainministeriö 2003) pidetään tietoturvallisuuden perustana organisaation toimintaan liittyvien tietoturvariskien tunnistamista ja arvioimista. Tietoturvariskien pohjalta voidaan tehdä päätökset siitä, mitä toimenpiteitä tulee tehdä tietoturvan parantamiseksi. Tietoturvariskejä hallittaessa ensimmäisen toimenpiteen tulee olla organisaation toiminnan kehittäminen. Organisaation toiminnan kehittämiseen kuuluu toimintatavat, osaaminen ja johtaminen. Kun nämä asiat on saatu organisaatiossa toimiviksi, tulee keskittyä järjestelmien teknisiin suojauskeinoihin.

Valtionvarainministeriö (Valtionvarainministeriö 2008) tarkoittaa tärkein tekijä on ihminen ohjeessaan henkilöstöturvallisuudella henkilöstöstä aiheutuvien riskejä ja niiden hallintaa. Henkilöstöturvallisuutta ei pidä sekoittaa henkilöturvallisuuteen. Henkilöturvallisuudella tarkoitetaan henkilöihin kohdistuvien riskien hallintaa. Henkilöstöturvallisuus käsitetään osaksi yleisimpiä turvallisuuskäsiteitä. VAHTI-sanastossa määritellään käsite henkilöstöturvallisuus seuraavasti: "Henkilöstöön liittyvien tietoturvariskien hallinta henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan osalta.".

Ruohonen (Mika Ruohonen, 2002: 4) pitää henkilöstöturvallisuuden tärkeimpänä osa-alueena tietojärjestelmien suojaamista käyttäjien muodostamilta uhilta. Käyttäjien tekemiä vahinkoja on mahdollista vähentää opettamalla ja oheistamalla käyttäjiä jokapäiväisissä toimenpiteissä.

Henkilöstöriskienhallinta on systemaattinen prosessi, jota käyttämällä kontrolloidaan organisaation kohtaamia henkilöstöturvallisuuden riskejä. Henkilöstöriskienhallintaprosessi

mittaa ja vaikuttaa jatkuvasti riskien arviointiin, toteutukseen ja evaluointiin (Centre for the Protection of National Infrastructure 2007). Henkilöstö riskien arviointi keskittyy työntekijöihin, työntekijöiden pääsyyn organisaation tietoihin, riskeihin joita työntekijä asettaa organisaatiolle ja vastatoimien riittävyyteen. Se on henkilöstöturvallisuuden perusta (Centre for the Protection of National Infrastructure 2009).

Henkilöstö ja siitä johtuvat tietoturvatekijät ovat mahdollisesti tietojen eheyden, luottamuksellisuuden ja käytettävyyden uhkana. Usein uhkana pidetään henkilöstön aiheuttamia vahinkoja. Henkilön aiheuttamat vahingot voivat olla tahallisia tai tahattomia, mutta myös organisaation rakenteella ja sen panostuksella tietotekniikkaan on suuri merkitys tietoturvauhkien torjunnassa. Valtionvarainministeriö (Valtionvarainministeriö 2008) pitää tärkein tekijä on ihminen ohjeistuksessa henkilöstöjohtamisen keskeisenä osana; suunnitelmallista ja järjestelmällistä henkilöstön kehittämistä, johtamista ja henkilöstöasioiden hallintoa.

Valtionvarainministeriön teettämässä henkilöstöstä aiheutuvia tietoturvariskejä tehdyssä tutkimuksessa todetaan, että noin puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin. Valtionvarainministeriön (2008) tärkein tekijä on ihminen ohjeistuksessa määrittämät torjuntasuositukset liittyvät yleisimmin työn johtamiseen, valvontaan, tiedonkulkuun ja osapuolien yhteistyöhön.

Valtionvarainministeriö (2008) osoittaa tärkein tekijä on ihminen ohjeistuksessaan, että henkilöstöturvallisuus ja siihen sisältyvät käytettävyys-, eheys- ja salassapitovaatimukset on otettava mukaan jo organisaation tietoturvallisuutta ja toimintakulttuuria luodessa ja kehitettäessä. Henkilöstöturvallisuustyön kannalta keskeistä ovat suunnitelmallinen henkilöstön työhön palkkaaminen, kehittäminen, johtaminen, ohjeistaminen, käsittelyketjun tur-

vaaminen, riskikartoitukset, henkilöstön soveltuvuusarvioinnit, pääsynrajoitusmekanismit ja henkilöstöasioiden hallinto.

PK-RH (PK-RH 2009) pitää kaikkein kavalimpina riskeinä riskejä, joihin ei osata varautua. Riskien tunnistamisen jälkeen niiden suuruus arvioidaan, jotta riskit voidaan asettaa tärkeysjärjestykseen. Vasta tämän jälkeen riskejä voidaan hallita.

Kuusela & Ollikainen (Hannu Kuusela & Reijo Ollikainen, 1998: 252) mukaan strategiseen johtamiseen integroitu henkilöstöresurssien johtaminen, henkilöstösuunnittelu, rekrytointi, kehittäminen, arviointi ja palkitseminen ovat henkilöstöriskien hallinnan avain tekijät. Henkilöstö johtamisessa tulee varmistaa, että organisaatiolla on lyhyellä ja pitkällä aikavälillä käytettävissään paras mahdollinen henkilöstö.

Henkilöstö on organisaation toimintoja ylläpitävä taho. Valtionvarainministeriö (2003) osoittaa ohjeessaan riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, että jokapäiväisellä toiminnallaan henkilöstö kuitenkin muodostaa myös riskejä. Usein henkilöstö aiheuttaa vahinkoa tahattomasti, mutta myös tahallisen ilkivallan tekoa esiintyy. Tahattomiin vahinkoihin auttaa usein koulutus. Koulutuksella pyritään helpottamaan ja tehostamaan henkilöstön jokapäiväistä toimintaa. Henkilöstön jokapäiväisessä toiminnassa henkilön omat ominaisuudet vaikuttavat käyttäytymiseen. Henkilöt reagoivat erilailla tapahtumiin, joillakin on tapana mennä "paniikkiin" oudossa tai nopeaa ratkaisua vaativassa tehtävässä kun taas toiset pystyvät suoriutumaan rutiininomaisesti myös tällaisista työtehtävistä. Tahalliset vahingonteot liittyvät usein työsuhteen päättymiseen työnantajan erottaessa työntekijän. Yleensä työntekijän työsuhteen pituus vaikuttaa siihen miten paljon tietoa työntekijä vie mukanaan lähtiessään yrityksestä. Työntekijää erotettaessa, tulee organisaatiossa pitää kuitenkin huoli, että kulkuluvat, tunnukset, salasanat ja muut järjestelmien autentikointiin liittyvät tiedot päätetään mahdollisimman pian.

Valtionvarainministeriö (2008) listaa tärkein tekijä on ihminen ohjeistuksessa henkilöstöturvallisuuden tarkastelun kohteiksi: teknologian, organisaation, ihmisen, työtehtävän ja työympäristön välinen yhteys. Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa. Henkilöstöturvallisuudessa riskien hallinnassa arvioitavia kohteita ovat mm. henkilöstön soveltuvuus, toimenkuvat, sijaisjärjestelyt, tiedonsaanti- ja käyttöoikeudet, suojaaminen, turvallisuuskoulutus ja valvonta.

Tietoturvatyössä teknisten ja toiminnallisten menetelmien käytön, järjestelmien, laitteiden ja ohjelmistojen lisäksi suuri rooli jää henkilöstölle. Valtionvarainministeriö (2008) osoittaa tärkein tekijä on ihminen ohjeistuksessa, että organisaation on määriteltävä yksikäsitteisesti henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet. Määrittely voidaan toteuttaa esimerkiksi tehtävänkuvausten ja työsopimusten järjestelyjen avulla. Vastuu- ja velvollisuuskuvauksissa tulee määritellä ainakin salassapitovelvollisuuksiin, henkilöstö- ja asiakastoimintaan liittyvien tietojen käsittelyyn ja muihin erityisluontoisten tietoaineistojen käsittelyyn liittyvät erityisvelvoitteet.

Henkilöstöriskejä hallittaessa organisaatiossa tulee ottaa huomioon tietoaineistoturvallisuus ja hallinnollinen turvallisuus. Valtionvarainministeriä (2008) määrittää ohjeistuksessa: tärkein tekijä on ihminen, tietoaineistoturvallisuuden kattamaan käsittelysäännöt tietoaineiston synnystä sen tuhoamiseen asti. Hallinnollisessa turvallisuudessa tulisi kiinnittää huomiota: tiedon omistajuuteen, luokituksiin, käsittelysääntöihin, ohjeistukseen ja koulutukseen. Henkilöstöturvallisuudessa on otettava huomioon myös työprosessit ja käsittelyketjujen tietovirrat. Tietovirtoja suunniteltaessa tulee ottaa huomioon käsittelyketjujen turvaohjausmekanismit. Näitä mekanismeja ovat henkilöstön tahallisten ja tahattomien virheiden ennaltaehkäisy.

Valtionvarainministeriö (2008) pitää tärkein tekijä on ihminen ohjeistuksessaan henkilöstön merkitystä keskeisenä tietojen turvaamista toteutettaessa. Haasteena henkilöstöturvallisuus-toiminnassa on ihminen ei järjestelmät. Henkilöstö käsittelee tietoja vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja niiden käsittelyn päätyttyä tuhoamalla niitä. Lisäksi henkilöstöllä on keskeinen rooli tietovarastojen ja -järjestelmien ylläpidossa.

Allen (Julia H. Allen 2002: 6) osoittaa, että tietoturvapolitiikka toimii parhaiten, kun se kehitetään yhteistyössä henkilöiden kanssa joita tietoturvapolitiikka koskee. Vaikka johdon edustajat ovatkin vastuussa tietoturvapolitiikan linjojen asettamisesta, on heidän tehtävä yhteistyötä järjestelmien ylläpitäjien, käyttöhenkilöstön, turvahenkilöstön ja käyttäjien kanssa, jotta tietoresursseille saadaan määriteltyä realistiset ja toimivat teknilliset ja toiminnalliset turvakeinot.

Henkilöstöhallintoon kuuluu tietoturvallisuuteen liittyvien vastuiden määrittely, niistä tiedottaminen ja salassapitosopimukset. Valtionvarainministeriön (2006a) tietoturvallisuuden arviointi valtionhallinnossa ohjeistuksen mukaan vastuut tulee kirjata työntekijöiden toimenkuviin. Esimiehillä on vastuu seurata tietoturvallisuuden toteutumista omassa yksikössään ja alaistensa toiminnassa. Teknisten toteutusten ja käytännön ohjeistusten käyttötasoa voidaan arvioida tarkistuslistoilla. Tarkistuslistojen avulla pystytään tutkimaan miten paljon organisaatiossa panostetaan henkilöstöturvallisuuteen.

Suominen (Arto Suominen 2003: 28) osoittaa, että johdon on tarpeellista omaksua riskienhallinnan toimintamallit ja viedä ajattelua eteenpäin kaikilla organisaatiotasoilla. Riskienhallinta ei toimi tehokkaasti, jos se jätetään vain riskienhallinnan ammattilaisten ja järjestelmistä vastaavien tahojen hoidettavaksi.

Valtionvarainministeriö (2008) pitää tärkein tekijä on ihminen ohjeistuksessaan tärkeänä, että tietojärjestelmien käytettävyysriskien määriteltäessä arvioidaan henkilön merkitys organisaatiossa ja sen toiminnassa. Keskeisiä päätöksiä tehdessä henkilön asemaa ja paikallaoloa edellyttävä on päättäjä. Järjestelmien käytettävyyteen kriittiset toimenpiteistä vastaa järjestelmän avain henkilö. Mikäli henkilöön kohdistuu normaalia suurempi rikos- tai onnettomuusriski tulisi henkilö luokitella henkilöriskihenkilöksi.

Krutz & Vines (2003: 221) esittävät, että suurta turvaa vaativissa järjestelmissä käytettäisiin tehtävien eriyttämistä. Tehtävien eriyttämisessä tehtävät jaetaan useammalle kuin yhdelle henkilölle. Näin toimiessa yksi henkilö ei voi vaarantaa koko järjestelmän turvallisuutta. Useissa järjestelmissä pääkäyttäjällä on oikeudet järjestelmän hallinta- ja turvatoimintoihin. Tällaista vallan keskittämistä ei tulisi turvallisissa järjestelmissä tehdä. Yksi tapa tehdä tämä on kahden henkilön ohjaus. Kahden henkilön ohjauksessa kaksi eri työntekijää tarkastavat ja hyväksyvät toisensa tehdyt työt. Tällä tavoin voidaan pienentää petoksen riskiä.

Henkilöstön toimenkuvien määrittelyssä tulee ottaa huomioon myös pääsyoikeuksien myöntäminen. Henkilön toimenkuvan vaatiessa pääsyoikeutta liikkumaan tietyissä organisaation tiloissa tulee työntekijä valtuuttaa liikkumaan näissä tiloissa. Valtionvarainministeriön (2008) laatiman tärkein tekijä on ihminen ohjeistuksen mukaan, kulunvalvonta on oleellinen osa henkilöstötietoturvaa. Aitous on ominaisuus, jota tarvitaan käytettäessä apuvälineitä henkilöllisyyden todentamiseen. Todentamista ei tule käsittää ainoastaan henkilöllisyyden todentamiseksi. Aitouden todentaminen tulee kyseeseen aina, kun henkilöä ei ”tunneta” ja hänen tunnistamisessaan käytetään tunnistevälineitä tai tunnistevertailutietoja. Todentamisen vahvuus riippuu apuvälineitä käytettäessä koko luottamusketjun luotettavuudesta. Jokaiseen sidokseen on pystyttävä luottamaan ja jokaisen apuvälineen aitoudesta on voita varmistua.

Valtionvarainministeriö (2008) pitää tärkein tekijä on ihminen ohjeistuksessaan yhtenä henkilöstöturvallisuustyön tavoitteista oman henkilöstön aiheuttaman tuottamuksellisen uhkaan vähentämistä ohjeistamalla, auditoimalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin. Koska tietoturva kuuluu henkilöstöturvallisuuteen oleellisena osana, tietoturvallisuuden tulee näkyä jokapäiväisten arkisten toimien teko tavoissa. Henkilöstö saattaa toimia tietoisesti organisaation sisältä vakoilemalla tai sabotoimalla. Tällaiset henkilöstön toteuttaman tahallisen rikoksen onnistumisen mahdollisuus on minimoitava henkilöiden taustaselvitysten, huolellisen tietojen luokittelun, raportoinnin, sisäisen valvonnan ja sisäisen tarkastuksen, järjestelmiin olevien tunnusten myöntämisen rajoittamisella, -tunnusten tason määrittelemisellä, kulunhallinnan ja johdonmukaisen seuraamusmenettelyn avulla.

Valtionvaranministeriö (Valtionvaranministeriö 2006b) osoittaa henkilöstön tietoturva ohjeessaan, että suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki, ei siis vain tekniikka vaan myös henkilöstön jokapäiväiset toimintatavat ja asenteet.

Krutz & Vines (2003: 25-26) esittävät ihmisten olevan usein turvaketjun heikoin lenkki. Yleensä, koska ihmisiä ei ole koulutettu riittävästi tai he eivät tiedä mitä turvallisuus merkitsee organisaatiolle. Työntekijöiden tulisi ymmärtää millainen vaikutus heidän toimilla on organisaation turvallisuuteen ja millainen on organisaation omaisuuserien suojaamisen tarve. Jokaiselle työntekijälle tulisi antaa turvallisuustietoisuus koulutus. Turvallisuustietoisuus koulutuksessa painotetaan kolmea käsitettä: tietoisuus, valmennus ja koulutus. Tällainen koulutus osoittaa hyödyllisyytensä työntekijöiden käyttäytymisen ja yrityksen turvallisuuden parantumisena.

Kuusela & Ollikainen (1998: 264) osoittavat, että henkilöstön ammattitaidon kehittämisellä pyritään toteuttamaan strategiset tavoitteet ja avain-henkilöiden kehittämisellä varmistamaan yrityksen kyky pysyä markkinoiden kilpailussa mukana myös tulevaisuudessa.

Pirnes, Sahlman & Kajava (Jari Pirnes, Anssi Sahlman & Jorma Kajava 2000: 23) pitävät henkilöstövalmennuksen ensimmäisenä vaiheena henkilöstön tietotekniikkaosaamisen riittävyyden varmistamista. Aina ei riitä, että käyttäjä hallitsee oman työtehtävänsä, vaan käyttäjän tulisi ymmärtää myös koko prosessi johon hänen työtehtävänsä kuuluu.

Pirnes ym. (2000: 23) osoittavat, että henkilöstövalmennuksella pyritään takaamaan käyttäjän keinot tukea organisaation tietoturvapolitiikkaa jokapäiväisessä työssään ja käyttäjien tietoisuus tietoturvallisuuteen kohdistuvista uhkista.

Uusin tieto ja tekninen kehitys ovat usein kaikkien saataville lähes reaaliajassa. Inhimillisen tiedon ja taidon korvaaminen saattaa kuitenkin kestää vuosia. Tämän vuoksi henkilöstö muodostaa potentiaalisen tekijän jonka avulla yritys voi erottua edukseen. Kuusela & Ollikainen (1998: 251) pitävät henkilöstön osaamista organisaation tärkeimpänä kilpailuetuna.

Järjestelmän avainhenkilön palkkauksen yhteydessä tai vanhan työntekijän työnkuvan muuttuessa koskemaan uutta järjestelmään tulisi työntekijän tehtävänkuvauksessa varmistaa henkilön tavoitettavuus. Valtionvarainministeriö (2006a) osoittaa tietoturvallisuuden ohjeistuksessa valtion hallinnossa, että järjestelmä jossa työntekijä on avainhenkilö ollessa aikakriittinen, on saatavuus varmistettava varallaololla tai vähintään tavoitettavuus hälytystyön teettämiseksi. Järjestelmän ollessa aikakriittinen on saatavuuden kannalta tärkeää, että

avainhenkilö pystyy aloittamaan vaadittavat toimenpiteet määritellyssä aikaikkunassa. Tämä edellyttää usein varmistumista avainhenkilön sijainnista. Avainhenkilöstön käytettävyys on otettava huomioon virkamatkoja, lomia ja muita poissaoloja suunniteltaessa jolloin henkilö ei ole käytettävissä kriittiseen työtehtävään.

Usein lahjakkaiden työntekijöiden työpanos on moninkertainen verrattuna keskimääräiseen työntekijään. Hyvönen (Eero Hyvönen, 2003: 145) pitää tärkeänä, että yritys pitää kiinni tällaisista työntekijöistä ja yrittää houkutella lisää vastaavia yrityksen palvelukseen. Lahjakkaiden työntekijöiden pysyminen yrityksen palvelussa ja uusien palkkaaminen yrityksen palvelukseen vaativat yritykseltä panostusta. Yrityksen tulee ylläpitää mainettaan modernina ja joustavana työnantajana sekä tarjota työntekijälle teknisesti tarpeeksi haastavia työtehtäviä ja tarjota hyvä ansiotaso.

Weber (Ron Weber 1999: 244) suosittaa, että mikäli organisaatiossa on oma tietoturvavastaava ja hänellä alaisia tulisi tämän ryhmän vastata palveluiden tietoturvasta. Kuitenkin useissa organisaatioissa ei tällaista ole jolloin järjestelmien avainhenkilöt toimivat samalla järjestelmän tietoturvavastaavina. Näiden henkilöiden tehtäviin kuuluu vastuu varmistaa että järjestelmät ovat turvallisia. Järjestelmä on turvallinen kun odotettavissa olevien uhkien tapahtuessa menetykset ovat hyväksyttävällä tasolla.

Henkilöstöturvallisuudesta huolehtiminen alkaa rekrytoinnin yhteydessä tehtävistä taustatarkistuksista ja turvallisuusselvityksistä. Tarpeen vaatiessa rekrytoinnin yhteydessä suoritettavassa lääkärin tarkistuksessa voi olla myös huumetestaus. Valtionvarainministeriön (2006b) henkilöstön tietoturva ohjeen mukaan tarkistusten tavoitteena on varmistaa, että henkilö on sopiva erityistä tarkkaavaisuutta ja luotettavuutta edellyttävään tehtävään. Joi-

denkin tehtävien osalta tällä täytetään lainsäädännön asettamat vaatimukset. Rekrytoinnin jälkeen työntekijälle tulisi järjestää tietoturvakoulutus.

Miettinen (Juha E. Miettinen, 1999: 162-165) pitää henkilötietojen tarkistusta yhtenä henkilöstöturvallisuuden tärkeimmistä osa-alueista. Tällä tarkoitetaan, että työnantaja pyrkii selvittämään henkilöstön ja ulkopuolisten työntekijöiden taustat ennen työsuhteen alkamista. Näin toimimalla yritetään varmistua, ettei organisaation palvelukseen tule ei-toivottua henkilöstöä.

Työnhakijan arvioinnin tarkoituksena on selvittää kohteena olevan henkilön kykyä vastata työtehtävän asettamiin vaatimuksiin. Työnantajalla voi olla olemassa oman toiminnan kannalta merkittäviä arviointikriteerejä. Tällaiset arviointikriteerit voivat perustua työtehtävien sisältöön ja tehtävistä suoriutumisen erityisiin vaatimuksiin. Valtionvarainministeriö (2006b) suositteleekin henkilöstön tietoturva ohjeessaan, että työntekijää tulee arvioida myös työsuhteen aikana. Työsuhteen aikana tapahtuva arviointi voi liittyä esimerkiksi työntekijän toimenkuvan muuttuessa. Myös tällaisesta arvioinnista saadut tulokset tulee tallentaa henkilöstörekisteriin. Turvallisuusselvitysmenettelyllä työnantaja pyrkii henkilöstöturvallisuuden varmistamiseen.

Miettinen (1999: 162) listaa tärkeimmiksi henkilöstön taustatietojen selvitystavoiksi: viranomaistarkistus, työhistorian tarkistus, koulutustaustan tarkistus, luottotietojen ja maksuhäiriöiden tarkistus, yrityskytkentöjen tarkistus suosittelijoiden läpikäynti, julkaisutoiminnan läpikäynti ja henkilön tietojen etsintä Internetistä.

Kuusela & Ollikainen (1998: 227) esittävät, että salassapitovelvoitteiden tulee olla voimassa vähintään ajanjakson jonka aikana salassapidolla on merkitystä sopimuksen osapuolille. Käytännössä tämä tulisi toteuttaa sopimalla, että salassapitovelvollisuus on voimassa ikuisesti, vuosiin sidotun määräajan tai niin kauan kuin sopimuksen koskevilla tiedoilla on käytännön merkitystä.

Miettisen (1999: 165-166) mukaan yritysten ja yksityisten henkilöiden väliset salassapitosopimukset luovat perustan henkilöturvallisuuden toteuttamiselle sopimuksilla. Salassapitosopimukset tulee muotoilla siten, että ne ovat juridisesti sitovia asiakirjoja. Tästä syystä kummankin osapuolen on syytä tutustua ehtoihin huolella sopimuksiin ennen allekirjoittamista. Yritysten välisessä salassapitosopimuksessa on kyse tietoa luovuttavan ja tietoa vastaanottavan yrityksen yhteisistä menettelytavoista tietoa suojattaessa, luovutettaessa ja vastaanotettaessa. Henkilökohtaisella salassapitosopimuksella tarkoitetaan tietoa käsittelevän henkilön ja yrityksen välistä sopimusta jossa henkilö sitoutuu pitämään tiedot salassa ulkopuolisilta.

Kyrölä (Tuija Kyrölä, 2001: 153) muistuttaa, että yritys voi pyytää suojelupoliisia selvittämään työnhakijan taustatiedot. Mahdollinen työnantaja ei saa kuitenkaan kirjallista lausuntoa rekisterin sisällöstä. On myös huomioitava, että suomessa on samannimisiä henkilöitä joten henkilö tulee tarkasti yksilöidä virheellisten tietojen estämiseksi.

Työntekijän työsuhteen päättyessä on kaikki hänelle luovutetut oikeudet organisaation tietojärjestelmiin poistettava. Poiston tulee tapahtua viimeistään työntekijän viimeisenä työpäivänä. Miettinen (1999: 168) suosittaa, että tunnusten poistaminen aloitettaisiin jo silloin, kun työntekijän poislähtö on tullut yrityksen tietoon. Näin toimimalla pystytään pienentä-

mään mahdollisuutta, että työntekijä edes vahingossa ottaisi haltuunsa yrityksen omistamaa tietoaineistoa jota työntekijällä ei ole lupana viedä mukanaan.

Henkilön työsuhteen päättymiseen myös riitatilanteen seurauksena on varauduttava. Valtiovarainministeriö (2008) osoittaa tärkein tekijä on ihminen ohjeissa, että työntekijän, eronneen tai erotetun, pääsy organisaation tietojärjestelmiin on estettävä välittömästi eroilmoituksen jälkeen sekä huolehdittava järjestelmien lokien tarkistamisesta järjestelmien tavanomaisesta poikkeavan käytön selvittämiseksi. Kuvatussa tulehtuneessa tilanteessa on työntekijä saatettava työpisteelleen, josta hän valvotusti kerää henkilökohtaisen omaisuutensa, minkä jälkeen hänet saatetaan ulos toimitiloista. Samalla on huolehdittava työntekijälle luovutettujen käyttäjätunnusten, kulkulupien, avainten ja muiden pääsyoikeuksien peruuttamisesta ja pois ottamisesta.

Miettinen (1999: 162) pitää työ- tai sopimussuhteen loppumista huomattavasti vaikeampana prosessina kuin alkamista työnantajan kannalta katsottuna. Lähtevälle työntekijälle on ehtinyt kertyä mahdollisesti paljonkin arkaluontoista tietoa ja yrityksen fyysistä omaisuutta. Tietoaineiston asianmukainen palauttaminen on huomattavasti haastavampi toimenpide työ- tai sopimussuhteen päättyessä kun yrityksen fyysisen omaisuuden palauttaminen.

Miettinen (1999: 170) huomauttaa, että on tärkeää siirtää poislähtevän työntekijän työtehtävät asianmukaisesti muille työntekijöille tai yhteistyökumppaneille ja tiedottaa asiasta kaikille asianomaisille. Näin toimimalla yrityksen henkilökunta, yhteistyökumppanit ja asiakkaat osaavat olla yhteydessä oikeisiin henkilöihin pois lähteneen työtehtävistä.

Valtionvarainministeriön (2008) tärkein tekijä on ihminen ohjeistuksen mukaan, toiminnan jatkuvuuden varmistamiseksi on ennalta suunniteltava miten organisaatio varmistaa avainosaamisen. Tämä edellyttää varahenkilöiden etukäteen kouluttamista avaintehtäviin, ennen kuin avainhenkilö poistuu virastosta. Varahenkilöiden osaamista tulee harjoituttaa määräajoin. Jatkuvuuden varmistaminen pitkällä aikavälillä on suunniteltava ja määrätietoisesti toteutettava koulutusjärjestelmä, joka varmistaa toiminnan jatkuvuuden avaintehtävien henkilöstön siirtyessä mahdollisesti toisten työnantajien palvelukseen.

Henkilöstöjärjestelyitä tehdessä ja työnkuvia suunnitellessa tulee välttää organisaation toiminnan kannalta vaarallisia toimenkuva yhdistelmiä. Erityisesti pienissä yksiköissä jossa ei ole montaa työntekijää tulee helposti samalle työntekijälle toimenkuva joka liittyy useammalle organisaation tasolle. Tällaisia tilanteita ei aina pystytä välttämään ja tällaisen henkilön poissaoloon tulisi aina varautua. Mikäli työntekijän työnkuvaus sisältää kriittisiä toimintoja organisaation palveluiden kannalta tulisi hänellä olla määriteltynä varamies joka vastaa näistä kriittisistä palveluista ja näiden molempien työntekijöiden paikalla oloa voitaisiin edellyttää kriittisiä toimenpiteitä tehdessä.

Valtionvarainministeriö (2008) pitää tärkein tekijä on ihminen ohjeistuksessaan moniosaajien hankintaa ja koulutusta organisaation palvelukseen eräänä keinona sijaisuuksien järjestämiseen. Moniosaajat, jotka pystyvät korvaamaan toisiaan. Moniosaajien kouluttaminen on kuitenkin vaikeaa, koska muuttuvia osa-alueita tulee paljon. Moniosaajan ylläpidollinen työpanos jää helposti pieneksi koska hän ei ehdi tekemään ylläpitotoimenpiteitä, koska on opeteltava järjestelmissä tapahtuvia muiden ylläpitäjien tekemiä muutoksia ja niiden vaikutuksia. Moniosaajaa koulutettaessa tulee myös ottaa huomioon toimenkuvien monimutkaistuminen. Toimenkuvien monimutkaistuessa myös epäselvyydet kasvavat usean henkilön hoitaessa samoja tehtäviä.

Valtionvarainministeriö (2008) osoittaa tärkein tekijä on ihminen ohjeistuksessa, että on tärkeää varmistaa avainhenkilöiden käytettävyys myös loma-aikana. Avainhenkilöstön käytettävyyttä tulee seurata ja suunnitella lomat sekä muut poissaolot virkapaikalta siten, että sijaisjärjestelyt ovat mahdollisia. Sijaisjärjestelyissä on otettava erityisesti huomioon virka-aikana tapahtuvat virkamatkat jolloin henkilö ei tosiasiassa ole käytettävissä kriittiseen työtehtävään.

Henkilöstöturvallisuudessa tulee huomioida myös vuokratyövoima. Valtionvarainministeriö (2008) pitää tärkein tekijä on ihminen ohjeistuksessa henkilövuokrausta varteenotettavana mahdollisuutena, mikäli työtehtävä on yksinkertainen. Työtehtävän liittyessä monimutkaisten järjestelmien ja palveluympäristöjen hallitsemiseen ei ole hyödyllistä yrittää käyttää vuokratyövoimaa. Vuokratyövoiman kouluttamiseen tällaiseen toimenkuvaan on liian hidasta ja vaikeaa. Henkilövuokraukseen sisältyy myös turvallisuusriskejä, jotka organisaatiossa on arvioitava palvelujen käytössä.

Henkilöstöturvallisuus on organisaation tietoturvallisuuden keskeinen alue ja se koskettaa jokaista työntekijää. Henkilöstöturvallisuustyötä tehdessä on otettava huomioon, että työ on ennaltaehkäisevää. Tällä valtionvarainministeriö (2008) tarkoittaa tärkein tekijä on ihminen ohjeistuksessaan, että työn tarkoitus on puuttua riskeihin jo ennen kun poikkeamaa tapahtuu. Kuitenkin jokapäiväisessä toiminnassa joskus tapahtuu poikkeamia jolloin myös näihin tilanteisiin tulee ottaa kantaa henkilöstöturvallisuustyössä.

Henkilöstöturvallisuudessa tulee ottaa kantaa myös vierailijoiden valvonta. Työntekijä voi työtehtävissä tuoda vieraita organisaation tiloihin ja toimia heille isäntänä, mutta vapaa-aikana tämä välttämättä ole tarpeellista. Vierailijat tulee tarkastaa toiminnallisten tarpeiden mukaan. Vierailija voi olla satunnainen vierailija, jolloin hänelle tulisi myöntää kertaluon-

teinen pääsyoikeus. Vierailijan ollessa satunnaisesti työtehtävissä vieraileva henkilö, tulisi hänelle valtionvarainministeriön (2008) tärkein tekijä on ihminen ohjeistuksen mukaan myöntää pysyvä oikeus pääsyyn. Tällaisessa tapauksessa pääsyn tulee kuitenkin olla määräaikainen. Vieraalla tulee kuitenkin aina olla isäntä, jonka suosituksesta vieras valtuutetaan ja joka vastaa vierailijan toimista.

Järjestelmien ylläpitäjille tulee usein pyyntöjä tehdä uusia tunnuksia ylläpitämiinsä järjestelmiin. Chirillo (John Chirillo, 2001: 157) osoittaa, että on tärkeää varmistaa pyynnön esittäjän henkilöllisyys ennen tunnuksen luovuttamista käyttäjällä.

Käyttäjien oikeuksien hallintaa helpottamaan on olemassa käyttäjäryhmät. Käyttäjäryhmillä voidaan luoda isompia hallittavia kokonaisuuksia, joille voidaan antaa yhtenevät oikeudet. Hakala, Vainio & Vuorinen (Mika Hakala, Mika Vainio & Olli Vuorinen, 2006: 155-156) suosittelevat, että käyttäjille ei annettaisi suoraan oikeuksia vaan oikeuksien myöntö tapahtuisi käyttäjäryhmien avulla. Käyttäjä ryhmien avulla on myöhemmin helpompi muokata käyttäjien oikeuksia. On kuitenkin huomioitava, että aina ei ole mahdollista käyttää käyttäjäryhmiä oikeuksien määrittelyyn. Tällaisen poikkeuksen muodostavat järjestelmät jotka sisältävät käyttäjien henkilökohtaisia tietoja.

3. LAITTEISTO- JA TIETOLIIKENNETURVALLISUUS

Laitteistoturvallisuudella on tarkoitus turvata laitteiston elinkaari. Elinkaareen kuuluvat asennuksen, ylläpidon, turvallisen käytöstä poiston ja takuun lisäksi erilaiset tukipalvelut ja tukisopimukset. Valtionvarainministeriö (Valtionvarainministeriö 2009a) tarkoittaa laitteistoturvallisuutta koskevassa ohjeistuksessaan laitteistoturvallisuudella laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia Hallinnoinnissa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu.

Valtionvarainministeriö (2009a) laitteistoturvallisuus ohjeessaan kuvaa laitteistoturvallisuudella laitteistojen suunnitteluun, rakenteeseen, valmistukseen, kokoonpanoon, asennukseen, käyttöönottoon, kunnossapitoon ja laadunvarmistukseen liittyviä tietoturvallisuustoimenpiteitä. Laitteistoturvallisuuden tavoitteena on, että laitteiden suunnittelu, rakenne, kokoonpano, valmistus, kunnossapito ja laadunvarmistus on hoidettu niin, että laitteet toimivat luotettavasti. Teleyrityksen on käytettävä viestintäverkkojen ja viestintäpalveluiden tuottamiseen liittyvään toimintaan sellaisia laitteita, jotka ovat luotettavia ja käyttötarkoitukseensa sopivia. Laitteiden tulee olla myös rakenteeltaan suojattuja sähkömagneettisia häiriöitä ja ympäristöolosuhteiden aiheuttamia rasituksia vastaan määräysten ja säädösten mukaisesti. Viestintäverkkojen ja viestintäpalveluiden käytettävyydestä on huolehdittava riittävien ja tarkoituksenmukaisten varajärjestelyiden avulla. Esimerkiksi laitteistojen varaosien ja huoltopalvelujen saannista tulee varmistua.

Laitteiston koko elinkaareen liittyvissä palvelusopimuksissa määritellään palveluntaso. Palveluntasossa määriteltävillä rajoilla ja vasteajoilla on suuri vaikutus tietoturvatasoon ja tietoturvapoikkeamiin reagointiin. Valtionvarainministeriö (2009a) osoittaa laitteistoturvalli-

suus ohjeessaan, että palvelusopimusten vasteaikoihin tukeutumalla voidaan vähentää varastoitavaa varalaitteistoa. Näin toimiessa kuitenkin riippuvuus toimittajan kyvystä toimia vasteaikojen puitteissa kasvaa. On erityisen tärkeää, sopimuksilla määritellään toimenpiteet tilanteissa joissa joko koko palvelu sijaitsee palvelun tarjoajalla tai osa organisaation laitteista sijaitsee siellä. Tällaisessa tapauksessa joudutaan kiinnittämään huomiota yksittäisen laitteen fyysisen turvallisuuden järjestämiseen toisen osapuolen tiloissa ja tilojen käyttöoikeuksien hallintaan poikkeamatilanteissa. Näissä tapauksissa palvelusopimukset tulee määritellä koskettamaan koko järjestelmää ja sopimuksessa tulee vaatia riittävän tarkat selvitykset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään työajan ulkopuolella. Tämä tulee huomioida erityisesti tapauksissa joissa palvelu täytyy olla jatkuvasti asiakkaiden käytettävissä.

Valtionvarainministeriö (2009a) suosittaa laitteistoturvallisuus ohjeessaan, että laitteiston ylläpidossa tulee huolehtia poikkeamista toipumisesta. Poikkeaman tapahtuessa ja siitä toivuttaessa tulee kaikkien laitteiston tietojen oltava palauttavissa milloin tahansa. Tämä tarkoittaa, että laitteiston käyttöjärjestelmistä, ohjelmistoista, ohjelmistojen asetuksista ja ohjelmistojen sisältämistä operatiivisesta tiedosta tulee olla ajan tasalla olevat varmuuskopiot.

Paavilainen (Juhani Paavilainen, 2004: 13-14) pitää turvallisen järjestelmän toteutusprosessin lähtökohtana järjestelmän yksinkertaisuutta. Järjestelmä tulisi toteuttaa mahdollisimman yksinkertaiseksi ja kriittiset osat eriyttää muista järjestelmän osista. Tällä tavalla toteutetussa järjestelmässä on etuna, että kriittisten osien määrä saadaan minimoitua jolloin ne on helpompi toteuttaa korkealaatuisesti.

Tietokoneiden käyttöönottosuunnitelmaan tulee sisällyttää turva-asiat. Allen (2002: 28-73) osoittaa, että yleensä yritysten tietokoneiden käyttöönottosuunnitelmat käsittelevät tietoko-

neiden kustannuksia, asennusta, sovellus ohjelmistojen asennusta ja käyttäjien koulutusta. Kun käyttöönottosuunnitelmaan lisätään myös turva-asiat ja konfiguroidaan tietokoneet tietoturvavaatimusten mukaisesti, pystytään eliminoimaan useat tietoturva riskit liittyen verkkotietojärjestelmiin. Käyttöönottosuunnitelmasta on hyötyä kun joudutaan tekemään päätöksiä käytettävyyden ja tietoturvan välillä. Kun järjestelmät ovat konfiguroitu yhtenäisesti, voidaan järjestelmien käyttäytymistä ennustaa ja tällä tavoin helpottaa ylläpidon työtä ongelmatilanteissa.

Laitteiden ylläpitotoiminnassa ja huoltosopimuksissa on otettava huomioon tietoturvallisuusasiat muun muassa niin, että suojattavat tiedot eivät joudu näissä yhteyksissä asiattomien haltuun. Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) pidetään tärkeänä, että laitteiden asennuksesta, käyttöönotosta, tarkastamisesta ja käytöstä ylläpidetään ajan tasalla olevat ohjeet jotka on saatettu asianomaisten työntekijöiden tietoon. Ohjeissa tietoturvallisuusasiat on otettu huomioon tietoturvallisuuspolitiikan edellyttämällä tavalla.

Valtionvarainministeriö (Valtionvarainministeriö 2004) suosittaa valtionhallinnon keskeisten tietojärjestelmien turvaaminen ohjeistuksessaan, että järjestelmän laitteen käytöstä poistosta tulee laatia tarkka suunnitelma, jota seuraamalla tulee huomioitua kunkin poiston vaiheen vaatimukset. Mikäli jotain osaa järjestelmästä ollaan korvaamalla uudella laitteella ja vanhaa poistamassa tulee huomioida erityisesti mahdolliset vaiheet joiden kautta järjestelmä saadaan palautettua takaisin vanhaan kokoonpanoon. Laitteiston käytöstä poistossa tulee huomioida, että luottamuksellista jäännösdataa ei joudu sellaisten henkilöiden saatavaksi joilla ei siihen ole oikeutta.

Tietojärjestelmän perustana toimii laitteisto. Laitteiston tarjoamien palveluiden päälle rakennetaan sovelluksia jotka tarjoavat palveluita asiakkaalle. Weber (1999: 105) pitää laitteiston kehityksen hallintaa vastuussa järjestelmän analysoinnista, suunnittelusta, rakentamisesta, implementoinnista ja ylläpidosta.

Cheswick, Bellovin & Rubin (William R Cheswick, Steven M. Bellovin & Aviel D. Rubin, 2003: 260) pitävät palvelinta tietoturvallisena kun se testataan määrätyin aikavälein, palvelin on liitetty turvallisesti luotettavaan verkkoon, käyttöjärjestelmä on päivitetty ja konfiguroitu oikein, järjestelmän ylläpitäjät ovat autentikoitu vahvasti ja tarvitsevat fyysisen pääsyn palvelimelle. Muut käyttäjät lisäävät palvelimen tietoturvariskejä ja käyttäjätilien luomista tuli välttää jos vain mahdollista. Yleinen pääsy palvelimelle tulisi olla mahdollista vain pieneltä määrältä turvallisia tietokoneita, jotka on yhdistetty privaatilla ja hyvin salatulla yhteydellä turvalliseen palvelimeen.

Ruohonen (2002: 366-367) ehdottaa, että yksi tapa jolla järjestelmän ylläpitäjä voi testata palvelimensa tietoturvaa on yrittää itse murtautua palvelimelle. Murtautumisessa tulee käyttää samoja keinoja joilla ulkopuolinen voi yrittää murtautua palvelimelle. Jos tällaisen testin suorittaa ulkopuolinen taho, tulee tehdä yksityiskohtainen sopimus testitapauksesta: mitä testataan, miten testataan ja miten raportoidaan. Murtautumistestillä ei kuitenkaan voida todeta järjestelmää täysin turvalliseksi, järjestelmää ei voida koskaan osoittaa täysin turvalliseksi, ainoastaan turvattomaksi. Testin avulla voidaan löytää järjestelmästä mahdollisia tietoturva ongelmia. Testien ongelmana on kuitenkin niiden nopea vanheneminen. Koska aina kun järjestelmän komponentteja päivitetään, tulisi testi toistaa.

Splaine (Steven Splaine, 2002: 176) ehdottaa, että järjestelmän ylläpitäjän kannattaa harkita tietosaarekkeen luontia. Tietosaareke voidaan toteuttaa replikoimalla isäntä tietokannan tie-

to palvelimelle jossa web-sovellus sijaitsee. Kun tieto on replikoitu, poistetaan isäntä tietokannan ja web-palvelimen välinen verkkoyhteys.

Kaikkien organisaation kriittisten palveluiden tulee vaatia autentikointi. Hyvä tapa toteuttaa autentikointi on tunnus ja salasana suojaus. Kaikkein kriittisimmissä palveluissa Kajava & Remes (Jorma Kajava & Timo Remes, 2000: 15) suosittelevat kertakäyttöisten salasanojen käyttämistä.

Stallings & Brown (William Stallings & Lawrie Brown, 2008: 111) pitävät käyttöoikeuksien hallintaa tietoturvan keskeisimpänä elementtinä. Käyttöoikeuksien hallinnan periaate on: estää tunnistamattomien käyttäjien pääsy resurssiin, estää oikeutetun käyttäjän pääsy käyttämään luvattomia resursseja ja sallia oikeutetulle käyttäjälle pääsy luvallisiin resursseihin.

Allen (2002: 42-45) osoittaa, että usein eri palvelimia ja palveluita ylläpitävät eri vastuu henkilöt. Eristämällä palvelut omille palvelimilleen minimoidaan vastuuhenkilöiden kommunikoinnissa tapahtuvien epäselvyyksien aiheuttamat riskit. Palvelulle dedikoitu palvelin on myös helpompi konfiguroida vain tietylle palvelulle sopivaksi mikä vähentää palvelimella tarvittavien konfiguraatioiden tekemistä ja pienentää näiden konfiguraatioiden sisältämiä tietoturva riskejä. Tämän vuoksi palvelimelta kannattaa karsia kaikki turhat, ei käytössä olevat palvelut pois. Järjestelmiä konfiguroidessa voi hyvänä ohjesääntönä pitää ”kiellä ensin kaikki ja salli sitten tarvittavat”.

Schiffmanm, O’Donnell, Pennington & Pollino (Mike D. Schiffmanm Adam J. O’Donnell, Bill Pennington ja David Pollino, 2003: 280) ehdottaa, että Anonymous tileillä ei tulisi olla

luku ja kirjoitusoikeutta mihinkään hakemistoon. Jos kirjoitusoikeus tarvitaan, ei tulisi anonymous käyttäjälle antaa lukuoikeutta samaan hakemistoon.

Allen (2002: 56-58) pitää tärkeänä, että käyttöjärjestelmillä sijaitsevien tiedostojen käyttöoikeudet tarkastetaan säännöllisin väliajoin. Useissa käyttöjärjestelmissä on mahdollista määrittää yksilölliset tai käyttäjäryhmäkohtaiset käyttöoikeudet tiedostoille ja hakemistoille. Käyttöoikeuksien oikealla määrittelyllä voidaan vähentää riskiä tarkoituksellisten ja vahingossa tapahtuneiden tietomurtojen osalta. Myöntämällä järjestelmätason työkalujen käyttöoikeuden vain järjestelmän ylläpitäjille, estetään tavallista käyttäjää tekemästä turvallisuuteen liittyviä konfiguraatioita.

Chirillo (2001: 93-94) osoittaa, että sisään- ja ulostuloportit ovat kanava jonka kautta data liikkuu sisääntulo tai ulostulo laitteen ja prosessorin välillä. Näitä samoja portteja hyväksi käyttäen murtautujat yrittävät saada pääsyn palvelimelle, etsien avoimia tai kuuntelu tilassa olevia portteja. Murtautuja voi käyttää ohjelmaa joka käy kaikki palvelimen portit läpi minuuteissa. Tämän vuoksi on erittäin tärkeää, että kaikkia palvelimia ei liitetä suoraan Internettiin vaan palvelimen ja Internetin väliin laitetaan palomuuri jonka avulla ylimääräiset portit voidaan laittaa kiinni. Palvelimelta kannattaa poistaa myös kaikki ylimääräiset palvelut jotka ovat kuuntelu tilassa jossain portissa.

Palvelimen normaali käyttötila on yleensä hyvin turvattu. Allen (2002: 67-69) kuitenkin osoittaa, että palvelimella tapahtuvan huoltotyön aikana palvelimen turvataso saattaa olla alentunut hetkellisesti. Tällainen voi tapahtua kun palvelin on sijoitettu palomuurin taakse suojaan Internetistä tulevien hyökkäysten varalta ja palomuurista joudutaan avaamaan pääsy palvelimelle huoltotöiden vuoksi. Tällöin hyökkääjä voi hyödyntää tätä palomuurin sääntöä ja päästä käsiksi yrityksen sisäverkossa, palomuurin takana oleviin palvelimiin ja

niiden tietoihin. Seurauksena saattaa olla palvelimilla olevien tietoresurssien luottamuksellisuuden tai eheyden kärsiminen.

Kriittistä tietoa sisältävissä järjestelmissä pelkkä käyttäjän onnistunut kirjautuminen ei usein ole riittävä. Tällaisissa tapauksissa Stallings (William Stallings, 2000: 330) suosittaa, että kriittisten järjestelmien tietokannoissa tulee olla myös käyttäjienhallinta. Käyttäjänhallinnalla rajoitetaan käyttäjän pääsyä tietokannan eri tietoihin eritasoisilla käyttäjätunnuksilla.

Laitteistoriskejä mietittäessä tulee kiinnittää huomiota myös työntekijöiden työasemiin. Allen (2002: 25-26) listaa kolme tärkeää seikkaa:

1. Tiedon luottamuksellisuuden loukkaus. Tällainen voi tapahtua jos luvaton käyttäjä saa pääsyn koneelle, valtuutettu käyttäjä saa pääsyn tietoihin joihin hänellä ei ole oikeutta ja jos valtuutettu käyttäjä lähettää tietoja verkon yli käyttämättä asianmukaista salausta.
2. Tiedon eheyden muutos. Käyttäjä voi vahingossa tai tahallaan vääristää työasemalla olevia tietoja.
3. Tiedon saatavuuden estyminen. Käyttäjä ei voi käyttää työtehtävässään tarvitsemia resursseja (työasema, verkko, työasemalle tallennettu tieto tai työasemalla oleva palvelu).

Usein keskeiset järjestelmät vaativat toimiakseen tietovaraston. Valtionvarainministeriö (2009a) suosittaa laitteistoturvallisuus ohjeessaan, että keskeisien järjestelmien levyratkaisussa käytettäisiin vikasietoisia ratkaisuja. Datan käytettävyysvaatimusten korostuessa tulee levyjärjestelmän rakenteeseen ja sijoitukseen kiinnittää huomiota. Levyjärjestelmää suunniteltaessa tulee ottaa huomioon myös levyjärjestelmän kahdentaminen. Levyjärjestelmien

käytettävyyttä voidaan tukea erilaisilla RAID-ratkaisuilla. Valtionvarainministeriö (Valtionvarainministeriö 2001) muistuttaa kuitenkin, että vaikka levyjärjestelmässä käytettäisiin kahdennusta ja RAID-ratkaisua tulee levyjärjestelmä silti myös varmuuskopioida.

Allen (2002: 121-122) määrittelee palomuurin olevan laitteiston ja ohjelmiston yhdistelmä. Palomuurin käyttötarkoitus on kahden tai useamman verkon eriyttäminen toisistaan. Eriyttäminen tapahtuu verkkojen välistä liikennettä koskevien tietoturvapolitiikkojen toteuttamista. Osa palomuurilla eriytetyistä verkoista voi olla organisaation omassa hallinnassa, kuten organisaation sisäverkko. Toinen osa verkoista voi olla ulkoisia, organisaatiosta riippumattomia kuten Internet. Verkon palomuuri toimii ensimmäisenä puolustuksena ulkoverkosta tuleviin, yrityksen verkossa olevia palveluita ja luottamuksellista tietoa kohtaan olevia uhkia vastaan.

McClure, Scamray & Kurtz (Stuart McClure, Joel Scamray & George Kurtz, 1999: 314) suosittavat, että organisaation verkko tulee suojata ulkopuolisilta käyttäjiltä palomuurilla. Hyvin suunniteltu, konfiguroitu ja ylläpidetty palomuuri on luotettava laite Internetistä tulevien hyökkäysten torjumiseen. McClure *et al.* (1999: 337) osoittavat, että suurin osa palomuurien haavoittuvuuksista johtuu konfiguraatio virheestä ja ylläpidon laiminlyömästä laitteen tarkkailusta.

Allen (2002: 124) mukaan palomuurin yleisin käyttötarkoitus on erottaa organisaation sisäverkko Internetistä. Palomuuria suunniteltaessa tulee huomioida:

- palomuurin vikasietoisuus
- palomuurin suorituskyky
- käyttäjäkunta jotka käyttävät palveluita joita aiotaan tarjota Internetissä
- kuka ja miten palomuuria tullaan hallinnoimaan

- palomuurin resurssien tarve lähitulevaisuudessa

Palomuuria toteutettaessa täytyy valita toteutuksen arkkitehtuuri. Palomuuriarkkitehtuureita on olemassa kaksi eri tyyppiä: yksikerroksinen ja monikerroksinen. Yksikerroksisessa arkkitehtuurissa palomuuritoiminnon on sijoitettu yhteen fyysiseen palomuurilaitteeseen ja tämä laite on kytketty kaikkiin niihin verkkoihin joiden pääsynvalvonnasta palomuuri vastaa. Monikerroksisessa arkkitehtuurissa palomuuritoiminnot on jaettu pienelle joukolle palomuurilaitteita. Normaalisti palomuurilaitteet kytketään sarjaan jolloin niiden väliin jää aina demilitarisoitu vyöhyke (demilitariaed zone, DMZ). Monikerroksinen arkkitehtuuri on vaikeampi toteuttaa mutta tarjoaa paremman suojan ulkoverkosta, sisäverkkoon kohdistuvia hyökkäyksiä vastaan. Wikipedian artikkeli (DMZ) kuvaa demilitarisoitua aluetta fyysiseksi tai loogiseksi aliverkoksi, joka yhdistää organisaation järjestelmät turvattomampaan verkkoon. Demilitarisoitu alue on verkko kahden tai useamman palomuurin välissä. Demilitarisoidun alueen tarkoitus on lisätä organisaation lähiverkon turvatasoon uusi kerros.

Järvinen (Petteri Järvinen, 2006: 106-107) pitää palomuuria tärkeämpänä kuin virustentorjuntaohjelmistoa. Järvinen perustelee kantaansa koska palomuuri suojaa järjestelmää uhkilta joihin käyttäjä ei voi omilla toiminnoillaan vaikuttaa, kun taas virustentorjunnassa käyttäjän toiminnalla on keskeinen rooli.

Schiffmanm *et al.* (2003: 227) osoittavat, että palomuureja konfiguroitaessa tulee kiinnittää huomiota sääntöihin joilla voidaan kontrolloida porttien liikennettä perustuen MAC-osoitteiden hallintaan.

Allen (2002: 144-145) osoittaa, että yleisin syy palomuurien turvan ohittamiseen on palomuurin virheellinen konfiguraatio. Allen mukaan useissa lähteissä on esitetty tuloksia jois-

sa on osoitettu, että murtautumisyrityksistä palomuurijärjestelmää vastaan reilusti yli puolet on onnistunut virheellisten konfiguraatioiden aiheuttaman tietoturvauhkan vuoksi.

Allen (2002: 157) pitää tärkeänä, että palomuurijärjestelmä kerää lokeja palomuurin järjestelmän toiminnasta ja palomuurin säännöistä. On hyödyllistä jos palomuuri lähettää reaaliaikaisia hälytyksiä tärkeimmistä palomuurin tapahtumista. Tärkein syy lokien keräämiseen ja tulkitsemiseen on palomuurin jatkuvan toiminnan varmistaminen. Loki tietojen avulla voidaan seurata palomuurin tapahtumia, reagoida häiriöiden ennalta estämiseksi ja lokit helpottavat toipumista virhetilanteesta.

Krutz & Vines (2003: 48) osoittivat, että tunkeutumisen havaitsemisjärjestelmät ovat hyödyllinen komponentti tietoturvaa toteutettaessa. Tunkeutumisen havaitsemisjärjestelmä (Intrusion Detection System, IDS) helpottaa järjestelmän ylläpitäjää havaitsemaan onko organisaation tietoturvapolitiikkaa rikottu. Tunkeutumisen havaitsemisjärjestelmiä on kahdenlaisia: verkkoperustainen IDS ja Laiteperustainen IDS. Verkkoperustainen IDS tutkii reaaliajassa verkossa, palomuurin ympärillä tapahtuvaa liikennettä ja tuottaa tavallisesti luotettavia tietoja kuluttamatta verkon tai laitteen resursseja. Laiteperusteinen IDS tutkii tietokoneen järjestelmä- ja tapahtumalokeja ja tekee näistä raporttia käyttäjälle. Laiteperustaisen IDS:n ongelmana on monen järjestelmän puutteelliset lokitiedot. IDS järjestelmien ongelmana on myös niiden tuottaman suuren datamäärän tulkitseminen. Koska IDS tuottaa suuren määrän dataa, kuluttaa tämän datan läpikäynti ison ajan IDS:n ylläpitäjän työajasta.

Northcutt, Novak & McLachlan (Stephen Northcutt, Judy Novak & Donald McLachlan, 2002: 241-242) osoittavat, että mikään markkinoilla oleva hyökkäyksen havaitsemisjärjestelmä ei ole läheskään täydellinen. Monella niistä on mahdollista havaita suuri joukko hyökkäyksistä mutta mikään niistä ei pysty tunnistamaan kaikkia. Tämän vuoksi on tärke-

ää, että järjestelmän ylläpitäjät eivät käytä pelkästään valmiita havaitsemissovelluksia vaan käyttävät niitä lisänä murtojen havainnoinnissa.

Hakala ym. (2006: 183) pitävät tietoverkkojen ja tietojärjestelmien suunnittelun lähtökohtana organisaation toimintaprosesseja ja niistä johtuvia tietotarpeita. Tietotarpeiden vuoksi verkon ylläpitäjän tulee tuntea organisaation toimintaprosessit ja niiden vaikutukset tietojen käsittelyyn. Ennen järjestelmien suunnittelua tulisi määritellä missä ja miten organisaation tietoja halutaan säilyttää. On huomioitava, että kaikkea tietoa ei ole mahdollista suojata eikä se usein ole tarpeellistakaan. Organisaation tietojen suojausta suunniteltaessa kannattaa luoda tietojen luokitusjärjestelmä. Tietojenluokitusjärjestelmällä voidaan määritellä tiedon arvo ja luottamuksellisuus.

Tiedonsiirron turvallisuutta suunniteltaessa tulee huomioida ainakin seuraavat kolme asiaa: luottamuksellisuus, eheys ja käytettävyys. Krutz & Vines (2003: 61-64) osoittavat, että tietoverkkojen tietoturvasta vastaavan tulee olla selvillä etäkäyttöön liittyvistä tekniikoista. Näitä tekniikoita ovat: Puhelinverkot ja Internet-etäyhdeydet (esimerkiksi xDSL, ISDN, langattomat verkot, kaapelimodeemit, ym.) sekä organisaation televiestinnän etäyhteydet (VPN, SSL, SSH-2 ym.) ja Etäkäytön todennusjärjestelmät (esimerkiksi RADIUS, ym.).

Hakala ym. (2006: 184) suosittavat, että ennen tietoverkon suojaamisen suunnittelua ja toteutusta tulee päättä tietoverkon rakenne. Tietoverkkoon rakenteessa kuvataan: mihin segmentteihin palvelut laitetaan, millaisella kaapelointijärjestelmällä toteutetaan, mitä aktiivilaitteita käytetään ja mitä laajaverkkoliittymiä hankitaan. Tietoverkon rakenteessa tulee ottaa huomioon myös: ettei liikenteellisiä pullonkauloja pääse syntymään ja että organisaation sisäverkkoon ei päästä ulkopuolelta kuin suojattuja yhteyksiä pitkin.

Splaine (2002: 56-57) osoittaa, että rajoittamalla organisaation sisäverkon ulkopuolelle näkyvien laitteiden määrä mahdollisimman pieneksi, pystytään pienentämään tietomurtojen riskiä. Laiteiden yhteydet tulee huomioida myös organisaation sisäverkon sisällä. Kun organisaation sisäverkon segmenttien välillä laitteiden pääsy minimoidaan, pystytään pienentämään organisaation sisältä tulevien hyökkäysten uhkaa.

Allen (2002: 83-89) suosittelee, että palvelin joka tarjoaa palveluitaan Internetissä (esimerkiksi www-palvelin) tulisi sijoittaa erilliseen, suojattuun aliverkkoon. Tällä tavalla toimimalla voidaan varmistaa, ettei palvelimen ja Internetin välinen liikenne vaikuta yrityksen sisäverkon toimintaan ja muodosta näin ylimääräisiä tietoturvariskejä.

Jaakohuhta (Hannu Jaakohuhta, 2003: 85) pitää tärkeänä, että verkko tukee toteutukseltaan ja rakenteeltaan vikasietoisuutta ja mahdollistaa erilaisten vikasietoisten komponenttien käytön. Yhtä tärkeää on tarkastella verkon komponentteja, joilla verkko on rakennettu. Verkon komponentit ovat usein osa-alue josta johtuu verkon vikatilanteet ja verkon palveluiden saatavuuden heikkeneminen.

Organisaation tietoliikenneyhteyksien katkeaminen johtaa usein Jaakohuhtan (2003: 85) mukaan koko organisaation toiminnan keskeytymiseen. Nykyään useat palvelut toimivat saman tietoliikenne infrastruktuurin sisällä. Tällaisessa tapauksessa verkon vioittuminen muodostaa uhan kaikkien verkkopalveluiden saatavuudelle. Saatavuutta pyritään parantamaan verkon vikasietoisuudella. Vikasietoinen verkko jatkaa toimintaa vaikka osan siitä vikaantuessakin. Vikasietoinen verkko antaa toimiville aplveluille yhteyspalveluita, vaikka osa verkosta olevista palveluista on poissa käytöstä. Vikasietoinen verkko pyrkii muodostamaan yhteyden varayhteyden avulla.

Verkkolaitteet kuten reitittimet, kytkimet, hubit, palomuurit, kaapelimodeemit ja langattomat tukiasemat usein asennetaan, konfiguroidaan ja otetaan tuotantoon. Cheswick *et al.* (2003: 265) varoittavat, että usein tämän jälkeen laitteet unohdetaan. On kuitenkin tärkeää, että tuotannossa olevia verkkolaitteita valvottaisiin ja päivitettäisiin ja konfiguroitaisiin myös tuotantoon oton jälkeen. Verkkolaitteet tulisi konfiguroida samalla tavalla kuin palvelimetkin. Laitteille tulisi ottaa käyttöön vain tarvittavat palvelut, etenkin mikäli laitteella on tärkeä rooli tietoverkkojen yhdistämisessä.

Barmanin (Scott Barman, 2002: 73) mukaan verkon tietoturvalla ei aina tarkoitetta Internet yhteyden turvaamista vaan kaikkien verkkojen, yhteyksien ja liittymien suojaamista. Tällä tarkoitetaan yhteyden muodostamista tiedon ja käyttäjän välille. Lähtökohta yhteyden muodostamiselle on käyttäjän autentikointi. Autentikointi on ensimmäinen tapa suojata järjestelmä tai verkko. Verkon sisällä verkon arkkitehtuuria tulisi käyttää hyödyksi toteutettaessa verkon tietoturvaa.

Hakala ym. (2006: 183) osoittavat, että yleisin tietoverkkoihin kohdistuva uhka on tiedon saannin estymien. Estymisen voivat aiheuttaa verkon aktiivilaitteet, verkkokortti, kaapelointijärjestelmä tai palvelun tukkiva hyökkäys.

Iso organisaatio tarvitsee suuren määrä IP-osoitteita käyttöönsä. Hakala ym. (2006: 215) pitävät käytännössä mahdottomana, että iso organisaatio saisi hankittua vapaita B-luokkia tai yhdistämiskelpoisia C-luokkia riittävästi tarpeisiinsa. Organisaation kannattaakin rakentaa sisäisen IP-verkkonsa käyttämällä intranet-osoitteita. Intranet-osoitteita ei tarvitse rekisteröidä, eikä niiden välistä liikennettä välitetä Internetissä. Usein organisaation ulkopuolelle suuntautuva liikenne on vain murto-osa sisäisestä liikenteestä. Tällaisissa tapauksissa organisaatio voi käyttää osoitteenmuunnos-palvelua (Network Address Translation, NAT).

Osoitteenmuunnos-palvelun avulla organisaation sisäverkosta Intenettiin suuntautuvan liikenteen intranet-osoitteet muutetaan organisaation julkisiksi IP-osoitteiksi Internettiin liitetyssä reitittimessä ja vaihtaa paluupakettien julkisen IP-osoitteen intranet-osoitteeksi.

Kuusela & Ollikainen (1998: 242-243) esittävät, että kriittisillä palveluilla tulisi olla täydellinen varalaitteisto joka on käyttövalmiudessa jatkuvasti tai toimii osana varsinaista tuotantojärjestelmää. Usein kuitenkin riittää, että palvelu on siirrettävissä toiseen laitteistoon sallitussa aikaikkunassa. Siirtämisellä tarkoitetaan palvelun (prosessien, tiedostojen ja tietokantojen) siirtämistä toiselle palvelimelle.

Järjestelmän kaikkien laitteiden ohjelmistolla tapahtuva valvominen helpottaa ja nopeuttaa reagointia poikkeus tilanteisiin. Laitteistoturvallisuus ohjeessaan valtionvarainministeriö (2009a) osoittaa, että kaikki järjestelmän laitteet tullee olla jatkuvasti valvonnassa ohjelmien avulla ja niiden käyttöasteiden kehittymistä on seurattava säännöllisesti. Järjestelmien tietoturvapäivityksiä varten on oltava selkeät toimintaohjeet ja päivitykset in testattava ennen tuotantojärjestelmän päivitystä. Päivitysten hallinnassa tulee ottaa huomioon myös päivitysten mahdollinen peruminen. Päivitystenperuminen tulee olla mahdollista, mikäli päivityksessä havaitaan ongelmia.

Palvelunestohyökkäyksellä (Denial Of Service, DoS) tarkoitetaan verkkopalvelun ruuhkauttamista siten, että palvelu ei ehdi vastata oikeiden asiakkaiden pyyntöihin ja täten palvelu lamautuu (Wikipedia palvelunestohyökkäys). Tällaiset hyökkäykset maksavat vuodessa miljoonia yrityksille. Kustannukset tulevat ajasta jolloin palvelu ei ole käytettävissä, pienentyneestä liikevaihdosta ja ongelman ratkaisemiseen käytettyjen henkilöiden palkkauksesta. Palvelunesto hyökkäyksen tavoite ei ole järjestelmään tunkeutuminen vaan sen häirit-

seminen. Oleellisesti DoS hyökkäys vaikuttaa oikeiden käyttäjien työskentelyyn, verkon toimintaan, järjestelmiin tai muihin resursseihin.

Krutz & Vines (2003: 74-77) luokittelevat karkealla tasolla tietoverkkoa vastaan kohdistuvat hyökkäykset kuuteen eri luokkaan seuraavasti:

1. Verkon palveluiden luvaton käyttö. Verkon valtuutettu käyttäjä hyödyntää palveluita, joiden käyttöön hänellä ei ole oikeutta.
2. Verkon luvaton käyttö liiketoimintaan kuulumattomiin tarkoituksiin. Verkon käyttäjä käyttää verkkoa omiin tarkoituksiinsa.
3. Verkon salakuuntelu. Käyttäjä sieppaa luvattomasta paketteja verkosta.
4. Palveluiden estäminen ja muu palveluiden häirintä. Käyttäjä estää verkon palveluiden saatavuuden tukkimalla verkon resurssit.
5. Verkkoon tunkeutuminen. Ulkopuolinen käyttäjä tunkeutuu verkkoon.
6. Tunnustelu. Tunnustelu on salakuuntelun aktiivinen muoto. Käyttäjä kerää verkosta ja sen palveluista tietoa ennen verkkoon tunkeutumista tai palvelun estohyökkäyksen tekemistä.

Andersson (Ross Andersson, 2001: 387-389) osoittaa, että verkosta ja etenkin Internetistä tulleet hyökkäykset ovat kaikkein vaikeimpia selvittää koska mahdollisia tapoja tehdä hyökkäys verkosta tai sen avulla on lukematon määrä. Ideaali tilanteessa käyttäjät suorittaisivat hyvin koodattuja ohjelmia tietoturvallisella alustalla, mutta todellisuudessa tämä ei usein onnistu. Palomuurit tarjoavat tällaisissa tapauksissa ratkaisun pitämään suurimman osan hyökkääjistä palvelun ulkopuolella.

Schiffmanm *et al.* (2003: 268-270) osoittavat, että sessioiden kaappaus ja –salakuuntelun riskejä voidaan pienentää session datan koodaamisella (encription). Datan koodaamiseen on olemassa useita eri tapoja joista tulee valita käyttötapaukseen sopivin vaihtoehto.

Cheswick *et al.* (2003: 96) muistuttavat, että järjestelmien salasanat tulisivat olla riittävän vaikeita arvata ja riittävän pitkiä ja monimutkaisia murtaa nopeasti. Virheelliset kirjautumisyritykset tulisi kirjata lokiin mahdollista myöhempää tutkimusta varten.

Käyttäjän autentikointi prosessi sisältää useita riskejä. Stallings & Brown (William Stallings & Lawrie Brown, 2008: 99-101) määrittelevät riskeiksi: asiakas hyökkäyksen (client attack), jossa hyökkääjä yrittää saada käyttäjän tunnukset itselleen ilman yhteyttä kohde järjestelmään tai käyttäjän ja kohdejärjestelmän yhteyskäytävään. Palvelin hyökkäyksen (host attack), jotka suunnataan käyttäjä tiedostoon jossa salasanat, valtuutusavaimet tai biometriset pohjat ovat. Salakuuntelun (eavesdropping), hyökkääjä yrittää keksiä käyttäjän salasanan seuraamalla käyttäjän toimintaa, löytämällä käyttäjän ylöskirjoittaman salasanan, jollain muulla tavalla joka vaatii hyökkääjän ja käyttäjän välistä kontaktia tai keyloggerin avulla varastaa käyttäjän tunnukset. Replay, tässä hyökkääjä toistaa käyttäjän lähettämän vasteen. Troijan hevonen (Trojan horse), jossa haittaohjelma väittää käyttäjälle olevansa kohdejärjestelmä ja kysyy käyttäjältä tunnusta joka haittaohjelma sitten tallentaa hyökkääjälle myöhempää käyttö varten. Palvelunestohyökkäys (denial-of-service) yrittää poistaa käytöstä käyttäjän tunnistuksen ruuhkauttamalla sen palvelu pyynnöillä.

On yleisesti tiedossa, että on olemassa kolme erityylistä DDoS hyökkäystä. Stallings & Brown (2008: 266) listaavat ne seuraavasti:

1. Hyökkäyksen estäminen (ennen kuin hyökkäys on alkanut).
2. Hyökkäyksen tunnistaminen ja suodatus (hyökkäyksen aikana).

3. Hyökkäyksen lähteen selvittäminen ja tunnistaminen (hyökkäyksen aikana ja sen jälkeen).

Julkisen avaimen algoritmit pohjautuvat matemaattisiin funktioihin, eikä pelkkiin yksin kertaisiin jaksotettuihin operaatioihin. Stallings (2000: 62) pitää vielä tärkeämpänä, että julkisen avaimen salaus on asymmetrinen, jolloin tarvitaan kaksi avainta sanoman purkamiseen kun taas symmetrisessä tavassa riittää yksi avain. Kahden avaimen käytöllä on Stallingsin (2000 S.62) mukaan osoitettu olevan huomattavia etuja luotettavuudessa, avaimen jakelussa ja autentikoinnissa verrattuna yhden avaimen tekniikkaan.

Hakala ym. (2006: 183) huomauttavat, että monissa palvelinsovelluksissa ja verkon aktiivilaitteissa on ohjelmistovirheitä jotka mahdollistavat niitä koskevien suojausten kiertämisen palvelun kaatuessa.

Splaine (2002: 71) pitää tärkeänä, että kriittisen tiedon välitys tapahtuu kryptattuna tai fyysisesti suojatun yhteyden välityksellä. Nämä kaksi toimenpidettä yhdistämällä voidaan minimoida kriittiselle tiedolle aiheutuvat uhat.

4. OHJELMISTOTURVALLISUUS

Sovellus voidaan hankkia ulkopuoliselta taholta tai tehdä itse. Krutz & Vines (2003: 245) mukaan kuitenkin sovelluskehitykseen kuuluu aina tietoturvaa koskevia tekijöitä jotka tulisi huomioida sovelluksen hankinta prosessissa. Sovelluksen turvallisuudesta tulee myös aina varmistua ennen sovelluksen tuotantoon ottoa.

Ohjelmistoturvallisuudella tarkoitetaan tietoturvallisuuden osa-aluetta, joka käsittää muun muassa käyttöjärjestelmät, sovellusohjelmat ja tietoliikenneohjelmistot. Alueeseen kuuluvat ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt, ohjelmistojen laadunvarmistus sekä niiden ylläpitoon ja päivitykseen liittyvät turvallisuustoimet.

Hyvösen (2003: 142-144) mukaan ohjelmistoturvallisuuden tavoitteena on, että käyttöjärjestelmät, sovellusohjelmat, varusohjelmat sekä muut tärkeät ohjelmistot ja niiden asetukset ovat luotettavia ja toimivat oikein siinä käyttötarkoituksessa mihin ne on tehty. Ohjelmistoprojektin aiheena on usein uusi tuote. Uutta tuotetta kehitettäessä ympäristö on dynaaminen ja hyvin usein muuttuva. Tuotetta tehdessä tällaiseen ympäristöön yksityiskohtaisesti kuvatun ohjelmistoprojektisuunnitelman noudattaminen osoittautuu usein mahdottomaksi seurata.

Webin käytön yleistyessä Internetissä olevien palveluiden tietojen suojaamisen tärkeys on korostunut. Krutz & Vines (2003 S.xiii) osoittavat, että Internetissä oleviin palveluihin yleensä kohdistuvia uhkia ovat: tietomurto, palvelun estohyökkäys, kriittisten resurssien luvaton käyttö ja vahingolliset haittakoodit, jotka tuhoavat tai muuttavat tietoja.

Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) osoitetaan, että teleyrityksen on käytettävä viestintäverkkojen ja viestintäpalveluiden tuottamiseen liittyvään toimintaan sellaisia laitteita ja ohjelmistoja, joiden tietoturvallisuusriskit ovat hallittuja. Ohjelmistojen osalta tietoturvallisuusriskejä voidaan hallita muun muassa ohjelmistotuotteiden hankinnan, konfiguroinnin, käytön ja ylläpidon yhteydessä.

Yrityksen hankkiessa ohjelmistotuotteita tulee hankkijan kartoittaa toimittajan ja tuotteen yleinen luotettavuus ja asema markkinoilla sekä kyky huolehtia tukipalvelujen jatkuvuudesta. Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) pidetään tärkeänä, että ohjelmistojen osalta huolehditaan siitä, että ne on varustettu riittävillä tunnistamis-, pääsynvalvonta- ja tapahtumatietojen kirjaamisominaisuuksilla. Ohjelmistojen toimivuus, mukaan lukien em. ominaisuudet on testattava ennen ohjelmistojen käyttöönottoa.

Hajautettuja palveluita suunniteltaessa ja toteutettaessa Gollmann (Dieter Gollmann, 1999: 174) mukaan, tulee ottaa huomioon: tarvittavien autentikointien määrä kasvaa, eri komponentit eivät välttämättä täytä samoja tietoturva määrityksiä (mentävä vaativimman mukaan) ja käyttäjät sekä palveluiden ohjelmoijat eivät välttämättä ole tietoturva experttejä jolloin he voivat toiminnallaan aiheuttaa tietoturvariskin.

Allen (2002: 21) suosittelee järjestelmän ylläpitäjää tarkastamaan toimittajan esiasentamien tietokoneiden konfiguraatiot. Tyypillisesti toimittajat suosivat oletus konfiguraatioissa enemmän ominaisuuksia ja toimintoja kuin turvallisuutta. Tämän vuoksi on ylläpitäjän kon-

figuroitava uudet ja olemassa olevat palvelimet ja työasemat siten, että ne vastaavat organisaation tietoturvavaatimuksia.

Allen (2002: 42-45) suosittelee, että jokainen verkossa palvelujaan tarjoava sovellus sijaitsisi dedikoidulla, vain tätä palvelua varten olevalla palvelimella. Kun palvelin tarjoaa vain tarvittavat verkkopalvelut, ei muita palvelimella olevia palveluita voida käyttää palvelinta vastaan suunnatussa hyökkäyksessä. Jokainen palvelimelle asennettu palvelu kasvattaa palvelinta kohtaan tehtyjen onnistuneiden tietomurtojen riskiä.

Garfinkel & Spafford (Simon Garfinkel & Gene Spafford, 2002: 6-7) mukaan hyökkääjä voi huonosti kirjoitettu scriptiä tai ohjelmistoa hyväksi käyttäen murtautua palvelimelle ja muuttaa web-palvelimen asetuksia ja muokata tiedostoja. Hyödyntämällä tällaista haavoittuvuutta voi hyökkääjä luoda palvelimelle scriptin jonka avulla hyökkääjä voi saada täyden pääsyn palvelimelle.

Garfinkel & Spafford (2002 S.6-7) osoittaa myös, että vaikka web-palvelin olisi suojattu ja siinä ajettaisiin vain turvallisia scriptejä ja ohjelmistoja on mahdollista että hyökkääjä käyttää web-palvelimen käyttämää tietokanta palvelinta hyökkäykseen. Hyökkääjä hyökkää suoraan tietokantapalvelimelle ja voi tällöin saada pääsyn tietokannan tietoihin. Nämä molemmat hyökkäystavat ovat mahdollisia ja tulisi huomioida palvelinten ohjelmistoja suunniteltaessa ja käyttöönotettaessa.

Allen (2002: 39-42) osoittaa, että ohjelmistot ovat monimutkaisia ja niissä olevat tietoturvaongelmat ilmenevät vasta kun ohjelmisto on ollut laajassa käytössä. Vaikka suurin osa toimittajista yrittää reagoida toimittamissaan ohjelmistoissa oleviin tietoturvaongelmiin vä-

littömästi. Käytännössä aikaa kuluu kuitenkin ennen kuin toimittajan julkaisema päivitys on asennettavissa loppukäyttäjällä. Aika tässä välissä antaa hyökkääjälle mahdollisuuden hyödyntää tietoturva-aukkoa ja tällä tavoin hyökätä verkkoa tai tietoverkossa olevia tietokoneita vastaan. Tämän väliajan minimoimiseksi kannattaa ottaa huomioon, sovellusten tietoturva ongelmien jokapäiväinen seuranta, määritellä toimintamalli kun tietoturvaongelma havaitaan ja miten korjaukset hankitaan toimittajalta.

Allen (2002: 39) pitää käyttöjärjestelmien ja sovellusohjelmistojen päivitysten huomioimista tärkeänä. Päivitysten seurannan tulisi olla osa järjestelmän ylläpitäjän jokapäiväistä toimintaa. Kun toimittaja julkaisee uuden päivityksen, on ylläpitäjän arvioitava se, tehtävä päätös onko päivitys tarpeellinen ja myönteisessä tapauksessa asennettava päivitys. Tällaisten päivitysten asentaminen suojaa järjestelmiä tehokkaasti ja vähentää niiden alttiutta hyökkäyksille.

Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) osoitetaan, että käytön ja ylläpidon osalta tietoturvallisuusriskejä voidaan hallita muun muassa huolehtimalla siitä, että ohjelmistoista on käytössä mahdollisimman tietoturvalliset ja ajantasaiset versiot ja että ohjelmistojen konfiguroinnit suoritetaan tietoturvallisesti. Konfigurointien yhteydessä tulee huolehtia, että järjestelmissä ei ole sellaisia palveluja päällä, jotka eivät ole tarpeellisia järjestelmän tarkoituksenmukaisen käytön ja toiminnan kannalta.

Ohjelmistojen tietoturvapäivitysten säännöllisestä ja ajantasaisesta asentamisesta on huolehdittava. Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) suositetaan, että tietoturvapäivitysten toimivuus tarkistetaan ennen niiden asentamista tuotantojärjestelmiin ja päivitystä ei tule asentaa jos se aihe-

uttaa merkittävää vaaraa järjestelmien muulle toiminnalle. Viestintäverkkojen ja viestintäpalveluiden tuottamiseen käytettävissä järjestelmissä tulee olla riittävät ja tarkoituksenmukaiset suojausmekanismit tietoturvaloukkauksia vastaan. Suojausmekanismien tulee sisältää muun muassa virusten, matojen ja muiden haittaohjelmien torjuntamekanismit. Lisäksi järjestelmissä tulee olla mekanismit haitallisen liikenteen suodattamiseksi ja estämiseksi.

Usein sovellustoimittajan toimittamat ohjelmistot ja räätälöidyt sovellukset sisältävät virheitä. Kyrölä (2001: 115-116) pitää virheiden korjaamista sovellustoimittajan tehtävänä. Ohjelmiston korjauspaketin sovellustoimittaja voi toimittaa usealla eri tavalla käyttäjäorganisaatiolle, Internet-sivustojen ollessa yleisin toimintamalli. Räätälöityjä sovelluksia korjatessa, korjauksen voi suorittaa yrityksen sovellusvastuuhenkilö. Sovellusvastuuhenkilön päivittäessä ohjelmiston tulee ennen päivitystä ja sen jälkeen varmistua päivityksen vaikutuksesta liittymäsovelluksiin.

Palvelua käyttääkseen on käyttäjän kirjauduttava sovellukseen. Kirjautuminen vaatii tunnistuksen ja todennuksen. Krutz & Vines (2003: 36) tarkoittavat tunnistuksella toimenpidettä jolla käyttäjä ilmaisee henkilöllisyytensä järjestelmälle ja todennuksella varmistumista siitä, että käyttäjä on oikeasti henkilö joksi hän on itsensä järjestelmälle esitellyt olevansa. Tällainen kombinaatio on yleensä käyttäjätunnus ja salasana sovellukseen tai järjestelmään sisään kirjautuessa.

Allen (2002: 67-69) mukaan palvelinten hallinnointi etäyhteyden välityksellä aiheuttaa tietoturvariskin. Palvelinten hallinnollisiin toimenpiteisiin kuuluu käyttäjätietojen päivittäminen, lokien tarkastelu, ohjelmien asentaminen, ohjelmien konfigurointi ja ohjelmien poistaminen. Allen suosittaa, että ylläpidolliset toimenpiteet tehtäisiin palvelimissa paikallisesti koska se on turvallisempaa. Usein kuitenkin tämä on liian työlästä ja joskus jopa melkein

mahdotonta. Tällöin tuleekin ottaa huomioon hallinnnointikoneen, verkon ja hallinnoinnin kohteena olevan palvelimen turvallisuus.

McClure, Scambray & Krutz (Stuart McClure, Joel Scambray ja George Krutz, 2002: 555-576) osoittavat, että etäkäyttöohjelmat ovat erittäin hyödyllisiä järjestelmien ylläpitäjille. Järjestelmänylläpitäjä voi ottaa yhdetyttä käyttäjän koneeseen virtuaalisesti etäkäyttöohjelmiston avulla ja selvittää korjatakseen ongelman tai avustaakseen käyttäjää. Etäkäyttö ohjelmistojen käytössä tulee kuitenkin ottaa huomioon niiden konfigurointi ja tietoturvallisuusaukot joiden avulla hyökkääjä voi päästä kohdekoneeseen ja saada pääsyn arkaluontoiseen tietoon.

Ohjelmistojen varmuuskopiointi on tärkeä osa ohjelmistoturvallisuutta. Krutz & Vines (2003: 67-71) mukaan varmuuskopiointiin on olemassa useita eri menetelmiä, mutta he (Ronald L. Krutz & Russell Dean Vines) listaavat kolme perus menetelmää seuraavasti:

1. Täydellinen varmuuskopio (Full Backup). Tehdään varmuuskopio kaikista tiedostolistauksessa olevista tiedostoista.
2. Lisäävä varmuuskopio (Incremental Backup). Tehdään varmuuskopio vain äskettäin (esimerkiksi, tuona päivänä) lisätyistä ja muokatuista tiedostoista.
3. Eroavuuskopiointi (Differential backup). Tehdään varmuuskopio uusista tiedostoista ja tiedostoista joita on muutettu viimeisen täydellisen varmistuksen jälkeen.

WWW-palvelin sovellukset tuottavat tärkeää tietoa kun halutaan seurata palvelun toimintaa ja tietoturvaloukkauksia. Allen (2002: 94) tekee eron www-palvelun ja palvelimen käyttöjärjestelmien tuottamien loki tiedostojen välille. WWW-palvelimen käyttöjärjestelmä tuottaa itse lokitietoja, mutta nämä eivät usein riitä, kun selvitetään www-palvelimella tapahtuneita ulkoisia tietoturvaloukkauksia. WWW-palvelimen sovelluksen tuottamat lokit ovat

täydentäviä ja koskevat vain web-palvelun tapahtumia kun taas käyttöjärjestelmän lokeista selviää järjestelmän toiminnan tapahtumat. WWW-palvelinsovelluksen tuottamat loki tiedot ovat usein ainut paikka mistä selviää hyökkäys yritykset palvelua kohtaa. Yleensä palvelimen ja verkon lokit pystyvät antamaan hälytyksen jos palvelussa on tapahtunut jokin epäilyttävä tapahtuma joka vaatii tarkempaa tutkimista.

Allen (2002: 97-98) osoittaa, että www-palvelin yksinkertaisimmillaan kuuntelee käyttäjän pyyntöjä ja pyynnön tullessa palauttaa käyttäjälle käyttäjän pyytämän tiedoston. Kuitenkin harvalla www-palvelimella pelkästään tällainen palvelu riittää. On yleistä, että www-palvelin käynnistää lisätoimintoja: scriptejä tai plug-in-ohjelmia. Lisätoiminnot voivat liittyä käyttäjän lähettämän datan muokkaukseen, ohjelmien suorittamiseen tai tuottaa pyynnön mukana tulleesta datasta räätälöityä informaatiota. Lisätoimintojen implementoinnista www-palveluun voi aiheutua usein myös tietoturvauhkia. Monet onnistuneet hyökkäykset web-sivustoja vastaan on toteutettu hyödyntämällä jo tunnettuja ja yleisesti tiedossa olevia tietoturva-aukkoja.

Allen (2002: 105-106) suosittelee, että ennen kuin julkiselle www-palvelimelle tallennetaan luottamuksellista tai rajoitetulle käyttäjäkunnalle tarkoitettua tietoa, tulee määritellä turvavaatimukset ja suojausvaatimukset sekä varmistaa, että palvelimella käytössä olevilla suojaustekniikoilla voidaan täyttää nämä tarpeet. WWW-palvelimelle on olemassa useita suojaustekniikoita joilla voidaan eritasoiset käyttäjätunnukset omaavat käyttäjät tunnistaa. On yleistä, että suojaustekniikat pohjautuvat salaustekniikoihin. Salaustekniikoilla voidaan luoda salattu väylä www-selaimen ja www-palvelimen välille. Ilman salausta ulkopuolinen voi pasta käsiksi verkkoliikenteeseen www-palvelimen ja www-selaimen välillä ja pystyy pahimmassa tapauksessa tutkimaan ja muuttamaan luottamuksellista tai rajoitetulle käyttäjäkunnalle tarkoitettua tietoa vaikka tiedon hakija olisi järjestelmässä tunnistettu. Tämän seurauksena tiedon eheys ja luottamuksellisuus vaarantuvat. Yleisimpiä salaustekniikoita

ovat SSL(Secure Socket Layer), S/HTTP (Secure Hypertext Transport Protocol) ja SET (Secure Electronic Transaction).

Ohjelmistoihin kuuluvat käyttöjärjestelmät, hyötyohjelmat ja sovellukset. Stallings & Brown (2008: 17-18) nimeävät suurimmaksi ohjelmistoja koskevaksi uhkaksi, hyökkäys saatavuutta vastaan. Ohjelmisto ja eritoten sovellusohjelmat on helppo poistaa. Ohjelmisto on helppo tehdä käyttökelvottomaksi muuttamalla ja vahingoittamalla Ohjelmistojen korkeaa saatavuutta voidaan tukea ottamalla säännöllisesti varmistuksia uusimmista versioista. Vaikeampaa on selvittää ongelma kun ohjelmisto toimii erilailla kuin ennen. Stallings & Brown (2008: 18) määrittelevät myös ohjelmistopiratismin kuuluvan ohjelmisto uhkiin.

Jaakohuhta (2003: 65-66) pitää tärkeänä, että varmistukset säilytetään järjestelmästä erillisessä kiinteistössä palonkestävässä kassakaapissa. Tällöin vaikka järjestelmä tuhoutuisi, voidaan olla kuitenkin varmoja, että järjestelmä saadaan palautettua kohtuullisessa ajassa varmistuksista. Koska varmistukset sisältävät usein arkaluontoista tietoa, on varmistusten säilytyksessä huomioitava organisaation tietoturva ja tietosuoja määräykset.

Sovellukset joihin tallennetaan asiakastietoja, luetaan kriittisiin sovelluksiin. Salminen (Markus Salminen, 2009: 31) osoittaa, että asiakastietojen käsittely tulee aloittaa aina tietojen käsittelyn suunnittelulla. Tietojenkäsittelyn suunnitelman jälkeen voidaan edetä henkilötietojen käsittelyn aloittamiseen. Henkilötietojen käsittelyssä on huomioitava tiedon laadusta ja tulee varmistua tiedon tietoturvasta.

Uutta sovelluskomponenttia käyttöönotettaessa tulee se testata ensin testiympäristössä jossa voidaan todentaa komponentin toimivuus. Tässä vaiheessa tulee kiinnittää huomiota tieto-

turvaan ja varata riittävästi resursseja ja aikaa tuotannon käyttöönottoon. Brenton & Hunt (Chris Brenton & Cameron Hunt 2003: 24-25) purkavat uuden komponentin käyttöönoton neljään osaan:

1. Toiminnallisuus, varmistetaan että sovellus toimii odotusten ja vaatimusten mukaisesti.
2. Konfigurointi, varmistetaan että sovellus toimii oikein eri konfiguraatioilla.
3. Ylläpito, varmistetaan sovelluksen toimivuus, mahdollisten vikojen etsintä ja päivitettävyys.
4. Koodin katselmus, viimeinen vaihe. Käydään läpi sovelluksen koodi ja etsitään mahdollisia bugeja tai suunnitteluvirheitä. Puskurin ylivuodon ollessa yleisin ongelma sovelluksissa tulee puskureiden käsittelyyn kiinnittää erityistä huomiota.

Lars (Lars Klander, 1997: 641) ei pidä mitään ohjelmistoa virheettömänä ja tämän vuoksi vaativat jatkuvaa tarkkailua ja mahdollista päivittämistä. Koska turvallisten web ohjelmistojen kirjoittaminen ja testaaminen on vaikea tehtävä ja voi pahimmillaan altistaa koko järjestelmän hyökkäykselle. Garfinkel & Spafford (2002: 471) ehdottavat, että itse kirjoitettuja ohjelmia tehdessä tulee seurata tarkasti ohjelmointikielen tietoturvaohjeita ja tarkistuttaa valmis ohjelmisto jollain toisella, luotettavalla taholla.

Hakala ym. (2006: 336) huomauttavat, että sovellusten suunnittelussa tulee miettiä tarkasti tietojen saatavuutta ja käyttökelpoisuutta. Saatavuutta ja käyttökelpoisuutta mietittäessä tulee miettiä ohjelmistoteknisiä ratkaisuja, käyttöliittymän esitysmuotoa, sovelluksen nopeutta, sovelluksen aiheuttamaa verkko ja laitteistokuormaa.

Hyvönen (2003: 142) todistaa, että ohjelmistoprojekteissa lopputulokset syntyvät työtätekevien asiantuntijoiden toimesta. Asiantuntijoita ei tulisi johtaa käskyttämällä, vaan päälli-

kön on itse aktiivisesti osallistuttava työtehtäviin tekemällä yhteistyökumppaneiden ja asiantuntijoiden kanssa yhdessä työtä.

Allen (2002: 83) varoittaa, että web-palveluita tarjoavan palvelimen ollessa kaikille Internetissä avoin, voi kuka tahansa ympäri maailman tehdä palvelimelle palvelupyynnön. Vaikka palvelin itse ja palvelimelle asennetut sovellukset olisivat konfiguroitu turvallisiksi ja päivitetty viimeisimmillä tietoturvapäivityksillä on kuitenkin aina mahdollisuus, että hyökkääjä löytää uuden tietoturva-aukon. Järjestelmän ylläpitäjän tulee varautua tällaisiin tapauksiin jo ennakkoon ja suunnitella valmiiksi toimintamalli, mitä tehdään jos näin käy. Erityisesti tulee huomioida, että estetään hyökkääjän pääsy muille organisaation palvelimille ja estetään hyökkääjää kaappaamasta todennustietoja tai luottamuksellista tietoa verkosta jossa palvelin sijaitsee.

Krutz & Vines (2003: 229-230) osoittavat, että ohjelmistovalvontamekanismeja tulisi käyttää lisäämään ohjelmistoturvallisuutta. Ohjelmistovalvontamekanismeiksi luetaan seuraavat:

1. Virusten torjunta. Henkilökunnan ei anneta ladata ja asentaa mitä tahansa ohjelmia.
2. Ohjelmien testaaminen ennen käyttöön ottoa. Ohjelmistot on testattava ja niiden yhteen sopivuus todettava ennen tuotantoon ottamista.
3. Varusohjelmien käytön valvonta. Tehokkaat varusohjelmat saattavat vaarantaa käyttöjärjestelmän eheyden. Tällaisten varusohjelmien käyttöön on otettava kantaa organisaation tietoturvapolitiikassa.
4. Turvalliset ohjelmistomedioiden säilytyspaikat. Varmistetaan, että ohjelmistoihin ja varmuuskopioihin on pääsy vain niiden käyttöön valtuutetuilla henkilöillä.
5. Varmuuskopioiden valvontamekanismit. Varmuuskopioiden toimivuus tulee testata säännöllisin väliajoin jotta voidaan varmistua varmistusten käytettävyydestä ja eheydestä.

Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) suositetaan, että ohjelmistojen asennuksesta, käyttöönotosta ja käytöstä pidetään ajan tasalla olevat ohjeet jotka on saatettu asianomaisten työntekijöiden tietoon. Ohjeissa tietoturvallisuusasiat on otettu huomioon tietoturvallisuuspolitiikan edellyttämällä tavalla.

Finlexin suosituksessa määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa (2004) suositetaan, että ohjelmistojen varmuuskopiointi suoritetaan siten, että viestintäverkkojen ja viestintäpalvelujen toteuttamiseen liittyvistä ohjelmista on olemassa ajantasaiset varmuuskopiot. Varmuuskopioita tulee säilyttää lukituissa tiloissa ja erillään kyseisistä laitteista. Nämä varmuuskopiot on voitava ottaa käyttöön alkuperäisen tiedoston vaurioituessa esimerkiksi ohjelmistovian, laitevian tai laitetilassa tapahtuneen onnettomuuden jälkeen.

Andersson (2001: 388-389) toteaa, että koska murtautumistekniikat ovat suuresti riippuvaisia sovellusten tietoturva-aukoista, vaihtuvat tekniikat hyvin tiheästi kun uusia tietoturva-aukkoja löydetään sovelluksista ja jo löydettyjä korjataan. Tietoturva-aukkoja sisältäviä koneita on yhdistetty Internetiin satoja miljoonia joissa on käytössä turvattomia sovelluksia tai koneiden ylläpito on puutteellista.

Tietokantojen ollessa arvokkain resurssi organisaatiolle, tulisi se suojata usealla tietoturvatasolla. Tietoturvatasoja ovat: palomuuri, autentikointi mekanismit, yleinen käyttöoikeuksien hallinta, tietokannan salaus. Stallings ja Brown (2008: 166) pitävät tietokannan salaamista (encryption) viimeisenä tietokannan suojana hyökkääjiä vastaan.

Jaakohuhta (2003: 65) osoittaa, että järjestelmät tulisi tarkastaa määräajoin virustentorjuntaohjelmalla jolloin voidaan varmistua että järjestelmä ei sisällä viruksia ja samalla estää virusten tarttuminen varmistuksiin. Jos virus on pääsyt varmistuksiin, ei näitä varmistuksia tulisi käyttää palautumiseen.

Splaine (2002: 88), pitää tärkeänä, että sovelluksesta poistetaan kaikki tarpeettoman prosessit. Jokainen palvelimella oleva prosessi aiheuttaa tietoturva uhan ja palvelut minimoimalla voidaan pienentää palvelimeen kohdistuvia tietoturvauhkia huomattavasti. Mikäli hyökkääjä saa palvelun suorittamaan haittakoodia palvelimella suorittaa palvelu omilla oikeuksillaan hyökkääjän haittakoodin. Tämän vuoksi myös palveluiden oikeudet tiedostoihin ja tietokantoihin tulee minimoida.

Casey (Eoghan Casey, 2002: 222) osoittaa, että palvelinten käyttöjärjestelmien auditointi lokeja tulee seurata säännöllisesti. Auditointi lokeista järjestelmän ylläpitäjä voi pystyä päättelemään poikkeavia kirjautumisia ja tarkistaa kirjautuneen tunnuksen haltialta kirjautumisen oikeellisuuden ja väärinkäytös tilanteessa tehdä tarvittavat vastatoimenpiteet.

5. HENKILÖSTÖTURVALLISUUDEN ANALYSOINTI

Henkilöstöturvallisuutta tutkittaessa ensimmäisessä vaiheessa tutkija ja konsernin tietoturvavastaava selvittivät, minkälaisia riskejä henkilöstön toimintaan liittyy. Riskit listattiin ja niiden todennäköisyys ja vaikutus määriteltiin tarkastelemalla riskien toteutumista menneisyydessä sekä arvioimalla tapahtumia riskien toteutuessa tulevaisuudessa.

Toisessa vaiheessa käytiin läpi henkilöt joita tutkimus koskee. Henkilöitä otettiin tutkimukseen 15 kappaletta. Henkilöitä tutkittaessa määriteltiin riskeihin varautumiset ja mahdolliset kehitysehdotukset.

Kolmannessa vaiheessa kun tutkimus oli tehty, tulokset käytiin läpi tutkijan, tietohallintopäällikön, konsernin tietoturvapäällikön sekä osastojen esimiesten toimesta. Tässä vaiheessa korjaukselle määriteltiin vastuuhenkilö sekä korjaustyön kiireellisyys priorisoitiin.

Henkilöstöriskejä tutkittaessa on olemassa riski, että tutkimuksessa ei löydetä kaikkia tarvittavia riskejä. Tällöin löytämättömiin riskeihin ei osata varautua ja työn lopputuloksena saadussa raportissa ei voida määritellä jatkotoimenpiteitä näille riskeille.

Henkilöstöriskejä tutkittaessa on olemassa riski, että tunnistettuja riskejä ei osata luokitella oikein. Riskien vakavuuden arviointi joudutaan tekemään arvioimalla henkilön tärkeyttä organisaation liiketoiminnan kannalta ja henkilön vastuulla olevan palvelun kannalta. Tällaisissa tapauksissa joudutaan arvioimaan karkeiden arvioiden avulla riskien vaikutuksia,

eikä voida laskennallisesti tai muuten tarkasti määritellä olemassa olevan riskin vaikutusta organisaation liiketoimintaan.

5.1. Henkilöstön toimenkuvat

Työntekijän toimenkuvassa määritellään työntekijän vastuualueet. Vastuualueet tulisi suunnitella työsopimuksen yhteydessä, päivittää toimenkuvan muuttuessa ja tarkistaa säännöllisin väliajoin. Näin toimimalla voidaan pienentää riskiä, että jokin palvelu tai järjestelmä ei olisi kenenkään vastuulla. Henkilöstön toimenkuvia tutkittaessa pyrittiin selvittämään taulukoissa 1-3 kuvattuja riskejä ja niiden vaikutusta palveluiden ja järjestelmien toimintaan.

Taulukko 1.

Riski	Työntekijälle ei ole tehty kirjallista toimenkuvaa.
Tapahtuma	Toimenkuvassa määritellään työntekijän vastuulla olevat järjestelmät ja palvelut. Toimenkuvan puuttuessa on mahdollista, että jokin palvelu tai järjestelmä ei tule kenenkään vastuulle.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Toimenkuva laaditaan työsopimuksen yhteydessä.
Korjauksen vastuuhenkilö	

Taulukko 2.

Riski	Työntekijän toimenkuvaa ei päivitetä.
Tapahtuma	Työntekijä operoi palvelua tai järjestelmää joka ei ole hänen vastuullaan ja hänen vastuullaan olevat järjestelmät tai palvelut jäävät operoimatta tai pienemmälle huomiolle mikäli niitä ei ole siirretty jonkin toisen työntekijän vastuulle.

Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Toimenkuva tarkastetaan kehityskeskustelun yhteydessä.
Korjauksen vastuuhenkilö	

Taulukko 3.

Riski	Työntekijöiden toimenkuvat eivät kata kaikkia järjestelmiä, jolloin jokin järjestelmä ei ole kenenkään vastuulla.
Tapahtuma	Palvelua tai järjestelmää ei määrätä kenenkään vastuulle. Vikatilanteen sattuessa kukaan ei ole vastuullinen korjaamaan vikatilannetta, jotta palvelu tai järjestelmä saataisiin takaisin tuotantoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Yksiköllä lista palveluista ja järjestelmistä jossa on määritelty vastuuhenkilöt.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

5.2. Henkilöstön osaamisen varmistaminen

Henkilöstön osaamisen varmistamisella pyritään pienentämään riskejä jotka liittyvät työntekijän palvelun ja järjestelmien operointiin. Mikäli työntekijä ei pysty operoimaan palvelua tai järjestelmää puutteellisten tietojen vuoksi järjestelmän vikaantuessa virhetilanteesta toipuminen hidastuu tai pahimmassa tapauksessa estyy. Henkilöstön osaamisen varmistamista tutkittaessa pyrittiin selvittämään taulukoissa 4-7 kuvattuja riskejä ja niiden vaikutusta palveluiden ja järjestelmien toimintaan.

Taulukko 4.

Riski	Työntekijän toimenkuvan muuttuessa työntekijää ei perehdytetä uuteen toimenkuvaan kuuluviin töihin.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijä jonka vastuulla järjestelmä tai palvelu on ollut ennen opettaa uutta henkilöä ja kirjoittaa operoinnista tarvittavat ohjeet. Uudelle työntekijälle annetaan myös mahdollisuus käyttää ulkopuolisen tarjoamia kurssipalveluita.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 5.

Riski	Järjestelmän tai sen osien päivittyessä työntekijää ei kouluteta uusista ominaisuuksista.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijälle järjestetään mahdollisuus kouluttautua järjestelmän testipuolella.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 6.

Riski	Työntekijä unohtaa toimenkuvaansa kuuluvien töiden operointi toimenpiteet.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmän tai palvelun operoinnista kirjoitetaan ohjeet.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 7.

Riski	Työntekijän vastuulle määrätään järjestelmä jonka operointiin työntekijää ei ole perehdytetty.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmän tai palvelun operoinnista kirjoitetaan ohjeet.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

5.3. Avain henkilöstö

Avainhenkilöllä tarkoitetaan järjestelmästä tai palvelusta vastuussa olevaa henkilöä. Avainhenkilö on kriittinen osa järjestelmien ja palveluiden toimintaa ja operointia. Avainhenki-

löstöä tutkittaessa pyrittiin selvittämään taulukoissa 8-11 kuvattuja riskejä ja niiden vaikutusta palveluiden ja järjestelmien toimintaan.

Taulukko 8.

Riski	Avainhenkilöiden tavoitettavuutta ei määritellä työsopimuksessa.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Avainhenkilölle joka on vastuussa organisaation liiketoiminnan kannalta kriittisistä palveluista tai järjestelmistä tehdään sopimus tavoitettavuudesta työajan ulkopuolella.
Korjauksen vastuuhenkilö	

Taulukko 9.

Riski	Järjestelmän avainhenkilöä ei voida tavoittaa työajan ulkopuolella.
Tapahtuma	Palvelun tai järjestelmän operointi hidastuu tai pahimmassa tapauksessa estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Avainhenkilölle joka on vastuussa organisaation liiketoiminnan kannalta kriittisistä järjestelmistä, tehdään sopimus tavoitettavuudesta työajan ulkopuolella tai määritellään avainhenkilölle sijainen.
Korjauksen vastuuhenkilö	

Taulukko 10.

Riski	Palvelun avainhenkilöä ei voida tavoittaa työajan ulkopuolella.
Tapahtuma	Palveluun liittyviä päätöksiä ei voida tehdä.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Avainhenkilölle joka on vastuussa organisaation liiketoiminnan kannalta kriittisistä palveluista, tehdään sopimus tavoitettavuudesta työajan ulkopuolella tai määritellään avainhenkilölle sijainen.
Korjauksen vastuuhenkilö	

Taulukko 11.

Riski	Järjestelmää päivitetään ilman järjestelmän avainhenkilön paikalla-oloa.
Tapahtuma	Järjestelmän operointi vaikeutuu ja hidastuu riippuen päivityksessä tehtyjen muutosten määrästä.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Järjestelmän päivitysprosessille määritellään yhteinen toimintatapa ja päivitys dokumentoidaan.
Korjauksen vastuuhenkilö	

5.4. Työhöntuloprosessi

Miettinen (Juha E. Miettinen, 1999: 162-165) osoittaa, että työnantajan on tärkeätä varmistua uuden työntekijän taustoista ja soveltuvuudesta jo ennen työsuhteen alkua. Tällä tavoin

toimimalla yritys voi välttyä solmimasta työsopimusta ei toivotun henkilön kanssa. Yrityksen palkatessa uutta työntekijää on tärkeätä muistaa tehdä salassapitosopimus, mikäli uuden työntekijän toimenkuvassa käsitellään yrityksen salaisiksi määrittelemää tietoa. Tällä tavoin toimimalla yritys oi pienentää riskiä jossa yrityksen salaisuudet päätyisivät ulkopuolisen tietoon. Työhöntuloprosessi sisältää useita riskejä liittyen uuteen työntekijään. Näitä riskejä pyrittiin selvittämään taulukoissa 12-19 kuvattujen riskien avulla.

Taulukko 12.

Riski	Uuden työntekijän henkilöllisyyttä ei tarkisteta.
Tapahtuma	Töihin palkataan väärä henkilö
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työnhakijaa pyydetään todistamaan henkilöllisyys.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 13.

Riski	Uuden työntekijän taustaa ei tarkisteta.
Tapahtuma	Töihin voidaan palkata epäpätevä henkilö.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Suositukset, työhistoria ja koulutus varmistetaan sekä työntekijältä vaaditaan turvallisuusselvitys.
Korjauksen vastuuhenkilö	

Taulukko 14.

Riski	Uuden työntekijän sopivuutta ei tarkisteta.
Tapahtuma	Töihin voidaan palkata epäpätevä henkilö.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Työntekijälle tehdään soveltuvuustestaus.
Korjauksen vastuuhenkilö	

Taulukko 15.

Riski	Uutta työntekijää ei perehdytetä työhön.
Tapahtuma	Työntekijä on epäpätevä hoitamaan työtehtäviään ja aiheuttaa riskin toiminnallaan.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Työntekijän perehdytykseen määrätään vastuuhenkilö.
Korjauksen vastuuhenkilö	

Taulukko 16.

Riski	Uuden työntekijän kanssa ei tehdä salassapitosopimusta.
Tapahtuma	Työntekijä voi kertoa yrityksen tietoja kilpailijalle.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tehdään salassapitosopimus työsopimuksen yhteydessä.

Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 17.

Riski	Työntekijälle annetaan liian vähän käyttöoikeuksia.
Tapahtuma	Työntekijä ei pysty suoriutumaan työtehtävistään puutteellisten käyttöoikeuksien vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijän esimies pyytää tarvittavat käyttöoikeudet työntekijälle.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 18.

Riski	Työntekijälle annetaan liikaa käyttöoikeuksia.
Tapahtuma	Työntekijän tekemien väärinkäytösten riski kasvaa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijän esimies pyytää tarvittavat käyttöoikeudet työntekijälle.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 19.

Riski	Työnkierron yhteydessä ei päivitetä käyttöoikeuksia.
Tapahtuma	Työntekijän tekemien väärinkäytösten riski kasvaa.

Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijän esimies pyytää tarvittavat käyttöoikeudet työntekijälle.
Kehitysehdotukset	Otettaisiin käyttöön järjestelmä jossa listattu käyttäjän tunnukset ja tunnusten tasot.
Korjauksen vastuuhenkilö	

5.5. Prosessi työsuhteen päättyessä

Työntekijän työsuhteen päättyessä työntekijän kaikenlainen pääsy yrityksen omistamaan tietoaineistoon on päätettävä. Samalla on huolehdittava, että työntekijän kulkuoikeudet yrityksen tiloissa päätetään ja että työntekijä palauttaa yrityksen omaisuuden. Tärkein tekijä on ihminen ohjeistuksessaan valtionvaranministeriö (2008) pitää tärkeänä osana työsuhteen päättymistä erityisen tarkkaa loki tiedostojen seurantaa. Loki tiedostoja seuraamalla voidaan havaita työsuhteensa päättäneen entisen työntekijän pääsy yrityksen tietoaineistoon. Työsuhteen päättymistä tutkittaessa, pyrittiin selvittämään taulukoissa 20-23 kuvattuja riskejä.

Taulukko 20.

Riski	Työntekijän käyttöoikeuksia ei päätetä.
Tapahtuma	Työntekijällä on pääsy järjestelmään työsuhteen päätyttyä.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tehty lista työntekijöiden tunnuksista eri järjestelmiin.
Kehitysehdotukset	Otettaisiin käyttöön järjestelmä jossa listattu käyttäjän tunnukset ja tunnusten tasot.
Korjauksen vastuuhenkilö	

Taulukko 21.

Riski	Työntekijän työtehtäviä ei siirretä.
Tapahtuma	Työntekijän työt jäävät tekemättä ja kukaan ei ole vastuussa työntekijän vastuulla olleista järjestelmistä tai palveluista.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijöiden vastuulla oleville järjestelmille ja palveluille määrätty sijaiset.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 22.

Riski	Työntekijän ei palauta yrityksen omaisuutta.
Tapahtuma	Yritys menettää omaisuutta.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijälle luovutettava yrityksen omaisuus listataan rekisteriin luovutuksen yhteydessä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 23.

Riski	Työntekijän lähdöstä ei tiedoteta yrityksessä tai asiakkaalle.
Tapahtuma	Yrityksen työntekijät eivät saa yhteyttä työntekijään ja asiakkaiden kontakti yritykseen puuttuu.
Todennäköisyys	1-4

Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Yrityksessä on olemassa prosessi työsuhteen päättymiselle.
Kehitysehdotukset	Määritellään pohja poissaolo sähköpostiviestille.
Korjauksen vastuuhenkilö	

5.6. Sijaisjärjestelyt

Sijaisjärjestelyillä pyritään varmistamaan yrityksen toiminnan jatkuvuutta. On tärkeätä, että yritys varmistaa kriittisten järjestelmien ja palveluiden avainhenkilöiden tai sijaisten tavoitettavuuden työaikana ja työajan ulkopuolella. Tavoitettavuuden varmistamisella pienennetään riskejä liittyen järjestelmien ja palveluiden ongelmatilanteista toipumiseen ja operointiin. Sijaisjärjestelyihin liittyviä riskejä selvitettiin taulukoissa 24-26 kuvattujen riskien avulla.

Taulukko 24.

Riski	Työntekijän vastuulla oleville järjestelmille tai palveluille ei ole määritelty sijaista.
Tapahtuma	Järjestelmien tai palveluiden operointi hidastuu tai estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijän vastuulla oleville järjestelmille tai palveluille on määritelty sijainen.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 25.

Riski	Järjestelmän avainhenkilö ja hänen varamies ovat samaan aikaan

	poissa työpaikalta.
Tapahtuma	Järjestelmän operointi hidastuu tai estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmän operoinnista on tehty ohjeet.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 26.

Riski	Järjestelmän avainhenkilön varamies ei pysty suoriutumaan työtehtävästä puutteellisten tietojen vuoksi.
Tapahtuma	Järjestelmän operointi hidastuu tai estyy hetkellisesti.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmän operoinnista on tehty ohjeet.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

5.7. Työnkierto ja lomat

Työnkiertoon ja lomiin kuuluu riskejä liittyen liian laaja-alaiseen tietämykseen, osaamisen varmistamiseen ja tavoitettavuuteen. Työnkiertoon ja lomiin liittyviä riskejä tutkittiin taulukoissa 27-29 kuvattujen riskien avulla.

Taulukko 27.

Riski	Järjestelmän avainhenkilö ja sijainen eivät vaihda työtehtäviään määräajoin.

Tapahtuma	Järjestelmän operointi vain avainhenkilön hallinnassa ja vikatilanteen sattuessa avainhenkilön poissa ollessa järjestelmän operointi hidastuu tai estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Työntekijöiden esimiesten on määrättävä työtehtävien vaihdot.
Korjauksen vastuuhenkilö	

Taulukko 28.

Riski	Työntekijöiden kierrättäessä toimenkuvia työntekijä oppii tuntemaan laaja-alaisesti kontrollijärjestelmän.
Tapahtuma	Väärinkäytösten riski kasvaa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Työnkierrossa työtehtäviä ei vaihdeta vaan käsiteltävää tietoa tai asiakaskuntaa.
Korjauksen vastuuhenkilö	

Taulukko 29.

Riski	Työntekijä tavoitettavuutta ei varmisteta loma-aikana.
Tapahtuma	Työntekijän vastuulla olevan järjestelmän vikaantuessa toipuminen hidastuu.
Todennäköisyys	1-4
Vaikutus	1-4

Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Työntekijän kanssa tehdään sopimus työajan ulkopuolisesta tavoitettavuudesta.
Korjauksen vastuuhenkilö	

5.8. Ulkopuolinen työvoima

Ulkopuoliseen työntekijään liittyy samoja riskejä kuin yrityksessä työskentelevään työntekijään. Tärkein tekijä on ihminen ohjeistuksessaan valtionvarainministeriö (2008) kuitenkin osoittaa, että ulkopuolista työntekijää ei pitäisi palkata työtehtävään joka liittyy monimutkaisten järjestelmien ja palveluympäristöjen hallintaan. Ulkopuoliseen työvoimaan kohdistuvia riskejä tutkittiin taulukoissa 30-35 kuvattujen riskien avulla.

Taulukko 30.

Riski	Ulkopuolinen työntekijä luovuttaa tietoa kilpailijoille.
Tapahtuma	Kilpailijat voivat saada tietoon yrityksen salaisuuksia.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Ulkopuolisen työntekijän kanssa tehdään salassapitosopimus.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 31.

Riski	Ulkopuolinen työntekijä ei pysty suoriutumaan työtehtävästä osaamisen tai resurssien puuttumisen vuoksi.
Tapahtuma	Ulkopuolisesta työntekijästä riippuvat työt jäävät tekemättä tai ne valmistuvat hitaasti.

Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Ulkopuoliselle työntekijälle tehdään taustatutkimus.
Korjauksen vastuuhenkilö	

Taulukko 32.

Riski	Käytettäessä ulkopuolista työntekijää, yrityksessä ei ole kyseistä osaamista.
Tapahtuma	Ulkopuolisen toteuttaman järjestelmän tai palvelun operointi hidastuu tai estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Ulkopuoliselta työntekijältä vaaditaan dokumentaatio tehdystä työstä ja mahdollisen järjestelmän tai palvelun operoinnista.
Korjauksen vastuuhenkilö	

Taulukko 33.

Riski	Työsuhteen päätyttyä ulkopuoliseen työntekijään ei saada yhteyttä.
Tapahtuma	Ulkopuolisen työntekijän töistä löytyvien virheiden korjaaminen on vaikeata.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	

Kehitysehdotukset	Tehdään sopimus ulkopuolisen työntekijän kanssa tavoitettavuudesta ja vastuusta.
Korjauksen vastuuhenkilö	

Taulukko 34.

Riski	Työsuhteen päättyessä ulkopuolisen työntekijän tunnuksia ei päätetä.
Tapahtuma	Ulkopuolisella työntekijällä on pääsy yrityksen järjestelmiin työsuhteen päätyttyä.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Tehdään rekisteri tunnuksista ja niiden tasoista.
Korjauksen vastuuhenkilö	

Taulukko 35.

Riski	Työsuhteen päättyessä ulkopuolisen työntekijän verkkoyhteyksiä yrityksen verkkoon ei poisteta.
Tapahtuma	Ulkopuolisella työntekijällä on pääsy yrityksen verkkoon työsuhteen päätyttyä.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Tehdään rekisteri yhteyksistä ja dokumentoidaan yhteydet.
Korjauksen vastuuhenkilö	

5.9. Varautuminen poikkeusoloihin

Henkilöstöturvallisuustyö on usein ennalta ehkäisevää. Myös työntekijät voivat aiheuttaa toiminnalla poikkeustiloja. Poikkeusoloja tutkittaessa keskityttiin taulukoissa 36 ja 37 kuvattuihin riskeihin.

Taulukko 36.

Riski	Työntekijä luovuttaa tietoa ulkopuoliselle.
Tapahtuma	Ulkopuolinen voi saada tietoon yrityksen salaisuuksia.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Työntekijän kanssa tehty salassapitosopimus.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 37.

Riski	Yrityksen oma tai ulkopuolinen työntekijä ei pidä kiinni projektien aikatauluista.
Tapahtuma	Projektia ei voida suorittaa onnistuneesti vaaditussa aikataulussa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Määritellään ulkopuolisen työntekijän kanssa tehdyssä sopimuksessa sakko.
Korjauksen vastuuhenkilö	

6. LAITTEISTOTURVALLISUUDEN ANALYSOINTI

Laitteistoturvallisuuden tutkiminen aloitettiin jakamalla yksikön vastuulla olevat laitteistot palvelimiin, verkon aktiivilaitteisiin, levyjärjestelmiin, päätelaitteisiin ja kaapelointiin.

Ensimmäisessä vaiheessa tutkija, järjestelmäryhmän esimies ja konsernin tietoturvavastaava selvittivät, minkälaisia riskejä palvelinten toimintaan liittyy. Palvelimiin kohdistuvia riskejä tutkittaessa palvelimet jaettiin aluksi ryhmiin niiden käyttötarkoituksen mukaan. Kun palvelimet oli jaettu ryhmiin ja listattu, ruvettiin listoja käymään läpi palvelin kerrallaan. Palvelimeen liittyviä riskejä tutkittaessa tutkimusryhmään kuului tutkimuksen tekijä ja järjestelmän vastuuhenkilöt.

Tutkimusta tehtäessä palvelinten ja verkon aktiivilaitteiden yhteismäärä paisui yli 100 kappaleeseen. Päätelaitteita laskettiin olevan yli 400, mutta näitä ei jokaista tutkimuksessa käyty läpi vaan tutkittiin niihin liittyviä riskejä esimerkkikohtaisesti.

Verkonaktiivilaitteita tutkittaessa järjestelmäryhmän esimies, tietoturvavastaava ja tutkija määrittelivät verkonaktiivilaitteisiin liittyvät riskit. Riskien määrittelyn jälkeen tarkasteltiin aktiivilaitteiden avainkäyttäjien kanssa riskejä ja varautumista riskien toteutuessa.

Levyjärjestelmiä tutkittaessa järjestelmäryhmän esimies, tietoturvavastaava ja tutkija määrittelivät levyjärjestelmiin liittyvät riskit ja selvittivät riskeihin liittyvät varautumiset. Menneitä vikatilanteita tutkittaessa huomattiin, että laiterikko ja ohjelmistovirhe ovat yhdistelmä josta toipuminen on aiheuttanut menneisyydessä ongelmia.

Päätelaitteita tutkittaessa tutkija ja päätelaitteista vastaava määrittelivät päätelaitteisiin liittyviä riskejä. Seuraavaksi järjestelmäryhmän esimies, tietoturvavastaava ja tutkija tarkastelivat havaittuja riskejä ja selvittivät riskeihin liittyvät varautumiset.

Kaapelointia tutkittaessa järjestelmäryhmän esimies, tietoturvavastaava ja tutkija määrittelivät kaapelointiin liittyvät riskit ja selvittivät riskeihin liittyvät varautumiset. Kaapelointia tutkittaessa havaittiin dokumentoinnin muodostavan ison osan kaapelointiin liittyvistä riskeistä.

Merkittävä tutkimukseen liittyvä riski on, että riskejä määriteltäessä jää joukko palvelun toiminnan kannalta merkittäviä riskejä tunnistamatta. Riskin toteutuessa työn lopputuloksena saatavassa raportissa ei ole voitu ottaa kantaa näihin riskeihin, eikä niiden varalle ole osattu määritellä toimintasuunnitelmaa.

Toinen merkittävä riski liittyy tunnistettujen riskien luokitteluun. Riskien vakavuuden arviointi joudutaan tekemään arvioimalla palvelun tärkeyttä organisaation liiketoiminnan kannalta ja palvelua käyttävän käyttäjänkunnan kannalta. Tällaisissa tapauksissa joudutaan arvioimaan karkeiden arvioiden avulla riskien vaikutuksia, eikä voida laskennallisesti tai muuten tarkasti määritellä olemassa olevan riskin vaikutusta organisaation liiketoimintaan.

Kolmas merkittävä riski liittyy tunnistettujen riskien todennäköisyyteen. Riskin toteutumista on vaikea arvioida laitteistossa joka on vain lyhyen ajanjakson tuotannossa ja riski ei ole toteutunut. Tällaisissa tapauksissa riskin todennäköisyys joudutaan arvioimaan karkean arvion avulla, eikä arvioitu tulos välttämättä vastaa laitteiston todellisen riskin toteutumisen todennäköisyyttä.

6.1. Käyttöönotto

Laitteiston käyttöönotossa tulee huomioida kustannukset, asennukset ja koulutus. Laitteiston käyttöönottoon liittyviä riskejä tutkittiin taulukoissa 38-42 kuvattujen riskien avulla.

Taulukko 38.

Riski	Uusi laitteiston hinta liian korkea.
Tapahtuma	Uudesta laitteistosta saatu hyöty ei vastaa kustannuksia ja yritys menettää omaisuutta uuden laitteiston vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitehankintojen yhteydessä suhteutetaan saatavat hyödyt ja kustannukset.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 39.

Riski	Laitteisto ei vastaa sille asetettuja vaatimuksia.
Tapahtuma	Laitteistoa ei voida käyttää suunniteltuun käyttötarkoitukseen.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Ennen laitehankintaa määritellään laitteiston vaatimukset.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 40.

Riski	Työntekijää ei perehdytetä uuden järjestelmän avulla suoritettavista työtehtävistä.
Tapahtuma	Uuden laitteiston avulla suoritettavat työtehtävät valmistuvat hitaasti.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestetään koulutusta enne uuden laitteiston käyttöön ottoa.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 41.

Riski	Laitteistoa ei testata testijärjestelmässä.
Tapahtuma	Laitteisto ei toimi tuotannossa oikein tai on mitoitettu väärin.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tetataan laitteiston sopivuus testi ympäristössä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 42.

Riski	Uuden järjestelmän kriittisiä osia ei eriytetä.
Tapahtuma	Uudesta järjestelmästä tulee monimutkainen ja vaikea operoitava.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus

Varautuminen	Kriittiset osat eriytetään ja minimoidaan järjestelmässä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.2. Huolto ja kunnossapito

Huolto ja kunnossapito ovat kriittinen osa järjestelmiä. Vikatilanteen sattuessa, kriittiset järjestelmät on saatava mahdollisimman nopeasti takaisin tuotantokäyttöön. Tuotantokäytöissä tapahtuvien katkosaikojen minimoimiseksi huolto- ja kunnossapitosopimukset ovat tärkeitä. huolto- ja kunnossapitoa tutkittaessa keskityttiin taulukoissa 43-46 kuvattuihin riskeihin.

Taulukko 43.

Riski	Huollon yhteydessä ulkopuolisella on pääsy yrityksen tieto-omaisuuteen.
Tapahtuma	Ulkopuolisella on pääsy yrityksen tieto-omaisuuteen.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmän avainhenkilö valvoo tapahtuvaa huoltoa.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 44.

Riski	Huoltosopimusten vaste ei vastaa järjestelmän kriittisyyttä.
Tapahtuma	Järjestelmän huoltoa ei aloiteta riittävän nopeasti ja tämän vuoksi huoltoaika pitenee jonka aikana järjestelmä ei ole tuotantokäytössä.
Todennäköisyys	1-4
Vaikutus	1-4

Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Huoltosopimuksessa määritellään vasteaika.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 45.

Riski	Huoltosopimusta ei tehdä.
Tapahtuma	Laitteiston vikaantuessa laitteiston korjaaminen viivästyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitehankinnan yhteydessä tehdään huoltosopimus.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 46.

Riski	Huoltosopimus päättyy.
Tapahtuma	Laitteiston vikaantuessa laitteiston korjaaminen viivästyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Huoltosopimukset tarkastetaan määräajoin.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.3. Käytöstä poisto

Laitteiston käytöstä poiston yhteydessä on vaara, että yrityksen tieto-omaisuus joutuu ulkopuolisen saataville. Tähän liittyvää riskiä tarkasteltiin taulukossa 47 kuvatun riskin avulla.

Taulukko 47.

Riski	Laitteistoa poistettaessa käytöstä tallennusmedia jää tyhjentämättä.
Tapahtuma	Ulkopuolinen voi saada pääsyn tallennusmedialle jääneeseen tietoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistoa poistettaessa käytöstä kaikki sen tallennus mediat irrotetaan laitteistosta ja huolehditaan tallennusmedioiden tuhoamisesta.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.4. Käytettävyys

Kriittisten järjestelmien ja palveluiden korkea käytettävyys on ensisijaisen tärkeää. Järjestelmien ja palveluiden korkealla käytettävyydellä varmistetaan työntekijöiden pääsy järjestelmiin ja palveluihin jolloin käyttäjät pystyvät suoriutumaan omista järjestelmissä tekemistään työsuorituksista nopeasti ja tehokkaasti. Käytettävyyttä tutkittaessa tarkasteltiin taulukoissa 48-50 määriteltyjä riskejä.

Taulukko 48.

Riski	Poistetaan vahingossa tiedostoja.
Tapahtuma	Tiedostojen saatavuus estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus

Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 49.

Riski	Poistetaan vahingossa konfiguraatiotiedostoja.
Tapahtuma	Järjestelmä tai palvelu toimii virheellisesti tai toiminta estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 50.

Riski	Järjestelmä tai palvelu toimii hitaasti.
Tapahtuma	Järjestelmässä tai palvelussa suoritettavat työtehtävät valmistuvat hitaasti ja tällä järjestelmässä toimivien työntekijöiden työpanos kärsii.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Järjestelmää tai palvelua valvotaan ohjelmistoilla jolloin voidaan ennustaa hitautta.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.5. Laitetyyppien erityisvaatimuksia

6.5.1. Palvelimet

Suuri osa tässä työssä käsitellyistä riskeistä liittyy palvelimiin ja niiden toimintaan. Palvelinten toimintaa liittyy useita ja kaikkien riskien huomioiminen on vaikeaa ja työlästä. Tietojärjestelmiä tutkittaessa palvelin on osa joka usein tarjoaa palveluita käyttäjille. Palvelimen vikaantuessa palvelimen tarjoamat palvelut eivät ole enää käytettävissä. Palvelimiin liittyviä riskejä on tutkittu taulukoissa 51-67 kuvattuja riskejä käyttäen.

Taulukko 51.

Riski	Palvelin hajoaa.
Tapahtuma	Palvelin ei pysty tarjoamaan palveluita.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein ja kriittiset laitteistot kahdennettu.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 52.

Riski	Sähköverkossa katkos.
Tapahtuma	Sähkökatkoksen vuoksi palvelin ei pysty tarjoamaan palveluita.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelin kytketty UPS järjestelmään
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 53.

Riski	Palvelinta ei ole kytketty UPS-järjestelmään.
Tapahtuma	Palvelin ei pysty tarjoamaan palveluita.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelimet kytketään tuotantoon oton yhteydessä UPS-järjestelmään.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 54.

Riski	Palvelimen paikallinen levy hajoaa.
Tapahtuma	Kahdennettujen paikallisten levyjen ja RAID-tietojärjestelmän vuoksi palvelin pystyy jatkamaan tuotantoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelimissa kahdennetut levyt joissa RAID-tietojärjestelmä. Lisäksi laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 55.

Riski	Palvelimen paikalliset levyt hajoavat.
Tapahtuma	Palvelin ei pysty tarjoamaan palveluitaan.
Todennäköisyys	1-4

Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 56.

Riski	Palvelimen levyjärjestelmä hajoaa.
Tapahtuma	Palvelin ei pysty tarjoamaan palveluitaan.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 57.

Riski	Palvelimella oleva prosessi tai palvelu pois päältä.
Tapahtuma	Prosessi tai palvelu ei ole saatavilla.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palveluita ja prosesseja valvotaan ohjelmallisesti ja palvelun tai prosessin kaatuessa tulee tapahtumasta hälytys jolloin prosessi tai palvelu voidaan käynnistää uudestaan mahdollisimman nopeasti.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 58.

Riski	Palvelimeen kohdistetaan DDOS hyökkäys.
Tapahtuma	Palvelin ruuhkautuu ja palvelimen palveluiden tarjonta hidastuu tai estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 59.

Riski	Tietomurto palvelimelle.
Tapahtuma	Käyttäjä saa pääsyn palvelimelle ja sen sisältämiin tietoihin.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelimelle pääsee kirjautumaan vain yrityksen omasta sisäverkosta määritellyistä osoitteista.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 60.

Riski	Ulkopuolinen saa järjestelmänvalvojan tunnuksen.
Tapahtuma	Ulkopuolinen saa pääsyn palvelimelle tallennettuun tietoaineistoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus

Varautuminen	Palvelimelle pääsee kirjautumaan vain yrityksen omasta sisäverkosta määritellyistä osoitteista.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 61.

Riski	Ulkopuolinen saa palvelun pääkäyttäjäntunnuksen.
Tapahtuma	Ulkopuolinen saa pääsyn palveluun ja palveluun tallennettuun tietoaineistoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palveluun pääsee kirjautumaan vain yrityksen omasta sisäverkosta määritellyistä osoitteista.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 62.

Riski	Ulkopuolinen saa palvelun käyttäjäntunnuksen.
Tapahtuma	Ulkopuolinen saa pääsyn toisen käyttäjän tietoihin.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 63.

Riski	Palvelin varastetaan.
Tapahtuma	Varas saa pääsyn palvelimelle tallennettuun tietoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelimesta otetaan nauhavarmistus määritellyin aikavälein jolloin palvelin on nopeammin korvattavissa.
Kehitysehdotukset	Palvelimen tallennusmedia salataan.
Korjauksen vastuuhenkilö	

Taulukko 64.

Riski	Palvelimelle pääsee kirjautumaan ulkoverkosta järjestelmänvalvojan tunnuksella.
Tapahtuma	Ulkopuolinen voi päästä kirjautumaan koneelle saatuaan järjestelmänvalvojan tunnuksen.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Palvelimelle pääsee kirjautumaan vain yrityksen omasta sisäverkosta määritellyistä osoitteista.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 65.

Riski	Palvelun tietokanta hajoaa.
Tapahtuma	Tietokantapalveluiden tarjonta estyy.
Todennäköisyys	1-4

Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 66.

Riski	Tietokantojen välinen tiedonvälitys (replikointi) hajoaa.
Tapahtuma	Palvelimilla on tietokannoissa eri tietoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tiedonvälitystä valvotaan ohjelmallisesti ja tehdään hälytys replikoinnin hajotessa.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 67.

Riski	Käyttäjä lähettää roskapostia palvelun avulla.
Tapahtuma	Sähköpostin toimitus hidastuu ja palvelu voi joutua mustille listoille.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Postin toimitukseen tehty rajoittimia.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.5.2. Päätelaitteet

Päätelaitteet ovat laitteita joita yrityksen työntekijät käyttävät suoriutuakseen työtehtävistään. Päätelaitteet ovat usein työntekijöiden henkilökohtaisia jolloin niiden seuranta ja valvonta on helpompaa. Päätelaitteita tutkittiin taulukoissa 68-72 kuvattujen riskien avulla.

Taulukko 68.

Riski	Päätelaitteelle asentuu haittaohjelma.
Tapahtuma	Päätelaite toimii virheellisesti ja saattaa levittää haittaohjelmaan muille päätelaitteille.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Päätelaitteelle asennetaan paikallinen virus- ja palomuuriohjelmisto.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 69.

Riski	Laiterikko.
Tapahtuma	Laite joudutaan korvaamaan uudella.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 70.

Riski	Päätelaitteelle ei ole asennettu laitekohtaista palomuuria.

Tapahtuma	Päätelaiteelle voi asentua haittaohjelma.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 71.

Riski	Kannettavan työaseman kiintolevyä ei ole salattu.
Tapahtuma	Kannettavan tietokoneen joutuessa ulkopuolisen käsiin saa ulkopuolinen pääsyn tietokoneelle tallennettuun tietoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Kaikkien kannettavien tietokoneiden kiintolevyt salataan.
Korjauksen vastuuhenkilö	

Taulukko 72.

Riski	Päätelaitteella konfiguraatiovirhe.
Tapahtuma	Päätelaite toimii virheellisesti ja saattaa häiritä muiden verkon laitteiden toimintaa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	

Korjauksen vastuuhenkilö	

6.5.3. Levyjärjestelmät

Levyjärjestelmät tarjoavat palveluitaan päätelaitteille ja palvelimille. Levyjärjestelmissä säilytettävä tieto usein varmistetaan varmistusmedialle toisin kuin päätelaitteet. Tämän vuoksi on suositeltavaa, että yrityksen kriittinen tietoaineisto säilytettäisiin levyjärjestelmässä eikä päätelaitteiden tallennusmedialla. Levyjärjestelmiä tutkittaessa havaittiin, että levyjärjestelmiä kahdennettaessa tuli kahdennus toteuttaa kahdella aidosti erillisellä autonomisella järjestelmällä. Tällöin levyjärjestelmät eivät tiedä toisistaan ja toisen vikaantuminen ei vaikuta mitenkään toisen toimintaan. Levyjärjestelmiä tutkittiin taulukoissa 73-76 kuvattujen riskien avulla.

Taulukko 73.

Riski	Laitteistosta hajoaa kiintolevy.
Tapahtuma	Laitteisto osaa itse toipua kiintolevyn rikosta ja rikkoontunut kiintolevy voidaan vaihtaa laitteiston ollessa tuotannossa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 74.

Riski	SAN verkko ei toimi.
Tapahtuma	Tietoaineistoa ei menetetä mutta tietoaineisto ei ole saatavilla.
Todennäköisyys	1-4
Vaikutus	1-4

Vakavuus	Todennäköisyys * vaikutus
Varautuminen	SAN verkko kahdennettu
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 75.

Riski	Laitteiston ohjelmistossa ohjelmistovirhe.
Tapahtuma	Laitteisto toimii virheellisesti ja on mahdollisuus, että laitteistolle tallennettu tieto menetetään.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistosta otetaan nauhavarmistus määritellyin aikavälein.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 76.

Riski	Laiterikko.
Tapahtuma	Laitteiston komponentit kahdennettu, tuotanto siirtyy kokonaisuudessaan toimivalle komponentille.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteiston komponentit on kahdennettu.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.5.4. Kaapelointi

Kaapeloinnin avulla järjestelmät ja laitteet liitetään fyysisesti toisiinsa. Nopeutta ja luotettavuutta vaativien järjestelmien on suositeltavaa käyttää tiedonsiirtoon kaapeloinnin välityksellä tapahtuvaa tiedonsiirtoa. Kaapelointiin liittyviä riskejä tutkittiin taulukoissa 77-79 määriteltyjen riskien avulla.

Taulukko 77.

Riski	Kohteessa käytetään heikkolaatuista kaapelointia.
Tapahtuma	Tiedonsiirto hidastuu.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 78.

Riski	Kaapelia ei sijoiteta turvalliseen ympäristöön vaan se jätetään alttiiksi ulkoisille vahingon aiheuttajille.
Tapahtuma	Kaapelointi voi rikkoutua.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Kaapelin kytkennät tarkastetaan ennen tuotantoon ottoa.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 79.

Riski	Kuitukaapeli jätetään puhdistamatta asennuksessa.
Tapahtuma	Tiedonsiirto katkeilee tai ei toimi ollenkaan.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Kuitukaapelia kytkettäessä liittimet puhdistetaan.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.5.5. Verkonaktiivilaitteet

Verkonaktiivilaitteet ovat kriittinen osa tietojärjestelmien toimintaa. Tietojärjestelmien välinen tiedonsiirto tapahtuu verkonaktiivilaitteiden välityksellä. Verkonaktiivilaitteen vikaantuessa ja tiedonsiirron tämän vuoksi estyessä tietoverkossa olevia palveluita käyttävän järjestelmän toiminta estyy ainakin osittain. Tutkimuksessa verkonaktiivilaitteisiin kuuluivat: kytkimet, reitittävät laitteet, palomuurit ja UTM. Näihin liittyviä riskejä tutkittiin taulukoissa 80-89 määriteltyjen riskien avulla.

Taulukko 80.

Riski	Laiterikko.
Tapahtuma	Laite kahdennettu, tuotanto siirtyy toimivalle laitteelle. Rikkoutunut laite joudutaan korvaamaan uudella.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 81.

Riski	Pääkäyttäjätunnukselle ei ole määritelty salasanaa.
Tapahtuma	Ulkopuolinen pääsee kirjautumaan laitteelle oletus salasanalla.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Käyttöönoton yhteydessä pääkäyttäjätunnukselle määritellään salasana.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 82.

Riski	GBIC (Gigabit interface converter) hajoaa.
Tapahtuma	Laite toimii puutteellisesti. Vikaantunut komponentti on korvattava uudella.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Varastossa ylimääräisiä GBIC moduleita.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 83.

Riski	Laitetta ei ole kytketty UPS-järjestelmään.
Tapahtuma	Sähkökatkoksen tapahtuessa laitteen toiminta estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus

Varautuminen	Laite kytketty UPS-järjestelmään.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 84.

Riski	Ohjelmistopäivitys rikkoo laitteen.
Tapahtuma	Laite toimii virheellisesti.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteistossa 2 Flash muistikomponenttia.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 85.

Riski	Ohjelmistossa ohjelmistovirhe.
Tapahtuma	Laite toimii virheellisesti.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteisto on kahdennettu.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 86.

Riski	Konfigurointi virhe.
Tapahtuma	Laite toimii virheellisesti.

Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteisto on kahdennettu.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 87.

Riski	Ulkopuolinen saa pääkäyttäjän tunnuksen.
Tapahtuma	Ulkopuolinen pääsee kirjautumaan laitteeseen.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Laitteeseen pääsee kirjautumaan vain yrityksen sisäverkosta määritellyistä osoitteista.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 88.

Riski	Configuration backupin otto unohtuu.
Tapahtuma	Laiterikon tapahtuessa korvaavan laitteen konfigurointi hidasta.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 89.

Riski	Active – standby toimivuutta ei ole käyttöön oton jälkeen testattu säännöllisesti.
Tapahtuma	Aktiivisen laitteen rikkoutuessa ei voida olla varmoja standby laitteen toimivuudesta tuotannossa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Active – standby laitteiden aktiivista laitetta vaihdellaan määräajoin.
Korjauksen vastuuhenkilö	

6.6. Tietoliikenneverkkojen suunnittelu ja dokumentointi

Tietoliikenneverkkoja suunniteltaessa Hakala, Vainio ja Vuorinen (Mika Hakala, Mika Vainio ja Olli vuorinen, 2006: 183) määrittelevät tietoverkkojen suunnittelun lähtökohtana olevan organisaation tietotarpeet. Kruzt ja Vines (Ronald L. Krutz & Russell Dean Vines 2003: 61-64) taas lisäävät suunnittelussa tärkeäksi asiaksi tietoverkkojen tietoturvan. Tietoliikenneverkkojen dokumentointi osoittautui tutkimuksessa erittäin tärkeäksi. Tietoverkon vikojen paikannus, kehittäminen ja käyttö vaativat dokumentaation tuekseen. Hyvä dokumentaatio helpottaa tietoverkkojen operointia. Tietoverkkoihin liittyviä riskejä tutkittiin taulukoissa 90-93 kuvattujen riskien avulla.

Taulukko 90.

Riski	Kaapelointia ei dokumentoida.
Tapahtuma	Kaapeloinnin operointi hidastuu puutteellisen dokumentaation vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus

Varautuminen	
Kehitysehdotukset	Dokumentointi tarkastettaisiin määräajoin.
Korjauksen vastuuhenkilö	

Taulukko 91.

Riski	Kaapeloinnin yhteydessä kaapeleiden päät jäävät nimeämättä.
Tapahtuma	Kaapeloinnin operointi hidastuu puutteellisen dokumentaation vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Dokumentointi tarkastettaisiin määräajoin.
Korjauksen vastuuhenkilö	

Taulukko 92.

Riski	Dokumentointi ei ole ajan tasalla.
Tapahtuma	Kaapeloinnin operointi hidastuu puutteellisen dokumentaation vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Dokumentointi tarkastettaisiin määräajoin.
Korjauksen vastuuhenkilö	

Taulukko 93.

Riski	Dokumentointi ei ole riittävä.
Tapahtuma	Kaapeloinnin operointi hidastuu puutteellisen dokumentaation vuoksi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Dokumentointi tarkastettaisiin määräajoin.
Korjauksen vastuuhenkilö	

6.7. Tietoliikenneverkkojen varmistukset ja varajärjestelyt

Varmistuksilla ja varajärjestelyillä pyritään varmistamaan tietoverkon toimivuus myös vikatilanteen sattuessa. Kuten myös Jaakohuhta (Hannu Jaakohuhta, 2003: 85) toteaa, organisaation tietoliikenneyhteyksien katkeaminen johtaa usein koko organisaation toiminnan keskeytymiseen. Tietoliikenneverkkojen varmistukset ja varajärjestelyt on mahdollista toteuttaa useilla erilaisilla teknisillä toteutuksilla. Näitä varmistuksia ja varajärjestelyitä tutkittaessa käytettiin taulukoissa 94 ja 95 kuvattuja riskejä.

Taulukko 94.

Riski	Verkon kaapelointi katkeaa.
Tapahtuma	Katkenneessa kaapelissa tiedonsiirto estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Verkot toteutettu kahta reittiä jolloin toimiva osa hallitsee tuotannon.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 95.

Riski	Verkkoon kytketään laite joka toimii virheellisesti.
Tapahtuma	Verkko toimii virheellisesti tai sen tuotanto toiminta estyy kokonaan.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Verkot jaetaan pienemmiksi osakokonaisuuksiksi jolloin vika voidaan eristää koskemaan vain osaa verkosta.
Korjauksen vastuuhenkilö	

6.8. Tietoliikenneverkkojen operointi ja valvonta

Operointi ja valvonta ovat kriittisiä osia tietoliikenneverkkoja. Tietoliikenne verkkojen valvonta helpottaa tietoliikenneverkkojen operointia. Vikatilanteen sattuessa valvontatyökalut voivat usein ilmoitta missä osassa tietoliikenneverkkoa vika on ja tällä tavoin vikatilanteesta toipuminen nopeutuu. Tietoliikenneverkkojen operointia ja valvontaa tutkittaessa kiinnitettiin huomiota taulukoissa 96-98 kuvattuihin riskeihin.

Taulukko 96.

Riski	Verkon fyysinen valvonta puuttuu.
Tapahtuma	Verkkoon voidaan kytkeä laitteita kenenkään huomaamatta.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	

Korjauksen vastuuhenkilö	

Taulukko 97.

Riski	Operointi- ja valvontayhteyksiä ei eroteta tuotantoverkosta.
Tapahtuma	Virhetilanteen sattuessa tuotantoverkko sekä operointi- ja valvontayhteydet estyvät.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Operointi- ja valvontayhteyksiä on erotettu tuotantoverkosta.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 98.

Riski	Verkon operointiin käytetään suojaamatonta protokollaa.
Tapahtuma	Verkkoon voidaan kytkeä laitteita kenenkään huomaamatta.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Operoinnissa sallitaan vain salatut yhteydet.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

6.9. Varautuminen poikkeusoloihin

Laitteistojen poikkeustilanteista toipumisen helpottamiseksi, Kuusela ja Ollikainen (Hannu Kuusela ja Reijo Ollikainen, 1998: 242-243) suosittavat, että kriittisillä palveluilla olisi täydellinen varalaitteisto joka on käyttövalmiudessa ja osana tuotantojärjestelmää. Tällaisen

varajärjestelmän ylläpito lisää ylläpitäjän työmäärää mutta on samalla edellytys kriittisille järjestelmille. Kriittisiä varajärjestelmiä toteutettaessa tulee kiinnittää huomiota, että varajärjestelmä on myös tuotantokäytössä samanaikaisesti tuotantojärjestelmän kanssa. Tällä tavoin toimimalla saadaan varmuus, että varajärjestelmä toimii tuotantojärjestelmän vikaantuessa. Tutkittaessa varautumista poikkeustiloihin käsiteltiin taulukoissa 99-104 määriteltyjä riskejä.

Taulukko 99.

Riski	Varmistus media korruptoituu.
Tapahtuma	Varmistusmedialta ei voida suorittaa palautusta.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 100.

Riski	Varmistusten palautusta ei testata.
Tapahtuma	Vikatilanteessa ei voida olla varmoja, että varmistusten palautus on mahdollista.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Varmistusten palautus testataan määräajoin.
Korjauksen vastuuhenkilö	

Taulukko 101.

Riski	Varmistuslaitteisto vioittuu.
Tapahtuma	Varmistusten otto ja palautus ei onnistu. Laitteisto on korvattava uudella.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 102.

Riski	Palvelin kytketty UPS-järjestelmään mutta UPS-järjestelmä mitoitettu väärin.
Tapahtuma	UPS järjestelmä ei pysty tarjoamaan sähköä sähkökatkoksen sattuessa riittävän pitkään jolloin UPS-järjestelmään kytketyt laitteet eivät toimi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	UPS-järjestelmien mitoitukset tarkastetaan määräajoin.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 103.

Riski	UPS-järjestelmään kytketään laitteita jotka eivät ole kriittisiä sähkökatkon sattuessa.
Tapahtuma	UPS järjestelmä ei pysty tarjoamaan sähköä sähkökatkoksen sattu-

	essa riittävän pitkään jolloin UPS-järjestelmään kytketyt kriittiset laitteet eivät toimi.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Henkilöstöä ohjeistetaan sähköliittimien kytkemisestä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 104.

Riski	Verkkoon kytketään laite jonka kautta ulkopuolinen saa pääsyn yrityksen sisäverkkoon.
Tapahtuma	Ulkopuolinen saa pääsyn yrityksen sisäverkkoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Verkkoon asennettaisiin laite joka havaitsee verkkoon kytketyt laitteet.
Korjauksen vastuuhenkilö	

7. OHJELMISTOTURVALLISUUDEN ANALYSOINTI

Ohjelmistoturvallisuuden tutkiminen tehtiin yhdessä laitteistotutkimuksen kanssa. Yhdistetyssä tutkimuksessa järjestelmät käytiin läpi yksitellen laitteisto ja ohjelmistoriskeihin liittyvien riskien osalta. Ohjelmistotutkimusta suoritettaessa ohjelmistot jaettiin kahteen ryhmään: itse tehtyihin ja ulkopuolisten tekemiin sovelluksiin. Itse tehtyjen sovellusten analysoinnissa kiinnitettiin huomiota sovelluksen elinkaaren tekovaiheeseen. Ulkopuoliselta toimittajalta hankituissa sovelluksissa kiinnitettiin huomiota päivityksiin ja lisensseihin.

Ohjelmistoturvallisuutta tutkittaessa merkittävä riski liittyy tunnistettujen riskien luokitteluun. Joissain ohjelmistoissa voi olla toimintoja jotka eivät toimi oikein mutta jotka tiedostetaan. Tiedossa oleviin ohjelmistovirheisiin liittyvien riskien vakavuutta on helpompi arvioida kuin riskejä joihin liittyvien ohjelmistojen toimintaa ei täysin tunneta, jolloin riskien vakavuuden arviointi joudutaan tekemään arvioimalla palvelun tärkeyttä organisaation liiketoiminnan kannalta ja palvelua käyttävän käyttäjänkunnan kannalta. Tällaisissa tapauksissa joudutaan arvioimaan karkeiden arvioiden avulla riskien vaikutuksia, eikä voida laskennallisesti tai muuten tarkasti määritellä olemassa olevan riskin vaikutusta organisaation liiketoimintaan.

Toinen ohjelmistoturvallisuutta tutkittaessa esiintyvä merkittävä riski liittyy tunnustettujen riskien todennäköisyyteen. Riskin toteutumista on vaikea arvioida ohjelmistoissa koska ohjelmistojen luonteen mukaan ne voivat kirjoittaa samalle muistialueelle ja sotkea tällä tavalla toistensa toimintaa. Tällaisissa tapauksissa riskin todennäköisyys joudutaan arvioimaan karkean arvion avulla, eikä arvioitu tulos välttämättä vastaa ohjelmiston todellisen riskin toteutumisen todennäköisyyttä.

7.1. Ohjelmistot

Tietoturva-aukkoja voi olla monen tasoisia. Tietoturva-aukkojen vakavuus vaihtelee koko palvelun kaappauksen mahdollistavista aukoista vaarattomiin, käyttäjien omien istuntojen tietojen muokkaamiseen. Ohjelmistoista löytyy tietoturva aukkoja koko ohjelmiston elinkaaren ajan. On tärkeää seurata sovellusten viimeisimpien päivitysten julkaisuita jolloin voidaan reagoida mahdollisen tietoturvariskin toteutumiseen mahdollisimman nopeasti. Ohjelmiston tietoturva-aukkoja tutkittaessa pyrittiin selvittämään taulukossa 105 kuvattua riskiä ja sen vaikutusta palveluun.

Taulukko 105.

Riski	Ohjelmassa tietoturva-aukko.
Tapahtuma	Ulkopuolinen voi saada palvelun täyden käyttöoikeuden tai palvelun tarjonta estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Sovellukseen liittyvien päivitysten seuranta ja asennus.
Kehitysehdotukset	Tietoturva-aukkoja sisältävät sovellukset päivitetään.
Korjauksen vastuuhenkilö	

7.2. Ohjelmistoasennukset

Konfigurointi virheet voivat aiheuttaa monen tasoisia tietoturvariskejä. Pahimmassa tapauksessa palvelun tiedot voivat joutua ulkopuolisen käsiin tai palvelun toiminta estyy. Konfigurointi virheiden mahdollisuus on melko suuri, koska ihminen toteuttaa konfiguroinnin, voi konfiguraatio virhe johtua asetusten tekijän tiedon puutteesta tai muista inhimillisistä tekijöistä. Ohjelmistoasennuksia tutkittaessa tutkittiin taulukossa 106 kuvattua riskiä ja sen vaikutusta palveluun.

Taulukko 106.

Riski	Konfiguraatio virhe.
Tapahtuma	Ulkopuolinen voi saada palvelun täyden käyttöoikeuden tai palvelun tarjonta estyy.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Ennen palvelun tuotantoon siirtämistä asetukset tarkastetaan.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.3. Päivitykset

Sovelluksen vanhassa versiossa saattaa olla toiminto, joka päivityksellä paikataan. Päivittämätön sovellus voi aiheuttaa sovellukseen tietoturva-aukon tai aiheuttaa sovelluksen virheellisen toiminnon. Sovelluksen vanhassa versiossa saattaa olla tietoturva-aukko, joka päivityksellä paikataan. Päivittämätön sovellus voi aiheuttaa sovellukseen tietoturva-aukon. Joissain tapauksissa uusi päivitys saattaa rikkoa sovelluksen tai aiheuttaa sovelluksen virheellisen toiminnan ja on palattava vanhaan versioon. Ohjelmistopäivityksiä tutkittaessa tutkittiin taulukoissa 107-109 kuvattuja riskejä ja niiden vaikutusta palveluun.

Taulukko 107.

Riski	Uusimpia päivityksiä ei asenneta.
Tapahtuma	Sovellukseen saattaa jäädä virheellisesti toimiva toiminto.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Sovellukseen liittyvien päivitysten seuranta ja asennus.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 108.

Riski	Uusimpia tietoturvapäivityksiä ei asenneta.
Tapahtuma	Sovellukseen saattaa jäädä tietoturva-aukko.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Seurataan sovellusten uusimpia päivityksiä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 109.

Riski	Uusin päivitys rikkoo sovelluksen.
Tapahtuma	Sovelluksen toiminta estyy tai osa sovelluksesta toimii virheellisesti.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Asennetaan päivitykset ensin testiympäristöön.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.4. Etäkäyttö

Sovelluksen etäkäyttö ilman suojattua yhteyttä aiheuttaa tietoturvariskin. Tällaisessa tapauksessa ulkopuolinen voi kaapata yhteyden tai salakuunnella liikennettä ja saada tällä tavoin pääsyn järjestelmään. Ohjelmiston etäkäyttöä tutkittaessa tutkittiin taulukossa 110 kuvattua riskiä ja sen vaikutusta palveluun.

Taulukko 110.

Riski	Sovellusta käytetään ilman suojattua yhteyttä.
Tapahtuma	Ulkopuolinen saa pääsyn suojaamattomassa yhteydessä liikennöitävään tietoon ja voi tätä kautta saada pääsyn järjestelmään tai järjestelmän sisältämään arkaluontoiseen tietoon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Käytetään vain salattuja yhteyksiä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.5. Eheys ja käytettävyys

Palvelun tietojen eheys on turvattavissa ja käytettävyys ovat turvattavissa. Palvelun tietojen eheyden aleneminen aiheuttaa ongelmia palvelun käyttäjille koska käyttäjät eivät voi luottaa palvelun tarjoamiin tietoihin. Palvelun käytettävyyden aleneminen aiheuttaa työntekijän työtehon aleneman tai pahimmassa tapauksessa työn teko estyy. Tutkittaessa ohjelmiston eheyttä ja käytettävyyttä selvitettiin taulukoissa 111-114 kuvattua riskiä ja niiden vaikutusta palveluun.

Taulukko 111.

Riski	Ohjelmiston käyttö mahdotonta hitauden vuoksi.
Tapahtuma	Työn teko hidastuu ja yritykselle voi koitua taloudellista vahinkoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Varataan palvelulle riittävästi resursseja palvelimelta jolloin palvelun käytettävyys säilyy hyvänä.
Kehitysehdotukset	

Korjauksen vastuuhenkilö	

Taulukko 112.

Riski	Palveluun on tallennettu virheellistä dataa.
Tapahtuma	Sovelluksen sisältämä tieto on virheellistä. Tiedon käyttötarkoitus ja luottamuksellisuus määrittelevät toteutuneen riskin vakavuuden.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Palvelusta ajetaan varmistuslistoja säännöllisin välein ja tehdään pistokokeita tietojen eheyden tarkistamiseksi.
Korjauksen vastuuhenkilö	

Taulukko 113.

Riski	Palvelun tieto on muutettu virheelliseksi.
Tapahtuma	Sovelluksen sisältämä tieto on virheellistä. Tiedon käyttötarkoitus ja luottamuksellisuus määrittelevät toteutuneen riskin vakavuuden.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	Palvelusta ajetaan varmistuslistoja säännöllisin välein ja tehdään pistokokeita tietojen eheyden tarkistamiseksi.
Korjauksen vastuuhenkilö	

Taulukko 114.

Riski	Ohjelmistossa on ohjelmistovirhe.
Tapahtuma	Ohjelmisto toimii virheellisesti tai sisältää tietoturva-aukon.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.6. Lisenssit

Ohjelmistojen käyttöön kuuluu olennaisena osana ohjelmistojen käyttäjälisenssit. Useiden ohjelmistojen käyttö edellyttää ohjelmiston lisenssiä jota ilman ohjelmistoa ei voida käyttää. Ohjelmisto lisenssejä tutkittaessa tutkittiin taulukoissa 115–117 kuvattuja riskejä ja niiden vaikutusta palveluun.

Taulukko 115.

Riski	Uusia lisenssejä ei ole tilattu.
Tapahtuma	Sovellus saattaa lakata toimimasta tai organisaatiolle koituu taloudellisia vahinkoja.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 116.

Riski	Lisenssit vanhenevat.
Tapahtuma	Sovellus saattaa lakata toimimasta tai organisaatiolle koituu taloudellisia vahinkoja.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 117.

Riski	Palvelulla on liian vähän käyttäjälisenssejä.
Tapahtuma	Sovellus saattaa lakata toimimasta tai organisaatiolle koituu taloudellisia vahinkoja.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.7. Versionhallinta

Tärkeä työkalu ohjelmistokehityksessä on versionhallinta. Versionhallinnalla pidetään kirjaa keskitetysti lähdekoodin muutoksista. Versionhallinnan puuttuminen vaikeuttaa ohjelmistokehitystä päällekkäisten ohjelmistopäivitysten vuoksi. Ohjelmiston versionhallintaa tutkittaessa tutkittiin taulukossa 118-120 kuvattua riskiä ja niiden vaikutusta palveluun.

Taulukko 118.

Riski	Versionhallinta ei toimi.
Tapahtuma	Sovelluskehitys hidastuu ja voidaan menettää tietoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 119.

Riski	Ohjelmistotuotannossa päivitetään tuotantoon väärä versio.
Tapahtuma	Sovelluskehitys hidastuu ja voidaan menettää tietoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tehtävät muutokset versionhallinnassa on erikseen hyväksyttävä.
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

Taulukko 120.

Riski	Versionhallinnasta poistetaan kriittinen versio.
Tapahtuma	Sovelluskehitys hidastuu ja voidaan menettää tietoa.
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	Tehtävät muutokset versionhallinnassa on erikseen hyväksyttävä. Varmistukset.

Kehitysehdotukset	
Korjauksen vastuuhenkilö	

7.8. Varautuminen poikkeusoloihin

Ohjelmistojen riskejä tutkittaessa havaittiin taulukossa 121 havaittu riski. Tämä riski on olemassa siihen varautuminen ja siitä toipuminen on usein hankalaa, koska se usein johtuu kolmannesta osapuolesta.

Taulukko 121.

Riski	Sovelluksen toimittaja ei pysty toimittamaan tukipalveluita ja niiden saanti estyy.
Tapahtuma	
Todennäköisyys	1-4
Vaikutus	1-4
Vakavuus	Todennäköisyys * vaikutus
Varautuminen	
Kehitysehdotukset	
Korjauksen vastuuhenkilö	

8. JOHTOPÄÄTÖKSET

Tutkimuksen tavoitteena oli tehdä kohde yrityksen IT-palveluista vastaavan osaston vastuulla oleville tietojärjestelmille riskianalyysi. Riskianalyysin tuli kattaa yrityksen tietohallinnon vastuulla olevien järjestelmien ja henkilöiden riskit.

Nykyisin tietojärjestelmät ovat usein kriittinen osa yrityksen liiketoimintaa. Tietojärjestelmiin kohdistuu niiden kriittisyyden vuoksi monenlaisia vaatimuksia. Tietojärjestelmien on kyettävä tarjoamaan käyttäjälle korkean asteen käytettävyyttä ja luotettavuutta. Tietojärjestelmien usein odotetaan toimivan myös virheettömästi.

Tietojärjestelmien riskien hallinta koostuu lukuisista komponenteista. Hyvän riskien hallinnan perustana toimii riskien havaitseminen, ymmärtäminen ja luokittelu. Hyvässä riskianalyysissä on pystytty tunnistamaan tarpeelliset riskit ja arvioimaan niiden vakavuus riittävällä tarkkuudella. Yrityksen tietojärjestelmiä koskevan riskianalyysin avulla helpotetaan riskien pienentämistä yrityksen liiketoiminnankannalta kannalta tärkeiden palveluiden tai järjestelmien osalta hyväksytylle tasolle.

Riskianalyysissä määriteltyjen riskien avulla voidaan reagoida löydettyihin riskeihin. Löydettyjen riskien vakavuuden kuvatessa riskin tärkeyttä, riskit voidaan järjestää tärkeys järjestykseen ja tehdä jatkotoimenpiteet tärkeysjärjestyksessä.

Riskianalyysiä tehdessä havaittiin laitteistojen kahdennuksen aiheuttavan tuotannossa ongelmia. Palvelukonsepti koostuu usein useista järjestelmistä jolloin yhden järjestelmän vikaantuessa koko palvelukonseptin toiminta estyy.

Laitteistoja kahdennettaessa Active-Standby ratkaisuissa havaittiin ongelmia. Aktiivisen järjestelmän vikaantuessa ja tuotannon siirtyessä standby järjestelmälle, ei usein voida olla varmoja tuotannon laadukkaasta toiminnasta. Ongelmana tällaisessa ympäristössä on standby järjestelmän puutteelliset päivitykset ja testaus. Mikäli palvelu halutaan toteuttaa Active-Standby ratkaisulla, tulisi aktiivisen ja standby järjestelmien rooleja vaihdella määräajoin, jolloin voidaan varmistua molempien järjestelmien toimivuudesta. Tutkimuksen perusteella järjestelmien kahdennus kannattaa toteuttaa kahdella aktiivisella järjestelmällä, jolloin tuotanto toimii samanaikaisesti molemmissa järjestelmissä. Tällaisessa ympäristössä toisen järjestelmän vikaantuessa, kaikki palvelupyynnöt menevät automaattisesti vielä toiminnassa olevalle järjestelmälle.

Levyjärjestelmiä kahdennettaessa havaittiin parhaaksi ratkaisuksi toteuttaa kahdennus kahdella täysin autonomisella, toisistaan erillään olevalla järjestelmällä. Näin toimimalla toisen ympäristön vikaantuminen ei vaikuta toiseen ympäristöön koska ympäristöt ovat erotettu toisistaan täysin.

Tietoverkkojen dokumentointia tutkittaessa havaittiin riittävän dokumentaation olevan kriittinen osa tietoverkkoja. Tietoverkot tarjoavat palveluitaan tietojärjestelmille jolloin tietoverkon vikaantuessa myös tietoverkon laatu alenee ja palveluiden tarjonta mahdollisesti estyy. Tietojärjestelmien operoinnin ja valvonnan laatu laskee huomattavasti, mikäli tietoverkkoja ei ole rakennusvaiheessa ja muutos- tai päivitystöitä tehdessä dokumentoitu tarkasti.

Tutkimus osoittaa, että yrityksellä tulisi olla elvytyssuunnitelma. Elvytyssuunnitelmassa kuvataan miten toteutuneen uhka skenaarion jälkeen toivutaan tilaan, jossa liiketoiminta jatkuu normaalisti.

LÄHDELUETTELO

Allen, Julia H. (2002). *Verkkotietoturvan hallinta – CERT*.Helsinki: IT Press. ISBN 951-826-588-7.

Anderson , Ross (2001). *Security Engineering*. United States of America: WILEY. ISBN 0-471-38922-6.

Barman, Scott (2002). *Writing Information Security Policies*. United States of America: New Riders Publishing. ISBN 1-57870-264-X.

Brenton, Chris & Hunt, Cameron (2003). *Network Security*. California: SYBEX. ISBN 0-7821-4142-0.

Casey, Eoghan (2002). *Handbook of computer crime investigation*. California: Academic press. ISBN 0-12-163103-6.

Centre for the Protection of National Infrastructure (2007). *Personnel security: threats, challenges and measures* [online]. UK: Centre for the Protection of National Infrastructure [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.cpni.gov.uk/Docs/Pers_Sec_TCM_v2.pdf>.

Centre for the Protection of National Infrastructure (2009). *Risk assessment for personnel security* [online]. UK: Centre for the Protection of National Infrastructure [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.cpni.gov.uk/Docs/Risk_Assessment_Ed_3.pdf>.

Cheswick William R., Bellovin , Steven M. & Rubin Aviel D. (2003) *Firewalls and Internet security*. Reading: Addison-Wesley. ISBN 020163466X.

Chirillo, John (2001). *Hack attacks revealed*. New York: John Wiley & Sons, Inc. ISBN 0-471-41624-X.

Finlex (2004). *Suositus määräyksen viestintävirasto 47 B/2004 M soveltamisesta teleyrityksen tietoturvassa* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.finlex.fi/pdf/normit/5206-SMS47B%5B1%5D.pdf>.

Garfinkel, Simon & Spafford, Gene (2002). *Web Security, Privacy & Commerce*. California: O'reilly. ISBN 0-596-00045-6.

Gollmann, Dieter (1999). *Computer security*. England: John Wiley &Sons Ltd. ISBN 0-471-97844-2.

Hakala Mika, Vainio Mika & Vuorinen Olli (2006). *Tietoturvallisuuden käsikirja*. Jyväskylä: Decondo Finland Oy. ISBN 951-846-273-9.

Hyvönen, Eero (2003). *Ohjelmistoliiketoiminta*. Vantaa: WSOY. ISBN 951-0-26996-4.

Jaakohuhta, Hannu (2003). *Tietojärjestelmien luotettavuus*. Helsinki: IT Press. ISBN 951-826-229-2.

Järvinen, Petteri (2006) *Paranna tietoturvaasi*. Jyväskylä: Decendo. ISBN 951-846-289-5.

Kajava, Jorma & Remes, Timo (2000) *Intranet security from organizational point of view*. Oulu: Oulun yliopisto. ISBN 951-42-5576-3.

Klander, Lars (1997). *Hacker Proof*. Houston: Jamsa Pr. ISBN 1-884133-55-X

Krutz, Ronald L. & Vines, Russell Dean (2003), *Tietoturvasertifikaatti – CISSP*. Helsinki: IT-Press. ISBN 951-826-657-3

Kuusela, Hannu & Ollikainen, Reijo (1998). *Riskit ja riskienhallinta*. Vammala: Tampere University Press. ISBN 951-44-4303-9.

Kyrölä, Tuija (2001) *Esimies ja tietoriskien hallinta*. Juva: WS Bookwell Oy. ISBN 951-0-25645-5.

McClure Stuart, Scamray Joel & Kurtz George (1999). *Hacking Exposed, Network security secrets & solutions*. United States of America: Osbourne/McGraw-Hill Berkeley ISBN 0-07-212127-0.

McClure Stuart, Scambray Joel & Krutz George (2002). *Hakkeroinnin torjunta*. Jyväskylä: Gummerrus kirjapaino Oy. ISBN 951-762-802-1.

Miettinen, Juha E. (1999). *Tietoturvallisuuden johtaminen*. Helsinki: Kauppakaari Oyj. ISBN 952-14-0229-6.

Northcutt Stephen, Novak Judy & McLachlan Donald (2002). *Verkkomurtojen havaitseminen*. Jyväskylä: Gummerrus kirjapaino Oy. ISBN 952-14-0437-X.

Paavilainen, Juhani (2004). *Tietoturvallinen ohjelmointi*. Tampere: Tampereen yliopistopaino Oy. ISBN 951-44-5914-8.

Pirnes Jari, Sahlman Anssi & Kajava Jorma (2000). *Tietoturva ja sisäinen valvonta*. Juva: Oulu university press. ISBN 951-42-5833-9.

PK-RH Pk-yrityksen riskienhallinta (2000 – 2009) *Henkilöstöriskit* [online]. Espoo: VTT [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.pk-rh.fi/riskilajit/henkiloriskit/henkiloriskit >.

Ruohonen, Mika (2002). *Tietoturva*. Jyväskylä: Docendo Finland Oy, SanomaWSOY. ISBN 951-846-163-5.

Salminen, Markus (2009). *Tietosuoja sähköisessä liiketoiminnassa*. Helsinki: Talentum Media Oy. ISBN 978-952-14-1370-4.

Schiffmanm Mike D., O'Donnell Adam J., Pennington Bill & Pollino David (2003). *Hack-esr's challenge 2 – Test Your Networ Security & Forensic Skills*. California: Osborne. ISBN 0-07-222630-7.

Splaine, Steven (2002). *Testing web security*. Indianapolis: Wiley Publishing, Inc. ISBN 0-471-23281-5.

Stallings, William (2000). *Network security essentials*. New Jersey: Prentice-Hall, Inc. ISBN 0-13-016093-8.

Stallings, William & Brown, Lawrie (2008). *Computer security*. New Jersey: Pearson Education Inc. ISBN-13 978-0-13-513711-6, ISBN-10 0-13-513711-X.

Suominen, Arto (2003). *Riskienhallinta*. Helsinki: WSOY. ISBN 951-0-26878-X.

Valtionvarainministeriö (2001). *Valtionhallinnon lähiverkkojen tietoturvallisuussuositus* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf >.

Valtionvarainministeriö (2003). O*hje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53828/53827_fi.pdf>.

Valtionvarainministeriö (2004). *Valtionhallinnon keskeisten tietojärjestelmien turvaaminen* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20041201Valtio/01_VAHTI_5_2004.pdf>.

Valtionvarainministeriö (2006a). *Tietoturvallisuuden arviointi valtionhallinnossa* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf>.

Valtionvarainministeriö (2006b). *Henkilöstön tietoturvaohje* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3375/3378_fi.pdf>.

Valtionvarainministeriö (2008). *Tärkein tekijä on ihminen* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf>.

Valtionvarainministeriö (2009a). *Laitteistoturvallisuus* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus >.

Valtionvarainministeriö (2009b). *Tietoaineistoturvalliuus – tietopääoman hallinta* [online]. Helsinki: valtionvarainministeriö [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus-tietopaaoman-hallinta>.

Weber, Ron (1999). *Information systems control and audit*. New Jersey: Prentice Hall. ISBN 0-13-947870-1.

Wikipedia (2011). *Palvelunestohyökkäys* [online] [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://fi.wikipedia.org/wiki/Palvelunestohy%C3%B6kk%C3%A4ys>.

Wikipedia (2010). *DMZ* [online] [siteerattu 1.11.2011]. Saatavana World Wide Webistä: <URL:http://fi.wikipedia.org/wiki/Demilitarisoitu_alue_%28tietotekniikka%29>.