Sähkö- ja tietoliikennetekniikan osasto

Timo Karsisto

Tietoturvariskianalyysin tehostaminen työkalun avulla

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten.

Espoossa 1.2.2007

Työn valvoja	Prof. Raimo Kantola
Työn ohjaaja	DI Massimo Nardone

Tekijä:	Timo Karsisto
Työn nimi:	Tietoturvariskianalyysin tehostaminen työkalun avulla
Päivämäärä:	1. helmikuuta, 2007 **Sivumäärä:** 101 + 12
Osasto:	Sähkö- ja tietoliikennetekniikan osasto
Professuuri:	S-38 Tietoverkkolaboratorio
Työn valvoja:	prof. Raimo Kantola, Tietoliikennetekniikan professori
Työn ohjaaja:	Massimo Nardone, DI

Nykypäivän tietoturvahaasteet ja uhkat vaativat nopeaa toimintaa. Tietoturvaorganisaation tehtävä on vastata näihin haasteisiin. Järjestelmällinen tietoturvanhallinta ja toimiva tietoturvaorganisaatio ja -työ voivat ennaltaehkäistä tietoturvavälikohtauksia sekä valmistaa organisaatiota toimimaan määrittelemänsä tavoitetason ja periaatteidensa mukaisesti.

Erityisen suuren huomion kohteena tietoturvassa ovat tekniset yksityiskohdat kuten virukset ja madot. Tietoturva on kuitenkin huomattavasti laajempi käsite. Yksi työn tavoitteista on tarjota lukijalle kattava kuva mistä tietoturvassa on kyse. Tietoturvan kokonaisuuden ymmärtäminen on pohja ja edellytys analyyttiselle ajattelulle. Yksi tietoturvaorganisaation tehtävä on riskianalyysin tekeminen. Riskianalyysin tarkoituksena on ennaltaehkäistä ja löytää organisaation järjestelmistä, prosesseista ja ihmisistä perimmäisiä syitä riskeille ja ennenkaikkea ehkäistä näiden toteutumista. Riskien tiedostaminen ja niiden lieventäminen on välttämätöntä organisaation turvallisuuden kannalta.

Tämän työn puitteissa tarkastellaan tietoturvaa, tietoturvaorganisaatiota, sen tehtäviä ja erityisesti riskienhallintaa ja riskianalyysiprosessia. Tavoitteena on kehittää tehokas työväline riskianalyysin suorittamiseen. Yhtäältä työkaluun tulee valita toteutettavat standardit ja toisaalta menetelmä, jolla työtä ohjataan.

Työkaluun toteutettaviksi standardeiksi valittiin ISO 17799, COBIT 4.0, BSI 100-3 ja VAHTIn uhkalistoja. Sähköisen riskianalyysityökalun menetelmäksi valittiin oma variantti potentiaalisten ongelmien analyysistä (POA). Tietoturvastandardien puolesta haasteena oli saada tiivistettyä ja sovitettua standardit sähköiseen työkaluun sopivaksi. Standardeista pyrittiin valitsemaan ainoastaan ydinasiat ja ne pyrittiin esittämään mahdollisimman ymmärrettävässä muodossa. Standardien toteuttamisessa työkaluun onnistuttiin erinomaisesti. Työkaluun valittu menetelmä osoittautui myös tehokkaaksi ja tarkoitukseen sopivaksi.

Kehitettyä työkalua arvioitiin asiantuntija-arviointien perusteella. Arviointitulosten perusteella työkalu sopii riskianalyysin tekemiseen erinomaisesti. Erityiskiitosta työkalussa sai sen joustavuus sisällön suhteen. Työkalua pidettiinkin ennen kaikkea kehitysalustana, johon on helppo tuoda uutta sisältöä.

Avainsanat: tietoturva, riskianalyysi, ISO17799, COBIT, riski-/uhkakartoitus

Author:	Timo Karsisto
Title:	Intensifying Information Security Risk Analysis with a Tool
Date:	February 1, 2007 **Number of pages:** 101 + 12
Department:	Department of Electrical and Communications Engineering
Professorship:	S-38 Networking laboratory
Supervisor:	Raimo Kantola, Professor of Communications Technology
Instructor:	Massimo Nardone, M.Sc. (Tech.)

Today's information security challenges and threats require fast response time. Information security organisations responsibility is to respond to these challenges. Systematic information security management and effective information security organisation can prevent security incidents of happening and prepare organisation to operate within its defined goals and principals.

In area of information security technical issues such as viruses and worms gain especially great attention. However information security is much wider concept. One goal of the thesis is to offer the reader a comprehensive picture of information security. Comprehensive understanding of information security is the base and prerequisite of analytical thinking.

One of the information security organisation's tasks is to do risk analysis. The purpose of risk analysis is to prevent and acknowledge fundamental causes of risks in organisations systems, processes and people. Acknowledging and mitigating risks is crucial for the sake of the organisations security.

Within this thesis we are going to get acquainted with information security, information security organisation and its tasks, risk management and risk analysis process. The goal of thesis is to develop an effective risk analysis tool. The tool has two sides: implemented standards and the working method.

Chosen standards for the tool were ISO 17799, COBIT 4.0, BSI 100-3 and threat catalogues from VAHTI. Chosen method for the electronic tool was analysis method of potential problems (POA). The challenge with information security standards was to compress them and keep them still in comprehensive form. The challenge was also to fit the standard and its structures to the electronic tool. Fitting and implementing the standards to the tool succeeded well. The chosen method also turned out to be well fitted and effective.

The developed tool was evaluated by information security professionals. The results show that the developed tool is well suited for its purpose. Flexibility of the content was found especially good feature. The tool was considered as a development platform where importing new content is easy.

Keywords: Information Security, Risk Analysis, ISO 17799, COBIT, Risk assessment

Esipuhe

Tietoturva on ollut minulle aina erityisen läheinen aihe. Halusin nimenomaan keskittyä tietoturva-aiheeseen myös diplomityössäni.

Keväällä 2006 minulle tarjoutui tilaisuus diplomityön tekemiseen riskianalyysityökalun kehittämisestä. Sattumien summana Rational Requisite Pro työkalua päätettiin käyttää riskianalyysityökaluna, ja minä aloitin työkalun kehittämisen. Loppu onkin historiaa.

Haluan erityisesti kiittää Arto Viljasta hänen avoimista kommenteistaan ja mielipiteistään työn, riskianalyysin ja standardien suhteen. Haluan myös kiittää työni ohjaajaa Massimo Nardonea hänen opastuksestaan ja näkemyksistään tietoturva-alalla. Erityiskiitoksen ansaitsee myös minun perheeni ja avopuolisoni pitkäaikaisesta tuesta ja ymmärryksestä opintojeni aikana.

Espoo, 1. helmikuuta, 2007

Timo Karsisto

Sisällysluettelo

Liitteet

Lista kuvista

Lista taulukoista

Käsitteet ja lyhenteet

Aivoriihi	*Eräs ideointimenetelmä, jota voidaan käyttää muun muassa ongelmien ratkaisuun*
Analyysiryhmä	*Tietoturvariskianalyysin suorittava ydinjoukko ihmisiä. Normaalisti 3-5 ihmistä*
Auditointi	*Järjestelmän tai kokonaisuuden tarkastaminen tiettyjä kriteereitä vasten*
Aukkoanalyysi	*engl. Gap Analysis*
Autentikointi	*Lähetyksen, viestin tai esimerkiksi lähettäjän oikeellisuuden varmistaminen*
Autorisointi	*vrt. Valtuuttaminen*
BSI	*Saksan valtionhallinnon kansallinen tietoturvatoimisto, joka määrittelee muutamia omia tietoturvastandardeja, saks. Bundesamt für Sicherheit in der Informationstechnik*
C.I.A	*Tietoturvan kulmakivet eli luottamuksellisuus, eheys ja käytettävyys, engl. Confidentiality, Integrity and Availability*
CERT	*Tietoturvaan keskittynyt organisaatio, joka toimii keskeisenä koordinointikeskuksena nousevien tietoturvauhkien, -haavoittuvuuksien ja –välikohtausten kanssa*

CERT/CC	*kts. CERT*
CIAPP	*Organisaation tietovarojen suojaamisohjelma, engl. Corporate Information Asset Protection Program*
CMM	*Kypsyysmalli eli Capability Maturity Model*
COBIT	*engl. The Control Objectives for Information and related Technology on ISACAn luoma kokoelma parhaita käytäntöjä informaatioteknologiajohtamisen alalla*
Common Criteria	*Kansainvälinen tietoturvastandardi ISO 15408*
Eheys	*Tieto ei ole muuttunut tai tuhoutunut tahallisesti tai tahattomasti*
Haavoittuvuus	*Heikkous, joka voi mahdollistaa järjestelmän hyväksikäytön*
IPPD-CMM	*engl. Integrated Product and Process Development – Capability Maturity Model*
ISACA	*engl. Information Systems Audit and Control Association*
ISO 13335	*engl. Information Technology – Security Techniques – Management of Information and Communications Technology Security*
ISO 17799	*Yksi tunnetuimmista tietoturvastandardeista*

ISO 21827	*kts. SSE-CMM*
ISO 27001	*Tietoturvastandardi, joka määrittelee tietoturvan hallintomallin. Käytetään rinnakkain ISO 17799 kanssa*
ISO 7498-2	*Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture*
ISO/IEC	*Kansainvälinen standardointiorganisaatio*
ISSO	*Tietojärjestelmien tietoturvapäällikkö eli engl. Informations Security Systems Officer*
Kiistämättömyys	*Tiedolle tehdyt muutokset ovat tiedossa ja ovat kiistämättömiä, engl. non-repudiation*
Kontrolli	*Eri tietoturvastandardit määrittelevät kontrolleja tai kontrollitavoitteita. Kontrolleja voidaan hyväksikäyttää riskianalyysin tukena tai vaatimuksina*
Kriittinen voimavara	*engl. Critical Asset*
Kvalitatiivinen riskianalyysi	*Riskianalyysityyppi, joka ei pyri arvioimaan tarkkoja kustannuksia*
Kvantitatiivinen riskianalyysi	*Riskianalyysityyppi, joka pyrkii asettamaan riskeille ja niiden toteutumiselle eksaktit rahalliset kustannukset*

Kypsyysmalli	*engl. CMM*
Käytettävyys	*Tietojärjestelmäresurssit ovat niitä tarvitsevien saatavissa, engl. Availability*
Lainmukaisuus	*engl. Compliance*
Luottamuksellisuus	*Tiedon tahallisen tai tahattoman paljastumisen estämistä, engl. Confidentiality*
MASS	*engl. Method for Designing Secure Solutions*
OCTAVE	*CERT Coordination Centerin (CERT/CC) kehittämä tieturvariskien arviointimenetelmä*
Oikeudenkäyntikelpoisuus	*Todisteet ovat kiistämättömiä ja voidaan esittää oikeudessa todisteena*
OSI-malli	*7-portainen malli, engl. ISO Reference Model for Open Systems Interconnection*
PDCA/PDCA-prosessimalli	*engl. Plan-Do-Check-Act*
POA	*Potentiaalisten ongelmien analyysimenetelmä*
Tietoturvapolitiikka	*Ohjeistus, jossa kuvataan organisaation linjaus tietoturvallisuuteen*
Pääsynvalvonta	*Ennaltamääritettyjen autorisointisääntöjen toimeenpanemismekanismi*
Rational Requisite Pro	*Ohjelmistokehitykseen tarkoitettu ´ vaatimustenhallintatyökalu*

Riskianalyysi	*Systemaattinen tapa tunnistaa tarkastelukohdetta koskevia uhkia ja niiden seurauksia*
Riskianalyysimenetelmä	*Viitekehys tai menetelmä, jonka mukaan riskianalyysiprosessi viedään läpi*
Riskiarviointi	*kts. Riskianalyysi*
Riskien arviointikriteeristö	*Kriteerit, joita käytetään arvioitaessa riskejä, uhkien suuruksia ja seurauksien vakavuuksia. Kriteeristö määritellään yleensä osana riskianalyysiprosessia*
Riskien lievennyssuunnitelma	*Suunnitelma, joka kuvaa kuinka kriittisimmiksi todettuja riskejä tullaan pienentämään*
Riskienhallinta	*Systemaattinen toiminta riskien ennaltaehkäisemiseen, tiedostamiseen ja hallitsemiseen.*
Riskikartoitus	*kts. Riskianalyysi*
Riskiluku	*Uhkan toteutumistodennäiköisyyden ja seurauksien vakavuuden tulo*
SE-CMM	*engl. Systems Engineering - CMM*
Sokkotestaus	*engl. Blind Testing*
SSE-CMM	*engl. Systems Security Engineering - CMM*

Suojakeino	*engl. Safeguard*
SW-CMM	*engl. Sofware Engineering -CMM*
Tietoturvan hallintamalli	*kts. ISO 27001*
Tietoturvan kulmakivet	*kts. C.I.A.*
Tietoturvatapahtuma	*engl. information security event*
Tietoturvavälikohtaus	*engl. Information Security Incident*
Tietoturvauhka	*Potentiaalinen tapahtuma, joka uhkaa tarkastelukohdetta*
Vaatimuksenmukaisuus	*engl. Compliance*
VAHTI	*Valtionhallinnon tietoturvallisuuden johtoryhmä*
Valtuuttaminen	*Oikeuksien antaminen, mukaan lukien mahdollisuuden päästä määrättyyn tietoon tai resursseihin*
Voimavara	*engl. Asset*
VPN	*engl. Virtual Private Network*
VTT	*Valtion Teknillinen Tutkimuslaitos*

1. Johdanto

1.1. Alkusanat

Nykyajan organisaatioiden viestintä ja toiminta perustuvat pitkälti tietokoneisiin, verkkoihin ja sähköiseen viestintään. Yhä suurempi osa kriittisistä tiedoista on sähköisessä muodossa. ja nopeat tietoliikenneyhteydet ovat arkipäivää. Tietoverkot ovat keskeisessä asemassa yritysten välisessä kommunikaatiossa. Ulkoistaminen ja keskittyminen ydinliiketoimintaan ovat yleisiä trendejä. Ulkoistamisella pyritään kustannustehokkuuteen tai suurempaan joustavuuteen[1]. Tämä aiheuttaa sen, että yhteydet ja yhteistyö organisaatioiden välillä kasvaa. Ulkoistamisessa erityisen tietoturvauhan muodostaa se, että tietoja annetaan ulkopuoliselle taholle[2].

Nousevana haasteena on kehittää organisaatio, joka pystyy toimimaan uhkia ja riskejä kohtaan ennaltaehkäisevästi. Haasteita aiheuttaa se, että tietoturvallisuus ei ole ainoastaan oman organisaation asia vaan myös alihankkijat ja yhteistyökumppanit ovat merkittävässä roolissa.

---

[1] *Mika Pajarinen, Ulkoistaa vai ei – outsourcing teollisuudessa, Elinkeinoelämän tutkimuslaitos, sarja B 181, Taloustieto Oy, Helsinki, 2001*

[2] *Jorma Kajava, Sami J.P. Heikkinen, Paavo Jurvelin, Tero Viiru ja Päivi Parviainen, Tietojenkäsittelyn ulkoistaminen ja tietoturva, Oulun yliopisto, Working papers series B 42, Oulu, 1996*

Riskienhallinnan merkitys kasvaa uudessa turbulentissa yritysmaailmassa. Organisaatioiden on tehtävä jatkuvaa riskianalyysia ja sen on tiedettävä riskit, joita se ottaa. Tietoverkkoriskit vaativat usein organisaatioilta erittäin nopeaa reaktioaikaa. Uhkiin ja riskeihin vastaamiskyky on keskeistä yritysten menestymisen kannalta.

Riskianalyysi on merkittävässä roolissa riskienhallinnan kannalta. Riskianalyysin viitekehyksenä on mahdollista käyttää lukuisia eri standardeja. Organisaatiot käyttävät useita erilaisia standardeja osana riskienhallintaansa. On olemassa kansainvälisiä tietoturvastandardeja, joiden voidaan sanoa olevan yleisesti hyväksyttyjä ja käytettyjä riskianalyysin viitekehyksenä. Tässä työssä pyritään paneutumaan juuri näihin standardeihin.

1.2. Työn tavoitteet

Työn tavoitteena on tutkia ja analysoida keskeisiä tietoturvastandardeja ja – käytäntöjä, joita voidaan käyttää riskikartoitus/-analyysityön pohjana. Tietoturvastandardeja on lukuisia ja monet organisaatiot määrittelevät omia käytäntöjä tai standardeja. Standardointiorganisaatioita on lukuisia, joista osa on kansainvälisiä ja osa kansallisia. Ongelmana ja tavoitteena työssä on valita käsittelyn kohteeksi standardeista ne, jotka ovat mahdollisimman hyväksyttyjä ja arvostettuja kautta maailman.

Työ keskittyy tietoturvariskianalyysiin ja sen prosessin läpiviemiseen, ja tietoturvariskianalyysityökalun kehittämiseen. Keskeisenä osana riskikartoitustyötä on menetelmä, jota käytetään viitekehyksenä läpi koko prosessin. On olemassa monia menetelmiä, joista osa on kehitetty puhtaasti riskikartoitus ja -analyysityöhön. Tämän lisäksi on olemassa monia yleiskäyttöisiä ongelmien ratkaisumenetelmiä. Työn haasteena on pyrkiä valitsemaan menetelmistä tarkemman tarkastelun kohteeksi mahdollisimman sopivat menetelmät.

Kokonaisuudessaan työn tavoitteena on kehittää oma riskikartoitus/-analyysityökalu. Kehitystä rajoittavat ohjelmiston ominaisuudet. Haasteena on onnistua valitsemaan

työkaluun toteutettavaksi sopivat standardit, joita riskikartoitusprosessi tulee noudattamaan. Haasteena on myös valita sopiva metodiikka prosessin läpiviemiseksi.

Tahtotila on kehittää riskianalyysityökalu asiantuntijan tai ulkopuolisen konsultin käyttöön. Kehitettyä riskianalyysityökalua tullaan evaluoimaan asiantuntija-arvioinnin avulla. Tarkoituksena on kehittää ja määritellä riskikartoitusprosessia ja sen läpiviemistä sähköisen työkalun avulla. Omana osuutena työssä tullaan kehittämään oma riskianalyysityökalu asiantuntijan tai konsultin käyttöön.

1.3. Työn rajaus

Tämän työn puitteissa asioita pyritään tarkastelemaan asiantuntijan tai ulkopuolisen konsultin näkökulmasta, vaikkakin tarkasteltavat asiat ovat organisatorisia. Kehitettävän työkalun käyttöä tullaan tarkastelemaan samasta näkökulmasta. Standardeissa ja menetelmissä pyritään antamaan enemmän painoa ja syvyyttä erityisesti niille, jotka soveltuvat ulkopuolisen konsultin/asiantuntijan käyttöön.

Näkökulmana riskikartoitukseen ja riskianalyysiin pidetään läpi työn asiantuntijanäkökulmaa. Riskianalyysin näkökulmana on nimenomaan tietoturvallisuus. Standardeissa, menetelmissä ja koko prosessissa pyritään keskittymään valitsemaan lähestymistapa, joka parhaiten soveltuu asiantuntijan käyttöön.

2. Tietoturvan kokonaisuus

Tietoturva on ollut tärkeä asia kautta aikojen. Sen merkitys on korostunut ja ehkä myös kärjistynyt tietokonemaailman tuomien riskien ja uhkien kautta. Tietoturvasta on muodostunut koko kansan käsite, mutta valitettavasti tietoturva-käsite mielletään käsittävän vain murto-osan tietoturvan todellisesta kokonaisuudesta.

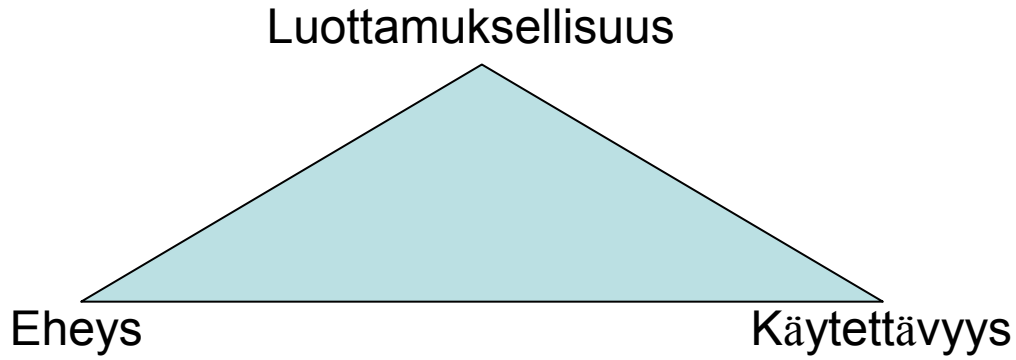
Yleisesti mielletään, että Internetin salausmenetelmät, virustutkat ja haittaohjelmien poistajat ovat tietoturvaa. Monesti myös mielletään, että tietoturva muodostuu hyvin pitkälti teknisistä asioista, jotka liittyvät vahvasti tietokoneisiin ja järjestelmävalvojat ovat tietoturva-alan rautaisia ammattilaisia. Edellä mainitut asiat liittyvät vahvasti tietoturvaan, mutta tietoturva on olennaisesti laajempi käsite. Tietoturvaan voidaan lukea kuuluvaksi muun muassa henkilöstön, fyysisen ympäristön ja yhteistyösuhteiden aiheuttamien riskien hallinta ja ehkäiseminen.

Tässä kappaleessa kuvataan tietoturvan kokonaisuus, sen kulmakivet ja osa-alueet sekä keskeisiä tietoturvakäsitteitä.

2.1. Tietoturvan kulmakivet

Näkemyseroista huolimatta pohjautuvat eri tietoturvakuntien näkemykset samaan kolmijakoon. Tietoturvan kulmakivet muodostavat luottamuksellisuus (engl.

confidentiality), eheys (engl. integrity) ja käytettävyys (engl. availability)[3]. Seuraavassa on esitetty tietoturvan kulmakivet(Kuva 1).



Kuva 1: Tietoturvan kulmakivet.

Luottamuksellisuudella tarkoitetaan tiedon tahattoman tai tahallisen paljastumisen estämistä. ISO-standardointiorganisaatio määrittelee luottamuksellisuuden tarkoittavan tiedon varmistamista siten, että vain valtuutetuilla henkilöillä on pääsy siihen[4].

Eheydellä varmistetaan, että tiedolle ei ole tehty valtuuttamattomia muutoksia. Eheys tarkoittaa sitä, että viestin sisältö on sitä mitä sen on tarkoituskin olla. Useissa tapauksissa viestin/tiedon eheys tulee olla varmistettavissa.

Käytettävyys puolestaan tarkoittaa sitä, että tiedot ja resurssit ovat aina niitä tarvitsevien ja niihin valtuutettujen käytettävissä.

Kulmakivien muodostamaan kolminaisuuteen viitataan usein englannin kielessä lyhenteellä C.I.A(Confidentiality, Integrity, Availability). Tämä tietoturvan peruskolmikko määrittelee ja asettaa lukuisia vaatimuksia järjestelmille tai prosesseille.

Luottamuksellisuus, eheys ja käytettävyys ovat määritelmiltään hyvin yksinkertaisia, mutta niiden vaikutussuhteet muihin asioihin ovat erittäin monimutkaisia. Tämän

[3] *Ronald L. Krutz and Russell Dean Vines: The CISSP Prep Guide, Second Edition, Wiley Publishing Inc., 2004*

[4] *http://en.wikipedia.org/wiki/Confidentiality*

kolmikon voidaan ajatella muodostavan viitekehyksen koko tietoturvallisuudelle. Seuraavassa kappaleessa käsitellään tietoturvallisuuden peruspalveluita.

2.2. Tietoturvan yleiset peruspalvelut

Jokaiselle järjestelmällä tulee määritellä tietoturvafunktiot, jotka ovat sellaisenaan konkreettisia tietoturvatarpeita. On kuitenkin mielekkäämpää määritellä tietoturvapalveluita yleisellä tasolla, koska eri järjestelmien ja organisaatioiden tarpeet ovat hyvin yksilöllisiä.

Yleisiä eli geneerisiä tietoturvapalveluita on neljä pääluokkaa ja kaksi johdettavissa olevaa luokkaa: Yleisten tietoturvapalveluiden pääluokat ovat: *luottamuksellisuus*, *eheys*, *autenttisuus* ja *kiistämättömyys*. Näistä pääluokista osittain johdettavat luokat ovat *pääsynvalvonta* ja *käytettävyys*[5]. Nämä palvelut ovat sovellettavissa useimpiin tietojärjestelmiin.

Luottamuksellisuus

Tietojärjestelmässä oleva tai saatavissa oleva tieto on vain niiden käyttöön tarkoitettujen tahojen saatavissa. Saatavuudella voidaan tarkoittaa muun muassa tietojen tulostamista, näyttämistä näytöllä tai esittämistä missä tahansa muussa muodossa.

Eheys

Tiedot ja järjestelmät ovat luotettavia ja niiden tilaa tai tietoja voi muuttaa vain muutoksiin oikeutetut tahot. Eheys edellyttää sitä, että tieto tai järjestelmä on sitä mitä sen on tarkoitus olla. Tämä pitää sisällään luonnollisesti sen, että muutoksia voi tehdä vain valtuutettu henkilö. Eheys pitää myös sisällään vaatimuksen, että ohjelmat ja järjestelmät eivät muuta tietoja esimerkiksi vikatilanteiden johdosta.

Autenttisuus

Autenttisuus liittyy vahvasti käyttäjän tai tahon tunnistamiseen. Autenttisuudella tarkoitetaan sitä, että osapuolet voivat yksiselitteisesti ja luottamuksellisesti tunnistaa

[5] *Esa Kerttula: Tietoverkkojen tietoturva, Liikenneministeriö, Oy Edita Ab, , ISBN:951-37-2904-4, 2000*

toisensa. Autenttisuus tietojen osalta tarkoittaa muun muassa tiedon alkuperän, päivämäärän ja sisällön oikeellisuutta.

Kiistämättömyys

Kiistämättömyydellä tarkoitetaan varmuutta tiedon tai transaktion tapahtuneille toimenpiteille. Kiistämättömyys liittyy läheisesti oikeudenkäyntikelpoisuuteen. Tässä asiayhteydessä tapahtumien tulee olla kiistämättömiä ja todisteiden tulee olla niin pitäviä, että voidaan todistaa kuka tai mikä on tehnyt ja mitä. Kiistämättömyyden periaate voi rikkoontua mm. huonon suojaamisen tai autentikoinnin johdosta.

Näistä neljästä peruspalvelusta voidaan johtaa vielä kaksi palvelua: *pääsynvalvonta* ja *käytettävyys*.

Pääsynvalvonta

Pääsynvalvonta palvelu tarjoaa pääsyn tietoihin, palveluihin ja järjestelmiin. Pääsynvalvontajärjestelmä liittyy läheisesti valtuuttamiseen ja autentikointiin.

Käytettävyys

Käytettävyydellä tarkoitetaan sitä, että järjestelmien tiedot ja resurssit ovat niitä tarvitsevien käytössä kun niitä tarvitaan.

Edellä esitellyistä tietoturvapalveluista on nähtävissä johdettavuus tietoturvan kulmakivistä *eheydestä, luottamuksellisuudesta ja käytettävyydestä*. Edellä esitetyt palvelut ovat vielä yleisellä tasolla ja näistä voidaan edelleen jatkojalostaa tarkempia palveluita tai kokonaisuuksia järjestelmäkohtaisesti. Kaikkien tietoturvafunktioiden tai palveluiden voidaan ajatella olevan johdettavissa tietoturvan kolmikosta ja myös näistä yleisistä tietoturvapalveluista.

2.3. Tietoturvallisen tietojärjestelmän suunnitteleminen

Tähän mennessä olemme käyneet läpi tietoturvan peruskäsitteet, yleiset peruspalvelut ja tietoturvan kulmakivet. On aiheellista esitellä muutama lähestymistapa tietoturvallisen tietojärjestelmän suunnittelemiselle. Tietoturvallisuus tulee ottaa huomioon jo

suunnitteluvaiheessa eikä vasta esimerkiksi riski-/uhkakartoituksessa ilmenneiden asioiden korjaamisena. Tietoturvan huomioon ottaminen tietojärjestelmien suunnittuvaiheessa vaikuttaa lähinnä teknisen tietoturvan alueeseen. Seuraavaksi kuvataan lyhyesti kaksi eri lähestymistapaa tietoturvallisen tietojärjestelmän suunnittelemiselle. Nämä kaksi eri lähestymistapaa ovat ISO 7498-2-standardin määrittelemä tietoturva-arkkitehtuuri ja IBM:n kehittelemä MASS (Method for Designing Secure Solutions).

Aiemmin on kuvattu tietoturvan yleiset peruspalvelut. Seuraavaksi tietoturvan palveluita viedään asteen verran konkreettisemmalle tasolle eli funktionaalisiin palveluihin. Molemmat arkkitehtuurimallit kuvaavat viisi funktionaalista palvelua.

MASS

MASS on kehitetty tutkimalla Common Criterian asettamia vaatimuksia ja nämä vaatimukset on sitten jaettu viiteen operationaaliseen luokkaan: a*uditointi* (engl. Audit), *pääsynvalvonta* (engl. Access Control), *vuonvalvonta* (engl. Flow Control), *valtuutus ja identiteetit* (engl. Identity and Credentials) ja *Ratkaisun eheys* (engl. Solution Integrity)[6]. Nämä luokat muodostavat MASSin toiminnalliset alajärjestelmät.

ISO 7498-2

ISO 7498-2-standardi kuvaa tietoturva-arkkitehtuurin ja määrittelee suunnittelun lähtökohdiksi viisi funktionaalista luokkaa. Nämä luokat ovat: *autentikointi*, *pääsynvalvonta*, *tiedon luottamuksellisuus*, *tiedon eheys* ja *kiistämättömyys*[5]. ISO 7498-2:n määrittelemä arkkitehtuurimalli perustuu OSI-referenssimallin 7-portaiseen ajatteluun. OSI-malli määrittelee abstraktin tietokone- ja tietoliikenneverkon protokollasuunnittelumallin[7]. Valitettavasti nykypäivän Internetissä ei ole selkeästi eroteltavissa kaikkia seitsemää porrasta.

Siirryttäessä abstrakteista määritelmistä yksityiskohtaisempiin ja funktionaalisempiin tietoturvapalveluihin on pantava merkille, että ylimmän ja abstrakteimman tason

[6] *J.J Whitmore, A Method for Designing Secure Solutions, IBM Systems Journal, Vol 40, No 3, 2001*

[7] *http://en.wikipedia.org/wiki/OSI_model*

tietoturvan määrittelemät kulmakivet ovat keskeisessä asemassa ja jatkojalostaminen pohjautuu niiden määrittelemiin tarpeisiin.

2.4. Tietoturvan osa-alueet

Tietoturvan voi jakaa monella tavalla eri osa-alueisiin. Seuraavaksi esitellään tietoturvallisuuden jakomalli, joka on laajassa käytössä valtionhallinnossa ja monissa organisaatioissa. Valtiovaraministeriön alainen Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI, http://www.vm.fi/tietoturvallisuus) julkaisee säännöllisesti tietoverkkojen turvallisuuteen tietoturvaan suosituksiaan tai hyviä käytäntöjä. VAHTI käyttää tietoturvajaotteluun mallia, joka jakautuu kahdeksaan osa-alueeseen. Nämä osa-alueet ovat: *Hallinnollinen tietoturvallisuus, Henkilöstöturvallisuus, Fyysinen turvallisuus, Tietoliikenneturvallisuus, Laitteistoturvallisuus, Ohjelmistoturvallisuus, Tietoaineistoturvallisuus* ja *Käyttöturvallisuus*[8]. Seuraavaksi kuvataan lyhyesti mitä osa-alueet pitävät sisällään.

2.4.1. Hallinnollinen tietoturvallisuus

Perustana hallinnolliselle tietoturvallisuudelle on organisaation laatima tietoturvallisuuspolitiikka. Tietoturvapolitiikassa tulisi olla määriteltynä keskeiset tietoturvallisuuden periaatteet ja toimintatavat[9].

Hallinnollisen tietoturvan alueella määritellään koko organisaation kanta tietoturvaan. Johdon sitoutuminen ja tietoisuus tietoturvallisuusriskeistä ohjaa organisaation tietoturvallisuustoimintaa. Hallinnolliseen tietoturvaan voidaan lukea kuuluvaksi johdon tietoisuus tietoturvauhkista, tietoturvallisuuden johtaminen organisaatiossa, tietoturvallisuuden hallintamenettelyt ja henkilöstön koulutus tietoturvallisuuteen ja riskitietoisuuteen.

---

[8] *Valtionvarainministeriö: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003/7, ISBN 951-804-408-2, Edita Prima Oy, 2003.*

[9] *Valtionhallinnon tietoturvallisuuden johtoryhmä, Valtion viranomaisen tietoturvallisuustyön yleisohje, Valtionvarainministeriö, 1/2001*

Keskeisenä osana hallinnollista tietoturvaa on myös oman organisaation ulkopuolisten sidosryhmien, asiakkaiden ja kumppanien suhteiden ja yhteistyön hallinta. Ulkoisiin tahoihin liittyviä vastuita hallinnollisen tietoturvan alueella on suhteiden hallinta, tietoturvaratkaisut, yhteistoiminnan tietoriskien tunnistaminen, verkosto ja alihankintasuhteiden käynnistys ja ylläpito ja ulkopuolisten kuten asiakkaiden tai kumppanien käynnit organisaatiossa.

Yleisohjeistus tietoturvallisuuden toimintaan koko organisaatiossa, sekä sisäisesti että ulkopuolisten tahojen kanssa, tulisi olla määritelty organisaation tietoturvapolitiikassa. Johdon tehtävä on noudattaa ja vaalia tietoturvapolitiikan noudattamista koko organisaatiossa.

Hallinnollista tietoturvallisuutta voidaan pitää yhtenä tärkeimmistä tietoturvan osa-alueista, koska organisaation tietoturvallisuus toiminta hyvin pitkälti muodostuu hallinnollisen tietoturvallisuuden kautta. Tietoturva koskee jokaista työntekijää ja kaikkea suojattavaa omaisuutta kuten tietoa. Ylemmän johdon vastuulla on tietoturvakulttuurin luominen, vaaliminen ja viestiminen myös alemmille organisaatiotasoille aina yksilöihin asti.

2.4.2. Henkilöstöturvallisuus

Henkilöstöturvallisuus käsittää henkilöstöön liittyviä asioita. Näitä ovat muuan muassa henkilöiden toimenkuvat, varahenkilöt, sijaisuudet, tiedonsaanti- ja käyttöoikeudet, turvallisuuskoulutus ja valvonta.

Hallinnollisina toimenpiteinä henkilöstöturvallisuuteen liittyvät työsopimukset, salassapitosopimukset, taustatarkistukset ynnä muut. Monet tietoturvallisuuden alan standardit kiinnittävät erityistä huomiota henkilöstöturvallisuuteen. Tietoturvastandardeja käsitellään myöhemmin tässä diplomityössä. Ihmiset on nimetty usein suurimmaksi tietoturvallisuusuhkaksi[10]. Suurin osa tietoturvatapahtumista on ihmisten itsensä aiheuttamia, tahallisesti tai tahattomasti. Yksinkertaisimmillaan ihminen

[10] *Rich Mogull, Building a Security-Aware Enterprise, 17 January 2002*

voi avata sähköpostin, jossa on virus ja täten virus voi tehdä tuhoja organisaation verkossa sekä omistajan koneella. Tämä voitaisiin yksinkertaisimmillaan estää lisäämällä työntekijöiden tietoisuutta tietoturva-asioista.

2.4.3. Fyysinen turvallisuus

Fyysinen turvallisuus käsittää organisaatioiden tuotanto- ja toimitilojen suojaamisen. Suojaaminen edellyttää kulunvalvontaa, palo-, vesi-, räjähdys-, ilmastointi, sähkö-, murtoturvallisuutta, vartiointia ja valvontaa. Fyysiseen turvallisuuteen mukaan luetaan myös tietojen kuljettamisjärjestelyjen turvallisuus.

Olennaista fyysisen turvallisuuden suunnittelussa on ottaa huomioon kaikki nämä asiat sekä aika ajoin varmistua että kontrollit toimivat. Teknisillä laitteilla on usein myös vaatimuksia toimintaympäristölleen ja se on otettava huomioon suunniteltaessa fyysistä turvallisuutta. Esimerkiksi palvelimien valmistajat ilmoittavat laitteilleen raja-arvot ilmankosteuden, lämpötilan ja sähkönsyötön osalta. Monet luonnonilmiöt voivat myös aiheuttaa haasteita kuten maanjäristykset. Esimerkiksi kovalevyt ovat alttiita tärähdyksille, ja voimakkaat sähkökentät voivat tuhota sähkömagneettisia medioita.

2.4.4. Tietoliikenneturvallisuus

Tietoliikenneturvallisuus pitää sisällään koko tietoliikennelaitteiston ja sen luetteloinnin, hallinnan, ylläpidon, ongelmatilanteet ja niiden kirjaamisen, käytön ja toiminnan valvonnan, liikenteen ja verkon salaamisen, verkon hallinnan ja tiedon varmistamisen. Esimerkkejä tietoliikenneturvallisuuden huomioitavista konkreettisista asioista ovat: reititykset, verkon hallinta ja valvonta, salauskäytännöt ja salaaminen, palomuurit, verkon ja tietojen varmistukset, varajärjestelyt ja ulkopuoliset yhteydet ja tarjoajat.

Yhtenä merkittävä tietoliikenneturvallisuuden vastuualueena on eri ratkaisujen ja ohjelmistojen arviointi ja hyväksyntä. Kuten aikaisemmin mainittiin tietoturva-termin kärjistyneestä käsityksestä. Kärjistynyt tietoturvakäsitys mieltää tietoturvan nimenomaan teknispainotteiseksi tai ainoastaan tietoliikenneturvallisuuden osa-alueen käsittäväksi.

2.4.5. Laitteistoturvallisuus

Laitteistoturvallisuus käsittää tietojenkäsittely- ja tietoliikennelaitteiden käytettävyyden varmistamisen. Käytettävyyden varmistaminen edellyttää toiminnan, kokoonpanon, kunnossapidon ja laadunvarmistuksen.

2.4.6. Ohjelmistoturvallisuus

Ohjelmistoturvallisuus käsittää ohjelmistot, sovellukset ja muut tietoliikenneohjelmistot ja käyttöjärjestelmät. Ohjelmistoturvallisuuden vastuualueeseen kuuluu ohjelmistojen tunnistamis-, pääsynvalvonta, varmistusmenettelyt, eristäminen, tarkkailu- ja paljastustoimet, lokitiedon kerääminen, ohjelmistojen turvallisuustoimet ja laadunvarmistus.

2.4.7. Tietoaineistoturvallisuus

Tietoaineistoturvallisuuden vastuualue käsittää asiakirjat, tiedostot ja muut tietoaineistot. Tietoaineistoturvallisuuden tehtävänä on varmistaa näiden käytettävyys, luottamuksellisuus ja eheys. Tietoaineistoturvallisuuden vastuulla on tietojen/tietoaineistojen luokittelu ja luettelointi. Tämä pitää sisällään tietovälineiden ja –aineistojen asianmukaisen hallinnan, säilytyksen, käsittelyn ja hävittämisen.

Tietoaineistoturvallisuuden keskeisenä roolina on tunnistaa suojattavat tiedot ja määritellä niille tarpeellinen suojaustaso. Tiedon luokittelu on yksi keino tämän aikaansaamiseksi. Hierarkkinen tiedon luokittelumalli asettaa eri luokitustason tiedoilla omat norminsa käsittelyn, säilytyksen ja käytöstä poistamisen osalta.

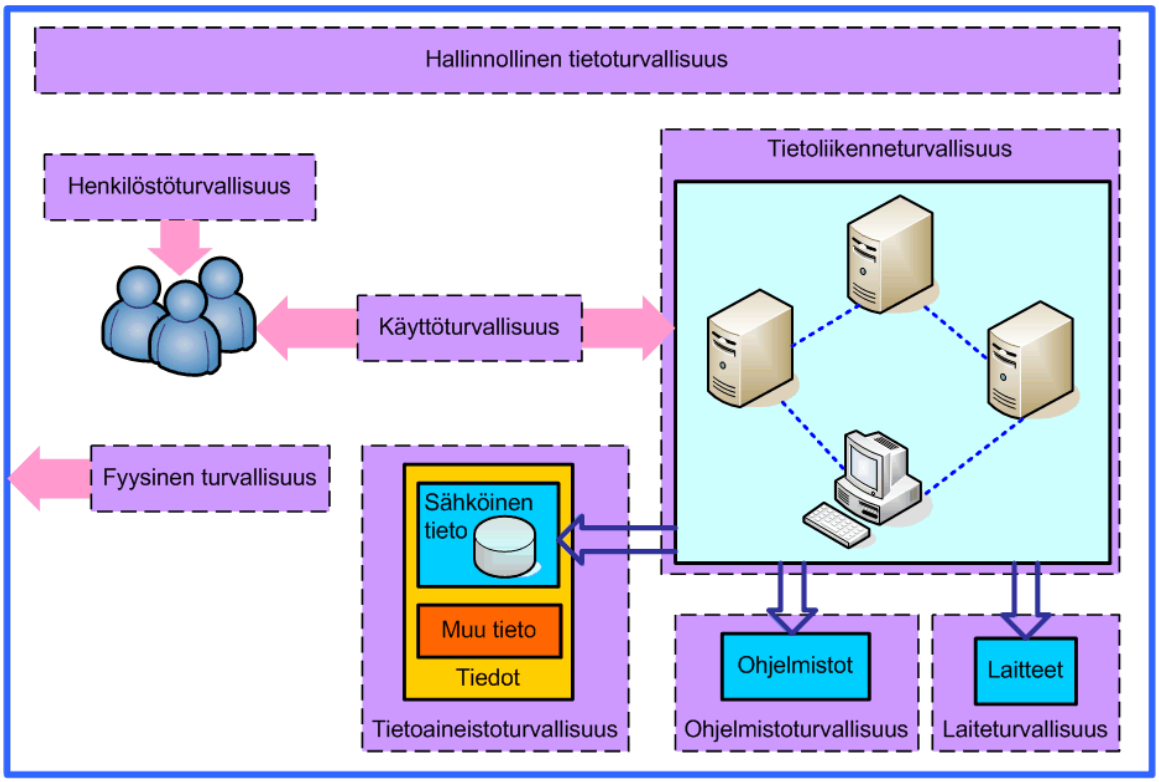
2.4.8. Käyttöturvallisuus

Käyttöturvallisuus on vastuussa tietotekniikan, tietojenkäsittelyn ja käyttöympäristön jatkuvuudesta. Käyttöturvallisuus pitää myös sisällään edellisten tuki-, huolto ja kehittämistoimien turvallisuuden. Käyttöturvallisuuteen liittyvät muuan muassa varmuuskopioinnit ja niiden säilytys, laitteiden huollot ja yleiset käyttöoikeudet.

Käyttöturvallisuuden osa-alueelle kuuluu keskeisenä kokonaisuutena etätyöympäristöjen turvallisuus. Käyttöturvallisuus varmistaa yksinkertaisuudessaan sen, että laitteita ja palveluita on turvallista käyttää.

2.4.9. Tietoturvan osa-alueiden yhteenveto

Esitelty tietoturvajako on vain yksi lukuisista. Valtionhallinnossa käytettävä malli valittiin, koska se tuo hyvin esiin tietoturvan kokonaisuuden monimuotoisuuden. Alla olevassa kuvassa on hahmoteltu tietoturvajaottelu graafisesti sekä eri komponenttien vaikutussuhteet(Kuva 2).



Kuva 2: Tietoturvan osa-alueet ja niiden vaikutussuhteet kokonaisuuteen.

Yllä olevassa kuvassa *Hallinnollinen tietoturvallisuus* on sijoitettu ylös kuvaamaan sitä, että se on koko organisaation tietoturvallisuuden ohjaava tekijä. *Henkilöstöturvallisuus* osoittaa henkilöihin, joihin se vahvasti liittyy. *Käyttöturvallisuus* on yhdistetty sekä henkilöihin että järjestelmään. Henkilöt ovat kuitenkin keskeisessä roolissa käyttöturvallisuuden alueella, he voivat tehdä virheitä ja aiheuttaa joko tahallista tai tahatonta vahinkoa. *Tietoliikenneturvallisuus* on sijoitettu tietoverkkojärjestelmän

ympärille. Kuvan siniset nuolet, jotka on suunnattu tietoverkkojärjestelmästä *sähköiseen tietoon*, *ohjelmistoihin* ja *laitteisiin.* kuvaavat että nämä komponentit ovat osa tietoverkkojärjestelmää. *Ohjelmistoturvallisuus* pitää sisällään tietoverkkojärjestelmän ohjelmistokomponentit. *Laiteturvallisuus* pitää puolestaan sisällä laitteiston. Laitteistoon voi kuulua myös muita kuin tietoverkon laitteita. *Tietoaineistoturvallisuus* käsittää kuvassa sekä tietojärjestelmien sähköisen tiedon että muut tiedot kuten arkistoidut paperit tai dokumentit. *Fyysinen turvallisuus* viittaa kuvassa kehykseen, joka on piirretty kuvan ympärille. Tällä viitteellä pyritään kuvaamaan, että kehys ympärillä on koko organisaation fyysinen turvakehä. Fyysinen turvallisuus koskee koko organisaation työ- ja tuotantotiloja.

Edellä esitettyä tietoturvan jaottelumallia voidaan pitää raskaana. Malli kuitenkin havainnollistaa hyvin kuinka laaja kokonaisuus tietoturvallisuus on. Malli sisältää kaikki tietoturvaan liittyvät oleelliset alueet, vaikkakin osa alueista voi olla osittain päällekkäisiä. Tulemme huomaamaan myöhemmin työssä, että tietoturvastandardit käsittelevät hyvin pitkälti samoja osa-alueita kuin edellä esitelty tietoturvan jakomallikin. Tietoturvaosa-alueiden tunteminen ja tiedostaminen on kriittistä kattavan riskianalyysin tekemiseksi.

3. Tietoturva organisaatiossa

Usein tietoturvallisuus mielletään erilliseksi osa-alueeksi ja asiaksi, josta vastaavat erikseen nimetyt henkilöt. Organisaatioiden tietojärjestelmät ovat niin monimutkaisia, ettei yksittäinen henkilö voi tuntea koko järjestelmää. Tämän seikan takia tietoturva ei voi olla yksittäisen henkilön vastuulla vaan tietoturvavastuullinen ajattelutapa on iskostettava jokaiseen työntekijään tai järjestelmän käyttäjään. Tietoturvan tulisikin olla mukana kaikessa tekemisessä, jota tapahtuu organisaatiossa.

Tietoturvallisuutta voidaan pitää näkökulmana asioihin tai miltei ajattelutapana. Tämän ajattelutavan iskostaminen organisaation jokaisen yksilön toimintaan on tavoitetila. Tietoturvaorganisaatio on koko organisaation tietoturvallisuuden organisaattori ja motivaattori. Keskeisenä osana tietoturvallisuutta on tietoturvakulttuuri. Vallitsevan tietoturvakulttuurin tulisi olla sellainen, että tietoturva mielletään tärkeäksi asiaksi ja se osataan ottaa huomioon organisaation toiminnan ja tavoitteiden näkökulmasta riittävällä ja tarkoituksenmukaisella tavalla.

Tietoturvakulttuuria ei voi kuitenkaan luoda ainoastaan julkaisemalla tietoturvaohjeistuksia ja pitämällä tietoturvakoulusta. Tietoturvallisuustoiminta ja sen tavoitteet tulisi saada sidottua yrityksen liiketoiminnallisiin tavoitteisiin. Hyvän tietoturvakulttuurin puolesta puhuu fakta, että suurin osa tietoturvatapahtumista tai tietovuodoista johtuu nimenomaan ihmisistä[10]. On selvää, että tällaisilla tapahtumilla voi

olla joko taloudellisia seurauksia tai välillisesti esimerkiksi maineellisia haittavaikutuksia. Seuraavassa kappaleessa käsitellään tietoturvaorganisaatiota, sen tehtäviä ja rooleja.

3.1. Tietoturvaorganisaatio

Tietoturvaorganisaatio on jokaisessa organisaatiossa erilainen. Pienemmissä organisaatioissa ei ole välttämättä resursseja erilliselle tietoturvaorganisaatiolle. Tällaisissa organisaatioissa tietoturva on usein tietoteknisessä mielessä järjestelmäylläpitäjän vastuulla. Viimekädessä johto on kuitenkin vastuussa tietoturvallisuudesta.
Järjestelmäylläpitäjän tietoturvavastuuta ja tietoturvatoimintaa kontrolloidaan kuitenkin ylemmän johdon tai esimiehen toimesta. Vastuunjako tämänlaisessa tilanteessa toimii siten, että järjestelmävastaavan vastuulla on toteuttaa tietoturvatoimet, joista on sovittu. Yleensä ylläpitäjän vastuulla olevat tietoturvatoimintaan liittyvät aktiviteetit ovat palomuurien hallinta, VPN:n hallinta, virustorjunnan hallinta, ympäristöjen käyttöoikeudet, tietoturvapäivitysten tekeminen ympäristöihin, varmuuskopioinnit ja mahdollisesti sähköpostin suodattaminen (engl. filtering). Mikäli organisaatio päättää standardoida tietoturvaratkaisuitaan, tulee ainakin tämän yhteydessä suorittaa riskianalyysi, joka selvittää systemaattisesti riskikohteet, riskien todennäköisyyden, riskien vakavuuden ja niistä aiheutuvat seurannaisvaikutukset[11]. Riskianalyysiä käsitellään tarkemmin myöhemmin työssä.

Järjestelmäylläpitäjä on vastuussa tietoturvakontrollien toteuttamisesta ja ylläpitämisestä. Useissa tilanteissa järjestelmäylläpitäjä on myös suunnitteleva henkilö, ja ylempi johto ainoastaan hyväksyy hankintaehdotukset.

Pienemmässä organisaatiossa riskienhallinta keskittyy usein liiketoimintariskeihin, joita ylempi johto analysoi. Pienillä organisaatioilla ei ole resursseja ylläpitää erillistä tietoturvaorganisaatiota.

[11] *Arto Suominen, Riskienhallinta, WSOY, Helsinki, 2003*

3.1.1. Tehtävät ja roolit

Aikaisemmin turvahenkilöt olivat saaneet kokemuksensa tyypillisesti puolustusvoimien, valtion tai julkishallinnon puolelta. Nämä henkilöt osasivat suojella hyvin kaikkea aineellista omaisuutta, oli se sitten ihmisiä tai asioita. Nämä henkilöt olivat alallaan erittäin päteviä ja heillä oli käytössään pitkäaikaisen kehittelyn läpikäyneitä työkaluja, metodeja ja tekniikoita. Tilanne on kuitenkin muuttunut tietotekniikan myötä. Nykyajan tietoturvahenkilöiltä vaaditaan yleensä perinteistä osaamista ja myös ymmärrystä tietojärjestelmistä ja tietotekniikasta. Näitä hybridihenkilöitä ovat *tietojärjestelmien tietoturvapäälliköt*(engl. Information Systems Security Officer, ISSO)[12]. Englanninkielisessä kirjallisuudessa tällaisesta henkilöstä käytetään lyhennettä ISSO. Seuraavissa kappaleissa käsitellään tietoturvaorganisaatioon ja sen toimintaan liittyviä standardeja. Standardit ovat ohjeistuksia tietoturvatoimille ja tietoturvaorganisaation muodostukselle ja toiminnalle. Standardeissa ei määritellä tai nimitetä selviä rooleja, joita tietoturvaorganisaatiossa on. Kuten aiemmin mainittu, on tietoturvaorganisaatio kaikissa organisaatioissa erilainen. Seuraavaksi esitellään eräs yksittäisestä roolista lähtevä tietoturvaorganisaation muodostamisen viitekehys. Tämä rooli on edellä mainittu *tietojärjestelmien tietoturvapäällikkö*, ISSO.

Tietojärjestelmien tietoturvapäällikön tehtävät ja vastuut

Tietojärjestelmien tietoturvapäällikön tehtävät voidaan karkeasti jakaa kolmeen osa-alueeseen: *ihmisten johtaminen* (engl. managing people), *organisaation tietovarojen suojaamisohjelman liiketoiminnan johtaminen* (engl. managing the business of CIAPP) ja *organisaation tietovarojen suojaamisohjelman prosessien johtaminen* (engl. managing CIAPP processes). Organisaation tietovarojen suojaamisohjelmaa kutsutaan englanninkielisessä kirjallisuudessa lyhenteellä CIAPP (engl. Corporate Information Asset Protection Program). Seuraavaksi esitellään kunkin osa-alueen tehtäviä.

[12] *Gerald L. Kovacich, The Information Systems Security Officer's Guide – Establishing and Managing an Information Protection Program, Second Edition, ISBN 0750676566, Butterworth Heinemann, 2003*

Ihmisten johtaminen

Ihmisten johtamisen osa-alue käsittää ammatillisen maineen rakentamisen, hyvien liiketoimintasuhteiden ylläpitämisen ja muutostenhallinnan. Vastuualueelle kuuluu myös hyvän työilmapiirin ylläpitäminen, ihmisten kehittäminen ja positiivisen ryhmätyöympäristön/-ilmapiirin luominen. Ihmisten kehityksen painopiste on työsuorituspohjaisuudessa a tavoitelähtöisyydessä.

Organisaation tietovarojen suojaamistoiminnan liiketoiminnan johtaminen

Tämän osa-alueen vastuualueet sisältävät asiakas-/toimintalähtöisyyttä kaikessa toiminnassa, vastuunottamista päätöksenteossa, tulosorientoituneisuutta ja strategista ajattelutapaa. Osa-alueen vastuulle kuuluu myös resurssien suunnittelemista ja johtamista. Tehtävässä vaaditaan ennen kaikkea ongelmanratkaisukykyä, henkilökohtaisen vastuun ja omistajuuden hyväksymistä ja hyvin perustellun liiketoimintapäätöksenteon käyttämistä.

Organisaation tietovarojen suojaamistoiminnan prosessien johtaminen

Tämän tehtäväosa-alueen vastuisiin luetaan projektien suunnitteleminen ja toteuttaminen, laadun varmistaminen ja järjestelmien toimintatarkoituksien varmistaminen ja säilyttäminen. Tehtäväosa-alue myös edellyttää jatkuvaa työtaidon, osaamisen ja tietotaidon ylläpitämistä.

Kuten yllä olevista tehtäväalueista voidaan päätellä, on tietojärjestelmien tietoturvapäällikön toimenkuva määritelmän mukaan hyvin laaja. Sopivalta henkilöltä edellytetään ymmärrystä liiketoiminnasta, ymmärrystä tietojärjestelmien ja tietotekniikan tietoturvasta ja kykyä johtaa ja kehittää ihmisiä.

Edellä kuvattu tietojärjestelmien tietoturvapäällikkö on vastuussa koko organisaation tietoturvallisuustoiminnan koordinoimisesta ja tietoturvaorganisaation muodostamisesta, ylläpitämisestä ja kehittämisestä. Luonnollisesti tietoturvapäällikkö tarvitsee johdon tukea ja resursseja pystyäkseen toimimaan tehtävässään.

3.1.2. Standardit

Seuraavaksi käsitellään kaksi tietoturvastandardia, joiden pääpaino on tietoturvan organisoimisessa ja tietoturvaorganisaation toiminnassa. Organisaation asennoituminen ja toimivan tietoturvaorganisaation toimivuus on oleellinen osa toimivaa ja ennaltaehkäisevää riskienhallintaa. Standardien tarkoitus on ohjata tietoturvatyöskentelyä hallitumpaan suuntaan ja ohjeistaa tietoturvatoimintaa. Hallitulla lähestymistavalla pystytään mahdollisesti iskostamaan tietoturvakulttuuria ja ajattelua organisaatioon sekä ennaltaehkäisemään riskien muodostumista. Järjestelmällinen tietoturvan hallinta ei välttämättä pienennä tai ehkäise riskejä, mutta toiminta keskittyy kuitenkin kriittisesti tarkastelemaan tietoturvaa ja täten tarjoaa usein tiedon olemassa olevista riskeistä. Pahimpia riskejä ovat juuri tiedostamattomat riskit.

ISO 27001

ISO 27001 – standardilla on hyvin kattava lähestymistapa tietoturvaan. Standardin puitteissa tieto-käsite sisältää tiedon kaikki muodot kuten dokumentit, kommunikoinnin, keskustelut, viestit, nauhoitukset ja valokuvat. Tieto-käsite pitää sisällään kaiken digitaalisen tiedon, sähköpostit, faksit ja puhelinkeskustelut[13].

ISO 27001 on kehitetty sertifiointitarkoituksiin. Standardin avulla voidaan sertifioida tietty osa organisaation tietoturvatoiminnasta. Tämän standardin tapauksessa sertifioitava osa-alue on standardin määrittelemä tietoturvan hallintomalli (engl. Information Security Management System). Kokonaisuudessaan standardissa määritellään vaatimuksia tietoturvan hallinnoimiselle. Standardi koostuu kontrollikohdista kuten ISO 27001:een läheisesti liittyvä ISO 17799 standardikin.

ISO 27001:2005-standardi (Information Technology – Security Techniques – Information security management systems – Requirements) määrittelee tietoturvan hallintamallin. Standardissa keskitytään käsittelemään ISMS:iä (engl. Information Security Management System), josta käytetään tämän työn puitteissa vapaa suomennosta

[13] *ISO/IEC 27001:2005 Information Security Standard Translated into Plain English, Praxion Research Group Limited, 2006, http://praxiom.com/iso-27001.htm*

tietoturvan hallintamalli. Vaihtoehtoinen suomennos voisi olla *tietoturvallisuuden hallintamalli.*

Standardi tarjoaa mallin tietoturvan hallintamallin muodostamiselle, käyttöönottamiselle, operoimiselle, valvomiselle, katselmoimiselle/tarkastamiselle, ylläpitämiselle ja kehittämiselle[14]. ISO 27001- ja ISO 17799-standardi muodostavat kokonaisuuden, jossa ISO 27001 käsittelee tietoturvan hallintamallia, joka pohjautuu ISO 17799-standardin implementointiohjeistukseen. ISO 17799 -standardia käsitellään tarkemmin tietoturvastandardit osiossa.

ISO 27001-standardi suosittelee prosessimaista lähestymistapaa tietoturvan hallintamallin yhteydessä käytettäväksi. Kaikkien tietoturvahallintamallin prosessien yhteydessä suositellaan käytettävän PDCA-prosessimallia (engl. Plan-Do-Check-Act). PDCA-malli sisältää 4 vaihetta, jotka ovat suomennettuja: *suunnittelu, toteutus, tarkistaminen* ja *toimiminen*. Esimerkkinä prosessin läpiviemisestä: suunnitellaan tietoturvan hallintomalli, toteutetaan ja operoidaan tietoturvan hallintamallia, tarkistetaan tietoturvan hallintamallin politiikat, kontrollit, prosessit ja proseduurit, toimimisessa ylläpidetään ja kehitetään tietoturvan hallintamallia paremmin vastaamaan tietoturvallisuuden tarpeita.

Tiivistetysti standardi muodostuu seuraavista suuremmista kokonaisuuksista: *tietoturvan hallintomallin muodostaminen, tietoturvan hallintomallin hallinnointi, tietoturvan hallintamallin auditointi, tietoturvan hallintamallin katselmointi* ja *tietoturvan hallintamallin kehittäminen*[13]. Alla on kuvattu kunkin osa-alueen toimintoja.

Tietoturvan hallintamallin muodostaminen

Tämä osio kuvaa hallintamallin vaatimuksia, suunnittelua, määrittelyä, toteuttamista ja operoimista, tarkkailua ja katselmointia, dokumentointia ja dokumenttien kehitystä ja hallintaa. Lyhyesti tämä osio kuvaa tietoturvan hallintamallin keskeiset vaatimukset ja elinkaaren mukaan lukien toiminnot eri vaiheissa.

---

[14] *ISO/IEC FDIS 27001:2005(E), Information technology – Security techniques – Information security management systems - Requirements*

Tietoturvan hallintamallin hallinnointi

Tämä osio sisältää toimintoja ja vaatimuksia, joita vaaditaan organisaation johdolta. Vaatimukset ovat esivaatimuksia hallintamallin operoinnille pitäen sisällään muun muassa johdon sitoutuneisuutta, resurssien saatavuutta ja pätevien ihmisten saatavuuden varmistamista.

Tietoturvan hallintamallin auditointi

Tässä osiossa standardia, kuvataan auditointiproseduurien muodostaminen, suunnittelu ja tekeminen.

Tietoturvan hallintamallin katselmointi

Katselmointi-osiossa kuvataan kuinka katselmointi suoritetaan. Osio pitää sisällään kuvauksen tehtävistä ja asioista, joita katselmoinnissa tulisi ottaa huomioon. Katselmointi osio jakaantuu karkeasti kolmeen osaan: *katselmoinnin tekeminen johdon toimesta*, *katselmoinnin syötteet* ja *katselmoinnin tuotokset*. Katselmoinnissa arvioidaan tietoturvan hallintamallin sopivuutta, tehokkuutta ja mahdollista kehittymistarvetta. Syötteenä katselmoinnissa toimii muun muassa edelliset katselmointitulokset, sekä auditoinnissa esiintyneet tulokset. Pääasiallisesti syötteenä käytetään edellisiä mittaustuloksia ja aiempia korjaustoimenpiteitä. Tuotoksena syntyvät katselmoinnin päätökset ja toimenpiteet. Toimenpiteet voivat liittyä kehitykseen, ajanmukaistamiseen, resurssien allokointiin tai puuttumalla asioihin, jotka voivat vaikuttaa hallinnointijärjestelmän toimivuuteen.

Tietoturvan hallintamallin kehittäminen

Kehittämisosiossa kuvataan toimia, joita tulee ottaa huomioon hallintamallin kehittämisessä. Toimia on peruslaadultaan kahdenlaisia: korjaavia ja ennaltaehkäiseviä. Luonnollisesti ongelmien havaitseminen ennalta on kustannustehokkaampaa kuin korjaavat toimenpiteet kun asiat ovat jo tapahtuneet.

SSE-CMM

Kypsyysmalleja on useita ja ne keskittyvät tarkastelemaan eri osa-alueita. Kaikkien kypsyysmallien tarkoitus on määritellä ja mitata jonkin organisaation toiminnan kannalta kriittisen osa-alueen kykyä suoriutua sille määritellyistä tehtävistään. Yhteistä kypsyysmalleille on se, että ne kaikki määrittelevät eri kypsyystasoja.

Parhaiten tunnettu kypsyysmalli on ohjelmistokehityksen kypsyysmalli SW-CMM (engl. Software Engineering - Capability Maturity Model). Muita kypsyysmalleja on tehty muuan muassa järjestelmätoimintaan (SE-CMM, Systems Engineering – CMM) ja integroituun tuotteen ja prosessien kehitykseen (IPPD-CMM, engl. Integrated Product and Process Development)[15].

Tämän kappaleen puitteissa käsitellään SSE-CMM:ää (engl. Systems Security Engineering Capability Maturity Model), *tietoturvaprosessien kypsyysmallia*. SSE-CMM:stä on tehty standardi, ISO 21827. Kypsyystasoja on viisi, ja ne on numeroitu yhdestä viiteen. Viides taso on paras mahdollinen. Jokaiselle tasolle on määritelty tietty kypsyys, jolla organisaation prosessien tulee olla.

SSE-CMM mittaa ja määrittelee organisaation kykyä toteuttaa tietoturvan hallintajärjestelmän prosesseja. SSE-CMM on prosessilähtöinen tietoturvallisten järjestelmien kehitysmetodi, jota voidaan käyttää tietoturvatoiminnan kehittämiseen. Malli tarjoaa arviointiviitekehyksen tietoturvatoiminnalle. Kypsyystasot ja prosessien mittaaminen mallin mukaan tarjoaa todisteita organisaation tietoturvaprosessien kypsyydestä. Tästä voi olla apua muuan muassa sopimusneuvotteluiden tai yhteistyöprojektien muodostuksen yhteydessä[16].

SSE-CMM prosessialueet

SSE-CMM on jaettu prosesseihin ja kypsyystasoihin. Prosessit määrittelevät miten tietoturvatoimintoja tulisi kehittää ja parantaa. Kypsyystasot puolestaan mittaavat

[15] *http://www.sei.cmu.edu/cmmi/models/models.html*

[16] *Matt Bishop, Introduction to Computer Security, ISBN 0-321-24744-2, Prentice Hall PTR, 2004*

tietoturvaprosessien tehokkuutta. SSE-CMM määrittelee 11 tietoturvan perusprosessialuetta (engl. Security Base Practices)[17].

- PA01 Tietoturvakontrollien hallinta (engl. Administer Security Controls)
- PA02 Vaikuttavuuden arviointi (engl. Assess Impact)
- PA03 Tietoturvariskien arviointi (engl. Assess Security Risks)
- PA04 Uhkien arviointi (engl. Assess Threat)
- PA05 Haavoittuvuuksien arviointi (engl. Assess Vulnerabilities)
- PA06 Varmuus-/takausargumenttien rakentaminen (engl. Build Assurance Arguments)
- PA07 Tietoturvan koordinointi (engl. Coordinate Security)
- PA08 Tietoturvatoiminnan tarkkailu (engl. Monitor Security Posture)
- PA09 Tietoturvatiedon jakaminen (engl. Provide Security Input)
- PA10 Tietoturvatarpeiden määritys (engl. Specify Security Needs)
- PA11 Tietoturvan tarkistaminen ja validointi (engl. Verify and Validate Security)

Prosessialueiden lyhenne PA tarkoittaa prosessialuetta (engl. Process Area). SSE-CMM määrittelee vielä yli 60 perusprosessia näihin 11 prosessialueeseen. Edellä esitetyt prosessialueet ovat nimenomaan tietoturva-alueen perusprosesseja. Tämän lisäksi SSE-CMM määrittelee vielä 10 perusprosessialuetta organisaatio- ja projektitoiminnalle.

SSE-CMM kypsyystasot

SSE-CMM määrittelee viisi kypsyystasoa, jotka ovat: *epämuodollinen suoritustapa* (engl. Performed Informally), *suunniteltu ja seurattu* (engl. Planned and Tracked), *hyvin määritelty* (engl. Well Defined), *kvantitatiivisesti hallittu* (engl. Quantitatively Controlled), ja *jatkuvasti kehittyvä* (engl. Continuously Improving). SSE-CMM:n määrittelemät kypsyystasot on esitetty alla.

[17] *Systems Security Engineering Capability Maturity Model SSE-CMM, Model Description Document, version 3, 2003*

Taso 1: Epämuodollinen suoritustapa

Perustoimet prosesseista suoritetaan yleisesti ottaen hyvin. Perustoimien suoritusta ei jyrkkäotteisesti ole suunniteltu tai seurattu. Suoritus on riippuvainen yksilön tietotaidosta ja työstä. Organisaation yksilöt tunnistavat aktiviteetit, joita tulisi tehdä, ja on olemassa sitoutuneisuus tehdä näitä aktiviteetteja, kun se on ajankohtaista tai sitä vaaditaan. Prosesseita syntyy tunnistettavia työtuotoksia.

Taso 2: Suunniteltu ja seurattu

Prosessialueiden perustoimintoja ja niiden suoritusta suunnitellaan ja seurataan. Suoritusta verifioidaan määriteltyjen proseduurien mukaisesti. Työtuotokset vastaavat määriteltyjä standardeja ja vaatimuksia. Pääasiallinen ero ensimmäiseen tasoon on se, että prosessien suoritus on suunniteltua ja hallittua.

Taso 3: Hyvin määritelty

Prosessien perustoiminnot suoritetaan hyvin määriteltyjen prosessien mukaan hyväksikäyttäen hyväksyttyä ja räätälöityä versiota standardista. Prosessit ovat hyvin dokumentoituja. Suurin ero toiseen tasoon on se, että prosessien suunnittelu ja hallinta tehdään organisaation laajuisen standardointiprosessin mukaisesti.

Taso 4: Kvantitatiivisesti hallittu

Prosessialueiden suorituksesta kerätään yksityiskohtaisia mittoja ja niitä analysoidaan. Tämä mahdollistaa kvantitatiivisen ymmärryksen prosessin kypsyydestä ja luo paremmat edellytykset prosessien suorituksien ennalta-arviointiin. Prosessin suoritusta hallitaan objektiivisesti ja työtuotokset ovat kvantitatiivisesti tunnettuja. Pääasiallinen ero kolmanteen tasoon on se, että prosessien hallinta ja ymmärrys on kvantitatiivista.

Taso 5: Jatkuvasti kehittyvä

Kvantitatiivisen prosessisuorituksen tavoitetasot tuottavuuden ja tehokkuuden puolesta johdetaan organisaation liiketoimintatavoitteista. Kvantitatiivinen seuranta mahdollistaa jatkuvan prosessikehityksen liiketoimintatavoitteita vasten. Tämä mahdollistaa uusien ideoiden ja innovatiivisten pilotointitekniikoiden koestamisen. Suurin ero neljänteen tasoon on se, että tässä tasossa prosesseja jalostetaan ja parannetaan jatkuvasti.

3.2. Arviointimenetelmät

Tietoturvaorganisaatio on vastuussa tietoturvallisuudesta, ja uhkiin ja riskeihin varautuminen vaatii ajanmukaista tietoisuutta asioista. Määräajoin suoritettavat erilaiset arvioinnit antavat kuvan nykytilanteesta ja mahdollistavat tietoturvan kehittämisen turvallisempaan suuntaan. Erilaiset tahot määrittelevät hieman eri tavalla tietoturvallisuuteen liittyvät tarkastukset tai arvioinnit. Tämän työn puitteissa esitettävä arviointimenetelmien jaottelumalli on yleisesti kirjallisuudessa esitetty malli. Seuraavissa kappaleissa läpikäytävät tietoturvallisuuden arvioinnit ovat: Sisäinen auditointi (engl. Internal Audit), Ulkoinen auditointi (engl. External Audit), Itsearviointi (engl. Self-Assessment), Haavoittuvuusarviointi (engl. Vulnerability Assessment), Tunkeutumisarviointi (engl. Penetration Assessment) ja Riskiarviointi (engl. Risk Assessment)[18]. Auditointi on sanana anglistinen ilmaisu ja sen oikeampi suomennos on tarkastus, usein kuitenkin tietoturvallisuusalallakin käytetään termiä auditointi. Alla on tiivistelmä arviointimenetelmistä, niiden käytöstä ja tuotoksista(Taulukko 1).

[18] *Eric Maiwald & William Sieglein: Security Planning & Disaster Recovery, McGraw-Hill/Osborne, ISBN 0-07-222463-0, 2002*

Taulukko 1: Tietoturvallisuuden arviointimenetelmät

Arviointityyppi	Käyttö	Tuotokset
Sisäinen auditointi	Organisaation sisäinen auditointiosasto tekee sisäisiä auditointeja ajoittain ja auditoinnin kohteena oleva taho ei voi yleensä päättää milloin auditointi tapahtuu. Tarkastuksen tulokset esitellään yleensä järjestelmän omistajille ja asiaan liittyville johtajille.	Sisäisessä auditoinnissa voi paljastua puutteita ja kohtia, jotka eivät täytä organisaation/auditointiosaston vaatimuksia. Näihin epäkohtiin tulee reagoida ja kertoa mitä kullekin löydökselle tullaan tekemään.
Ulkoinen auditointi	Ulkoisen auditoinnin suorittaa organisaation ulkopuolinen taho. Yleinen ulkopuolinen auditoija on kirjanpito-/tilitoimisto. Ulkopuolinen auditointi voidaan ostaa myös muilta tahoilta. Ulkoisen auditoinnit tulokset esitellään yleensä ylemmällä johdolle tai johtokunnalle	Ulkoisessa tarkistuksessa esiintyneisiin epäkohtiin tulee reagoida ja kertoa miten esiintyneet epäkohdat tullaan korjaamaan.
Itsearviointi	Itsearviointi on arviointi, jonka tekevät järjestelmän omistajat tai muuten järjestelmän kanssa tekemisissä olevat tahot. Itsearviointia tulisi suorittaa aina, jos järjestelmässä/organisaatiossa tapahtuu isoja muutoksia. Itsearvioinnin tekeminen on myös suotavaa erilaisten tapaturmien jälkeen sekä ennen kuin oletetaan että järjestelmää tullaan auditoimaan joko sisäisesti tai ulkoisesti	Tarjoaa paremman käsityksen vallitsevasta tietoturvatilasta. Itsearvioinnin vaarana on arvioinnin puolueellisuus/jääviys, koska sen suorittavat järjestelmän hyvin tuntevat tahot.
Haavoittuvuusarviointi	Haavoittuvuusanalyysiä/-arviointia tulisi tehdä kohtalaisen usein. Suositeltava määrä on 4 kertaa vuodessa tai muutoksien jälkeen.	Tarjoaa yksityiskohtaisen listan järjestelmän haavoittuvuuksista eri teknologioissa, ratkaisuissa ja ohjelmistoissa.
Tunkeutumisarviointi	Tunkeutumisarviointi tulisi tehdä erityisesti kriittisille järjestelmille, varsinkin niille jotka sijaitsevat avoimessa verkossa kuten Internetissä.	Tunkeutumisarviointi todistaa, että järjestelmän haavoittuvuudet ovat hyväksikäytettäviä (engl. exploitable).
Riskiarviointi	Riskiarviointi tulisi suorittaa säännöllisesti. Riskianalyysi tarjoaa hyvän kuvan tietoturvan nykytilanteesta.	Tarjoaa tarkan raportin tietoturva-alueista, joissa on heikkouksia. Riskiarviointi yleensä keskittyy enemmän suurempaan kokonaisuuteen kuin teknisiin yksityiskohtiin.

3.2.1. Sisäinen tarkastus

Sisäisiä tarkastusosastoja on yleensä vain suurissa organisaatioissa tai finanssialan organisaatiossa, jotka ovat julkisen valvonnan alaisia. Sisäinen tarkastus ja tarkkailu ovat yleisiä organisaation sisäisen valvonnan menetelmiä[19]. Kaikki rahaan liittyvät transaktiot ja käsittelyt ovat erityisen tarkkojen kontrollien alaisia. Osa määräyksistä, velvoitteista ja tarkastuksista tulee lain ja valtion puolesta. Varsinkin rahaliikenteen transaktioille on tiukat säädökset ja niiden oikeellisuudesta on varmistuttava. Tämän takia finanssialan yrityksillä on oma sisäinen tarkastusosasto.

Sisäisellä tarkastusosastolla on yleensä ainakin yksi tietojärjestelmätarkastaja, jolla on asianmukainen koulutus, ymmärrys ja sertifiointi informaatioteknologia-alan tietoturvakontrolleista. IT-auditoijan pääasiallinen rooli on varmistaa, että IT-infrastruktuuri on yhdenmukainen ja hyväksyttävä kaikkien yksityiskohtaisten säännösten ja rajoitusten kanssa, joihin organisaatio on sitoutunut tai sitä on velvoitettu sitoutumaan.

Sisäinen tarkastusosasto suunnittelee mitä järjestelmiä he aikovat tarkastaa vuoden aikana. Kun tarkastus suoritetaan, aloitetaan yleensä haastattelemalla järjestelmän omistajaa, kehittäjää ja muita ihmisiä, jotka ymmärtävät järjestelmän toimintaa. Tarkastajat pyrkivät arvioimaan kuinka arkaluontoista tietoa järjestelmä käsittelee, kuinka tärkeää on järjestelmän toimivuus liiketoimintaoperaatioille ja minkä tyyppisiä tietoturvakontrolleja järjestelmässä on käytössä. Viimeisenä vaiheena sisäiset tarkastajat tarkastavat tietoturvakontrollit ja varmistavat että ne ovat riittäviä.

Jos tarkastajalla on tuntemusta järjestelmästä ja sen kontrolleista, tehdään testitapauksia tietoturvakontrollien testaamiseksi. Usein tarkastajalla ei ole riittävää ymmärrystä järjestelmästä ja tällöin tarkastaja luottaa asiantuntijoilta saamiinsa vastauksiin. Tällaisissa tilanteissa usein tarkastajalle esitellään ja näytetään miten tietoturvakontrollit toimivat. Tarkastuksissa käytetään usein apuna tietoturvallisuuteen ja kontrolleihin

[19] *Jari Pirnes, Anssi Sahlman, Jorma Kajava, Tietoturva ja sisäinen valvonta, Oulun yliopisto, Working papers series B 62, Oulu, 2000*

liittyviä tarkistuslistoja. Kontrolleja ja tarkistuslistoja ohjeistavat useat eri tahot ja standardit.

3.2.2. Ulkoinen tarkastus

Ulkoisia tarkastuksia tekevät yleensä tarkastustoimistot tai muut lain säätämät tahot tai toimijat. Ulkoisia tarkistuksia tehdään yleensä vuosittain. Ulkoiset tarkastukset ovat yleensä raskaita, kalliita ja aikaa vieviä hankkeita.

Lainsäädäntö tai muut määräykset voivat vaatia ulkoisten tarkastuksien tekemistä. On myös mahdollista, että yhteistyökumppani voi vaatia ulkoista tarkastusta. Esimerkiksi pankin kanssa toimiva taho, joka käsittelee tai on tekemisissä arkaluontoisen finanssialantiedon kanssa, voidaan vaatia tarkastettavaksi.

Yleisimmin käytetty auditointityyppi on SAS-70-auditointi. SAS-70-tarkastus ottaa huomioon fyysiseen tietoturvallisuuteen, loogiseen pääsynvalvontaan, muutoksen hallintaan, onnettomuuksista toipumiseen (engl. disaster recovery) ja politiikoihin ja menetelmiin liittyviä asioita[18].

3.2.3. Itsearviointi

Itsearviointi on usein kustannustehokkain tapa varmistaa ja arvioida järjestelmiä. Itsearvioinnin vaarana on objektivisuuden kärsiminen, koska arvioinnin tekijä on yleensä järjestelmän omistaja, käyttäjä tai joku muu joka tuntee järjestelmän hyvin. Itsearvionnin tulee kuitenkin olla suunniteltua ja organisoitua. Itsearvionnin on myös syytä perustua asianmukaisiin menetelmiin. On varmistuttava, että siihen on varattu oikeat henkilöt ja että heillä on aikaa ja osaamista arvioinnin tekemiseksi.

Itsearviointi poikkeaa sisäisestä ja ulkoisesta auditoinnista siten, että se on muodoltaan vapaa. Laajuus ja soveltamisala ovat vapaasti valittavissa ja se voi olla hyvinkin kapea tai yksityiskohtainen alue, jota halutaan tarkastella. Itsearviointeja yleensä suoritetaan ennen kuin sisäinen tai ulkoinen auditointi on tulossa. Myös muutosten jälkeen järjestelmät olisi hyvä arvioida.

Suurimpana haasteena itsearvioinnille on selkeän ajan löytäminen arvioinnin kunnolliselle tekemiselle. Ihmisten päivittäiset työtehtävät haittaavat usein arvioinnin tekemistä. Tämän takia itsearviointia varten olisi hyvä muodostaa oma arviointiorganisaatio, työsuunnitelma tarkastettavasta kohteesta ja aikataulu. Objektiivisuuden lisäksi arvioijien tulisi pystyä olemaan kriittisiä arvioidessaan järjestelmää. Kriittisyys voi tarkoittaa tekijälle itselleen lisää työtä, johon hänellä ei ole aikaa tai halua.

3.2.4. Haavoittuvuusanalyysi

Haavoittuvuusanalyysi on tekninen tarkastus-/analyysimenetelmä. Siinä missä muut arviointimenetelmät keskittyvät tarkastelemaan hallinnollista turvallisuutta, tietoturvakontrollimekanismeja ja prosessien turvallisuutta, keskittyy haavoittuvuusanalyysi tarkastelemaan järjestelmien heikkouksia tietoteknisestä näkökulmasta. Haavoittuvuusanalyysi on yleisin arviointimenetelmä.

Haavoittuvuusanalyysin tekemiseen on tarjolla runsaasti työkaluja. Haavoittuvuusanalyysin merkitys on kasvanut, koska yhä useammat palvelut sijaitsevat julkisessa verkossa. Tämän lisäksi hyökkäykset ovat yleistyneet ja hyökkääjien ei tarvitse olla alaa pitkää harrastaneita guruja, vaan he voivat olla kokeilunhaluisia nuoria, jotka lataavat Internetistä itselleen hyökkäystyökaluja. Työkaluja ovat muun muassa portti- ja haavoittuvuusskannerit kuten Nessus ja Nmap.

3.2.5. Tunkeutumisarviointi

Siinä missä haavoittuvuusanalyysi pyrkii löytämään järjestelmästä haavoittuvuuksia, pyrkii tunkeutumistestaus hyväksikäyttämään näitä haavoittuvuuksia. Haavoittuvuusanalyysi etsii vain mahdollisia heikkouksia, tunkeutumistestauksessa puolestaan pyritään käyttämään järjestelmää väärin. Tunkeutumistestausta kutsutaankin usein eettiseksi hakkeroinniksi.

Tunkeutumiseen on tarjolla useita työkaluja. Jos haavoittuvuusanalyysissa paljastuu esimerkiksi haavoittuvuus jossakin komponentissa, voidaan tätä yrittää hyväksikäyttää

(engl. exploit) järjestelmää vastaan. Tunkeutumistestauksen ei tarvitse pohjautua ainoastaan työkalujen löytämiin haavoittuvuuksiin vaan asiantuntija voi yrittää omin keinoin käyttää järjestelmää väärin. Järjestelmän väärinkäyttäjä voi olla organisaation ulkopuolinen taho tai tahattomasti tai tahallisesti väärinkäyttävä järjestelmän oikeutettu käyttäjä. Molempia mahdollisuuksia tulee tarkastella tunkeutumisarvioinnissa.

Tunkeutumistestaus tulee suunnitella huolella kuten kaikki testaaminen. Tunkeutumistestauksen tulee pohjautua johonkin metodiikkaan ja testauksesta tulee tehdä testaussuunnitelma. Järjestelmästä jaettavan tiedon määrä vaihtelee. Joissakin tapauksissa eettisen hakkeroinnin testaustiimille ei kerrota mitään järjestelmästä ja tätä kutsutaan sokkotestaukseksi (engl. blind testing). Täydellistä sokkotestausta käytetään yleensä kun järjestelmä on uusi ja sitä ei ole aiemmin testattu tai silloin kun halutaan tietää mitä järjestelmästä saadaan selville kertomatta mitään.

Sokkotestaukseen menee luonnollisesti huomattavan paljon aikaa, rahaa ja resursseja. Joskus on mielekkäämpää tehdä eettistä hakkerointia siten, että järjestelmä esitellään ja kerrotaan sen komponenteista. Tämän jälkeen tunkeutumistestaajat yrittävät käyttää järjestelmää hyväkseen.

3.2.6. Riskiarviointi

Riskiarviointi on arviointimenetelmistä laaja-alaisin. Se ottaa huomioon haavoittuvuudet, uhat ja seuraukset. Riskiarvioinnin toteuttamista voidaan kutsua riskikartoitukseksi tai riskianalyysiksi. Joskus puhutaan myös uhkakartoituksesta tai uhka-/riskikartoituksesta.

Riskikartoituksessa ei usein paneuduta pienimpiin yksityiskohtiin, vaan käsittely joudutaan pitämään korkealla tasolla. Riskikartoituksen tuloksia voidaan kuitenkin jatkojalostaa, kunhan riskit on tunnistettu ja vastuuhenkilöt niiden osa-alueille on löydetty. Riskianalyysityyppejä on useita ja monissa lähteissä ne jaotellaan eri tavalla. Yksi karkea jaottelutapa on jakaa riskianalyysi tietoturvariskeihin ja liiketoimintariskeihin. Riskianalyysissä esiintyneet asiat voivat olla suurempia kokonaisuuksia, jotka koskevat kokonaisia järjestelmiä tai prosesseja. Esiintyneiden

asioiden laajuus riippuu riskianalyysiin valitusta lähestymistavasta ja riskianalyysin rajauksesta.

3.3. Yhteenveto tietoturvaorganisaatiosta

Tietoturvaorganisaatiolla on yksi keskeinen tehtävä eli vastata organisaation tietoturvallisuudesta. Edellä esitetyt standardit, ISO 27001 ja SSE-CMM, ovat tapa formalisoida tietoturvaorganisaation toimintaa. Prosessit, standardit ja ennalta määritetyt tehtävät auttavat tietoturvaorganisaatiota työssään eli tietoturvan takaamisessa. Riskienhallinta on keskeinen osa tietoturvan hallintaa. Riskianalyysi pyrkii tarjoamaan tilannekuvan tietoturvan nykyhetkestä. Riskianalyysi on kuitenkin vain yksi tietoturvaorganisaation tehtävistä. Seuraavaksi käsitellään riskienhallinnan kokonaisuutta ja edelleen riskianalyysiä.

4. Riskienhallinnan kokonaisuus

4.1. Tietoturvariskien arviointi ja hallinta

Tietoturvariskien arviointi, hallinta ja riskianalyysi liittyvät kaikki läheisesti tietoturvaan. Edellä mainitut käsitteet tai toimet ovat yrityksen toimintaan kohdistuvien uhkien tunnistamismenetelmiä, joilla voidaan uhat tunnistaa tarkasti, ammattimaisen tehokkaasti ja nopeasti. Uhkien seurausvaikutusten analysointi kertoo miten uhkatekijät voivat vaikuttaa yrityksen päivittäiseen toimintaan[20]. Seurausvaikutusten analysoinnin tuloksena saadaan riskejä.

Riskillä voidaan ajatella olevan 3 eri ulottuvuutta: uhka, epävarmuus ja mahdollisuus[20]. Epävarmuus kuvaa uhkan tai riskin toteutumisen todennäköisyyttä. Varmuudella ei voida määritellä tapahtumisen tai toteutumisen todennäköisyyttä. Kolmas komponentti, mahdollisuus, kuvaa kehittämis-/hyötymahdollisuuksia, joita organisaatio voi saavuttaa riskin hallitsemisella. Eri kirjallisuuden lähteissä riski-käsite määritellään hieman eri termeillä, mutta keskeinen sisältö on pääosin sama.

[20] *Juha E. Miettinen, Tietoturvallisuuden johtaminen –näin suojaat yrityksesi toiminnan, ISBN 952-14-0229-6, Kauppakaari OYJ, 1999*

Riskiarviointi on erittäin merkittävä osa riskien hallintaa. Tämän diplomityön puitteissa riskiarvioinnin ja riskienhallinnan käsitteet pyritään kuitenkin pitämään erillään. Seuraavaksi käsitellään riskiarviointia.

4.1.1. Riskiarviointi

Riskien arviointiprosessia kutsutaan usein riskianalyysiksi tai riskikartoitukseksi. Tietoturvallisuuden alalla on epätäsmällisyyttä edellä mainittujen termien osalta. Joskus kirjallisuudessa määritellään riskianalyysin olevan ainoastaan tekninen tarkastusprosessi. Tämän työn puitteissa riskianalyysikäsite on laajempi eikä rajoitu ainoastaan tekniseen tarkastukseen. Riskianalyysi keskittyy tunnistamaan uhkia ja arvioimaan niiden mahdollisia vaikutussuhteita siinä missä riskien hallinta pyrkii toimimaan riskien lieventämiseksi.
Riskianalyysi tarjoaa ajankohtaisen tiedon tarkastelukohteeseen kohdistuvista potentiaalisista uhkista ja niiden seurauksista. Riskiarviointiprosessin eteneminen on kuvattu alla olevassa kuvassa[21](Kuva 3).

Kuva 3: Riskiarviointiprosessin eteneminen.

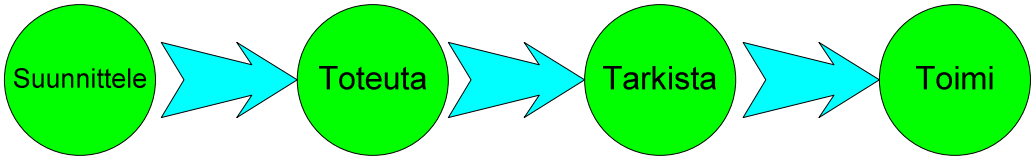
Riskiarviointiprosessi jakautuu kolmeen osaan: *tunnistamis-*, *analysointi-* ja *suunnittelu-*vaiheeseen. Tunnistamisvaiheessa pyritään tunnistamaan uhat, joita kohdistuu tarkastelukohteeseen. Analysointivaiheessa pyritään analysoimaan uhkien seurausvaikutuksia. Suunnitteluvaiheessa pyritään tunnistamaan kehitystarpeet eri osa-alueille. Kehityksen avulla voidaan parantaa suojausstrategiaa tai lieventää riskejä. Riskianalyysiprosessin eteneminen käsitellään yksityiskohtaisesti riskianalyysiprosessi-kappaleessa.

---

[21] *Christopher Alberts, Audrey Dorofee, Managing Information Security Risks: The OCTAVE Approach, ISBN 0-321-11886-3, Addison Wesley, 2002*

4.1.2. Riskienhallinta

Kuten aiemmin mainittu on riskien arviointi merkittävä osa riskienhallintaprosessia. Riskiarviointi on riskienhallinnan ensimmäinen vaihe ja se tarjoaa ainoastaan suuntaa, johon tietoturvallisuutta tulisi kehittää. Riskiarvioinnin jälkeen tulisi organisaation noudattaa alla esitettyä riskienhallinnan prosessimallia[21] (Kuva 4).



Kuva 4: Riskienhallinnan prosessimalli.

Riskienhallinnanprosessi jakautuu neljään vaiheeseen: *suunnittele*, *toteuta*, *tarkista* ja *toimi*. Prosessimalli mukailee aiemmin työssä esitettyä PDCA-prosessimallia (engl. Plan-Do-Check-Act) tietoturvallisuustoiminnalle. PDCA-prosessimallin vaiheet olivat suomennettuna: *suunnittelu*, *toteutus*, *tarkistaminen* ja *toiminen*. Tietoturvallisuuden hallintamallin määrittelevä ISO-27001-standardi suosittelee PDCA:ta käytettäväksi kaikessa tietoturvallisuustoiminnassa[13].

Kuten aiemmin mainittu, edellyttää riskien hallintaprosessin aloittaminen riskiarvioinnin tuloksia. Riskienhallinnan prosessimallin kuvaama sykli toteutetaan riskiarviointien välillä. Seuraavaksi kuvataan eri vaiheissa tehtävät toimet.

Suunnittelu-vaiheessa suunnitellaan suojausstrategia ja yksityiskohtainen riskien pienentämis-/lieventämissuunnitelma (engl. Risk mitigation plan) arviointitulosten pohjalta (riskiarviointivaiheen tuloksien pohjalta). Suunnitteluvaiheessa voidaan suorittaa myös kustannus-hyötyanalyysi (engl. cost-benefit analysis)eri strategioista ja aktiviteeteistä. Riskiarvioinnin suunnitteluvaiheessa suunniteltiin kehittämistä ja parantamista kun puolestaan riskienhallintaprosessin *suunnittelu*-vaiheessa suunnitellaan kuinka parannukset toteutetaan käytäntöön.

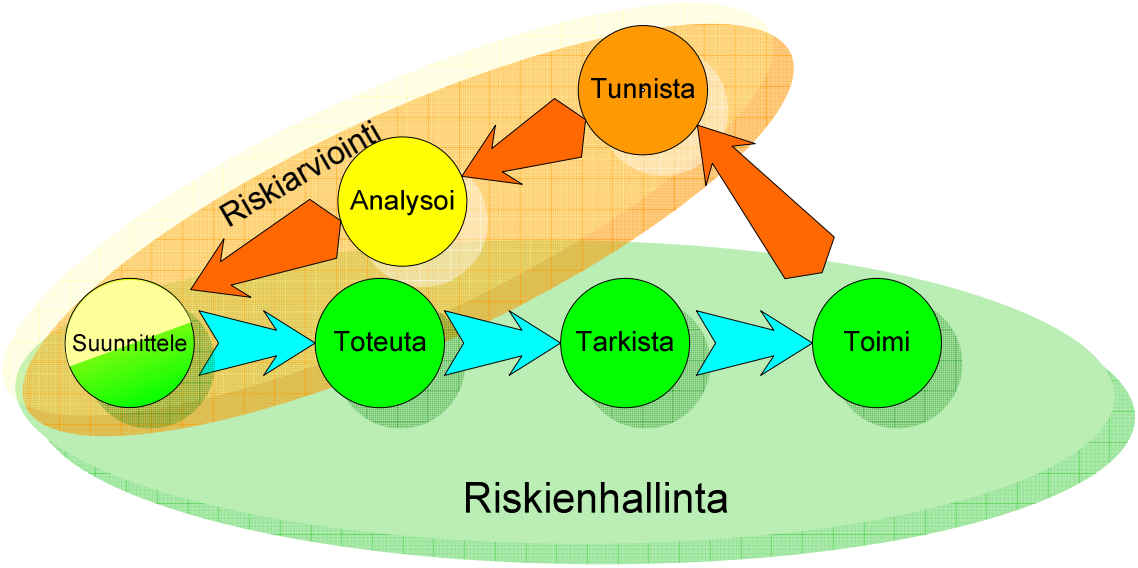
Toteutus-vaiheessa toteutetaan tehdyt suunnitelmat. Tässä vaiheessa myös tarkkaillaan riskejä ja niiden muuttumista.

Tarkastus-vaiheessa tarkkaillaan suunnitelmien tehokkuutta ja etenemistä.

Toiminta-vaiheessa pyritään hallitsemaan ja ohjaamaan suunnitelmapoikkeamia tekemällä korjaavia toimenpiteitä.

4.1.3. Riskiarvioinnin ja riskienhallinnan suhde

Riskienhallintaprosessin käynnistäminen edellyttää riskiarviointiprosessin läpiviemistä. Alla olevassa kuvassa on kuvattu riskiarvioinnin ja riskienhallinnan suhdetta[21](Kuva 5).



Kuva 5: Riskiarvioinnin ja riskienhallinnan suhde.

Yllä olevaan kuvaan on yhdistetty sekä riskiarviointiprosessin vaiheet (Kuva 3) että riskienhallinnan vaiheet (Kuva 4). Riskiarviointivaiheessa käydään tunnistamis-, analysointi- ja suunnitteluvaiheet läpi. Riskiarviointeja tulisi tehdä aika ajoin, esimerkiksi vuosittain. Arviointivaiheiden välissä suoritetaan riskienhallintaprosessin vaiheet: suunnittele, toteuta, tarkista ja toimi. On huomattava, että riskiarvioinnin ja riskienhallinnan suunnitteluvaihe eivät ole sama asia (vrt. Kuva 3 ja Kuva 4 sekä selitykset vaiheille). Riskiarvioinnin suunnitteluvaiheessa pyritään tunnistamaan *tietoturvallisuuden kehityskohteita*, siinä missä riskienhallinnan suunnitteluvaiheessa pyritään laatimaan *yksityiskohtainen riskien lieventämissuunnitelma*.

4.1.4. Riskienhallinnan keinot

Riskienhallinnan tavoite on reagoida riskiarvioinnissa esiintyneisiin riskeihin. Riskejä voidaan hallita monella tavalla. Keskeisiä toimintavaihtoehtoja riskien hallintaan ovat[8]:

Riskin välttäminen
Tämä on usein mahdollista vain jos kyseessä olevasta toiminnasta päätetään luopua kokonaan.

Riskin poistaminen
Yksittäisen riskin poistaminen on mahdollista, mutta seurauksena voi olla tukku uusia riskejä. Kaikkia riskejä ei voida poistaa kokonaan.

Riskin pienentäminen
Riskin pienentämisessä pyritään ensisijaisesti pienentämään tapahtumistodennäköisyyttä ja seurauksien vakavuutta.

Riskin siirtäminen
Riski voidaan siirtää esimerkiksi sopimuksilla tai vakuutuksille. Tällöin vastuu riskistä siirtyy vain eri taholle.

Riskin pitäminen omalla vastuulla
Osa riskeistä joudutaan pitämään omalla vastuulla tai riskin pitäminen omalla vastuulla on kannattavaa. Jos päätetään pitää riski omalla vastuulla, otetaan tietoinen riski uhan toteutumisesta.

Riskien pienentämisen toimia voivat olla esimerkiksi *tekniset toimenpiteet*, *organisaation toimintaan vaikuttavat toimenpiteet* tai *yksilöiden toimintamahdollisuuksiin vaikuttavat toimenpiteet*[8].

Teknisiä toimenpiteitä voivat olla muun muassa uudet laite- tai työtilaratkaisut, konesuojauksen kehittäminen, tekniset varmistukset, hälytinjärjestelmät tai huollon ja kunnossapidon parannukset.

Organisaation toimintaan vaikuttavia toimenpiteitä ovat yhteisistä pelisäännöistä sopiminen, valvonnan ja seurannan kehittäminen, toimintaohjeistuksien laatiminen, vastuista sopiminen, tiedonkulun ja työsuunnittelun parantaminen.

Yksilöiden toimintamahdollisuuksiin vaikuttavia toimia ovat muun muassa uusien työvälineiden hankinta, ohjeistukset, perehdytys ja koulutus, uudet työaika- tai työparijärjestelyt.

4.2. Riskianalyysiprosessi

Ennen riskianalyysiprosessin aloittamista tulee olla valittuna viitekehys, jonka puitteissa analyysi suoritetaan. Riskianalyysin viitekehyksenä käytetään yleensä jotain standardia. Tietoturvastandardeja käsitellään myöhemmin työssä tietoturvastandardit-kappaleessa. Siinä missä standardi määrittelee tarkastelualueen, määrittelee menetelmä sen miten prosessi viedään läpi. Menetelmiä käsitellään myöhemmin metodiikat-kappaleessa. Riskianalyysiprosessin aloittaminen edellyttää myös, että organisaation toiminnan tuntevat henkilöt ovat suunnitelleet riskianalyysille laajuuden, rajauksen, toteutussuunnitelman, aikataulun ja jatkotoimenpiteiden organisoinnin[8].

Riskien arvioinnin tarkoitus on tunnistaa tietoturvallisuuden uhkat, haavoittuvuudet ja pyrkiä arvioimaan mahdollisesti toteutuvien uhkien seurauksia. Keskeisiä käsitteitä riskianalyysin kannalta ovat: *uhka*, *riski*, *uhkan toteutumisen todennäköisyys*, *uhkan toteutumisen seurauksien vakavuus*. Uhkia analysoimalla pystytään tunnistamaan riskejä. Riskit muodostuvat uhkasta, sen toteutumisen todennäköisyydestä ja sen seurauksen vakavuudesta[8]. Riski voidaan esittää seuraavalla kaavalla[22]:

*Riski = uhkan toteutumisen todennäköisyys * uhkan toteutumisen seurausten vakavuus*

On luonnollista, että eri uhkat ovat seurauksien vakavuudeltaan ja toteutumistodennäköisyydeltään eriarvoisia. Riskianalyysissä pyritäänkin etsimään

[22] *Valtionhallinnon tietoturvallisuuden johtoryhmä, Valtionhallinnon tietoturvakäsitteistö, ISBN 951-804-404-8, VAHTI 4/2003*

merkittävimpiä uhkia, jotka muodostavat suurimpia riskejä. Kaikkia uhkia ei voida torjua kokonaan, joten analysoimalla uhkia ja muodostamalla niistä riskejä voidaan tietoturvallisuustoimintaa keskittää suurimpien riskien hallintaan.

Riskianalyysiprosessilla on neljä peruselementtiä. Nämä elementit ovat: *kvantitatiivinen riskianalyysi* (engl. quantitative risk analysis), *kvalitatiivinen riskianalyysi* (engl. qualitative risk analysis), *voimavarojen/suojattavien kohteiden arvottaminen* (engl. asset valuation process) ja *suojakeinon valinta* (engl. safeguard selection)[3].

Kvantitatiivinen riskianalyysi

Kvantitatiivisen ja kvalitatiivisen riskianalyysi ero on yksinkertainen: kvantitatiivinen riskianalyysi pyrkii asettamaan objektiivisia numeerisia arvoja riskianalyysissa esiintyneille komponenteille kun puolestaan kvalitatiivinen riskianalyysi ei pyri arvioimaan eksakteja rahallisia kustannuksia.. Kvantitatiivinen riskianalyysi pyrkii arvioimaan rahallisesti potentiaalisia häviöitä riskin toteutumisesta.

Kvantitatiivinen riskianalyysi edellyttää, että seuraavat elementit ovat määritelty ja tunnistettu: *suojauskohteen arvo*, *uhkan vaikutus, uhkan todennäköisyys, suojakeinon tehokkuus, suojakeinon hinta, epävarmuus* ja *todennäköisyys*. Täysin kvantitatiivisen riskianalyysin tekeminen on mahdotonta, koska monia asioita joudutaan arviomaan kvalitatiivisesti. Objektiivisen ja eksaktin rahallisen arvon määritteleminen on erittäin haasteellista. Kvantitatiivinen riskianalyysiprosessi on erittäin laaja ja raskas hanke.

Kvalitatiivinen riskianalyysi

Kvalitatiivinen riskianalyysi perustuu subjektiivisiin arvioihin ja tulokset eivät ole mitattavissa suoraan rahassa. Kvalitatiivinen arviointi asettaa aineettomampia arvoja tiedon menettämiselle kuin kvantitatiivinen arviointi.

Siinä missä täysin kvantitatiivisen riskianalyysin suorittaminen on mahdotonta, on täysin kvalitatiivisen riskiarvioinnin tekeminen mahdollista. Kvalitatiivinen arviointi ei pyri asettamaan kovia kustannuksia eri elementeille ja on enemmän skenaariopainotteinen kuin kvantitatiivinen. Kvalitatiivisen riskianalyysiprosessin läpiviemiseen tarvitaan uhat, niiden toteutumistodennäköisyydet ja seurausten vakavuudet.

Kvalitatiivisessa riskiarvioinnissa tarkastelukohteen riskien suuruudet ovat verrannollisia keskenään eivätkä ole absoluuttisia arvoja. Tämä johtaa siihen, että eri skenaarioiden riskit eivät ole vakavuuksiltaan keskenään verrannollisia.

Kvalitatiivista riskianalyysiä voidaan edelleenjalostaa kvantitatiivisempaan suuntaan. Kvantitatiiviseen arviointiin tarvitaan tilastotietoja lukuisista asioista. Uhkien todennäköisyyksien arviointiperusteena voi olla esimerkiksi eri komponenttien vioittumistietoja ja ihmisen toiminnan virhetietojen tilastoja. Yksi kvantitatiivinen riskianalyysimenetelmä on Courtneyn - menetelmä, joka on hyväksytty Yhdysvaltain valtion virastojen viralliseksi riskianalyysistandardiksi. Courtneyn - menetelmä perustuu ei-toivottujen tapahtumien odotetun esiintymistaajuuden sekä rahallisten vahinkojen suuruuden avulla laskettavaan vahingon odotusarvoon[8].

Suojattavien kohteiden arvottaminen

Suojattavien kohteiden arvottaminen on tehtävä huolimatta siitä suoritetaanko kvalitatiivista tai kvantitatiivista riskianalyysia. Arvon tunnistaminen tai arvottaminen on kaikkien auditointimetodien perusvaihe. Yleinen virhe on toteuttaa tietoturvakontrollit ilman asianmukaista suojattavien kohteiden tunnistamista tai arvottamista. Tämä johtaa usein siihen, että tietoturvakontrolli ei anna tarvittavaa suojaa kohteelle, ei ole taloudellisesti kannattava tai se suojaa väärää kohdetta.

Suoritettaessa kvalitatiivista riskianalyysia on tunnistettava tärkeimmät suojattavat kohteet, vaikka niiden arvottaminen olisikin skenaariopohjaista ja kvalitatiivista. Subjektiivisen arvottamisen riskinä ovat väärät arviointiperusteet tai järjestelmän tuntemuksen puute. Tämän takia arvottamis-/tunnistamisprosessissa tulee olla mukana hyvin tarkastelukohteen tuntevia henkilöitä. Suojattavia kohteita on voitu tunnistaa organisaatiotasolla, mutta tarkasteltaessa pienempiä kokonaisuuksia tai järjestelmiä voi olla mahdollista, että suojattavia kohteita tulee uudelleen arvioida tai tunnistaa.

Suojakeinon valinta

Riskien tunnistamisen jälkeen suurimpia riskejä pyritään usein lieventämään. Suojauskeino on tapa lieventää riskiä. Suojauskeinon kriittinen ja läpikohtainen arviointi on erittäin merkittävässä roolissa riskin lieventämisen kannalta.

Riippuen riskianalyysin luonteesta voi suojakeinot olla aineettomia tai aineellisia. Esimerkki aineettomasta tai hallinnollisesta suojauskeinosta on henkilöstön tietoturvakouluttaminen. Aineellisia suojakeinoja ovat esimerkiksi uudet laiteinvestoinnit kuten palomuurit.

Suojakeinon valinnassa tulee ottaa huomioon, miten ratkaisu vaikuttaa riskiin. Eli mikä on jäännösriski muutoksen jälkeen. Jäännösriskillä tarkoitetaan jäljelle jäävää riskiä. Suojauskeinon valinta voi myös tukea tulevaisuuden suunnitelmia. Esimerkiksi suojauskeino voi olla teknisten tietoturvatuotteiden vaihtaminen toisen valmistajan tuotteisiin. Tällöin valinnan perusteena voi olla se, että kyseisen valmistajan tuotteisiin siirtymiseen on sitouduttu tulevaisuudessa. Suojauskeino voidaan implementoida käytäntöön ennen suunniteltua siirtymistä, jos päätetään että riski on niin iso että ennenaikainen siirtyminen kannattaa. Suojauskeinon valinnassa tulisi välttää väliaikaisten ratkaisujen käyttöönottamista, jollei ole pakko.

Tietoturvariskien arviointi ja hallinta – kappaleessa esiteltiin riskiarviointiprosessi ylemmällä tasolla. Riskiarviointiprosessi jaettiin kolmeen vaiheeseen: *tunnista*, *analysoi* ja *suunnittele*. Seuraavaksi kuvataan eri vaiheissa tehtäviä toimintoja.

4.2.1. Tunnista

Tunnistamisvaihetta voidaan kutsua myös nimellä uhkakartoitus. Riskianalyysiprosessille on valittu standardi tai joku muu viitekehys. Standardi voi tarjota erilaisia läpikäytäviä kontrolleja tai potentiaalisia uhkia. On myös mahdollista riskianalyysissä käyttää erilaisia uhkalistoja, joita määrittelevät lukuisat tahot.

Tunnistamisvaiheessa pyritään tunnistaa uhat, jotka kohdistuvat tarkastelukohteeseen. Käytettäessä valmiita uhka-/tarkastuslistoja on mahdollista, että listan uhkista saadaan avainsanoja ja keksitään johdannaisia uhkia. On yleistä, että uhkia voi tulla erittäin suuri määrä. Tässä vaiheessa uhkia ei vielä analysoida tai jätetä tarkastelun ulkopuolelle.

4.2.2. Analysoi

Edellisen vaiheen, tunnista-vaiheen, tuotoksia analysoidaan tässä vaiheessa. Analysointi vaiheessa pyritään muodostamaan potentiaalisista uhkista riskejä. Riskien muodostaminen tehdään arvioimalla uhkien seurauksien vakavuutta ja toteutumistodennäköisyyttä. Analysointivaiheen jälkeen uhkat ovat muodostuneet riskeiksi. Riskit yleensä myös järjestetään vakavuusjärjestykseen.

4.2.3. Suunnittele

Suunnittele-vaiheessa kehitetään suojausstrategia ja riskien lieventämissuunnitelma. Suunnitteluvaiheessa tunnistetaan ja suunnitellaan toimet, joita tulisi tehdä riskien pienentämiseksi. Tässä vaiheessa päätetään miten ja mihin analyysissä esiintyneisiin asioihin reagoidaan.

4.3. Riskienhallinnan tarkastelukulmat

Riskienhallintaa tehdään lukuisilla eri osa-alueilla. Tämän työn puitteissa keskitytään kuitenkin tarkastelemaan tietoturvariskien hallintaa. Tietoturvariskienkin hallintaa voidaan tarkastella eri tasoilta.

Tietoturvariskien osalta usein viitekehyksenä käytetään jotakin standardia. Standardeja käsitellään työssä myöhemmin standardit-kappaleessa. Tässä kappaleessa esitellään lyhyesti mahdollisia tarkastelukulmia riskien hallinnalle.

Tietoturvariskienhallinnan tarkastelukulmat voidaan jakaa esimerkiksi seuraavasti: *liiketoiminnallinen näkökulma*, *hallinnollinen näkökulma* ja *tekninen näkökulma*. Edellä esitelty jaottelu on kirjoittajan oma näkemys. Tämän lisäksi tarkastelualueen rajaus voi vaihdella aina suppeasta laajaan. Suppeammassa tarkastelussa luonnollisesti voidaan paneutua yksityiskohtaisemmalle tasolle siinä missä laajemmassa rajauksessa joudutaan pysymään yleisellä tai korkeammalla tasolla. Seuraavaksi käsitellään tarkastelukulmat.

Liiketoiminnallinen näkökulma

Liiketoiminnallisessa lähestymistavassa tietoturvariskejä ja niiden mahdollisia vaikutuksia pyritään sitomaan liiketoimintaan. Tietoturvariskien sitominen liiketoimintaan on loogista, organisaation päällimmäinen tavoitehan on tuottaa voittoa eli rahaa. Liiketoimintaan sitomisessa on kuitenkin omat rajoituksensa. Yksityiskohtaisten asioiden vaikutusta liiketoimintaan on miltei mahdoton määritellä. Tämän takia liiketoiminnan näkökulmasta tarkasteltaessa abstraktio tai yleistystaso on pidettävä korkealla.

On esimerkiksi selkeää, että strategisten tietojen vuotaminen tai paljastuminen vaikuttaa liiketoimintaan. Toisaalta on erittäin hankalaa määritellä palomuurisäännöstön puutteellisuudesta aiheutuvan riskin liiketoiminnallista vaikutusta. Esimerkkinä liiketoiminnallisen näkökulman huomioonottavasta viitekehyksestä on COBIT. On kuitenkin eriteltävä liiketoimintariskit, jotka usein liittyvät liiketoimintaoperaatioihin. Liiketoimintaan vaikuttavat tietoturvariskit liittyvät yleensä tietoon tai tietojärjestelmiin[18]. COBITia käsitellään tarkemmin standardit-kappaleessa.

Hallinnollinen näkökulma

Hallinnollinen lähestymistapa keskittyy tarkastelemaan kuinka tietoturvaa hallitaan. Hallinnollinen näkökulma esimerkiksi voi tarkastella tietoturva organisaatiota, prosesseja, tietoturvakäytäntöjä, henkilöstön tiedottamista ja kouluttamista. Tälle lähestymistavalle on tyypillistä, että tarkastelu keskittyy vahvasti organisaatioon ja sen toimintaan. Esimerkkinä hallinnollisen tietoturvan lähestymistavasta on ISO17799 ja ISO27001. ISO17799-standardia käsitellään myöhemmin standardit-kappaleessa.

Tekninen näkökulma

Teknisessä näkökulmassa keskitytään usein tarkastelemaan teknisiä yksityiskohtia. Tekniseen riskinäkökulmaan soveltuu avuksi hyvin tarkistuslistat, koska abstraktiotaso on matala. Tekninen riskienhallinta on usein jalkautettu jokaiselle organisaatiotasolle tai osastolle. Teknisien riskien tarkastelu ei yleensä kata useita eri organisaatiotasoja.

Teknisessä riskienarvioinnissa voidaan keskittyä esimerkiksi organisaation henkilöstön työasemiin, palvelimiin, muihin verkkokomponentteihin kuten palomuureihin ja

kytkimiin, fyysiseen turvallisuuteen kuten kulunvalvontaan, paloturvallisuuteen tai vastaavaan.

4.4. Konsultin rooli riskikartoituksessa

Konsultilla voi olla monenlaisia rooleja. Riskikartoituksen kannalta oleelliset roolit konsultille tai ulkopuoliselle asiantuntijalle ovat menetelmän asiantuntija tai fasilitaattori[23]. Ulkopuolinen konsultti, joka on tietoturva-alan ammattilainen, tuntee metodiikat ja standardit hyvin. Eräs konsultin tehtävistä on toimia fasilitaattorina eli ohjata ja innostaa keskustelua tai toimintaa oikeaan suuntaan. Konsultti voi ohjata keskustelua aiemman kokemuksen perusteella ja ohjata tarvittaessa keskustelua esimerkiksi omilla huomioilla tai avainsanoilla. Konsulteilla voi olla valmiita avainsanalistoja kerätty aiemmista kartoituksista.

Riskikartoituksessa asiakas määrittelee omien asiantuntija-arvioidensa mukaan riskien vakavuudet, konsultin tehtävä on auttaa tässä. Konsultti toimii asiantuntijana analyysin etenemisessä ja läpiviemisessä. Usein riskikartoitus tehdään jonkun standardin mukaan ja tällöin ulkopuolisesta asiantuntijasta on erityisesti hyötyä. Konsultti voi olla myös ainoastaan menetelmän asiantuntija. Uhka- ja riskikartoituksessa ilmapiiristä tulee saada arvosteluvapaa ja osallistujia tulee kannustaa luovaan ajatteluun. Ideointivaiheessa usein esiintyykin aika villejä ideoita.

Ulkopuolisen konsultin käyttäminen on erityisen hyödyllistä, jos organisaatio on siirtymässä uudenlaiseen riskienhallinnan lähestymistapaan. Monet organisaatiot haluavat siirtyä standardoituun tietoturvan hallintaan. Konsulttia voidaan esimerkiksi käyttää ainoastaan ensimmäisellä kerralla menetelmän opettajana ja seuraavina vuosina prosessi voidaan suorittaa organisaation omin voimin.

[23] *Karri Kosonen, Paul Buhanist & al., Muutoksen etulinjassa, 3.painos, ISBN 952-91-0240-2, Hämeenlinna 2002, Karisto Oy*

5. Tietoturvastandardit

Tietoturvastandardeja on olemassa useita kymmeniä, ellei satoja. Tämän työn puitteissa keskitytään erityisesti riskianalyysiin ja standardeihin, jotka sopivat tietoturvariskien arviointiin. Aikaisemmin työssä esitettiin, että riskienhallinnan lähestymistapa voi olla liiketoiminnallinen, hallinnollinen tai puhtaasti tekninen. Edellä esitetty jaottelu on kirjoittajan oma esitys kuinka riskienhallinta tai tietoturvastandardit voidaan karkealla tasolla jaotella.

Standardointi organisaatioita on lukuisia ja monilla mailla on omat standardinsa. Yhdysvallat on merkittävä vaikuttaja standardialalla. Valitettavasti monet näistä standardeista perustuvat Yhdysvaltain omaan lainsäädäntöön ja sen aiheuttamiin rajoituksiin. Tämän työn puitteissa standardeja pyritään lähestymään kansainvälisestä tai Eurooppalaisesta näkökulmasta. Käsiteltäviksi standardeiksi tämän kappaleen puitteissa on valittu mahdollisimman suosittuja ja hyväksyttyjä standardeja. Kappaleen puitteissa esitellään standardeja, jotka pohjautuvat eri tarkastelukulmaan. Tarkastelukulmat ovat aiemmin mainitut tekniset, hallinnolliset ja liiketoiminnalliset. On syytä tähdentää, että nämä kolme tasoa ovat viitteellisiä. Tekninen taso keskittyy enemmän teknisiin yksityiskohtiin esimerkiksi yrityksen laskentaympäristöön. Hallinnollinen näkökulma ei käsittele tietoturvaa ainoastaan teknisenä vaan ottaa huomioon myös organisatorisia asioita. Liiketoiminnalliseksi nimetty näkökulma pyrkii sitomaan tapahtumat jossain määrin liiketoiminnan tavoitteisiin.

Tämän kappaleen puitteissa pyritään keskittymään standardeihin riskianalyysin näkökulmasta. ISO17799-tietoturvastandardi jakautuu kahteen osaan, joista toinen osa ISO27001 on käsitelty työssä aikaisemmin tietoturva-organisaatiokappaleessa. Kappale etenee teknisistä standardeista hallinnollisten kautta liiketoiminnan huomion ottavampaan suuntaan. Teknisen tason standardeja on lukuisia ja niistä eniten käytettyjä on vaikea määritellä, koska luonteensa vuoksi ne ovat hyvin tarkasteluympäristöspesifejä. Tekniseksi standardiksi on valittu hyvin tunnettu BSI ja sen tarjoamat uhkalistat tai tekniset tarkastuslistat. Hallinnollisena standardina käsitellään ISO17799-standardia. Liiketoimintanäkökulman omaavana standardina käsitellään COBIT.

5.1. BSI Standard 100-3

BSI eli Bundesamt für Sicherheit in der Informationstechnik on Saksan valtionhallinnon kansallinen tietoturvatoimisto tehtävänään toimia keskeisenä informaatioteknologia-tietoturvapalvelujen tarjoajana. BSI on Saksan kansallisen tietoturvallisuuden virasto tavoitteenaan edistää IT-tietoturvaa Saksassa[24]. Suomella on myös hieman vastaava ryhmä, VAHTI eli Valtionhallinnon tietoturvallisuusryhmä.

BSI on määritellyt oman riskianalyysistandardin, joka pohjautuu IT-Grundsschutziin (IT-Grundschutz tarkoittaa vapaasti suomennettuna IT:n perussuojausta). IT-Grundschutzin piiriin kuuluu muutama standardi: BSI Standard 100-1: Information Security Management Systems, BSI Standard 100-2: IT-Grundschutz Methodology ja BSI Standard 100-3: Risk Analysis based on IT-Grundschutz.

BSI 100-1 on linjassa ISO 27001-standardin kanssa (esitetty työssä aiemmin tietoturvaorganisaatio-kappaleessa). BSI 100-1 käsittelee tämän lisäksi ISO standardeja ISO 17799 ja ISO 13335. BSI 100-1 esittää edellä mainittujen ISO-standardien keskeisen sisällön ja pyrkii käsittelemään joitakin asioita yksityiskohtaisemmalla tasolla kuin ISO-standardit sellaisenaan tarjoavat.

[24] *BSI, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/english*

BSI 100-2 kuvaa metodin, joka kuvaa kuinka IT:n tietoturvanhallinta muodostetaan ja operoidaan käytännössä.

BSI 100-3 keskittyy riskianalyysin tekemiseen käyttäen hyväkseen IT-Grundschutzin luetteloita[25]. BSI 100-3 on prosessina erittäin teknispainotteinen tietoturva-analyysistandardi. Käytännössä riskianalyysin läpivieminen pohjautuu IT-infrastruktuurin ja sen heikkouksien tarkasteluun. IT-Grundschutz tarjoaa tätä varten kattavat uhka- ja suojakeinoluettelot.

BSI 100-3 on esimerkki teknisestä tietoturvariskianalyysistandardista. Riskianalyysi voidaan suorittaa ainoastaan tässä mittakaavassa, mutta on myös mahdollista käyttää viitemateriaalina BSI:n tai VAHTIn tarjoamia uhkaluetteloita tehtäessä esimerkiksi ISO17799:n mukaista riskianalyysia.

IT-Grundschutzin uhkaluettelo jakautuu seuraaviin osa-alueisiin: ylivoimaiset esteet (engl. Force Majeure), organisatoriset puutteet (engl. Organisational Shortcomings), ihmisten virheet (engl. Human Failure), tekniset vikaantumiset (engl. Technical Failure) ja tahalliset teot (engl. Deliberate Acts).

BSI:n riskianalyysistandardi pohjautuu hyvin pitkälti tarkistuslistoihin. Kuten aiemmin mainittu tarjoaa VAHTI omat uhkaluettelonsa (mukana myös Pk-yrityksen riskienhallinta työvälisarjassa, www.pk-rh.com). Teknisen ja uhkaluettelopohjaisen riskianalyysin hyvänä puolena on sen keveys.

5.2. ISO 17799

ISO 17799 – standardi määrittelee ohjeet ja perusperiaatteet organisaation tietoturvanhallinnan muodostamiselle, toteutukselle, ylläpidolle ja kehitykselle. ISO 17799 tarjoaa ainoastaan ohjeistuksia eikä määrittele syvällisellä tasolla kuinka tietoturvatoiminta tulisi muodostaa ja ylläpitää. Standardin tarjoamat ohjeistukset

[25] *Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-3, Risk Analysis based on IT-Grundshutz, version 2.0*

pidetään korkealla tasolla läpi koko standardin ja toteutuksen yksityiskohtiin ei paneuduta.

ISO 17799 on kansainvälinen tietoturvastandardi. Kansainvälisen tietoturvastandardin julkaiseminen edellyttää, että 75 % kansallisista päätäntäelimistä antaa äänensä kannattaakseen standardin julkaisemista. ISO-organisaatio on julkaissut 2 puhtaasti tietoturvaan liittyvää standardia: ISO 17799 ja ISO 27001. ISO 27001 – standardia on käsitelty aikaisemmin tietoturvaorganisaatiokappaleessa. ISO 17799 on erittäin tunnettu ja käytetty tietoturvastandardi. ISO 17799:stä on julkaistu kaksi versiota: ISO/IEC 17799:2000 ja ISO/IEC 17799:2005[26]. Vuoden 2005 versio korvaa aiemman version ja tämän kappaleen ja työn puitteissa käsitellään ainoastaan uudempaa versiota. Termillä ISO 17799 viitataan nimenomaan ISO/IEC 17799:2005:een. ISO 17799-standardi määrittelee keskeisimmät termit ja käsitteet. Seuraavassa kappaleessa käsitellään työn kannalta oleellisimmat käsitteet, joita standardissa määritellään.

5.2.1. Käsitteet

ISO 17799:ssä määritellään muuan muassa seuraavat käsitteet:

Voimavara/suojattava kohde (engl. asset):
Mikä tahansa, jolla on arvoa organisaatiolle.

Kontrolli (engl.control):
keinot riskien hallintaan, mukaan lukien politiikat, proseduurit, ohjeistukset, käytännöt tai organisaation rakenteet, jotka voivat olla hallinnollisia, teknisiä, johdollisia (engl. management), tai lain vaatimia.

Ohjeistus (engl. guideline):
Kuvaus, joka selventää mitä tulisi tehdä miten saavuttaakseen politiikkojen asettamat tavoitteet.

---

[26] *ISO/IEC 17799:2005(E), Information technology – Security techniques – Code of practice for information security management, Second edition 2005-06-15*

Tietoturva (engl. information security):
Varmistaa luottamuksellisuuden, eheyden ja käytettävyyden säilyttäminen. Mukaan lukien muut asiat kuten autenttisuus (engl. authenticity), vastuuvelvollisuus (engl. accountability), kiistämättömyys (engl. non-repudiation) ja luotettavuus/toimintavarmuus (engl. reliability).

Tietoturvatapahtuma (engl. information security event):
Tietoturvatapahtuma on järjestelmän tunnistama tapahtuma, palvelun tai verkon tila joka viittaa mahdolliseen tietoturvarikkomukseen tai tietoturvalaitteen vikaantumiseen, tai entuudestaan tuntematon tapahtuma, joka voi olla tietoturvakytkentäinen.

Tietoturvavälikohtaus (engl. information security incident):
Tietoturvavälikohtaukseen viittaa yksittäinen tai useampi ei-haluttu tai ennalta odottamaton tietoturvatapahtuma, joilla on merkittävä todennäköisyys vaarantaa liiketoimintaoperaatiot ja tietoturvallisuus.

Politiikka (engl. policy):
Kokonaisaikomus ja suunta, jonka johto on formaalisti esittänyt.

Riski (engl. risk):
tapahtuman todennäköisyyden ja sen seurauksen yhdistelmä.

Riskianalyysi (engl. risk analysis):
Systemaattinen tiedon käyttäminen lähteiden tunnistamiselle ja riskiarvioinnille

Riskiarviointi (engl. risk assessment):
Riskianalyysin ja riskien evaluoinnin kokonaisprosessi.

Riskien evaluointi (engl. risk evaluation):
Prosessi, jossa verrataan arvioitua riskiä annettuja riskikriteerejä vasten, jotta voidaan määritellä riskin merkittävyys.

Riskienhallinta (engl. risk management):
Koordinoituja aktiviteettejä organisaation ohjaamiseksi ja kontrolloimiseksi riskien huomioon ottavaksi. Riskienhallinta käsittää usein riskiarvioinnin (engl. risk assessment), riskien käsittelemisen (engl. risk treatment), riskin hyväksymisen (engl. risk acceptance) ja riskistä kommunikoimisen (engl. risk communication).

Riskin käsittely (engl. risk treatment):
Prosessi joka valitsee ja toimeenpanee toimet riskin muuttamiseksi.

Uhka (engl. threat):
Ei-halutun tapahtuman potentiaalinen seuraus, joka voi vaarantaa järjestelmän tai organisaation.

Haavoittuvuus (engl. vulnerability):
Voimavaran tai voimavarojen heikkous, jota voidaan hyväksikäyttää yhden tai useamman uhkan kautta.

Seuraavassa kappaleessa siirrytään käsittelemään standardin rakennetta.

5.2.2. Rakenne

ISO 17799:n jakautuu 11 osa-alueeseen. Nämä 11 osa-aluetta pitävät sisällään 39 päätietoturvallisuusaluetta (engl. main security categories). Päätietoturvallisuus alueet käsittävät: kontrollitavoitteen (engl. control objective) määritellen mitä tulee saavuttaa sekä yhden tai useamman kontrollin, joiden toimeenpanolla kontrollitavoite voidaan saavuttaa. Seuraavaksi esitellään lyhyesti ISO 17799:n 11 osa-aluetta lyhyine kuvauksineen niiden keskeisestä sisällöstä.

1. **Tietoturvapolitiikka (engl. Security Policy)**
   Tietoturvapolitiikka osio ohjeistaa tietoturvapolitiikan muodostamista ja tarkastamista. Tietoturvapolitiikka muodostaa pohjan tietoturvallisuuden hallinnalle.

Tietoturvapolitiikka on myös osoitus johdon sitoutuneisuudesta. Tietoturvapolitiikan jalkauttaminen koko organisaatioon on yksi tietoturvallisuuden haastavimmista tehtävistä. Haasteena on se, että tietoturvapolitiikka voi sisältää vierasta terminologiaa tavalliselle työntekijälle ja toisaalta työntekijän voi olla vaikeata yhdistää politiikan määrittelemiä käsitteitä ja ohjeistuksia jokapäiväiseen työhön.

2. Tietoturvaorganisaatio (engl. Organisation of Information Security)

Tietoturvaorganisaatio kappale ohjeistaa johdon sitoutuneisuutta tietoturvaan, tietoturvan koordinointia, tietoturvaroolien allokointia, tietojenkäsittelytilojen valtuuttamista, salassapitosopimuksia, virkavalta- ja muita tietoturva-alan erikoisyhteyksien muodostamista, tietoturvatarkistuksia, ulkoisiin osapuoliin liittyvien riskien hallintaa. Tietoturvaorganisaatio liittyy läheisesti ISO 27001 – standardiin, joka käsittelee tietoturvallisuuden hallintamallia ja ohjeistaa sen muodostamiseen.

3. Voimavarojen hallinta (engl. Asset Management)

Voimavarojen hallinta ohjeistaa voimavarojen luetteloinnin, omistajuuden ja hyväksyttävän käytön. Osa-alue ohjeistaa myös tiedon luokitteluun, nimeämiseen ja käsittelyyn.

4. Henkilöstöturvallisuus (engl. Human Resources Security)

Henkilöstöturvallisuus käsittää tietoturvaroolit ja vastuut, henkilöstön taustatarkistukset, työsuhteen alun ja työsopimuksen ehdot, toimet työsuhteen aikana, toimet työsuhteen päättyessä, johdon vastuut, henkilöstön tietoturvatietoisuus ja –koulutus ja rangaistustoimenpiteet tietoturvavälikohtauksissa.

5. Fyysinen- ja ympäristöturvallisuus (engl. Physical and Environmental Security)

Tämä osa-alue käsittää fyysisen turvamuurin (engl. security perimeter), fyysisen pääsynvalvonnan, kaikkien organisaatioiden tilojen turvaamisen, turvautumisen ulkoisia ja ympäristöllisiä uhkia vastaan, turva-aluetyöskentelyn (engl. working in secure areas), laitteistoturvallisuuden pitäen sisällään laitteiston turvaamisen

erilaisilta uhkilta, kaapelointiturvallisuuden, laitteiston ylläpitämisen/huoltamisen, etätyöturvallisuuden, turvallisen laitteistojen hävittämisen tai uudelleen käyttämisen.

6. Viestintäyhteyksien ja toimintojen hallinnointi (engl. Communications and Operations Management)

Tämä osa-alue käsittelee käyttöproseduureja ja vastuita pitäen sisällään proseduurien dokumentoinnin, muutosten hallinnan, vastuiden jakamisen, kehitys- testi ja tuotantoympäristöjen eriyttämisen; kolmannen osapuolen palveluntuottajien hallinnan käsittäen muun muassa palvelun toimittamisen, seuraamisen, tarkistamisen ja muutosten hallinnan; järjestelmäsuunnittelun ja –hyväksynnän; suojautumisen haitalliselta koodilta (virukset ynnä muut); varmuuskopioinnin; tietoverkkotietoturvan hallinnan; median hallinnan; tiedonvaihtamisen pitäen sisällään vaihtopolitiikat ja –proseduurit, vaihtosopimukset, fyysisen ja sähköisen median siirtämisen; sähköisen kaupankäynnin; valvonnan (engl. monitor)pitäen sisällään lokituksen, lokien seurannan, järjestelmän käytön seurannan, lokien suojaamisen, virhelokituksen ja kellojen synkronoinnin.

7. Pääsynvalvonta (engl. Access Control)

Pääsynvalvonta osa-alue käsittää pääsynvalvontapolitiikan; käyttäjän pääsynhallinnan; käyttäjän vastuut; verkon pääsynhallinnan; käyttöjärjestelmien pääsynhallinnan; ohjelmistojen ja tiedon pääsynhallinnan; etä- ja mobiilityön hallinnan.

8. Tietojärjestelmien hankinta, kehitys ja ylläpito (engl. Information Systems Acquisition, Development and Maintenance)

Tämä osa-alue käsittää tietojärjestelmien tietoturvavaatimukset; ohjelmistojen oikean käyttäytymisen/prosessoinnin pitäen sisällään tiedon validoinnin, sisäisen prosessoinnin kontrolloimisen ja tiedon eheyden; kryptografiset kontrollit; tiedostojärjestelmien tietoturvallisuuden; tuki- ja kehitysprosessien tietoturvallisuuden; teknisen haavoittuvuuksien hallinnan.

9. **Tietoturvavälikohtausten hallinnointi (engl. Information Security Incident Management)**

   Tämä osa-alue käsittää tietoturvatapahtumien ja heikkouksien raportoinnin; tietoturvavälikohtausten ja –parannusten hallinnan käsittäen vastuut ja proseduurit, oppimisen välikohtauksista ja todisteiden keräämisen.

10. **Liiketoiminnan jatkuvuuden hallinnointi (engl. Business Continuity Management)**

    Tämä osa-alue käsittelee liiketoiminnan jatkuvuuden hallintaa pitäen sisällään tietoturvan liittämisen osaksi liiketoiminnan jatkuvuuden hallintaprosessia, liiketoiminnan jatkuvuus ja riskiarvioinnin, jatkuvuussuunnitelmien kehittämisen ja toteutuksen tietoturvan huomioonottavasti, liiketoiminnan jatkuvuussuunnittelun viitekehyksen ja jatkuvuussuunnitelmien testauksen, ylläpidon ja arvioinnin.

11. **Vaatimuksenmukaisuus (engl. Compliance)**

    Vaatimuksenmukaisuus käsittää yhdenmukaisuuden lain asettamisen vaatimusten mukaisesti; yhdenmukaisuuden tietoturvapolitiikoiden ja -standardien sekä teknisen yhdenmukaisuuden ja tietoturvatarkastuksien huomioonottamisen. Osa-alueen nimi voisi yhtä hyvin olla lainmukaisuus. Esimerkkinä Suomessa noudatettavista laeista Laki yksityisyyden suojasta työelämässä [Laki 759/2004][27] ja Sähköisen viestinnän tietosuojalaki [SVTSL 516/2004][28].

ISO 17799:n kontrollitavoitteet ja itse kontrollit ovat tarkoitettu toteutettavaksi, jotta riskiarvioinnissa tunnistetut vaatimukset täyttyisivät[26]. ISO 17799:ää käytetään usein riskiarvioinnin pohjana.

5.3. COBIT

ISACA eli Information Systems Audit and Control Association (www.isaca.org) havaitsi, että tarkastajat käyttivät omia tarkistuslistojaan arvioidessaan

[27] *Laki yksityisyyden suojasta työelämässä 13.8.2004/759*

[28] *Sähköisen viestinnän tietosuojalaki 16.6.2004/516*

informaatioteknologian (IT) kontrolleja ja niiden tehokkuutta. Auditoijat puhuivat eri termeillä liiketoimintajohdolle ja IT-asiantuntijoille. Tämän kommunikaatio-ongelman ratkaisuksi kehitettiin COBIT. COBIT tarjoaa viitekehyksen, joka perustuu kokoelmaan yleisiä IT-prosesseja liiketoimintajohtajien, IT-harjoittajien ja auditoijien ymmärtämässä muodossa[29]. Ennen kaikkea COBITin lähestymistapa on liiketoimintakeskeinen, prosessiorientoitunut, kontrollipohjainen ja mittausta suosiva. Vuosien saatossa COBITista on kehittynyt avoin standardi ja se on kansainvälisesti omaksuttu IT-hallinnon tehokkaan implementoimisen ja toimimisen kontrollimalli. COBIT ja ISO17799 ovat kaksi kansainvälisesti käytettyä standardia.

COBITin näkökulmasta yrityksen- ja IT-hallinta ovat erittäin riippuvaisia toisistaan, yrityksenhallinta on riittämätöntä ilman IT:n hallintaa ja toisinpäin[30]. Myös COBIT suosittaa työssä aiemmin esitetyn PDCA-mallin (engl. Plan-do-Check-Act) käyttämistä ongelmien ratkaisemisessa ja prosessien kehittämisessä. Tiedon tarve (yrityksenhallinta) ja tiedontarjonta (IT:n hallinta) täytyy suunnitella (Suunnittelu-Plan). Tieto ja mahdolliset tietojärjestelmät pitää toteuttaa, toimittaa/hankkia ja käyttää (Tee-Do). Hankitun ja käytetyn tiedon tuotokset tulee olla mitattavissa suunnitteluvaiheessa määriteltyjä mittareita vasten (Tarkista-Check). Poikkeamia tutkitaan ja korjaavia toimia tehdään (Toimi-Act).

5.3.1. Rakenne

Tällä hetkellä uusin versio COBITista on neljäs versio. COBITissa on 34 korkean tason tavoitetta (geneeristä prosessialuetta), jotka käsittävät edelleen 215 kontrollitavoitetta. COBIT on prosessilähtöinen standardi ja se jakaa geneeriset prosessialueet neljään toimialueeseen: Suunnittele ja organisoi (engl. Plan and Organize), Hanki ja toteuta (engl. Acquire and Implement), Toimita ja tue (engl. Deliver and Support) ja Valvo ja arvioi (engl. Monitor and Evaluate)[31].

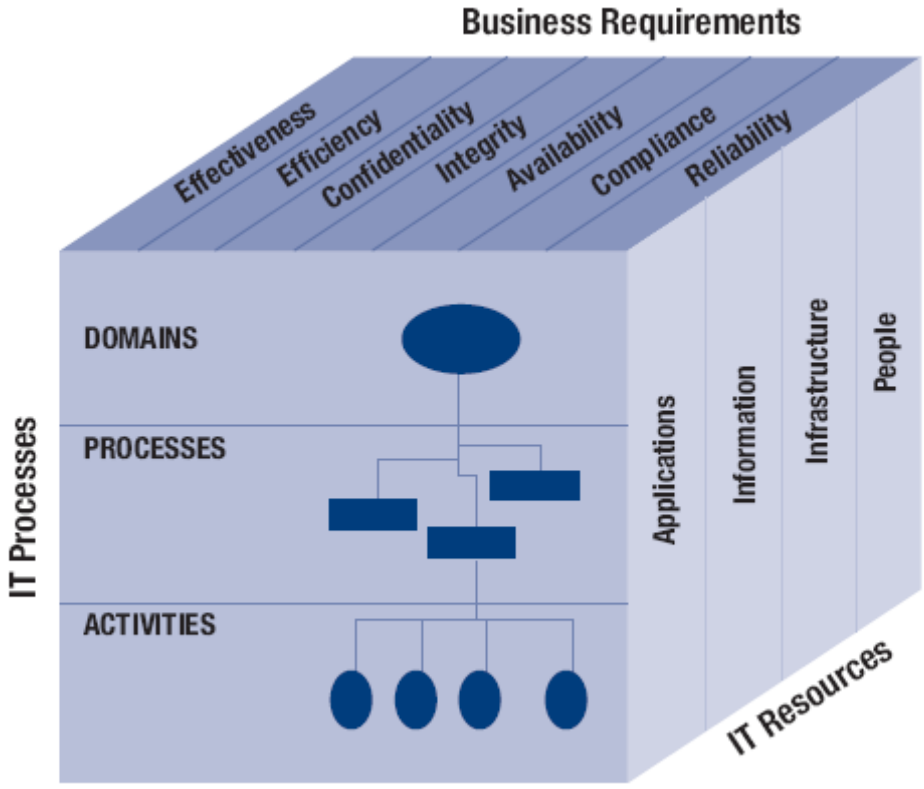
[29] *Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit, ISACA*

[30] *COBIT MAPPING: MAPPING OF ISO/IEC 17799:2000 WITH COBIT, 2NDEDITION, ISACA*

[31] *Cobit 4.0, ISACA*

COBIT käyttää omaa kypsyysmalliaan, jossa on kuusi määriteltyä tasoa (0-5). Jokaiselle geneeriselle prosessialueelle on määritelty oma kypsyysjaottelu ja vaatimukset eri tasoille. Yksinkertaistettuna COBITin 34 prosessialuetta sisältävät omat määritelmät prosessin kypsyydelle sekä useita kontrolleja geneeriselle prosessialueelle.

Kuten aiemmin mainittu on COBIT liiketoimintakeskeinen. COBITissa on kolme eri ulottuvuutta, jotka otetaan kaikki huomioon. Nämä ulottuvuudet ovat: IT-prosessit, IT-resurssit ja IT-tavoitteet. Yhteenvetona IT-prosessit hallinnoivat IT-resursseja tavoitteenaan täyttää IT:n tavoitteet, jotka on sidottu liiketoimintatavoitteisiin. Tätä kolmiulotteisuutta kutsutaan COBIT-kuutioksi (engl. COBIT Cube). Alla on kuva COBIT-kuutiosta(Kuva 6).



Kuva 6: COBIT-kuutio, Lähde:Cobit 4.0.

Yllä olevassa kuvassa on tiivistetty COBITin viitekehysmalli. IT-prosessit muodostuvat toimialueista (engl. Domains), prosesseista (engl. Processes) ja aktiviteeteista (engl. Activities). IT-resurssit voidaan puolestaan jakaa sovelluksiin (engl. Applications), tietoon (engl. Information), infrastruktuuriin (engl. Infrastructure) ja ihmisiin (engl.

People). Liiketoimintatavoitteet jakautuvat seitsemään osa-alueeseen: vaikuttavuuteen (engl. Effectiveness), hyötysuhteeseen (engl. Efficiency), luottamuksellisuuteen (engl. Confidentialiaty), eheyteen (engl. Integrity), käytettävyyteen (engl. Availability), lainmukaisuuteen/vaatimuksenmukaisuuteen (engl. Compliance) ja luotettavuuteen (engl. Reliability). Liiketoimintatavoitteissa on mukana työn alkupuolella esitetyt tietoturvan kulmakivet: eheys, luottamuksellisuus ja käytettävyys. Seuraavaksi paneudutaan IT-prosessien toimialueisiin ja niiden määrittelemiin korkean tason tavoitteisiin.

Suunnittele ja organisoi

Suunnittele ja organisoi osa-alue käsittää strategiaa ja taktiikoita. Tavoitteena on tunnistaa hyvä tapa, jolla IT tukee mahdollisimman paljon liiketoimintatavoitteiden saavuttamista. Osa-alue myös korostaa IT:n organisatorisen ja infrastruktuurisen puolen huomioonottamista optimaalisten tulosten ja parhaan hyödyn saavuttamiseksi IT:n tuella. Osa-alueella paneudutaan miettimään IT ja liiketoimintastrategian suhdetta, organisaation kykyä käyttää resurssejaan, organisaation jäsenten ymmärrystä IT:n tavoitteista, IT-riskienhallintaa ja ymmärtämistä ja IT-järjestelmien laatua ja kykyä palvella liiketoimintatavoitteiden saavuttamista[31]. Alla olevassa taulukossa on listattu korkean tason kontrollitavoitteet(Taulukko 2).

Taulukko 2: Suunnittele ja organisoi – osa-alueen korkean tason kontrollitavoitteet[31].

Suunnittele ja organisoi (engl. Plan and Organise)	
P01	Määrittele strateginen IT-suunnitelma (Define Strategic IT Plan)
P02	Määrittele tietoarkkitehtuuri (Define Information Architecture)
P03	Määritä teknologinen suunta (Determine Technological Direction)
P04	Määrittele IT-prosessit, -organisaatio ja -vaikutussuhteet (Define the IT Processes, Organisation and Relationships)
P05	Hallinnoi IT-investointeja (Manage IT Investment)
P06	Kommunikoi johdon asettamat tavoitteet ja suunta (Communicate Management Aims and Direction)
P07	Hallinnoi IT-henkilöstöresursseja (Manage IT Human Resources)
P08	Hallinnoi laatua (Manage Quality)
P09	Arvioi ja hallitse IT-riskejä (Assess and Manage IT Risks)
P010	Hallinnoi projekteja (Manage Projects)

Hanki ja toteuta

Hanki ja toteuta – osa-alue keskittyy IT:n vaatimusten tunnistamiseen, teknologian hankkimiseen ja toteuttamiseen osaksi organisaation olemassa olevia liiketoimintaprosesseja. Osa-alue myös korostaa ylläpitosuunnitelman kehittämistä siten, että IT-järjestelmien ja sen komponenttien elinikä pitenee. Ylläpitosuunnitelman kehittämisen tulee varmistaa, että ratkaisut ovat linjassa ja tukevat liiketoimintatavoitteita. Osa-alue keskittyy tarkastelemaan tukevatko uusien projektien ratkaisut liiketoimintatavoitteita, valmistuvatko uudet projektit ajallaan ja pysyvätkö ne niille asetetussa budjetissa, toimivatko uudet järjestelmät asianmukaisesti ja aiheuttavatko muutokset keskeytyksiä nykyisiin liiketoimintatapoihin. Alla olevassa taulukossa on listattu osa-alueen korkean tason kontrollitavoitteet(Taulukko 3).

Taulukko 3: Hanki ja toteuta – osa-alueen korkean tason kontrollitavoitteet[31].

Hanki ja toteuta (engl. Acquire and Implement)	
AI1	Tunnista automatisoidut ratkaisut (Identify Automated Solutions)
AI2	Hanki ja ylläpidä sovellusohjelmistot (Acquire and Maintain Application Software)
AI3	Hanki ja ylläpidä teknologiainfrastruktuuria (Acquire and Maintain Technology Infrastructure)
AI4	Mahdollista toiminta ja käyttö (Enable Operation and Use)
AI5	Hanki IT-resurssit (Procure IT Resources)
AI6	Hallinnoi muutoksia (Manage Changes)
AI7	Toimeenpane ja akkredidoi ratkaisut ja muutokset (Install and Accredit Solutions and Changes)

Toimita ja tue

Toimita ja tue – osa-alue keskittyy vaadittujen palvelujen toimittamiseen mukaan lukien palvelun toimittamisen, tietoturvan ja jatkuvuuden hallinnan, käyttäjien palvelutuen ja operatiivisten tilojen tiedon hallinnoinnin. Osa-alue käsittelee IT-palveluiden toimitusta liiketoiminta prioriteettien linjassa, IT-kustannusten optimointia, työvoiman kykyä käyttää IT-järjestelmiä tehokkaasti ja turvallisesti ja onko luottamuksellisuus, eheys ja käytettävyys toteutettu asianmukaisesti. Alla olevassa taulukossa on lueteltu osa-alueen korkean tason kontrollitavoitteet(Taulukko 4).

Taulukko 4:Toimita ja tue – osa-alueen korkean tason kontrollitavoitteet[31].

Toimita ja tue (engl. Deliver and Support)	
DS1	Määritä ja hallinnoi palvelutasoja (Define and Manage Service Levels)
DS2	Hallinnoi kolmannen osapuolen palveluja (Manage Third-Party Services)
DS3	Hallinnoi suorituskykyä ja kapasiteettia (Manage Performance and Capacity)
DS4	Varmista palvelujen jatkuvuus (Ensure Continuous Service)
DS5	Varmista järjestelmien turvallisuus (Ensure Systems Security)
DS6	Tunnista ja allokoi kustannukset (Identify and Allocate Costs)
DS7	Kouluta käyttäjiä (Educate and Train Users)
DS8	Hallinnoi Service Desk:iä ja välikohtauksia (Manage Service Desks and Incidents)
DS9	Hallitse atk-kokoonpanoa (Manage the Configuration)
DS10	Hallinnoi ongelmia (Manage Problems)
DS11	Hallinnoi tietoa (Manage Data)
DS12	Hallinnoi fyysistä ympäristöä (Manage the Physical Environment)
DS13	Hallinnoi toimintoja (Manage Operations)

Valvo ja arvioi

Valvo ja arvioi – osa-alue käsittelee suorituskyvyn hallinnointia, sisäisten kontrollien valvomista ja lainmukaisuuden täyttymistä. Osa-alue keskittyy IT-suorituskyvyn mittaamiseen ja ongelmien havaitsemiseen, johdon vastuuseen sisäisten kontrollien tehokkuudesta, IT-suorituskyvyn ja liiketoimintatavoitteiden väliseen yhteyteen ja riskien, kontrollien, lainmukaisuuden ja suorituskyvyn mittaamiseen ja raportointiin. Alla olevassa taulukossa on esitetty korkean tason kontrollitavoitteet toimialueelle(Taulukko 5).

Taulukko 5: Valvo ja arvioi – osa-alueen korkean tason kontrollitavoitteet[31].

Valvo ja arvioi (engl. Monitor and Evaluate)	
ME1	Valvo ja arvioi IT-prosesseja (Monitor and Evaluate IT Processes)
ME2	Valvo ja arvioi sisäistä kontrollia (Monitor and Evaluate Internal Control)
ME3	Varmista lainmukaisuus (Ensure Regulatory Compliance)
ME4	Takaa IT-hallinta (Provide IT Governance)

5.4. Näkökulma ja lähestymistapaerot

Tämän kappaleen puitteissa käsiteltiin tarkemmin kolme erittäin suosittua tietoturvastandardia, BSI 100-3, ISO 17799 ja COBIT. Valituista standardeista kukin kuvaa jokseenkin aikaisempaa tietoturvatarkastelukulmien jakoa. Tarkastelukulmat olivat tekninen, hallinnollinen ja liiketoimintaan sidottu näkökulma.

Näistä standardeista BSI 100-3:a voidaan pitää teknisenä. BSI-standardi keskittyy käsittelemään teknisiä ja konkreettisia asioita. ISO 17799-standardia voidaan pitää esimerkkinä painotukseltaan hallinnollisesta mallista. ISO 17799-standardi ei keskity teknisiin yksityiskohtiin vaan pitää asiat korkeammalla tasolla. COBITin lähestymistapa on puolestaan prosessi- ja liiketoimintalähtöinen.

Standardeista ei voida yksimielisesti sanoa, mikä niistä on paras, koska jokaisella organisaatiolla on erilainen lähestymistapa tietoturvaan. Joskus voi olla aiheellista käyttää BSI:n standardia, joskus ISO 17799 tai COBITia. Standardin valitseminen riippuu hyvin pitkälti mitä asioita halutaan painottaa. BSI:n standardi on helpoiten lähestyttävä, koska se painottuu hyvin pitkälti teknisiin tarkastuslistoihin. Vaikka ISO 17799-määrittelee myös tarkastuslistanomaisen listan kontrolleja, vaatii niiden syvällinen ymmärtäminen enemmän perehtymistä.

On myös luonnollista, että standardin monimutkaistuessa ja muuttuessa konkreettisemmasta abstraktimpaan muuttuu riskianalyysiprosessin läpivieminen raskaammaksi. Toisaalta analyyttisemmällä ja syvemmällä tarkastelulla voidaan löytää ongelman perimmäiset aiheuttajat eikä vain keskity korjaamaan jo toteutuneita riskejä, vaan ennaltaehkäisemään niiden syntymistä.

6. Riskianalyysimetodiikat

Aiemmin työssä on käsitelty riskianalyysiprosessia yleisellä tasolla. Tämän kappaleen tarkoituksena on esitellä erilaisia metodiikoita viedä riskianalyysiprosessi läpi. Metodiikkojen valinnassa on otettu huomioon standardit, jotka on esitelty standardit-kappaleessa. Standardien lähestymistapa ja rakenne vaikuttaa oleellisesti metodin valitsemiseen. Toisaalta metodiikan valintaa rajoittaa työssä kehitettävä työkalu. Valittavan metodiikan tulee soveltua myös kehitettävän työkalun työtapaviitekehykseksi. Kolmantena kriteerinä metodiikoiden valintaan on työkalun suunniteltu käyttötarkoitus. Työkalu pyritään kehittämään tietoturvakonsultin tai muun asiantuntijan työkaluksi. Edellinen rajoittaa riskianalyysin raskautta. Metodiikaksi pyritään valitsemaan mahdollisimman yksinkertainen ja tehokas työskentelytapa. Tarkemmin käsiteltäviksi metodiikoiksi on valittu potentiaalisten ongelmien analyysi ja OCTAVE.

Käsiteltäviksi harkittiin myös S-vector:ia, Common Criteriaa, CORASta, FRAPia, SPRINT ja SARAa. S-vector –metodi sisältää teknisiä, proseduurisia ja rakenteellisia komponentteja[32]. S-vector soveltuu erityisesti verkkosovellusten tietoturvan arviointiin. FRAP on Thomas Peltierin luoma metodi. Metodin tarkoitus on tarjota organisaatiolle mahdollísuus suorittaa riskianalyysi oman henkilöstön voimin[33]. SPRINT ja SARA ovat

[32] *Barton, Russell R., Hery, William J., Liu Peng, An S-vector for Web Application Security Management*

[33] *Peltier, Thomas, Peltier Associates Facilitated Risk Analysis Process (FRAP), 2003*

Information Security Forumin suosittelemia standardeja (http://securityforum.org). SPRINT muodostuu sanoista Simplified Process for Risk Identification ja SARA puolestaan sanoista Simple to Apply Risk Analysis.

6.1. Potentiaalisten ongelmien analyysi

Potentiaalisten ongelmien analyysia suositellaan käytettäväksi monen tahon toimesta. Potentiaalisten ongelmien analyysi – menetelmää suosittelevat käytettäväksi VAHTI[8] (Valtionhallinnon tietoturvallisuuden johtoryhmä), VTT:n riskianalyysimenetelmäsivustot[34] sekä Pk-yrityksen riskienhallinnan työvälinesarja[35].

Potentiaalisten ongelmien analyysi (POA) jakautuu useaan vaiheeseen. Seuraavaksi kuvataan kuinka analyysivaihetta tulisi valmistella. Tämän jälkeen POA:n vaiheita kuvataan yksityiskohtaisella tasolla.

6.1.1. Analyysin valmistelu

Toteutuksen edellytyksenä on organisaation johdon tuki siten, että analyysiä varten on käytössä tarvittava aika ja resurssit. Potentiaalisten ongelmien analyysin valmistelu aloitetaan rajaamalla tarkastelun kohde. Loppuraportin yhteydessä on syytä dokumentoida riskianalyysin rajaukset. Mahdollisia tarkastelukohteita analyysissa voivat olla seuraavat:

- Tietoturva-arkkitehtuuri
- Tietojen säilyttäminen ja käyttö
- Sovellus tai sovellukset
- Käyttöympäristö (mukaan lukien palvelimet, työasemat ja tietoliikenne)
- Fyysinen ympäristö
- Henkilöstö
- Ulkoisten palveluiden käyttö

---

[34] *VTT-riskianalyysit, Riskianalyysin menetelmät, http://riskianalyysit.vtt.fi/*

[35] *PK-yrityksen riskienhallinta, http://www.pk-rh.com/*

- Hankinnat

Analyysiryhmällä on vetäjä, jolla on merkittävä rooli. Vetäjän ei tarvitse tuntea erityisen hyvin tarkastelukohdetta, vaan hänen tulee tuntea menetelmä (POA) ja ohjata keskustelua tarvittaessa. On todettu, että ulkopuolinen henkilö tai konsultti pystyy johtamaan keskustelua paremmin kuin järjestelmän hyvin tunteva henkilö. Ulkopuolinen pystyy tuomaan uutta näkemystä jo iskostuneeseen ajattelutapaan. Analyysiryhmän vetäjän tehtäviä ovat muun muassa:

- Työryhmän kokoaminen
- Tarvittavan tiedon hankkiminen kohteesta
- Kokousaikataulun ja toteutussuunnitelman laatiminen
- Työryhmän perehdyttäminen analyysimenetelmään (POA)
- Kokousten vetäminen
- Tulosten raportointi ja tiedottaminen
- Jatkotoimenpiteiden suunnittelu ja organisointi

6.1.2. Analyysityöryhmä ja sen perustaminen

Analysointi tehdään suhteellisen pienessä asiantuntijaryhmässä. Analyysiryhmän sopiva koko on vetäjän lisäksi 3-6 henkilöä. Ryhmään valitaan henkilöitä, joilla on aikaa osallistua useisiin analyysikokouksiin. Osallistujien tulisi myös olla avoimia uusille ideoille ja valmiita toimimaan rakentavassa hengessä. Ryhmään valittavat henkilöt vaihtelevat tarkastelukohteesta ja rajauksesta riippuen. Analyysiryhmän jäsenten ei tarvitse olla jokaisen alueen asiantuntijoita, vaan ryhmän kokouksiin voidaan kutsua eri osa-alueiden vierailijoita tarpeen mukaan. Ydinryhmän jäsenien tulisi kuitenkin pysyä mieluiten samana koko analyysin ajan.

6.1.3. Potentiaalisten ongelmien analyysin vaiheet

POA jakautuu karkealla tasolla neljään vaiheeseen. Nämä neljä vaihetta ovat: *Uhkien ja vaarojen tunnistaminen aivoriihessä, Uhkien ja vaarojen arviointi, Toimenpide-*

ehdotusten kehittäminen ja Analyysin raportointi. Alla olevassa taulukossa on kuvattu vaiheita ja niiden sisältöä(Taulukko 6).

Taulukko 6: POA:n vaiheet.

Vaihe	Kuvaus vaiheesta	Vaiheen tuloste
Uhkien ja vaarojen tunnistaminen aivoriihessä	Osa 1: Hiljainen aivoriihi	Vaaraluettelo
	Osa 2: Keskustelumuotoinen aivoriihi	
Uhkien ja vaarojen arviointi	Osa1: Jatkokäsiteltävien uhkien valinta	Alustavat riskianalyysilomakkeet (uhkat ja vaarat syineen ja seurauksineen sekä riskien arviointi lomakkeelle kirjattuna)
	Osa 2: Käsiteltäväksi valittujen uhkien syiden ja seurausten selvittäminen ja riskin suuruuden arviointi	
Toimenpide-ehdotusten kehittäminen	Tämä vaihe voidaan käsitellä arviointivaiheen yhteydessä tai erillisissä kokouksissa	Lopulliset analyysilomakkeet
Analyysin raportointi		Loppuraportti, jonka liitteenä on uhka- ja vaaraluettelot ja analyysilomakkeet

Uhkien ja vaarojen tunnistaminen aivoriihessä

Tunnistamisvaihe jakautuu POA:ssa kahteen osaan. Ensimmäinen vaihe on hiljainen aivoriihi. Hiljaisessa aivoriihivaiheessa idealomaketta kierrätetään analyysiryhmän jäsenien kesken. Jokainen jäsen saa idea-lomakkeen ja kirjaa siihen kolme uhkaa tai ongelmaa. Tämän jälkeen lomake kierrätetään seuraavalle jäsenelle. Kun jäsen on lukenut idea-lomakkeen kolme kohtaa täyttää hän lomakkeeseen kolme uhkaa tai ongelmaa lisää. Lomakkeita kierrätetään kunnes lomakkeet ovat täynnä tai ideat tyrehtyvät. Yleensä hiljaisen aivoriihen aikana ei puhuta uhkista. Ainoastaan vetäjä ohjaa lomakkeiden kierrättämistä tai esittelee mahdollisia avainsanoja ideoinnin avuksi.

Toisessa vaiheessa siirrytään keskustelumuotoiseen aivoriiheen. Keskustelumuotoisessa aivoriihessä keskustellaan esiintyneistä uhkista tai ongelmista. Tässä vaiheessa on myös mahdollista kirjata lisää uhkia. Vaiheen tarkoitus ei ole kuitenkaan vielä analysoida uhkia tai ongelmia tarkemmin.

Molemmissa aivoriihissä kunnioitetaan aivoriihen periaatteita kuten vapaamielisyyttä uusia ideoita kohtaan, villejä ideoita ja sitä että toisten ideoita ei arvostella, syytellä tai selitellä. Uhkien ja vaarojen tunnistamisvaiheen tuotoksena syntyy vaaraluettelo, jota käytetään hyväksi seuraavissa vaiheissa.

Uhkien ja vaarojen arviointi

Uhkien ja vaarojen arviointi jakautuu kahteen osaan. Ensimmäisessä osassa pyritään luokittelemaan tunnistamisvaiheessa saatuja uhkia tai ongelmia.

1. vaihe: Ideoiden luokittelu

Karsintaa suoritetaan sellaisille, jotka ovat lähes mahdottomia, epätodennäköisiä tai eivät koske tarkastelukohdetta. Uhkat tai ongelmat voidaan lajitella esimerkiksi kolmeen luokkaan:

1. Jatkokäsittelyä edellyttävät uhkat
2. Vanhat ja luotettavasti hoidossa olevat uhkat
3. Vailla käytännön merkitystä olevat uhkat

Vaikka kaikkia uhkia ei käsitellä yksityiskohtaisesti analyysivaiheessa, niin niitä ei kuitenkaan saa hylätä kokonaan, vaan ne voidaan kirjata esimerkiksi osaksi loppuraporttia.

2.vaihe: Uhkien arviointi ja riskiluvun määritys

Ideoiden luokitteluvaiheessa jatkokäsittelyyn määriteltyjä uhkia tarkastellaan yksityiskohtaisessa analyysityöryhmässä. Analyysin vetäjän tehtävä on esitellä kukin jatkokäsiteltävä uhka yksitellen ja johtaa myös puheita. Ensin arvioidaan kullekin uhkalle mahdollinen tilanne, jossa se voisi toteutua. Tarkoituksena on tunnistaa syitä, tilanteita ja olosuhteita, joissa uhka mahdollisesti toteutuisi. Uhkan kuvauksien jälkeen uhkille arvioidaan tapahtumisen todennäköisyys ja seurauksien vakavuus. Näiden tulona saadaan riskiluvut ja tällöin uhkat konkretisoituvat riskeiksi.

Toimenpide-ehdotusten kehittäminen

Toimenpide-ehdotukset riskien lieventämiseksi voidaan tehdä arviointi-/analyysivaiheen yhteydessä.

Raportointi

Analyysilomakkeiden lisäksi on hyvä laatia loppuraportti, josta voidaan todeta mitä on tehty, miten on tehty, ketkä ovat osallistuneet analyysiin, analyysin keskeiset tuotokset ja jatkosuunnitelmat. Potentiaalisten ongelmien analyysin analyysilomake on esitetty liitteessä(Liite 1).

6.2. OCTAVE

OCTAVE on CERT Coordination Centerin (CERT/CC) kehittämä tieturvariskien arviointimenetelmä[21]. CERT/CC on osa SEI:tä (engl. Software Engineering Institute). SEI on kansallisesti tuettu tutkimus- ja kehityskeskus ohjelmistokehitykselle. CERT/CC puolestaan ohjeistaa Internet-sivustojen tietoturvassa sekä tarjoaa työkaluja ja tekniikoita järjestelmien turvaamiseksi hyökkääjiltä.

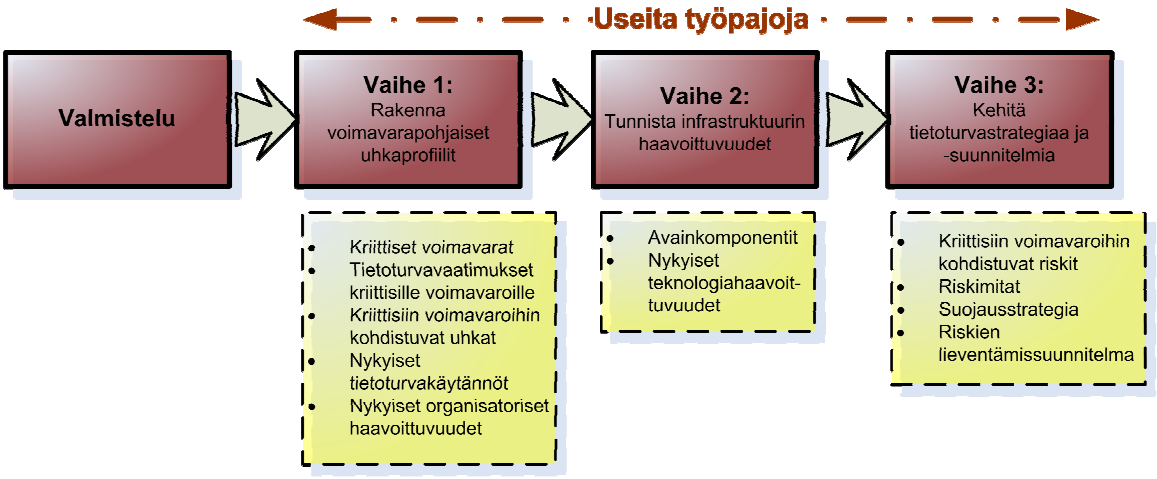
OCTAVE muodostuu englanninkielen sanoista Operationally Critical Threat, Asset, and Vulnerability Evaluation. Vapaasti suomennettuna OCTAVE on operatiivisesti kriittisten uhkien, voimavarojen ja haavoittuvuuksien arviointimenetelmä. OCTAVEn lähestymistapa määrittelee järjestelmällisen ja organisaationlaajuisen tietoturvariskein arviointimenetelmän, joka käyttää useita eri metodeja. Käytetyt metodit ovat linjassa ja yhdenmukaisia OCTAVEn lähestymistavan kanssa.

OCTAVE-metodin lähestymistapa on kolmivaiheinen. Vaiheet ovat:

1. *Rakenna voimavarapohjaiset uhkaprofiilit (engl. Build Asset-Based Threat Profiles)*
2. *Tunnista infrastruktuurin haavoittuvuudet (engl. Identify Infrastructure Vulnerabilities)*
3. *Kehitä tietoturvastrategiaa ja –suunnitelmia (engl. Develop Security Strategy and Plans)*

Näissä vaiheissa keskitytään tarkastelemaan organisatorisia sekä teknologisia asioita. Tarkoituksena on myös koota ymmärrettävä kokonaiskuva organisaation tietoturvatarpeista. Koko prosessi sisältää useita työpajoja, joista jokainen vaatii osallistujien yhteistyötä ja vuorovaikutusta.

Ylätasolla OCTAVE jakautuu kolmeen vaiheeseen, jotka edelleen jakautuvat kahdeksaan prosessiin. Ensimmäisessä vaiheessa on neljä, toisessa vaiheessa kaksi ja kolmannessa vaiheessa on kaksi prosessia. Alla on kuva OCTAVE-menetelmän vaiheista(Kuva 7).



Kuva 7: OCTAVE-menetelmän vaiheet.

Yllä olevassa kuvassa on tiivistetty kunkin vaiheen keskeisimmät tavoitteet(Kuva 7, kuvassa keltaisissa katkoviivalaatikoissa). Vaiheissa 1-3 pidetään useita työpajoja. Työpajoja on kahdenlaisia: 1. fasilitoituja keskustelusessioita eri organisaation jäsenten kanssa ja 2. työpajoja, joihin osallistuu vain analyysiryhmän jäsenet, tarkoituksenaan suorittaa erilaisia aktiviteetteja ainoastaan analyysiryhmän voimin.

Työpajoissa on nimetty johtaja sekä kirjuri. Johtajan tai vetäjän tehtävänä on valita työpajassa käytettävä päätöksentekotapa (esim. äänestys, yhteisymmärrys) ja varmistaa, että osallistujat ymmärtävät roolinsa ja ovat kykeneviä osallistumaan pajatoimintaan. Vetäjän ei tarvitse olla sama henkilö kaikissa työpajoissa. Kirjurin tehtävä on tehdä työpajasta pöytäkirja ja kirjata oleelliset päätökset. Seuraavaksi käsitellään kuvassa esitetyt vaiheet yksityiskohtaisella tasolla(Kuva 7).

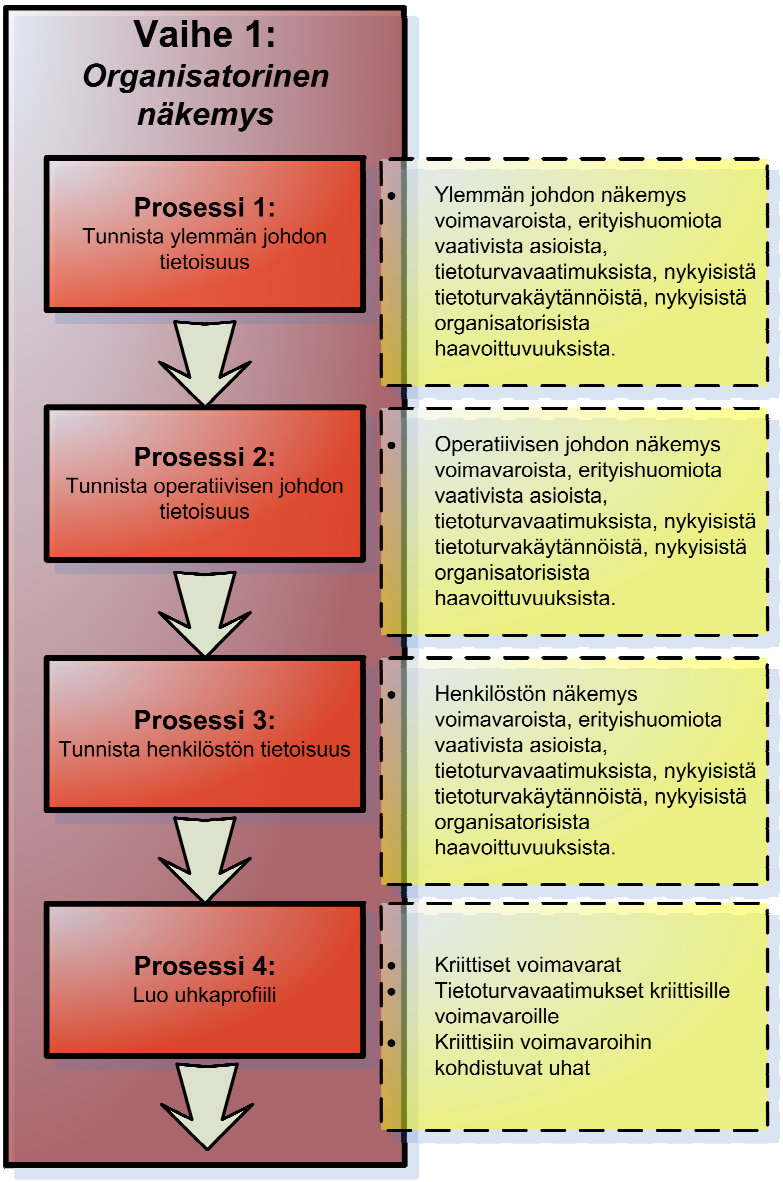
6.2.1. Valmistelu

Ennen koko prosessin aloittamista tulee suorittaa valmistelut OCTAVEa varten. Valmistelu edellyttää ylemmän johdon sitouttamista, analyysiryhmän nimeämistä, asianmukaisen rajauksen linjaamista OCTAVE-menetelmää varten ja osallistujien valitsemista. Edellä mainitut toimet on esitetty yllä olevassa kuvassa Valmistelu-laatikolla(Kuva 7).

Johdon sitouttaminen ja tuki on kriittistä, jotta OCTAVEn läpiviemistä varten on käytettävissä tarvittavat resurssit ja osallistuva henkilöstö on myös sitoutunutta. Analyysitiimin jäsenillä tulee olla tarvittava tieto ja osaaminen prosessin läpiviemiseksi. Analyysitiimin jäseniltä vaaditaan myös kykyä tunnistaa tilanteet, joihin vaaditaan lisäosaamista tarvittavan tiedon saamiseksi/ymmärtämiseksi. Tarkastelulaajuus tulee rajata käsittämään operatiivisesti tärkeät alueet. Tarkastelulaajuus ei saa kuitenkaan olla liian laaja, koska analyysi jää liian pinnalliseksi ja analyysitiimin on hankala analysoida kaikkea informaatiota. Liian suppea tarkastelulaajuus puolestaan vähentää analyysin tulosten merkityksellisyyttä. Tiedon ja ongelmien keräämistä varten toimiviin työpajoihin tulee valita osallistujat. Osallistujien tulee olla eri organisaatiotasoilta, jotta tietoa saadaan kaikilta oleellisilta organisaatiotasoilta. Osallistujat tulee valita tarkoin heidän tietojensa ja osaamisalueidensa perusteella. Seuraavassa kappaleessa käsitellään OCTAVEn ensimmäinen vaihe.

6.2.2. Vaihe 1

Kuten aiemmin mainittu, muodostuu OCTAVEn ensimmäinen vaihe neljästä prosessista. Alla on kuva ensimmäisen vaiheen sisällöstä ja prosessien ylätason kuvauksista (Kuva 8).



Kuva 8: OCTAVE-menetelmän 1. vaiheen prosessit ja niiden kuvaukset.

OCTAVE-menetelmän ensimmäisen vaiheen prosessit ovat: *Tunnista ylemmän johdon tietoisuus*, *Tunnista operatiivisen johdon tietoisuus*, *Tunnista henkilöstön tietoisuus* ja *Luo uhkaprofiili*.

Prosessit 1-3

Kolme ensimmäistä prosessia keskittyvät tunnistamaan asioita ja keräämään tietoa eri organisaatiotasoilta. Vaiheiden aikana pidetään useita työpajoja, joiden kesto on kahdesta kolmeen tuntiin. Työpajojen vetovastuu on analyysitiimillä. Työpajoihin osallistuu eri

organisaatiotasoilta ihmisiä riippuen käsiteltävästä prosessialueesta. Prosessialuekohtaiset osallistujatahot ovat seuraavat:

- Prosessi 1: Ylempi johto
- Prosessi 2: Operatiivinen johto
- Prosessi 3: Yleinen henkilöstö, informaatioteknologiahenkilöstö

On huomattava, että yleinen henkilöstö ja IT-henkilöstö osallistuvat omiin erillisiin työpajoihin. Täten IT-henkilöstön työpajoissa voidaan keskittyä teknisempiin yksityiskohtiin.

Kolmen ensimmäisen prosessialueen tarkoituksena on *tunnistaa voimavarat*, *erityishuomiota vaativat asiat*, *tietoturvavaatimukset tärkeimmille voimavaroille* ja *kerätä tieto nykyisistä tietoturvakäytännöistä ja organisatorisista haavoittuvuuksista*. Seuraavaksi käsitellään nämä neljä osa-aluetta.

Tunnista voimavarat

Osallistujat tunnistavat organisaation voimavarat ja valitsevat niistä tärkeimmät. Osallistujat rationalisoivat ja keskustelevat syistä miksi he arvottivat juuri nämä voimavarat tärkeimmiksi. Voimavarat voidaan esimerkiksi jakaa seuraaviin ryhmiin: järjestelmät, tieto, sovellukset, laitteistot ja ihmiset.

Tunnista erityishuomioita vaativat asiat

Osallistujat pyrkivät tunnistamaan skenaarioita, jotka uhkaavat tärkeimpiä voimavaroja. Uhkakäsittelyssä keskitytään tarkastelemaan uhkien lähteitä ja seurauksia. Ryhmän kesken keskustellaan myös skenaarioiden potentiaalisista vaikutuksista organisaatiolle. Uhkien lähteitä voivat olla muun muassa seuraavat: tahalliset ja tahattomat ihmisten teot, järjestelmän ongelmat ja muut ongelmat. Seurauksia puolestaan ovat tiedon paljastuminen, voimavaran muuttuminen, menetys tai tuhoutuminen ja saatavuuden kärsiminen keskeytyksen takia.

Tunnista tietoturvavaatimukset tärkeimmille voimavaroille

Osallistujat tunnistavat tietoturvavaatimuksia tärkeimmille voimavaroille. Tämän lisäksi he arvioivat vaatimuksien hyviä ja huonoja puolia ja valitsevat näiden perusteella vaatimuksista tärkeimmät. Tietoturvavaatimukset koskevat tyypillisesti luottamuksellisuutta, eheyttä tai käytettävyyttä (tietoturvan kulmakivet). Tunnistaminen tehdään kahdessa vaiheessa:

1. Tunnista tietoturvavaatimukset jokaiselle tärkeälle voimavaralle
2. Priorisoi tietoturvavaatimuksia.

Kerää tieto nykyisistä tietoturvakäytännöistä ja organisatorisista haavoittuvuuksista

Osallistujat täyttävät kyselomakkeen, jolla selvitetään mitä tietoturvakäytäntöjä noudatetaan henkilöstön toimesta ja mitä ei. Kyselyn perustuu kerättyyn luetteloon hyvistä tietoturvakäytännöistä. Kyselyosuuden jälkeen osallistujat keskustelevat olemassa olevista tietoturvakäytännöistä ja haavoittuvuuksista tai heikkouksista, joita organisaatiossa on. Haavoittuvuudet ja heikkoudet voivat johtua puutteellisista tietoturvakäytännöistä tai niiden puuttumisesta kokonaan.

Prosessi 4: Luo uhkaprofiili

OCTAVE-menetelmän 1.vaiheen kolme ensimmäistä prosessivaihetta käsittelivät samoja asioita, mutta näkökulmataso vaihteli organisatorisesti. Uhkaprofiilin luomisvaiheessa yhdistetään ja analysoidaan tiedot, jotka kerättiin kolmen ensimmäisen vaiheen aikana.

Koko prosessi neljä on erittäin tärkeä, koska tämä asettaa rajauksen koko lopulle arvioinnille. Kriittisiä voimavaroja käytetään tarkastelun kohteena infrastruktuurin arvioimisessa vaiheessa 2, ja jos uhkaprofiileja käytetään riskianalyysin pohjana riskianalyysissä vaiheessa 3.

Prosessi 4 jakautuu karkeasti neljään vaiheeseen: *prosessivaiheissa 1-3 kerättyjen tietojen analysointi ja yhdistäminen*, *kriittisten voimavarojen valinta*, *kriittisille*

voimavaroille asetettujen tietoturvavaatimusten jatkojalostaminen ja *kriittisiin voimavaroihin kohdistuvien uhkien tunnistaminen*.

Aikaisemmissa prosessivaiheissa kerättyjen tietojen analysointi ja yhdistäminen
Eri vaiheiden tietojen yhdistämisprosessi mahdollistaa epäjohdonmukaisuuksien tunnistamisen eri organisaatiotasojen tai yksilöiden välillä. Analysoinnissa on myös tärkeää rakentaa globaali kuva tärkeistä voimavaroista. Tämä tapahtuu analysoimalla ja vetämällä yhteen eri organisaatiotasojen ja yksilöiden tuotokset. Yhdistely/-analyysivaihe (eli esivalmistelut, joissa valmistellaan prosesseissa 1-3 kerättyä materiaalia) sisältää seuraavat aktiviteetit:

1. Ryhmitä voimavarat organisaatiotason mukaan
2. Ryhmitä tietoturvavaatimukset organisaatio ja voimavarojen mukaan
3. Ryhmitä erityishuomiota vaativat asiat ja niiden vaikutukset organisaatiotason ja voimavaran mukaan

Kriittisten voimavarojen valinta
Riippuen organisaation koosta voi prosesseissa 1-3 tunnistettujen voimavarojen määrä olla jopa satoja. Jotta analyysin tekeminen olisi mahdollista ja tulokset eivät jäisi pinnallisiksi, tulee voimavaroista valita kriittisyyden perusteella tarkasteltavaksi vain muutama. Valintakriteerinä voimavaroille on organisaation mission ja liiketoimintatavoitteiden saavuttaminen. Valitut voimavarat ovat ainoat analysoitavat voimavarat myöhemmissä vaiheissa. Kriittisten voimavarojen valinta suoritetaan kolmessa vaiheessa:

1. Tunnista kriittiset voimavarat
2. Dokumentoi kriittisten voimavarojen valintaperusteet
3. Dokumentoi jokaisen kriittisen voimavaran kuvaus

Kriittisten voimavarojen tietoturvavaatimusten jatkojalostaminen
Tämä vaihe voi olla vaikea monelle analyysitiimille, koska se vaatii jokaiselle kriittiselle voimavaralle tietoturvavaatimusten määrittämistä keskittyen organisaation näkökulmaan. Analyysitiimin haasteena ovat aikaisempien työpajojen tuloksien ristiriitaisuudet ja aukot

tiedoissa. Tehtävä on jatkojalostaa ja konkretisoida tietoturvavaatimukset voimavaroille. Tämä alivaihe jakautuu kahteen vaiheeseen:

1. Kuvaa ja dokumentoi jokaisen kriittisen voimavaran tietoturvavaatimukset
2. Priorisoi jokaisen kriittisen voimavaran tietoturvavaatimukset

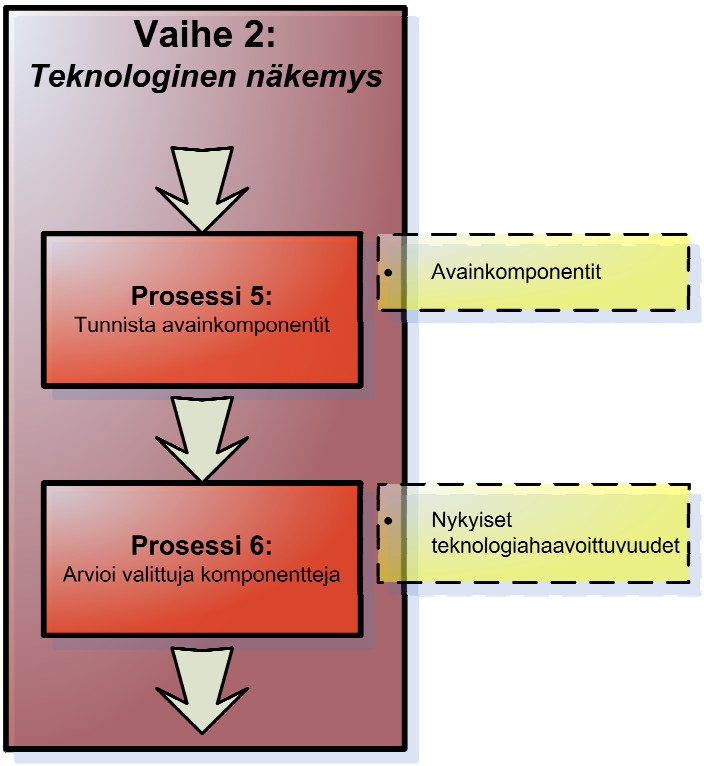
Kriittisiin voimavaroihin kohdistuvien uhkien tunnistaminen

Tämä on 1.vaiheen neljännen prosessin viimeinen vaihe. Vaiheen tarkoituksena on etsiä ja tutkia mahdollisia uhkia, jotka kohdistuvat jo valittuihin kriittisiin voimavaroihin. Tässä vaiheessa suoritetaan aukkoanalyysi (engl. Gap Analysis) erityishuomiota vaativille asioille. Tämän analyysin tuotoksena syntyy täydellinen uhkaprofiili jokaiselle kriittiselle voimavaralle. Uhkien tunnistaminen jakautuu edelleen kolmeen vaiheeseen:

1. Sovita erityishuomiota vaativat asiat yleiseen uhkaprofiiliin
2. Suorita aukkoanalyysi
3. Tarkista uhkaprofiilien yhtenäisyys ja perinjuurisuus (engl. Consistency and Completeness)

6.2.3. Vaihe 2

OCTAVEn toista vaihetta kutsutaan myös nimellä teknologinen näkemys, koska tässä vaiheessa keskitytään organisaation laskentainfrastruktuuriin (engl. Computing Infrastructure). Vaihe käsittää kaksi prosessia: *Tunnista avainkomponentit* ja *Arvioi valittuja komponentteja*. Alla olevassa kuvassa on kuvattu toisen vaiheen prosessit ja niiden ylätason kuvaukset (Kuva 9). Seuraavaksi käsitellään vaiheen prosessit.



Kuva 9: OCTAVE-menetelmän 2. vaiheen prosessit ja niiden kuvaukset.

Prosessi 5: Tunnista avainkomponentit

Siinä missä prosessissa 4 luotiin voimavarakohtaiset uhkaprofiilit, mietitään prosessissa 5 näiden tietojen pohjalta miten arvioida organisaation laskentaympäristöä teknologiahaavoittuvuuksien osalta. Jotta pystytään tunnistamaan todelliset riskit, tulee tässä prosessissa keskittyä arvioimaan niitä infrastruktuurin avainkomponentteja, jotka liittyvät jo määriteltyihin kriittisiin voimavaroihin. Haavoittuvuuksista kerätään tietoa vain niiden komponenttien osalta, jotka liittyvät kriittisiin voimavaroihin. Tämän prosessivaiheen tarkoitus on tunnistaa nämä avainkomponentit.

Tämä prosessi viedään läpi työpajojen avulla, joihin osallistuu ainakin analyysitiimi. Tarvittaessa työpajoihin otetaan mukaan teknologia-asiantuntijoita vastaamaan ja pohtimaan yksityiskohtaisia teknologiaongelmia ja –haavoittuvuuksia. Prosessi jakautuu kahteen aktiviteettiin: *Tunnista komponenttien pääluokat* ja *Tunnista tutkittavat infrastruktuurikomponentit*. Nämä aktiviteetit käsitellään seuraavaksi.

Tunnista komponenttien pääluokat

Tämän aktiviteetin puitteissa tarkastellaan kriittisiä voimavaroja ja uhkia ensimmäisestä vaiheesta. Näitä pyritään edelleen suhteuttamaan organisaation laskentaympäristöön. Tietoverkkoyhteysteitä tarkastellaan uhkaskenaariopohjalta, jotta voidaan tunnistaa tärkeät komponenttiluokat kriittisille voimavaroille. Käytännössä infrastruktuurin komponenttien ja kriittisten voimavarojen yhteyttä tarkastellaan ja pyritään tunnistamaan kriittiset komponentit.

Tarkastelussa rakennetaan uhkapuita, joiden toimija on käyttäjä. Erityistarkastelussa on tietoverkkoyhteystiet (engl. Network Access Paths). Käyttäjälähtöinen uhkapuu auttaa tunnistamaan tahallisen hyväksikäytön uhkaskenaariot, jotka kohdistuvat kriittisiin voimavaroihin teknologisten haavoittuvuuksien kautta. Tämä aktiviteetti sisältää kaksi alivaihetta:

1. Tunnista järjestelmä/-t, jotka liittyvät läheisesti kriittiseen voimavaraan
2. Tunnista komponenttien avainluokat

Tunnista tutkittavat infrastruktuurikomponentit

Tämän aktiviteetin tarkoituksena on tunnistaa tutkittavat infrastruktuurikomponentit. On muistettava keskittyä rajaamaan tarkastelu harvoihin ja kriittisimpiin. Tämä aktiviteetti jatkaa edellisen aktiviteetin työtä. Tunnistetuista komponenttien pääluokista tunnistetaan ja valitaan avainkomponentit teknologiahaavoittuvuustarkastelua varten.

Tämän aktiviteetin tavoitteena on tunnistaa riittävästi komponentteja kustakin komponenttiluokasta. Valittujen komponenttien perusteella tulisi olla mahdollista muodostaa ymmärrys koko laskentaympäristön nykyisistä haavoittuvuuksista. Aktiviteetti sisältää kaksi alivaihetta:

1. Valitse tarkasteltavat komponentit
2. Valitse lähestymistapa ja haavoittuvuustyökalut

Prosessi 6: Arvioi valittuja komponentteja

Prosessi 6 sisältää tiedonkeräämis- ja analysointitehtäviä. Ennen tätä prosessia on tunnistettu kriittiset voimavarat, voimavaroihin kohdistuvat uhkat, nykyiset tietoturvakäytännöt ja nykyiset organisatoriset haavoittuvuudet. Tämä prosessi keskittyy tarkastelemaan tarkemmalla tasolla valittuja infrastruktuurikomponentteja.

Prosessi 6 poikkeaa muista prosesseista, koska työpajatyöskentelyn aloittaminen edellyttää massiivisen teknisen haavoittuvuustarkastelun läpiviemistä. Nämä tekniset toimet sisältävät muun muassa haavoittuvuustyökalujen ajamista avainkomponentteja vasten. Prosessi muodostuu kahdesta alivaiheesta: *Haavoittuvuustyökalujen ajamisesta* ja *Teknologiahaavoittuvuuksien läpikäynnistä ja yhteen vetämisestä*.

Haavoittuvuustyökalujen ajaminen

Tässä alivaiheessa ajetaan haavoittuvuustyökalut, jotka valittiin prosessissa 5. Haavoittuvuustyökalut ajetaan valittuja komponentteja vasten. Tässä vaiheessa alustavasti tarkastellaan yksityiskohtaisia haavoittuvuusraportteja avainkomponenttikohtaisesti. Yksityiskohtaisista raporteista työstetään haavoittuvuustiivistelmät komponenttikohtaisesti, joissa on esimerkiksi listattu haavoittuvuuden nimi, kuvaus, vakavuus ja mahdolliset korjaustoimet. On huomioitava, että tämä vaihe vaatii erityisosaamista ja nämä henkilöt vievät tämän aktiviteetin läpi. Tämän aktiviteetin läpivieminen voi edellyttää organisaation ulkopuolista apua. Tarkemmalla tasolla tämä aktiviteetti jakautuu kahteen alivaiheeseen:

1. Haavoittuvuustyökalujen ajaminen
2. Haavoittuvuusraporttitiivistelmien valmistelu

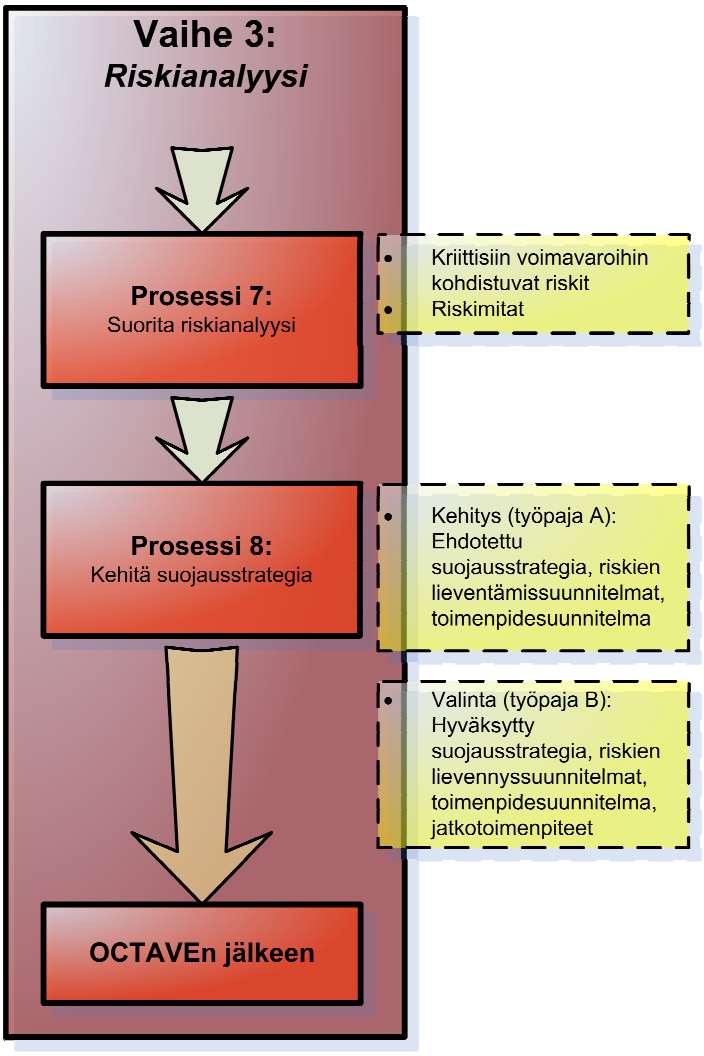
Teknologiahaavoittuvuuksien läpikäyminen ja yhteen vetäminen

Edellinen aktiviteetti edellytti informaatioteknologian ja tietoturvan erityisosaamista. Tämän aktiviteetin puitteissa teknologiahaavoittuvuudet käydään läpi ja vedetään yhteen analyysiryhmän voimin. Tämä aktiviteetti vaatii myös tehokasta kommunikointia teknologisista asioista ihmisille, jotka eivät välttämättä ole niin teknologiaorientoituneita.

Aktiviteetin toisena vaatimuksena on kyky ajatella teknologiatiedon merkityksestä organisaatiolle. Kriittisten voimavarojen uhkaprofiilit on myös syytä käydä läpi mahdollisten muutosten tai uusien uhkakuvien takia. On syytä myös tarkastella kriittisesti nykyisiä tietoturvakäytäntöjä ja organisatorisia haavoittuvuuksia.

6.2.4. Vaihe 3

OCTAVEn kolmannessa ja viimeisessä vaiheessa analyysitiimi tunnistaa organisaation kriittisiin voimavaroihin kohdistuvat riskit ja päättää miten näiden lieventämiseksi tulisi toimia. Analyysitiimi luo aikaisemmissa vaiheissa kerättyjen tietojen pohjalta suojautumisstrategian ja riskien lievennyssuunnitelman. Kolmas vaihe sisältää kaksi prosessia: *Suorita riskianalyysi* ja *Kehitä suojausstrategia*. Kolmas vaihe ja sen prosessit ylätason kuvauksineen on esitetty alla olevassa kuvassa(Kuva 10). Seuraavaksi siirrytään käsittelemään vaiheen kolme prosesseja.



Kuva 10: OCTAVE-menetelmän 3. vaiheen prosessit ja niiden kuvaukset.

Prosessi 7: Suorita riskianalyysi

Riskianalyysiprosessi viedään työpajojen avulla läpi. Työpajoihin osallistuu analyysiryhmä ja mahdollisesti analyysiryhmän ulkopuolisia asiantuntijoita. Jäseniltä vaaditaan ymmärrystä organisaation liiketoimintaympäristöstä, organisaation informaatioteknologiaympäristöstä, hyviä analyyttisiä taitoja ja hyvää kommunikointikykyä.

Riskianalyysiprosessi jakautuu kolmeen aliaktiviteettiin, jotka ovat:

1. Tunnista uhkien vaikutus kriittisiin voimavaroihin
2. Luo riskien arviointikriteeristö
3. Arvioi uhkien vaikutusta kriittisiin voimavaroihin

Seuraavaksi käsitellään riskianalyysiprosessin aktiviteetit.

Tunnista uhkien vaikutus kriittisiin voimavaroihin

Tämän aktiviteetin tarkoituksena on määritellä tarkalla tasolla uhkien/uhkakuvien mahdolliset vaikutukset kriittisiin voimavaroihin. Vaikutuksia ovat muun muassa tiedon paljastuminen, muuttuminen, katoaminen, tuhoutuminen ja keskeytys (engl. Interruption). Vaikutuksen kuvaus on kerronnallinen lausunto, joka kuvaa kuinka uhkan mahdollinen toteutuminen äärimmillään vaikuttaa organisaation tehtävään. Vaikutuskuvaukset liittävät voimavarat, uhkat ja organisaatiolle tärkeä asiat toisiinsa. Tämä aktiviteetti edelleen jakautuu kahteen alivaiheeseen:

1. Kerättyjen tietojen läpikäyminen
2. Kerronnallisten vaikutuskuvauksien luominen

Luo riskien arviointikriteeristö

Analyysiryhmä määrittelee tässä aktiviteetissä arvioinnissa käytettävät arviointikriteeristöt. Arviointikriteeristöt määrittelevät mitä tarkoitetaan suurella, keskinkertaisella tai pienellä vaikutuksella. Esimerkiksi yksi suuren riskin määritys voi olla, että organisaatio menettää 30 % kaikista asiakkaistaan. Kriteeristö on riippuvainen tarkastelukohteen rajauksesta. Tämä aktiviteetti jakautuu kahteen alivaiheeseen:

1. Tiedon läpikäyminen
2. Arviointikriteeristön määrittely

Arvioi uhkien vaikutusta kriittisiin voimavaroihin

Tässä aktiviteetissa uhkat konkretisoituvat riskeiksi. Uhka ja sen vaikutus muodostavat riskin. Aikaisemmin työssä on esitelty riskin määritelmä, joka oli että riski on uhkan todennäköisyyden ja sen seurausten vakavuuden tulo. Tässä aktiviteetissa analyysiryhmä käy läpi jokaisen riskin ja asettaa arvon edellisen aktiviteetin arviointikriiteristöjen mukaisesti (esim. keskinkertainen riski). Aktiviteetti jakautuu kahteen alivaiheeseen:

1. Tiedon läpikäyminen
2. Riskin vaikutuksen arviointi

Prosessi 8: Kehitä suojausstrategia

OCTAVE-menetelmän viimeinen prosessi muodostuu kahdesta työpajasta. Ensimmäiseen työpajaan osallistuvat analyysitiimin jäsenet sekä valitut organisaation jäsenet. Prosessin kokonaistavoite on kehittää suojautumisstrategia organisaatiolle, riskien lievennyssuunnitelmat riskeille, jotka kohdistuvat kriittisiin voimavaroihin, ja lähiaikoina tehtävät aktiviteetit. Seuraavaksi käsitellään prosessin kahdeksan työpajat: *Suojausstrategian kehitystyöpaja A* ja *Suojausstrategian kehitystyöpaja B*.

Suojaustrategian kehitystyöpaja A

Valmistelu

Valmisteluna tälle työpajalle tulee kerätä kyselyjen tulokset, jotka täytettiin OCTAVEn ensimmäisen vaiheen prosesseissa 1-3. Tämän lisäksi prosesseissa 1-3 tunnistetut tietoturvakäytännöt ja organisaation haavoittuvuudet tulee analysoida, jaotella ja yhdistellä organisaatiotason mukaan. Valmisteluvaihe jakautuu kahteen osaan: Kyselyjen tulosten yhteen vetäminen, Suojausstrategiainformaation analysointi ja yhteen vetäminen.

Kyselyjen tulokset vedetään yhteen ja raportista on nähtävissä kuinka eri organisaatiotasoilla tiedostetaan eri asiat. Kyselyn perusteella saadaan muun muassa selville henkilöstön tietoisuus ja mahdollisesti koulutustarpeet tietoturvakäytäntöihin tai osa-alueille.

Tunnistetut organisaation haavoittuvuudet pyritään myös jaottelemaan organisaatiotasoisesti. Esimerkkinä operatiivisen johdon tason organisaation haavoittuvuudesta voisi olla puutteellinen IT-henkilöstön koulutus.

Työpajatyöskentely

Työpaja sisältää neljä aktiviteettiä, joiden kuvaukset on esitetty alla olevassa taulukossa (Taulukko 7).

Taulukko 7: Suojausstrategian kehitystyöpaja A:n aktiviteetit.

Aktiviteetti	Kuvaus
Riskitiedon läpikäyminen	Jokainen analyysiryhmän jäsen käy itsenäisesti läpi seuraavat koko prosessissa tuotetut tiedot: 1. Kriittisiin voimavaroihin kohdistuvat uhat 2. Erityishuomiota vaativat asiat, koskien kriittisiä voimavaroja 3. Nykyiset tietoturvakäytännöt ja organisatoriset haavoittuvuudet 4. Potentiaalisten uhkien ja riskien vaikutukset organisaatioon 5. Valittujen komponenttien teknologiahaavoittuvuudet 6. Infrastruktuurihaavoittuvuusarvioinnin suositellut toimet
Suojausstrategian luominen	Analyysitiimi luo organisaatiolle suojausstrategiaehdotelman. Suojausstrategia määrittelee ne strategiat, joita organisaatio käyttää mahdollistaakseen, aloittaakseen, toteuttaakseen ja ylläpitääkseen omaa sisäistä tietoturvaa.
Riskien lievennyssuunnitelmien luominen	Analyysitiimi luo riskien lievennyssuunnitelman kriittisille voimavaroille. Lievennyssuunnitelma määrittelee vaadittavat toimenpiteet kriittiseen voimavaraan kohdistuvien riskin lieventämiseksi riski-/uhkakohtaisesti.
Aktiviteettilistan luominen	Analyysitiimi luo aktiviteettilistan. Aktiviteettilista määrittelee lähiaikojen toimet, joita organisaation henkilöt voivat ilman erikoiskoulutusta, politiikkamuutoksia jne.

Suojausstrategian kehitystyöpaja B

Valmistelu

Valmisteluna toiselle työpajalle tulee valmistella esitys ylemmälle johdolle. Tehtävä on haasteellinen, koska ylemmällä johdolla on rajoitetusti aikaa käytettäväksi tällaiseen toimintaan. Ylemmälle johdolle pidettävän esityksen olisi hyvä olla mitoitettu tuntiin tai kahteen. Esitys jakautuu kahteen osaan. Ensimmäinen osa tiivistää riskitiedot, jotka kerättiin arvioinnin aikana ja toinen osa esittelee tulokset ja suojausstrategian, riskienlievennyssuunnitelman ja aktiviteettilistan ominaisuudet.

Työpajatyöskentely

OCTAVE-menetelmän viimeinen työpaja sisältää alla olevassa taulukossa esitetyt aktiviteetit(Taulukko 8). Työpajaan osallistuu organisaation ylempi johto.

Taulukko 8: Suojausstrategian kehitystyöpaja B:n aktiviteetit.

Aktiviteetti	Kuvaus
Riskitietojen esittäminen	Ylemmälle johdolle esitetään seuraavat OCTAVE-prosessin aikana kerätyt asiat: 1. Nykyiset tietoturvakäytännöt ja organisaation haavoittuvuudet 2. Tiedot voimavaroista 3. Kriittisten voimavarojen riskiprofiilit
Suojausstrategian, lievennyssuunnitelmien ja aktiviteettilistan läpikäyminen ja jalostaminen	Suojausstrategia, riskien lievennyssuunnitelmat ja aktiviteettilista esitetään ylemmälle johdolle. Ylempi johto halutessaan muuttaa tai jalostaa näitä.
Seuraavien askelten luominen	Ylempi johto päättää kuinka suojausstrategia, riskien lievennyssuunnitelmat ja aktiviteettilista pannaan toimeen. Ylempi johto määrittelee: 1. Mitä tapahtuu ja mitä askeleita otetaan arvioinnin jälkeen 2. Kuka on vastuussa näistä toimista 3. Milloin nämä toimet aloitetaan ja milloin ne ovat valmiit

6.3. Yhteenveto menetelmistä

Tämän kappaleen puitteissa käsiteltiin tarkemmin kaksi mahdollista analyysimetodiikkaa tietoturva-analyysin viitekehykseksi. Käsitellyt metodiikat ovat potentiaalisten ongelmien analyysi ja OCTAVE. Metodiikat poikkeavat toisistaan huomattavasti. Potentiaalisten ongelmien analyysi on hyvin korkealla tasolla ja OCTAVE puolestaan on tarkasti määritelty prosessi, jossa on selkeät vaiheet.

Menetelmät valittiin tarkasti harkiten. Potentiaalisten ongelmien analyysi on erittäin yksinkertainen ja tehokas. Kuitenkin potentiaalisten ongelmien analyysi tarjoaa hyvin vähän työn tai prosessin ohjausta. Sähköistä työkalua ajatellen OCTAVE sellaisenaan ei suoraan sovellu työkalun työtapaviitekehykseksi. OCTAVEn ja sen prosessien vaiheiden implementoiminen työkaluun on kyllä mahdollista, mutta tietoturvastandardien sovittaminen osaksi OCTAVE-prosessia olisi hankalaa.

Toisaalta tämän työn puitteissa asioita pyritään tarkastelemaan konsultin tai ulkopuolisen asiantuntijan näkökulmasta. OCTAVE-prosessi on erittäin raskas ja aikaa vievä prosessi. OCTAVE ei suoranaisesti prosessina tue ulkopuolisia standardeja, koska OCTAVE on itseriittoinen. OCTAVE-prosessi perustuu kriittisiin voimavaroihin. Analyysin edetessä

kriittisiin voimavaroihin liittyvät komponentit pyritään tunnistamaan. Näitä komponentteja kutsutaan avainkomponenteiksi.

Potentiaalisten ongelmien analyysi on puhtaasti työmenetelmä eikä tarkemmin ota kantaa sisältöön tai muuhun prosessiin. Tämän takia POA soveltuu erittäin hyvin riskianalyysiprosessin työtavaksi, riippumatta tietoturvastandardista jota käytetään.

OCTAVE tarjoaa kuitenkin mielenkiintoisia näkökulmia ja prosesseja riskianalyysiin. Esimerkiksi arviointikriteeristöjen määrittelemiseen POA ei ota kantaa. Tämän työn puitteissa sähköisen riskianalyysintyökalu noudattaa hyvin pitkälti POA:n määrittelemää metodia. Kuitenkin OCTAVEssa on paljon hyviä käytäntöjä ja työtapoja, joita voidaan tarkastella työkalun kehittyessä. Vaikka OCTAVE:n ominaisuuksia ei suoranaisesti implementoisi työkaluun, voidaan hyviä asioita lisätä riskianalyysiprosessiin.

Erityisen hyvää OCTAVEssa on se, että se ottaa asioita huomioon eri organisaatiotasoilta ja pyrkii myös yhdistämään ja ratkomaan ristiriitaisuuksia näiden näkemyksien välillä. Tämä on yksi näkökulma, joka voitaisiin ottaa huomioon kokonaisriskianalyysiprosessissa. Esimerkiksi ISO 17799-standardin kohdalla organisaatiotasoajattelu voidaan ottaa huomioon osa-aluekohtaisesti. Riskianalyysin edetessä ydinanalyysiryhmän tueksi kutsutaan henkilöitä, joita osa-alue koskee. Esimerkiksi henkilöstöasioita käsiteltäessä paikalle voitaisiin kutsua henkilöstöasioiden asiantuntija.

7. Riskianalyysityökalun kehittäminen

7.1. Vaatimukset sähköiselle työkalulle ja valittu työkalu

Riskianalyysityö vaatii mahdollisuuden vapaamuotoiseen kuvaukseen, pienten lukujen käsittelemiseen ja usein myös taulukkomaisia piirteitä kuten sarakkeita, soluja tai kolumneja. Riskianalyysille on tyypillistä, että tietoa kertyy paljon, joten työkalun olisi hyvä tukea suurempien tietomäärien loogista käsittelyä.

Tämän diplomityön puitteissa sähköiseksi työkaluksi, jonka pohjalta riskianalyysityökalua kehitettiin, valittiin Rational Requisite Pro. Seuraavaksi kuvataan Rational Requisite Pron keskeiset piirteet.

Rational Requisite Pro

Rational Requisite Pro työkalu on alun perin tarkoitettu ohjelmistokehityksen vaatimustenhallintatyökaluksi. Työkalu on suunnattu ohjelmistokehittäjien käytettäväksi ja päätarkoituksellinen käyttötapa on keskitetyn tietokannan käyttäminen. Tällöin keskitetty tietokanta on palvelimella ja kehittäjillä on asennettuna Requisite Pro – ohjelmisto, joka ottaa tietokantayhteyden palvelimeen. Ohjelmistokehitys on ryhmätyötä ja muun muassa monet kypsyysmallit vaativat hallittua ohjelmiston kehitysprosessia. Vaatimuksienhallinta on keskeinen osa ohjelmistokehitystä.

Riskienhallinta tai riskianalyysityökaluna käytettäessä voidaan myös harkita keskitetyn kannan käyttöä. Tällöin esimerkiksi organisaation tietoturvavastaavilla olisi tietokantayhteys ja tunnukset keskitettyyn Rational Requisite-projektiin. Kuitenkin, koska tämän työn puitteissa pyritään kehittämään ulkopuolisen asiantuntijan tai konsultin näkökulmasta työkalua, ei keskitetyn kannan käyttäminen ole mielekästä.

Requisite Pro tarjoaa mahdollisuuden käyttää myös paikallista kantaa. Tällöin kanta on käyttäjän omalla tietokoneella. Requisite Pro:ssa on suora tuki esimerkiksi Microsoft Access – tietokannoille. On huomioitava myös, että lokaalin kannan käyttöä puoltaa tietoturvallisuus. Keskitetyn kannan käyttäminen vaatii pitkäaikaista suunnittelua ja pääsynvalvonnan määrittelemistä. Paikallista kantaa käytettäessä Requisite Pro – työkalu on täysin itsenäinen eikä tarvitse muita sovelluksia tai verkkoa toimiakseen. Seuraavaksi pohditaan vaatimusten ja riskien/uhkien suhdetta.

Vaatimukset ja tietoturvauhkat/-riskit

Ohjelmistokehityksessä vaatimukset pääosin kirjataan sopimusvaiheessa, on myös mahdollista, että vaatimuksia tarkennetaan tai lisätään projektin edetessä. Samaa ajattelumallia voidaan soveltaa muihinkin kuin esimerkiksi toiminnallisiin vaatimuksiin kuten tietoturvavaatimuksiin. Ensivaiheessa tietoturvavaatimukset voivat olla korkealla tasolla ja projektien edetessä tietoturvavaatimukset tulevat yksityiskohtaisemmiksi ja konkreettisimmiksi.

Tarkasteltaessa tietoturvastandardeja, jotka on usein esitetty ”tulisi tehdä”-muodossa, voidaan näiden asettamia kontrolleja pitää eräänlaisina vaatimuksina. Analyysiryhmällä on oma käsitys tietoturvasta oman organisaation tai järjestelmän osalta. On myös mahdollista, että organisaatiolla on oma tietoturvapolitiikka tai vaatimukset järjestelmille. Vaatimukset voivat olla organisaation sisäisiä tai ulkopuolisen asettamia vaatimuksia.

Analyysiryhmän tehtävänä on punnita ja priorisoida potentiaalisia vaatimuksia eli uhkia ja päättää, mitkä näistä ovat tärkeimpiä. Ohjelmistonkehityksessä vaatimuksilla on usein määreitä kuten prioriteettia, statusta, toteutusajankohtaa jne. Tietoturvariskeillä ja uhkilla on hyvin samantyyppisiä attribuutteja.

7.2. Työkalun rajoitteet ja toteutuksen rajaukset

Miltei välttämätön ominaisuus riskianalyysityökalulle on suurien tietomäärien looginen hallinta. Rational Requisite Pro tarjoaa kiitettävästi mahdollisuuksia suurempien tietomäärien hallintaan.

Ytimekkäästi tiivistettynä Rational Requisite Pro käsittelee vaatimuksia, joilla on attribuutteja. Tietokantapohjaisena sovelluksena työkaluun on mahdollista tehdä erilaisia hakuja eli näkymiä. Näkymien kriteereinä voivat olla esimerkiksi tietyt attribuuttien arvot tai vaatimustyypit. Riskianalyysimielessä voidaan ajatella, että eri standardit ovat eri vaatimustyyppejä. Tällöin voidaan hakea vain tietyn standardin kontrolleja/uhkia tai riskejä vaatimustyypin perusteella. Hakemista varten työkalussa on näkymät, jotka suodattavat tietokannasta kriteerejä vastaavat tulokset. Uhkilla ja riskeillä voi olla useita attribuutteja ja näkymä voidaan muodostaa attribuutteihin liittyvillä kriteereillä kuten esimerkiksi riskiluvun suuruuden mukaan. Näkymissä voidaan myös vapaasti päättää näytettävät attribuutit eli voidaan minimoida näkyvän tiedon määrä vain kyseisessä vaiheessa tarvittavaksi (vertaa kartoitus- ja analyysivaihe).

Työkalun hyvänä ja huonona puolena on se, että se on tarkoitettu puhtaasti vaatimustenhallintaan. Työkalu ei esimerkiksi tarjoa taulukkolaskenta tai piirtämisominaisuuksia. Hyvänä puolena mainittakoon työkalun yksinkertaisuus ja tehokkuus sille tarkoitetussa käyttötarkoituksessa.

Riskianalyysityökalun kehityksessä on pyritty mahdollisimman yksinkertaiseen ratkaisuun. Rational Requisite Pro:ta olisi mahdollista laajentaa kattamaan strukturoidumpaa raportointia ja sisältämään lisäosilla erilaisia ominaisuuksia kuten laskentatoimintoja. Kehityksessä kuitenkin pyrittiin minimoimaan asennettavien ja lisenssöitävien ohjelmistojen määrää.

Työkalun vienti- ja tuontiominaisuudet ovat riittävät, koska Rational Requisite Pro tukee csv-muotoista (Comma Separated Values) tietoa. Tiedon vieminen onnistuu myös suoraan Microsoft Exceliin tai Wordiin. Tietoa voi käytännössä viedä tai tuoda mistä tahansa csv-muotoa tukevasta ohjelmasta. Työkaluun tuotava tieto on suhteellisen vapaamuotoista, koska Rational Requisite Pro:n kentät ja näkymät ovat dynaamisia ja

vapaasti muokattavissa. Kuitenkin, jos tuotava materiaali poikkeaa huomattavasti jo toteutetusta rakenteesta, joudutaan Rational Requisite Pro:ssa tekemään manuaalista työtä tietojen sovittamiseksi.

7.3. Valitut standardit ja toteutus

Työkaluun valittiin toteutettavaksi ISO 17799:2005, COBIT, BSI:n uhkaluettelot ja VAHTI:ssa dokumentoituja uhkaluetteloita (samoja kuin Pk-yrityksen riskienhallinta työvälisarjassa, www.pk-rh.com). Työkalua on pääasiallisesti kehitetty ISO 17799:n mukaan tehtävän riskianalyysin läpiviemiseksi. Seuraavaksi kuvataan mitä sisältöä työkaluun on viety osa-aluekohtaisesti.

7.3.1. ISO 17799:2005

Työkalussa ISO 17799 – standardi on jaettu 11 standardin rakenteen mukaiseen osa-alueeseen. Vaatimuksiksi standardista on tuotu kaikki sen asettamat kontrollit. Kontrollit eivät ole vaatimuksia, vaan pikemminkin potentiaalisia uhkia tai riskejä.
ISO 17799:n mukaisen riskianalyysin läpiviemiseksi on valittu POA:n oma variantti, joka kuvataan tarkemmin menetelmän valinta - kappaleessa. Rakenne ja tietokantapohjaiset näkymät on suunniteltu mukailemaan omaa menetelmää. Jokainen osa-alue kansio sisältää näkymän karsimista, kartoitusta ja analyysiä varten.

Erityisesti ISO 17799-analyysia varten on tehty valmiit raportointipohjat, joiden avulla loppuraportin tekeminen on helppoa. Raportit sisältävät muun muassa näkymät hylättyihin uhkiin, riskiluvun mukaan jaoteltuihin riskeihin, näkymät riskin vakavuuden perusteella (sietämätön, merkittävä, kohtalainen, vähäinen ja merkityksetön) ja riskiluvun mukaan jaottelun toimenpiteiden jälkeen.

Työkalu on rakennettu ja suunniteltu siten, että uusien raporttien tekeminen on erittäin helppoa. Esimerkiksi, jos riskianalyysissä halutaan nimetä vastuuhenkilöitä riskeillä, voidaan helposti tehdä näkymä, joka tulostaa Microsoft Exceliin vietävän tiedoston henkilölle osoitetuista riskeistä. Mahdollisuudet ovat rajattomat raportoinnin osalta,

koska jo analyysivaiheessa työkalun riskeihin (kontrolli) voidaan lisätä omia attribuutteja, kuten vastuuhenkilö tai organisaatioyksikkö.

Uhkakartoituksen edetessä työkaluun on voi myös lisätä omia uhkia tai variaatioita standardin määrittelemistä kontrolleista. Työkalussa on myös mahdollista jäljitettävyys esimerkiksi mistä uhka on johdettu.

On myös mahdollista, että riskikartoituksen tulokset annetaan jatkojalostettavaksi vastuullisille henkilöille ja tämän jälkeen tarkennetut tiedot tuodaan takaisin työkaluun. Tällöin voidaan asettaa analyysiryhmän arvioima riskin suuruus ja asiantuntija voi tarkentaa ja perustella omaa arviotaan riskistä omaan kenttään.

Työkaluun on viety Microsoft Word-muotoiset dokumentit, jotka voidaan liittää osaksi loppuraportteja. Word-dokumentteihin dokumentoidaan valmiisiin pohjiin riskien arviointikriteerit, joita on käytetty riskianalyysissä. Arviointikriteeristö-lomakepohja on esitetty liitteessä(Liite 2).

7.3.2. COBIT

Työkalun käyttö on ensivaiheessa suunnattu ISO 17799-standardin mukaisen riskianalyysin läpiviemiseen. COBITin osalta työkaluun on viety kaikki COBITin keskeinen sisältö eli 34 prosessialuetta ja niiden sisältämät 215 kontrollitavoitetta kuvauksineen. Työkaluun on myös viety jokaisen prosessialueen kypsyysmalli kuvauksineen.

COBITille ei ole kehitetty omaa työmenetelmää, vaan POA –varianttia voitaneen käyttää myös COBIT-pohjaisen riskianalyysin läpiviemiseen. Uutena näkökulmana verrattuna ISO 17799:een on kypsyysmallit ja niiden käyttö. Kypsyysmallien käyttöä varten on tässä vaiheessa luotu valmiit näkymät, joissa on jokaisen kypsyystason määritelmät ja tämän lisäksi mahdollisuus kuvata prosessialueen nykytilaa ja arvioida COBITin määrityksiä vasten prosessialueen nykyistä kypsyysastetta.

7.3.3. BSI:n ja VAHTIn uhkaluettelot

Työkaluun on viety BSI:n IT-Grundschutzin uhkaluetteloiden sisältämät uhkat osa-alueittain. Uhkaluetteloiden osa-alueet on kuvattu aiemmin työssä tietoturvastandardit-kappaleessa BSI Standard 100-3 kohdassa. Työkaluun on viety myös VAHTIn uhkaluetteloita, jotka on samoja kuin Pk-yrityksen riskienhallinta työvälisarjassa (http://www.pk-rh.com).

Uhkaluetteloiden käyttötapa on vapaa. Niitä voi käyttää POA-varianttimenetelmän mukaisesti tai esimerkiksi tuki- tai avainsanalistoina ISO17799-standardin mukaisessa riskianalyysissa.

7.4. Valittu metodiikka ja sen kuvaus

Työkaluun pyrittiin valitsemaan mahdollisimman yksinkertainen ja tehokas menetelmä riskianalyysin läpiviemiseen. Rajoituksia menetelmälle asettaa käytettävä standardi sekä sähköinen työkalu, Rational Requisite Pro.

Pääpainona työkalussa on ISO17799-standardi ja tämän takia menetelmä pyrittiin sovittamaan tämän mukaiseksi. Valittu menetelmä on POA, kuitenkin joillakin muutoksilla. Menetelmän idea ja työtapa mukailee hyvin pitkälti potentiaalisten ongelmien analyysia. POA:n vaiheet tiivistetyssä muodossa on esitetty aiemmin työssä metodiikat-kappaleessa(Taulukko 6: POA:n vaiheet.Taulukko 6). Seuraavaksi kuvataan käytetty POA:n variantti.

7.4.1. POA-variantti

ISO17799-standardin mukaisen riskianalyysin eteneminen työkalussa on suunniteltu seuraavaksi:

1. Riskianalyysin rajauksen määritteleminen
2. Käytettävien arviointikriteerien määritteleminen
3. Uhkien ideointi-, karsinta- ja kartoitusvaihe
4. Analysointivaihe
5. Loppuraportin laatiminen

Potentiaalisten ongelmien analyysimenetelmä käsittelee yllä olevista vaiheista lähinnä vaiheita 3-4. Seuraavaksi kuvataan kukin vaihe yksityiskohtaisesti ja verrataan kuinka se eroaa POA:sta.

Riskianalyysin rajauksen määritteleminen

Riskianalyysin rajauksen määritteleminen tehdään analyysin aluksi. Rajaus ja kuvaus analyysin kohteesta kirjataan joko työkalussa olevaan valmiiseen Microsoft Word-dokumenttipohjaan tai jonnekin muualle. Rajaus on tarkoitus määritellä analyysiryhmän kesken ja täten muodostaa yhteisymmärrys analyysin laajuudesta ja rajauksista.

Käytettävien arviointikriteerien määritteleminen

Työkalussa on valmis dokumenttipohja, johon on tarkoitus määritellä käytettävät arviointikriteerit. Arviointikriteerit on suunniteltu määriteltäväksi ennen itse analyysin aloittamista. Määrittelyn on tarkoitus yhdenmukaistaa arviointiperusteet läpi koko analyysin. Vastaavasti mietittäessä asetettavia arvoja voi määritelmiä aina tarkastaa ja punnita niiden perusteella. Määriteltäviä kriteerejä ovat uhkan todennäköisyydet, seurauksien vakavuudet ja riskien vakavuudet. Arviointikriteeripohja on esitetty liitteessä 2. Arviointiasteikoksi uhkan todennäköisyyksille ja seurauksien vakavuudelle on määritetty 1-5 ja riskilukuasteikko on näiden tulo eli 1-25.

Uhkien ideointi-, kartoitus- ja karsintavaihe

Tämän vaiheen tarkoituksena on suorittaa potentiaalisille uhkille karsintavaihe ja mahdollisesti määritellä uusia potentiaalisia uhkia. ISO17799-standardin kohdalla kartoitus on suunniteltu eteneväksi standardin osa-alue kerrallaan. ISO17799-standardissa on 11 pääosa-aluetta.

Työkalu tarjoaa kartoitusta varten valmiit näkymät, joissa näkyy kontrolli, uhkan kuvaus ja validius. Uhkan kuvaus kenttään on tarkoitus tarkentaa uhkaa kyseisellä tarkastelurajauksella. Validius-kenttä voi olla arvoltaan tyhjä, kyllä tai ei. Jos uhka päätetään hylätä eli asetetaan validi-kentän arvoksi ”ei”, niin kyseinen uhka ei näy

seuraavien vaiheiden käsiteltävien uhkien tai riskien listalla. Uhka ei kuitenkaan tuhoudu, vaan ainoastaan epävalidit uhkat karsitaan pois jatkokäsittelynäkymistä. Hylättyjä uhkia varten on olemassa oma näkymä, josta voi tarkistaa mitä uhkia ja on hylätty ja mahdollisesti mistä syystä.

Karsintavaiheen näkymissä näytettävät kentät/attribuuttien arvot ovat muokattavissa. Työkalun käyttö on suunniteltu siten, että käytäessä kontrolleja kartoitusvaiheessa läpi, voidaan tarkastella ISO17799-standardia kyseisen kontrollin kuvauskohdasta ja miettiä miten se vaikuttaa järjestelmään ja onko se validi. Tässä vaiheessa on myös mahdollista lisätä uusia uhkia. Esimerkiksi ISO17799-mukainen kartoitusvaihe voitaisiin käydä läpi viidessä päivässä, siten että joka päivä käytäisiin keskimäärin kaksi ISO17799-standardin pääosa-aluetta läpi.

Verrattaessa lomakepohjaa POA:n lomakkeeseen, joka on esitetty liitteessä 1, uhkan kuvaus kenttä vastaa jossain määrin POA-lomakkeen ”Vaaraa/uhkaa aiheuttava tilanne”-kenttää. POAn lähestymistapa on hieman erilainen, joten lomakepohjaa on muokattu paremmin vastaamaan käyttötarkoitusta.

Analysointivaihe

Analysointivaiheessa jatketaan kartoitusvaiheen uhkien jalostusta edelleen riskeiksi. Analysointivaihe on suunniteltu käytäväksi ISO17799-standardin kanssa osa-aluekohtaisesti läpi. Kartoitusvaiheessa hylätyt uhat eivät ole mukana enää analysointivaiheen käsittelynäkymissä.

Analysointivaiheen lomake eli näkymä työkaluun sisältää seuraavat kentät/attribuutit: Uhkan kuvaus, Välitön seuraus, Välillinen seuraus, Nykyinen suojautuminen, Uhkan todennäköisyys, Seurauksen vakavuus, Riskiluku, Kehittämistarve, Toimenpide-ehdotus, Riskiluku toimenpiteen jälkeen ja Vastuuhenkilö. Idea on periaatteessa sama kuin POA:n lomakkeessa (Liite 1). POA-lomakepohjaa on vain muokattu hienojakoisempaan suuntaan. Seuraavaksi kuvataan analysointivaiheen kentät lyhyesti.

Uhkan kuvaus

Uhkan kuvaus-kenttä on täytetty jo kartoitusvaiheessa. Analysointivaiheessa tähän kenttään voi lisätä tarkennuksia.

Välitön seuraus

Välitön seuraus-kenttä kuvaa mitä välittömiä seurauksia uhkan toteutuminen aiheuttaa. Esimerkiksi sähkökatko voi aiheuttaa, että järjestelmän palvelimet sammuvat.

Välillinen seuraus

Välillinen seuraus-kenttä kuvaa seurauksia, jotka eivät suoraan aiheudu toteutuvasta uhkasta. Esimerkki välillisestä seurauksesta on että sulakkeen palaminen kaataa palvelun A, mutta jos palvelu B on riippuvainen palvelusta A, on palvelun B:n toimimattomuus palvelimen A-kaatumisesta johtuva välillinen seuraus.

Nykyinen suojautuminen

Nykyinen suojautuminen-kenttä kuvaa kuinka uhkaa vastaan on nykyisin varauduttu.

Uhkan todennäköisyys

Uhkan todennäköisyys-kenttä on lukuarvo väliltä 1-5, joka kuvaa uhkan toteutumisen todennäköisyyttä.

Seurauksen vakavuus

Seurauksen vakavuus kuvaa asteikolla 1-5 kuinka vakavia ovat uhkan seurauksen sen toteutuessa.

Riskiluku

Riskiluku-kenttä kuvaa uhkan toteutumistodennäköisyyden ja seurauksen vakavuuden tuloa. Riskiluku on kokonaisluku väliltä 1-25. Uhkan toteutumis-, seurauksen vakavuuskriteerit ja riskiluvun suuruus on määritelty arviointikriteerien määrittelyn yhteydessä.

Kehittämistarve

Kehittämistarve-kenttään kuvataan mahdollisia kehitysehdotuksia riskin lieventämiseksi.

Toimenpide-ehdotus

Toimenpide-ehdotus-kenttään kirjataan konkreettiset toimenpide-ehdotuksen riskin lieventämiseksi

Riskiluku toimenpiteen jälkeen

Tähän kenttään arvioidaan riskiluku toimenpiteiden jälkeen.

Vastuuhenkilö

Vastuuhenkilökenttä on vapaaehtoinen kenttä käytettäväksi riskianalyysissä. Tämän kentän tarkoituksena on nimetä vastuullinen riskin lieventämisen varmistamiseksi.

Loppuraportointi

Riskianalyysin tulosten loppuraportointia varten työkaluun on kehitetty erillinen raportointiosio. Raportointiosiossa on näkymät, jotka raportoivat keskeisimpiä tuloksia riskianalyysistä. Nämä raportit voi viedä suoraan Exceliin CSV-muodossa (engl. Comma Separated Values) tai Word-dokumenttiin. Loppuraporttia tukevia dokumentteja työkalussa ovat arviointikriteerien ja riskianalyysin rajauksen määritelmät.

Loppuraportointia varten työkalu raportoi muun muassa kaikki riskit riskiluvun suuruuden mukaan jaoteltuna, riskit vakavuuden perusteella (merkityksettömät, vähäiset, kohtalaiset merkittävät ja sietämättömät riskit), riskiluvun mukaan toimenpiteiden jälkeen, hylätyt uhkat ja vastuuhenkilön mukaan. Raportointi osuus on dynaamisesti muutettavissa ja omia raportointipohjia on helppo lisätä.

8. Riskianalyysityökalun arviointi

Rational Requisite Pro - työkalun arviointi tehtiin tämän työn puitteissa asiantuntija-arvioinnin avulla. Arviointia varten pyydettiin kolmea tietoturva-alan ja erityisesti riskianalyysityön asiantuntijaa osallistumaan työkalun arviointiin.

Näistä kolmesta asiantuntijasta yksi oli ollut mukana työkalun kehitysvaiheessa. Työkalun kehittäminen aloitettiin osana erästä riskianalyysiä. Tämän analyysin jälkeen työtä jatkettiin ja työkaluun lisättiin sisältöä, metodiikkaa ja ohjeistusta.

8.1. Asiantuntija-arvioinnin toteuttaminen

Arviointia varten järjestettiin tilaisuus, jossa esiteltiin kolmelle asiantuntijalla työkalun keskeiset ominaisuudet. Tilaisuudessa osallistujat pääsivät myös itse käyttämään työkalua. Työkalu sisältää ohjeistukset käyttöön, mutta Rational Requisite Pro -ohjelmisto oli arvioitsijoille entuudestaan tuntematon.

Arviointitilaisuuden aikana, jokainen osallistuja asensi itse riskianalyysityökalun työasemalleen ja pääsi käyttämään sitä opastetusti. Tilaisuuden jälkeen arvioitsijoilla oli muutamia viikkoja aikaa itsenäisesti testata työkalua.

Itsenäisen testauksen päätöksenä arvioitsijat täyttivät Microsoft Word-dokumentin, jossa oli esitetty verifiointikysymykset. Verifiointikysymykset vastauksineen on esitetty liitteessä(Liite 3).

8.2. Arviointitulosten analysointi

Riskianalyysityökalu arvioitiin suullisen ja kirjallisen palautteen perusteella. Alla on tiivistettynä arvioitsijakommenttien perusteella työkalun hyvät ja huonot puolet (alkuperäiset vastaukset on esitetty liitteessä 3):

Hyvät puolet:

- Requisite Pro on alustana vakaa, kevyt ja käyttöönottaminen on helppoa
- Riskianalyysimielessä työkalu on
    - selkeä,
    - joustava
    - yksinkertainen
    - tietosisällöltään riittävä
    - soveltuu hyvin kommunikointiin
    - mahdollistaa analyysiryhmän virtuaalisen yhteistyön keskitetyn tietokannan avulla
    - soveltuu hyvin riskianalyysityöhön
    - tukee riskianalyysiprosessin jatkuvuutta
    - työkalun käyttäminen ei vaadi käyttäjältä vahvaa tietoturva-alan kokemusta
- Testattu oikeassa käytössä ja todettu toimivaksi
- Kehitysalusta, joka mahdollistaa uuden sisällön tuottamisen suhteellisen pienellä vaivalla
    - uuden sisällön tuottamisen ja muokkaamisen helppous
- Suomenkielisyys
- Samaa projektia voidaan evaluoida useampia standardeja vasten
- Edullinen

Huonot puolet:

- Ei ole kaupallisesti valmis
- Vähemmän ominaisuuksia kuin kaupallisissa riskianalyysityökaluissa
- Yksinkertaisen kertolaskutoiminnallisuuden puuttuminen
- Suomenkielisyys

Pääosin arviointiin osallistuneet henkilöt pitivät kehitetystä työkalusta. Työkalua on myös käytetty jo yhdessä riskianalyysissä, joka tehtiin ISO 17799:2005:n mukaan. Arviointiin osallistujat olivat myös kaikki valmiita käyttämään kehitettyä työkalua riskianalyysityökaluna.

Ennen kaikkea työkalu tarjoaa potentiaalisen kehitysalustan tietoturvatyöskentelylle. Kehitetty työkalu tarjoaa vaihtoehdon riskianalyysityön lähestymiseen. Arviointiin osallistuneet henkilöt ovat kaikki saman organisaation jäseniä ja kehitetty riskianalyysityökalu on heidän käytettävissä. Kehitetty alusta/riskianalyysityökalu on yksi mahdollinen kehityssuunta riskianalyysityön edistämiseksi ja yhdenmukaistamiseksi.

Tässä vaiheessa riskianalyysityökalun kehittäminen ja käyttö muodostuu tarpeen mukaan. Aloite ja esittely on tehty. Työn puitteissa tehtyä asiantuntija-arviointia voidaan pitää riittävänä, koska arvioinnin kohteena ollut työkalu oli ensimmäinen versio. Laajamittaisen arvioinnin tekeminen on ajankohtaista, jos työkalun kehitystä päätetään jatkaa.

Tulevaisuudessa riskianalyysityöhön on yksi vaihtoehto enemmän valittavaksi. Kirjoittajan henkilökohtaisena motivaationa työkalun kehittämisessä oli uusien ideoiden tuominen ja uuden näkökulman tarjoaminen riskianalyysityölle.

Useat riskianalyysityökalut, jotka ovat kaupallisia, ovat hyvin pitkälti tuotteistettuja ja niiden käyttötarkoitus on rajattu hyvin tarkasti. Kehitetyn riskianalyysityökalun tarkoitus on tarjota joustavampi ja edullisempi vaihtoehto organisaation tietoturva-asiantuntijoille. Requisite Pro ei välttämättä kilpaile suoraan kaupallisten riskianalyysityökalujen kanssa, mutta se tarjoaa vaihtoehdon esimerkiksi Microsoft Excel-työkalulle.

Toisaalta riskianalyysin tekemisen kynnys on huomattavasti pienempi, koska työkalu on käytännössä kaikkien organisaation henkilöiden käytettävissä. Mielenkiintoisena näkökulmana riskianalyysityöhön tuo itse käytetty ohjelmisto. Ohjelmistoa käyttävät useat henkilöt, jotka eivät ole tietoturva-alan asiantuntijoita, koska Requisite Pro ei ole tarkoitettu ainoastaan riskianalyysityöhön. Esimerkkitilanteessa riskianalyysissä ilmenneitä asioita voidaan antaa jatkojalostettavaksi ihmisille, jotka ovat tottuneet jo käyttämään Requisite Pro - ohjelmistoa vaatimustenhallintatyökaluna. Tällöin itse työkalu ei aiheuta kynnystä, ainoastaan käyttötarkoitus poikkeaa totutusta.

9. Johtopäätökset

Tämän työn puitteissa on perehdytty yksityiskohtaisesti tietoturvariskianalyysiin. Kuten työn alkupuolella on pyritty painottamaan, on tietoturvaorganisaatiolla erittäin merkittävä rooli riskienhallinnan kokonaisuudessa, ja riskianalyysi on osa riskienhallintaa.

Riskianalyysi on aika ajoin toistettava riskienhallinnan prosessi. Riskianalyysin viitekehyksenä käytetään usein standardeja. Valitut standardit riippuvat hyvin paljon tarkastelukohteesta ja riskianalyysin rajauksesta. Riskianalyysityön kannalta olisi järkevää ja mielekästä käyttää samoja kriteerejä, eli esimerkiksi standardeja, toistuvissa riskianalyysiprosesseissa. Tämä mahdollistaa seurattavuuden ja verrattavuuden edellisiin riskianalyyseihin. Vastaavasti samaa tarkastelukohdetta analysoitaessa arviointikriteerit voisivat olla samoja, jotta tuloksia voitaisiin verrata edellisiin vuosiin. Yhtenä etuna saman standardin käytössä on sen käytön ja riskianalyysiprosessin jalostuminen ja syventyminen. Työssä esitellyt standardit, ISO 17799 ja COBIT, soveltuvat erinomaisesti yleisiksi korkeamman tason riskianalyysistandardeiksi.

Toimiva ja hyvin määritelty tietoturvatoiminta edesauttaa riskien järjestelmällistä hallitsemista. Riskianalyysityö menettää merkitystään, jollei organisaatio pyri lieventämään riskejä tai kehittämään tietoturvallisuustoimintaansa. Työn puitteissa esiteltiin kaksi tietoturvaorganisaatiota tai tietoturvatoimintaa määrittelevää standardia,

ISO 27001 ja SSE-CMM. ISO 27001 määrittelee tietoturvan hallintomallin, jota organisaatio voi käyttää esimerkiksi sertifiointitarkoituksiin. Määritelty tietoturvatoiminta ja –hallinta pyrkivät parantamaan organisaation kykyä vastata tietoturvallisuudestaan.
Riskianalyysin rajaus voidaan määritellä vapaasti tapauskohtaisesti. Rajaus on syytä pitää sopivan suppeana, jotta analyysissä pystytään keskittymään käsiteltäviin aiheisiin tarpeeksi syvällisesti. Liian laaja rajaus tekee riskianalyysiprosessista raskaan ja voi vähentää riskianalyysityön merkityksellisyyttä, koska tulokset jäävät usein pinnallisiksi.

Standardin valinnalla on suuri merkitys riskianalyysiprosessissa. Standardi tulee valita, siten että se soveltuu riskianalyysin tarkastelukohteeseen. Esimerkiksi teknistä järjestelmää tarkasteltaessa on syytä valita teknisempi standardi.

Työn puitteissa kehitetyn riskianalyysityökalun menetelmäksi valittiin kirjoittajan oma variantti potentiaalisten ongelmien analyysimenetelmästä. POA:n variantti osoittautui erittäin tehokkaaksi ja sopi rakenteeltaan hyvin sähköiseen työkaluun. Riskianalyysityössä menetelmä ei ota kantaa sisältöön, vaan pyrkii ohjaamaan työtä ja sen etenemistä.

Rational Requisite Pro – ohjelmiston päälle kehitetty riskianalyysityökalu miellytti ja herätti kiinnostusta tietoturva-alan ammattilaisissa, jotka osallistuivat työkalun arviointiin. Työkalua päästiin myös koestamaan käytännössä ja se soveltui hyvin tarkoitukseensa. Ennen kaikkea kehitetty työkalu on kehitysalusta, johon on helppo tuoda uutta sisältöä. Näillä näkymin työkalun kehitystä tullaan jatkamaan lähitulevaisuudessa.

10. Lähteet

[1] Mika Pajarinen, Ulkoistaa vai ei – outsourcing teollisuudessa, Elinkeinoelämän tutkimuslaitos, sarja B 181, Taloustieto Oy, Helsinki, 2001

[2] Jorma Kajava, Sami J.P. Heikkinen, Paavo Jurvelin, Tero Viiru ja Päivi Parviainen, Tietojenkäsittelyn ulkoistaminen ja tietoturva, Oulun yliopisto, Working papers series B 42, Oulu, 1996

[3] Ronald L. Krutz and Russell Dean Vines: The CISSP Prep Guide, Second Edition, Wiley Publishing Inc., 2004

[4] http://en.wikipedia.org/wiki/Confidentiality

[5] Esa Kerttula: Tietoverkkojen tietoturva, Liikenneministeriö, Oy Edita Ab, , ISBN:951-37-2904-4, 2000

[6] J.J Whitmore, A Method for Designing Secure Solutions, IBM Systems Journal, Vol 40, No 3, 2001

[7] http://en.wikipedia.org/wiki/OSI_model

[8] Valtionvarainministeriö: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, 2003/7, ISBN 951-804-408-2, Edita Prima Oy, 2003.

[9] Valtionhallinnon tietoturvallisuuden johtoryhmä, Valtion viranomaisen tietoturvallisuustyön yleisohje, Valtionvarainministeriö, 1/2001

[10] Rich Mogull, Building a Security-Aware Enterprise, 17 January 2002

[11] Arto Suominen, Riskienhallinta, WSOY, Helsinki, 2003

12] Gerald L. Kovacich, The Information Systems Security Officer's Guide – Establishing and Managing an Information Protection Program, Second Edition, ISBN 0750676566, Butterworth Heinemann, 2003

[13] ISO/IEC 27001:2005 Information Security Standard Translated into Plain English, Praxion Research Group Limited, 2006, http://praxiom.com/iso-27001.htm

[14] ISO/IEC FDIS 27001:2005(E), Information technology – Security techniques – Information security management systems – Requirements

[15] http://www.sei.cmu.edu/cmmi/models/models.html

[16] Matt Bishop, Introduction to Computer Security, ISBN 0-321-24744-2, Prentice Hall PTR, 2004

[17] Systems Security Engineering Capability Maturity Model SSE-CMM, Model Description Document, version 3, 2003

[18] Eric Maiwald & William Sieglein: Security Planning & Disaster Recovery, McGraw-Hill/Osborne, ISBN 0-07-222463-0, 2002

[19] Jari Pirnes, Anssi Sahlman, Jorma Kajava, Tietoturva ja sisäinen valvonta, Oulun yliopisto, Working papers series B 62, Oulu, 2000

[20] Juha E. Miettinen, Tietoturvallisuuden johtaminen –näin suojaat yrityksesi toiminnan, ISBN 952-14-0229-6, Kauppakaari OYJ, 1999

[21] Christopher Alberts, Audrey Dorofee, Managing Information Security Risks: The OCTAVE Approach, ISBN 0-321-11886-3, Addison Wesley, 2002

[22] Valtionhallinnon tietoturvallisuuden johtoryhmä, Valtionhallinnon tietoturvakäsitteistö, ISBN 951-804-404-8, VAHTI 4/2003

[23] Karri Kosonen, Paul Buhanist & al., Muutoksen etulinjassa, 3.painos, ISBN 952-91-0240-2, Hämeenlinna 2002, Karisto Oy

[24] BSI, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/english

[25] Bundesamt für Sicherheit in der Informationstechnik, BSI Standard 100-3, Risk Analysis based on IT-Grundshutz, version 2.0

[26] ISO/IEC 17799:2005(E), Information technology – Security techniques – Code of practice for information security management, Second edition 2005-06-15

[27] Laki yksityisyyden suojasta työelämässä 13.8.2004/759

[28] Sähköisen viestinnän tietosuojalaki 16.6.2004/516

[29] Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit, ISACA

[30] COBIT MAPPING: MAPPING OF ISO/IEC 17799:2000 WITH COBIT, 2NDEDITION, ISACA

[31] Cobit 4.0, ISACA

[32] Barton, Russell R., Hery, William J., Liu Peng, An S-vector for Web Application Security Management

[33] Peltier, Thomas, Peltier Associates Facilitated Risk Analysis Process (FRAP), 2003

[34] VTT-riskianalyysit, Riskianalyysin menetelmät, http://riskianalyysit.vtt.fi/

[35] PK-yrityksen riskienhallinta, http://www.pk-rh.com/

Liitteet

Liite 1: Potentiaalisten ongelmien analyysin analyysilomake.

POA analyysilomake

KOHDE: Laatijat:	Vaaraa/uhkaa aiheuttava tilanne	Seuraukset	Riski	Nykyinen varautuminen	Toimenpide-ehdotukset/ lisäkysymyksiä

Analyysin pvm:
Raportti:
Sivu ( )

Liite 2: Arviointikriteeristö

Riskianalyysissä käytettävä arviointikriteeristö

Uhkan toteumistodennäköisyyden arviointikriteerit 1-5:

5= erittäin todennäköinen riski:

Esimerkiksi uhka toteutuu >80 % todennäköisyydellä vuoden kuluessa.
Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

4=melko todennäköinen riski:

Esimerkiksi uhka toteutuu >50 % todennäköisyydellä vuoden kuluessa.
Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

3= melko harvinainen riski:

Esimerkiksi uhka toteutuu >30 % todennäköisyydellä vuoden kuluessa.
Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

2=harvinainen riski:

Esimerkiksi uhka toteutuu >10 % todennäköisyydellä vuoden kuluessa.
Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

1= erittäin harvinainen riski:

Esimerkiksi uhka toteutuu <10 % todennäköisyydellä vuoden kuluessa.
Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

Seurausten vakavuuden arviointiasteikko 1-5:

5=erittäin vakavat

Toiminta keskeytyy viikoiksi tai aikataulu vaarantuu merkittävästi. Seurauksena voi olla erittäin suuret taloudelliset tai maineelliset haitat. Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

4= vakavat

Toiminta keskeytyy päiviksi tai aikataulu vaarantuu kohtalaisesti. Seurauksena voi olla suuret taloudelliset tai maineelliset haitat. Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

3= haitalliset

Toiminta keskeytyy tunneiksi tai aikataulu vaarantuu lievästi. Seurauksena voi olla merkittävät taloudelliset tai maineelliset haitat. Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

2= melko vähäiset

Toiminta tai aikataulu voi häiriintyä. Seurauksena voi olla lieviä/pienehköjä taloudellisia tai maineellisia haittoja. Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

1= vähäiset

Ei vaikuta toimintaan tai aikatauluun. Seurauksena voi olla vähäisiä taloudellisia haittoja. Ei maineellisia haittoja. Tämän tilalle määritellään riskianalyysin puitteissa käytettävä kriteeristö.

Riskiluvun arvoasteikon määritykset (1-25):

25-15 =sietämätön riski

Koko toiminta on vaarassa ja toimenpiteet riskin poistamiseksi/pienentämiseksi on aloitettava välittömästi. Tämä korvataan omalla määritelmällä.

12-9 =merkittävä riski

Toiminta on osittain vaarassa ja riskin pienentäminen on välttämätöntä; toimenpiteet on aloitettava. Tämä korvataan omalla määritelmällä.

8-5 =kohtalainen riski

Koko toiminta ei ole vaarassa. Toimenpiteiden suunnittelu on kuitenkin aloitettava. Tämä korvataan omalla määritelmällä.

4-2 =vähäinen riski

Toimenpiteitä ei välttämättä tarvita. Uhka/riski on kuitenkin tiedostettu ja sen kehittymistä tulee seurata. Tämä korvataan omalla määritelmällä.

1 =merkityksetön riski

Toimenpiteitä ei tarvita. Tämä korvataan omalla määritelmällä.

Liite 3: Asiantuntija-arvioiden vastaukset

Vastaaja 1:

1. Kuinka hyvin työkalu soveltuu mielestäsi ISO17799:2005-pohjaiseen riskianalyysiin?

Olen ollut mukana projektissa, jonka yhteydessä Timo Karsisto on kehittänyt Rational Requisite Pro tuotteen pohjalta riskianalyysisovelluksen ISO 17799:2005 pohjaisen riskianalyysisovelluksen tekemiseen. Toki tätä tarkoitusta varten on olemassa monenlaisia työkaluja, mutta kokemusperäisesti monen tuollaisen sovelluksen toimivuus on jättänyt käytännön työssä toivomisen varaa mm. sovelluksen stabiliteetin suhteen. On pakko myöntää, että Timon aloittaessa työtään suhtauduin hieman epäileväisesti ajatukseen, voiko Rational Requisite Pro – tuotteen - mikä on alun perin ajateltu aikalailla erilaiseen käyttötarkoitukseen – pohjalta todella toteuttaa toimiva riskianalyysisovellus. Käytännön kokemus on osoittanut nämä epäilykseni ja pelkoni perusteettomiksi.

Nykymuodossaan riskianalyysisovellus täyttää mielestäni käytännön kenttätyön asettamat vaatimukset ISO 17799:2005 pohjaisen riskinalyysin tekemiseksi vallan mainiosti. Toki sovelluksesta puuttuu piirteitä, joita muista vastaavista sovelluksista saattaa löytyä. Käytännön työtä ajatellen tuollaiset piirteet ovat useimmiten lähinnä ”pintakuorrutusta” vailla käytännön merkitystä. Ja toisaalta positiivisena kääntöpuolena on sovelluksen säilyminen yksinkertaisena ja helppokäyttöisenä – jopa kaltaiselleni ei-tekniselle ihmiselle.

Riskianalyysisovellus on osoittanut myös toimivuutensa kommunikointivälineenä tehtäessä vuorovaikutteista ryhmätyötä. Sovellus toimii tällöin merkittävässä määrin riskianalyysiryhmän dokumentointi-, analyysi ja raportointivälineenä rakenteistaen ja ohjaten osaltaan riskianalyysin tekemistä. Riskianalyysiryhmän jäsenillä on mahdollista keskittyä primääriseen tehtäväänsä sivuasioiden asemasta.

Rational Requisite Pro pohjainen riskianalyysisovellus on osoittautunut myös äärimmäisen stabiiliksi. Piirteen merkitystä ei voi liiaksi korostaa – ja erityisen merkittävä se on ryhmätyössä, missä epästabiili työkalu saattaa vaarantaa koko työn.

Riskianalyysin tuloksilla on usein vaara jäädä vaille todellista käytännön hyödyntämistä. Se, että riskianalyysi tehdään Rational Requisite Pron avulla saavutettujen riskianalyysitulosten hyödyntäminen helpottuu tuotteen perinteisemmillä käyttöalueilla. Tässäkin mielessä riskianalyysisovellus helpottaa kommunikaatiota ”eri kieltä” puhuvien tahojen välillä.

Riskianalyysisovellus tukee myös ISO 17799:2005 standardin kannalta keskeistä riskianalyysin jatkuvuutta. Käytännössä sen käyttö kerryttää organisaation riskianalyysitietoissuutta.

Positiivisena piirteenä on pakko mainita myös se tapa, millä Timo Karsisto on kyennyt toteuttamaan Rational Requisite Pron avulla riskianalyysin tarpeet. Työkalu on osoittanut tässä mielessä myös joustavuutensa ja kykynsä vastata muuttuviin vaatimuksiin.

Näen myös riskinalyysisovelluksen osittaisen ”suomenkielisyyden” positiivisena piirteenä Suomen näkökulmasta. Yhä edelleen vieraskielisyys saattaa aiheuttaa ymmärrys/tulkintaongelmia.

2. Kuinka hyödylliseksi koit muun sisällön (muun kuin ISO17799)?

Koen riskianalyysisovelluksen olennaiselta osaltaan ”riskianalyysin kehitysalustaksi”, minkä yhtä ilmentymää edustaa ISO 17799:2005. Käytännössä tänä päivänä tehdään harvoin aivan puhdasoppisia riskianalyysejä vain yhden standardin pohjalta ja suuntaus usean standardin yhdistämiseen on pikemminkin voimistumassa. Myös eri maissa ja toimiloilla painotetaan eri standardeja jossakin määrin eri tavoin. Tässä suhteessa nyt valittu linja edustaa askelta oikeaan suuntaan myös sisällön osalta, mutta edustaa nyt valitun muun sisällön osalta lähinnä esimerkkiä. Pidän Timo Karsiston ansiona nimenomaan ”riskianalyysin kehitysalustan” kehittämistä, mille voidaan jatkossa sovittaa mikä tahansa standardi.

3. Kuinka hyvin mielestäsi ReqPro-soveltuu ominaisuuksiltaan riskianalyysityöhön ja kuinka näet työkalun kehitysmahdollisuudet?

Ks. vastaus 1 ja 2. Minusta ReqPro soveltuu vallan mainiosti riskinalyysiin. Timon työllään kumoamien ennakkokäsitysteni jälkeen uskon sen olevan mukautettavissa joustavana välineenä hyvin erilaisiin vaatimuksiin ja standardien piirteisiin. Selviö on myös se, että IT Governance – suuntauksen edelleen voimistuessa tarve hyvälle riskianalyysisovellukselle tulee kasvamaan. Miten vaatimukset sitä kautta tulevat muuttumaan jää nähtäväksi.

Mikäli riskianalyysisovellusta halutaan ajatella kaupallisen tuotteen näkökulmasta niin se edellyttää vielä lisätyötä. En kuitenkaan näe sitä tässä vaiheessa puutteena, koska tässä vaiheessa on keskitytty ainoastaan sen toiminnallisuuteen.

4. Jos olet käyttänyt tai tunnet muita samaan tarkoitukseen tehtyjä työkaluja, miten vertaisit kehitettyä työkalua niihin (voi verrata myös muihin työtapoihin kuten paperi- tai excel-pohjaisiin)?

Ks. 1, 3 & 3.

5. Kehitysehdotuksia työkalulle (käyttötavan, rakenteen tai implementoitujen standardien/sisällön suhteen)?

Näen riskianalyysisovelluksen pitkälti ”riskianalyysin kehitysalustana” ja siinä mielessä standardien lisääminen ja ”mappaaminen” toisiinsa myös työvälinetasolla olisi tottakai tervetullutta. Toki niitä löytyy maailmalta melkoinen määrä ja johonkin on ilman muuta vedettävä raja.

Ideaalimaailmassa riskianalyysisovelluksesta toivoisi löytyvän myös ohjaavan flow’n eli ammattilaisten työkalussa sellaista ei tarvita, mutta mitä enemmän sovellusta ajatellaan ”tilapäiskäyttäjien” työkaluna, sitä suuremmaksi sen merkitys kasvaa. Sama piirre liittyy myös muihin vastaaviin tuotteisiin.

Periaatteessa voisi myös ajatella sovellukseen sisällytettävän mm. raportointimalleja (en tarkoita tässä ”näkymiä”) erilaisiin tarkoituksiin. Tilanteita ja malleja tarvitaan erilaisia ja osaltaan ne toimivat ohjaavina ja rakenteistavina elementteinä.

”Toiveiden tynnyri” on tietysti aina rajaton...;)

6. Uskotko, että voisit käyttää työkalua riskianalyysityökaluna?
Kyllä – vallan mainiosti.

Vastaaja 2:

1. Kuinka hyvin työkalu soveltuu mielestäsi ISO17799:2005-pohjaiseen riskianalyysiin?
Riskianalyysikokemusteni ja nähdyn perusteella työkalu soveltuu erittäin hyvin ISO17799-pohjaiseen riskianalyysityöhön. Kyseisen standardin riskianalyysikriteeristöt oli implementoitu kiitettävällä ja erittäin selkeällä tavalla työkaluun. Lisäksi riskiaanalyysityöhön tarvittava ”default” tietosisältö (tietokentät) on riittävä. Työkalusta tekee erittäin hyvän se, että käyttäjä voi räätälöidä tarvittavat tietokentät (sarakkeet) mieleisekseen ja lisätä/poistaa juuri projektinsa käyttöön tarvitsemat kentät. Mittaristo oli 17799-osalta suomen kielinen ja standardin muuttuessa tulevaisuudessa, voi kääntämisestä tulla hidaste työkalun päivittämisessä. Lisäksi voisi olla, että englannin-kieliselle työkalulle yrityksessämme käyttäjäkunta olisi suurempi.

Myös muiden maailmalta löytyvien mittaristojen/kriteeristöjen ajaminen sisään järjestelmään näytti todella jouhevalta, mikäli mittaristo vain löytyy jollakin tavalla määrämuotoisena datana / taulukkona entuudestaan (tulkitse tuota ”määrämuotoisena datana” erittäin laajana käsitteenä). Tämä merkitsee sitä, että mikäli maailmalla tulee jokin uusi hyvä kriteeristö, niin ei tarvita atk-experttiä ajamaan tai koodaamaan kriteeristöä työkaluun!!! Erittäin hyvä asia!!! Tuosta täydet pisteet Timolle!!!

2. Kuinka hyödylliseksi koit muun sisällön (muun kuin ISO17799)?
Enpä ole vielä törmännyt työkaluun, jossa samaa projektia voisi katsoa läpi useampaa kriteeristöä vasten. Erittäin kiinnostavia ovat ISO:n lisäksi Common Criteria ja Cobit –

kontrollien / kriteerien hyödyntäminen, joita osittain olikin jo implementoitu järjestelmään. Lisäksi uusien ISACA/ITGI-SOX-kontrollien implementointi voisi olla käyttökelpoinen (mikäli ko. kontrollit on uudessa 2nd editionissa mietitty huolella). http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentFileID=12383

3. Kuinka hyvin mielestäsi ReqPro-soveltuu ominaisuuksiltaan riskianalyysityöhön ja kuinka näet työkalun kehitysmahdollisuudet?

Tärkein ominaisuus, jota tulisi kehittää, on se, että riskin suuruuden laskemisessa olisi automaattinen kertolasku toteutettu (nyt joutuu laskemaan päässä jokaisen riskin kohdalla; ei ole ATK-nykypäivää ;-)). Timon mukaan tuollainen simppeli moduuli tuohon löytyykin ja se olisi vielä implementoitava.

Raportointi on sellainen osa, jota en vielä osaa oikein kommentoida. On mielenkiintoinen alue ja avainasemassa on se, että mahdollisimman helposti ja vähällä käsineditoinnilla saadaan asiakas/projektiriippumatonta raporttia automaattisesti. Templatejen ja template-tekniikan käyttöön kannattaa laittaa paljon suunnitteluaikaa nyt alussa (hyvin tehtynä se vähentää merkittävästi työaikaa jatkossa!!!).

Myöskin ryhmätyöominaisuuksiin (usea kaveri tekee osia suuremmasta riskianalyysistä ja päivittää toisistaan tietämättä dataa => yhteinen taltio/kanta verkossa, lukitukset, päivitystiedot yms....) kannattaa kiinnittää huomiota.

Työkalu pohjautuu Rational-tuoteperheen erään tuotteen käyttöön ja en osaa sanoa sitä mitä rajoitteita se sisäisessä / asiakaskohtaisissa soveltamisissa aiheuttaa (lisenssivaikutukset, kustannusvaikutukset, tekniset yhteensopivuusasiat, jatkojalostustyökalut yms). Tätä tulisi miettiä huolella läpi ennenkuin tähän laittaa suuremmalti jatkopanostuksia.

Aika hyvä softi jo nyt!

4. Jos olet käyttänyt tai tunnet muita samaan tarkoitukseen tehtyjä työkaluja, miten vertaisit kehitettyä työkalua niihin (voi verrata myös muihin työtapoihin kuten paperi- tai excel-pohjaisiin)?

Olen käyttänyt erästä nimeltä mainitsematonta windows-työkalua, joka oli todella raskas työasemassa ja se oli joustamaton mittaristojen suhteen (esim. alirakenteissa tuli tietue-raja vastaan ja ko. rajan ylittyessä joutui temppuilemaan todella paljon ja ottamaan yhteyttä softan valmistaneeseen tyyppiin). Käytännössä tein sillä yhden projektin ja siihen se jäi. Hyvänä puolena ko. järjestelmässä oli erittäin hyvät raportointiominaisuudet.

Tällä hetkellä käytän exceliä, joka on muuten hyvä paitsi että automaattisia raportointiominaisuuksia siinä ei ole eikä se tue montaa muutakaan ominaisuutta, jotka Timon työkalussa ovat. Mutta toisaalta excel on simppeli ja itsekkin helppo modifioida ja sitä osaa käyttää erittäin monet ihmiset organisaatiossa (löytyy myös miltei kaikista toimistojen työasemista)...

5. Kehitysehdotuksia työkalulle (käyttötavan, rakenteen tai implementoitujen standardien/sisällön suhteen)?

ks. edelliset vastaukset.

6. Uskotko, että voisit käyttää työkalua riskianalyysityökaluna?

Voisi olla, jos tulee sopiva case eteen.

Summa Summarum: erittäin hyvää työtä.

Vastaaja 3:

1. How well do you think that the tools suits for ISO17799:2005 based risk analysis?

I think this tool suits very well the ISO 17799:2005 or any other standard. What I like most of this tool is that it is easy to use, fast to install and configure.
It seems to me that it can be easy used and understated also by other people who are not security experts.

2. How useful did you find the other content than the ISO17799 content?

Basically I sow how simple is to use more then one security standard within the very same risk management project and I don't see any particular reason why it shouldn't be used more then one standard like done particularly in US.
I can see as a interesting result using both ISO 17799:2005 and Common Criteria at the same time as far as we can easily divide who's control comes from which standard.

3. How well do you think that ReqPro features suit to risk analysis work and how do you see the potential of the tool?

Well remembering the features of other tool like COBRA I think ReqPro is a nice light alternative to all these very complex software for risk analysis purpose.
I think this tool has great potentiality to be developed further and become a complete risk analysis tool.

4. If you have used or know any other tools suited for the same purpose, how would they compare to this one (you can also compare to other methods such as Excel or plain paper work)?

Well I've been using for some time COBRA as Security Risk Analysis & Assessment, and ISO 17799 / BS7799 Compliance (please check http://www.riskworld.net/) but also Excel for much simple case.
I guess of course you will find pros and cons for any risk management tool. For instance COBRA worked very well with the ISO 17799 but it was very large as software not to mention the fact that it is very expensive. Excel, on the other hands, it is easy to use and fast but with lack of functionalities like importing and exporting from and towards other applications.
The ReqPro tool I found as quick as useful. Easy to import and export and also easy to install and add new attributes and fields.

5. Development ideas for the tool (concerning method of application, structure or implemented standards/content)?

Well to be honest I should use for a while and for a real project to understand the kind of development needs that we could add to this work. I think that adding, as you did, ISO 17799:205 and CC controls of course let this tool seem a much complete tool so I think adding more controls give more and more possibilities to the user to decide which

controls to use. It is also true that I think it would be nice to think about the structure of the contents since I think we need to help the user to understand which flow he should follow while using different standards and controls.

6. Do you believe that you could use the developed tool as risk analysis tool?

Yes I do believe that in future I could use the developed tool as risk analysis tool.