TIETOTURVALLISUUSARKKITEHTUURIN TEHOKAS KÄYTÄNTÖÖNVIENTI JA YLLÄPITO

10. Turvallisuusjohdon
koulutusohjelma
Teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 28.2.2010
Tarja Helkamäki

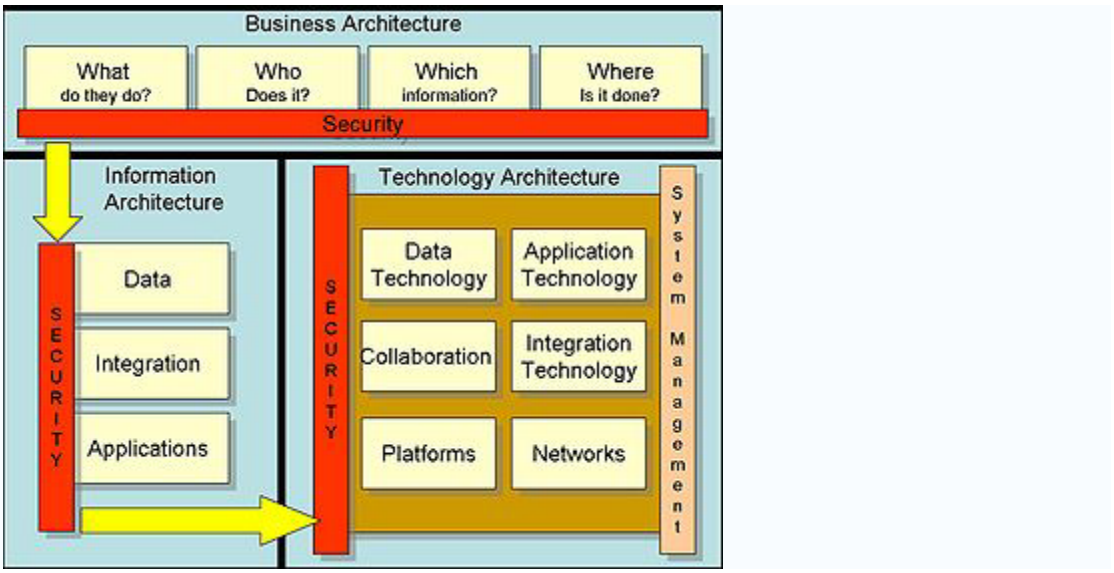
Sisällysluettelo

1 Tiivistelmä

Tietoturvallisuus on koettu usein asiaksi, joka nousee esiin vasta sitten kun sen puute aiheuttaa huomattavia poikkeamia ja vaaratilanteita. Lisäksi tietoturvallisuuden käytäntöönviennissä on keskitytty enemmän teknisiin ratkaisuihin unohtaen mitä kaikkea muuta tietoturvallisuuden varmistaminen vaatii. Parhaimmillaan yrityksissä on olemassa tietoturvallisuuden koulutusohjelmat, joilla henkilöstön tietoisuustasoa säännöllisesti parannetaan. Näillä eväillä on kuitenkin hankala ylläpitää vastausta jatkuvasti muuttuvan ympäristön vaatimuksiin. Jotain kattavaa ja laajamittaista, mutta kuitenkin yksinkertaistettua ja selkeää tarvitaan huomioimaan kaikki yrityksen tietoturvallisuutta kaipaavat toiminnot. Tietoturvallisuusarkkitehtuurin voisi ajatella olevan sellainen.

Tässä työssä on pyritty selvittämään, mikä on tietoturvallisuusarkkitehtuuri, miten se luodaan ja ylläpidetään vaatimuksia vastaavana. Keinoja selvittämiseen on tutkia ensin, onko olemassa jotain malleja tietoturvallisuusarkkitehtuurityön tukemiseen. Seuraavaksi on pohdittu, miten tietoturvallisuusarkkitehtuuri voitaisiin luoda ja mitä siinä pitää huomioida. Ja viimeiseksi, miten se viedään käytäntöön ja ylläpidetään. Kirjallisuuden ja oman kokemuksen lisäksi on haastateltu muutamaa tietoturvallisuusasiantuntijaa sen selvittämiseksi onko tietoturvallisuusarkkitehtuuri yleisesti käytössä tietoturvallisuuden ohjaamisessa.

Yrityksen tietoturvallisuusarkkitehtuuri (Enterprise information security architecture; EISA) on määritelty Wikipediassa [14] tavaksi soveltaa kaikenkattavasti ja tarkasti menetelmää, jolla kuvataan organisaation nykyinen tai tuleva rakenne tai käyttäytyminen tietoturvallisuusprosesseissa, tietoturvallisuusjärjestelmissä, henkilöstön tai organisaatioyksiköiden osalta siten, että ne ovat linjassa organisaation ydintavoitteiden ja strategisen suunnan kanssa. Wikipedian mukaan [14] tietoturvallisuusarkkitehtuuri on yritysarkkitehtuurin osajoukko, ja sen tarkoitus on varmistaa jäljitettävyys koko ketjun läpi liiketoimintastrategiasta teknologisiin ratkaisuihin asti. Alla on kuvattu tietoturvallisuuden liittyminen yrityksen arkkitehtuuritasoihin.



Kuva 1. Tietoturvallisuuden osuus arkkitehtuurikokonaisuudessa [14]

2 Johdanto

Yritysten paineet ja tarpeet kilpailukyvyn parantamiseen lisääntyvät jatkuvasti. Kilpailukyvyn parantaminen edellyttää yrityksiltä kokonaisvaltaista kehitystä eikä yksittäisen osaston tai prosessin toiminnan parantamista. Kokonaisvaltainen toiminnan parantaminen tuo toisaalta yrityksille paineita keskittyä ydinosaamiseensa ja ostaa muut palvelut palvelutoimittajilta tai alihankkijoilta.

Yritysten kehitystavoitteet ja toimintaympäristö vaikuttavat luonnollisesti myös tietoturvallisuuteen, jossa monimutkaistuvan toimintaympäristön vaikutukset monimutkaistavat tietoturvallisuustavoitteiden viestimistä ja toteutuksen varmistamista. Toiminnan ulkoistukset lisäävät sidosryhmien määrää, mikä on myös otettava huomioon tietoturvallisuutta kehitettäessä. Myös toimijoiden diversiteetti lisääntyy; ne toimivat eri aloilla eikä voida enää välttämättä olettaa, että palvelutoimittaja tuntee asiakkaan toimialan erityisvaatimukset. Jos se on oleellista, tuntemus ja vastuu on varmistettava sopimuksin ja koulutuksin, joissa vaatimukset tulevat riittävän selkeästi esiin. Vaatimusten toteutumi-

sen varmistaminen täytyy myös todentaa tavalla tai toisella, esimerkiksi säännöllisin tarkastuksin tai jollain muulla laadunvalvonnalla.

Tietoturvallisuus ymmärretään edelleen usein vain teknisiksi menettelyiksi, vaatimuksiksi ja työkaluiksi, kuten palomuurit tai haittaohjelmatorjunta. Samoin tietoturvallisuusarkkitehtuuri on tällöin käsitetty pelkästään tekniseksi arkkitehtuuriksi. Tietoturvallisuutta voidaan kuitenkin kuvata suhteessa palvelemaansa kokonaisuuteen esim. auton jarrujärjestelmäksi. Sherwoodin [1] esimerkkiä 'Mitä parempi jarrujärjestelmä, sitä nopeammin voi ajaa' eteenpäin kehitellen, jos jarruja käytetään säästeliäästi, ne voivat ruostua. Jarruja ei voi myöskään käyttää koko ajan, koska jos ne laahaavat, jarrupala ja -levy kiillottuu eikä enää jarruta kunnolla. Jarrujärjestelmä on kuitenkin suunniteltava ennen kuin se voidaan asentaa autoon. Mitä suurempi auto, sitä tehokkaampi jarrujärjestelmä tarvitaan. Analogisesti siirrettynä tietoturvallisuuteen, jarrujärjestelmä ja sen kehittäminen vastaavat tietoturvallisuusarkkitehtuuria ja jarrujen tehon määrittely riippuu tietoturvallisuusarkkitehtuurilla tuettavan kokonaisuuden koosta ja monimutkaisuudesta; so. yrityksen koko, ulkoistettujen osuuksien määrä ja merkittävyys, järjestelmien koko ja monimutkaisuus muun muassa ovat lopputulokseen vaikuttavia tekijöitä. Jarrun käyttötavat riippuvat taas tiestä, muusta liikenteestä jne.; siirrettynä tietoturvallisuuteen on huomioitava esimerkiksi käsiteltävien tietojen luottamuksellisuustaso sekä fyysinen ja looginen ympäristö.

Esimerkiksi IT Security Essential Body of Knowledge määrittelee tietoturvallisuusosaamisen 14 eri osa-alueeseen, joten tietoturvallisuus itsessäänkään ei ole pelkkää tekniikkaa. Osa-alueet [12] ovat tietojen suojaaminen, tietorikosten tutkiminen, liiketoiminnan jatkuvuus, poikkeamien hallinta, tietoturvallisuuskoulutus ja tietoturvallisuustietoisuuden lisääminen, IT-järjestelmien operointi ja ylläpito, tietoverkkojen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tuotteiden ja palvelujen hankinta, ulkoisten vaatimusten täyttäminen, riskien hallinta, strateginen johtaminen ja sovellusten turvallisuus. Kaikki edellä mainitut käsitellään tietysti tietoturvallisuuden näkökulmasta.

Vastaavan tyyppisiä rakenteita noudattavat myös mm. ISO 27000-standardiperhe tietoturvallisuuden hallintajärjestelmästä ja Valtion tietoturvatasot. Näiden vaatimuskokoelmien rakenteesta voi myös päätellä, että tekninen ratkaisumalli ei riitä tietoturvallisuuden varmistamiseksi. Tietoturvallisuuden toteutuminen muodostuu suurelta osin ihmisten asenteista, jotka viime kädessä varmistavat tai rapauttavat tietoturvallisuustavoitteet riippumatta teknisistä työkaluista.

Tietoturvallisuusarkkitehtuuri ei toimi erillisenä toimintona, vaan se on kytkettävä tarpeellisin tavoin yrityksen muuhun toimintaan. Jos näin ei tehdä, tietoturvallisuus säilyy erillisenä, kryptisenä, kustannuksia ja hitausmomentteja (so. jarru negatiivisessa tarkoituksessa) aiheuttavana asiana, jota ei voi kukaan tietoturvallisuusasiantuntijoita lukuun ottamatta ymmärtää. Jos taas tietoturvallisuus sovelletaan osaksi yrityksen toimintaa, liiketoiminta alkaa itsekin osata soveltaa ulkoa tulevia vaatimuksia omaan toimintaansa. Kytkeminen muuhun toimintaan edellyttää vastaamista liiketoiminnan odotuksiin ja tietoturvallisuuden viestimistä organisaatioon sen ymmärtämällä tavalla. Tietoturvallisuus on kuitenkin aina kompromisseja vaatimusten, riskien, kustannusten ja toimintatapojen kesken ja kompromissien tekeminen edellyttää jonkinlaista yhtenäistä käsitystä niistä liiketoiminnan ja tietoturvallisuusorganisaation välillä.

Yritysten voimakkaasti verkostoituneessa ympäristössä tietoturvallisuusvaatimukset on vietävä käytäntöön tehokkaasti ja kattavasti huolehtien myös muutoshallinnasta. Yleensä käytettävissä ei ole määrättömästi resursseja, joten se edellyttää tehokasta menettelyä tietoturvallisuuden viemiseksi osaksi normaaleja prosesseja. Ja tässä yhteydessä on muistettava, että tietoturvallisuusvaatimusten vastaanottajat tai toteuttajat sekä yrityksinä että henkilöstön osaamisalueiden osalta vaihtelevat huomattavasti. Toimiala, osaaminen, tietoturvatietoisuus, yrityksen koko, yrityskulttuuri jne. vaikuttavat olennaisesti vaatimuskokoelman käytäntöön vientiin.

Tietoturvallisuusarkkitehtuuri on viime kädessä jaettava ymmärrettäviin osaalueisiin, joita voidaan tarkentaa linjauksilla ja ohjeilla sekä käyttää työkaluja

niiden varmistamiseen ja valvontaan. Rakenteen on hyvä sisältää myös kypsyystasoajattelu, jolloin voidaan kehittää tietoturvallisuutta hallitusti ja vaatimusten mukaisesti, mutta kuitenkin askel kerrallaan.

Tämän tutkielman tarkoituksena on kuvata, minkälaisia tietoturvallisuuden vaatimuskokoelmia on olemassa, mitä tulee ottaa huomioon tietoturvallisuusarkkitehtuuria määriteltäessä, mitä tarkoitetaan tietoturvallisuusarkkitehtuurilla ja miten sitä voidaan ylläpitää ja kehittää. Tutkielma perustuu hyvin pitkälle asiantuntijoiden kanssa käytyihin keskusteluihin, omaan kokemukseen ja tarjolla oleviin harvoihin tietoturvallisuusarkkitehtuurimalleihin. Malliesimerkkinä tutkielmassa käytetään Suomessa yleisesti käytössä olevia ja erityisesti teleyritystä koskevia vaatimuksia. Haasteena rajauksen osalta on se, että tietoturvallisuus liittyy yrityksen toiminnassa kaikkeen tavalla tai toisella, jolloin kovinkaan syvällistä ja yksityiskohtiin menevää analyysia ei tutkielmassa voida esittää. Jo tietoturvallisuuden perusmäärittelyn (Confidentiality-Integrity-Availability) mukaisten näkökulmien huomiointi merkitsee sitä, että tietoturvallisuus vaikuttaa kaikkeen toimintaan. Toisaalta tietoturvallisuus on kokonaisvaltaisena ajatuksena vielä nuorempi kuin vaikkapa IT, joten mitään kovin laajaa tutkimusaineistoa ei ole vielä käytettävissä. Tavoitteena kuitenkin on, että tutkielman lopputuloksena on hyväksi havaittuja menettelyjä, joiden avulla verkostoituneen ympäristön tietoturvallisuusarkkitehtuuri hallitaan ja viedään käytäntöön.

Tässä työssä tietoturvallisuusarkkitehtuurilla tarkoitetaan kokonaisuutta, jonka lähtökohtana käytetään liiketoimintavaatimuksia, jossa huomioidaan tietoturvallisuuden eri osa-alueet, ja tietoturvallisuuden lisääntyvä merkitys liiketoiminnalle. Tietoturvallisuuden eri osa-alueet ovat tässä tiedon ja muiden kriittisten kohteiden suojaaminen, henkilöstöturvallisuus, fyysinen ja ympäristön turvallisuus, tietoliikenne, käyttötoiminnot, pääsyoikeudet, ICT-järjestelmät, tietoturvahäiriöiden hallinta, liiketoiminnan jatkuvuuden hallinta ja vaatimustenmukaisuus. Vaatimuksia voi tulla regulaation kautta, asiakasvaatimuksina tai yrityksen omista politiikoista.

3 Tietoturvallisuuden arkkitehtuurimalleja ja vaatimuskokoelmia

Tässä luvussa kuvataan erilaisia tietoturvallisuuteen liittyviä ja vaikuttavia malleja ja standardeja. Mallien rakennetta kuvattaessa on käytetty englantia silloin kun alkuperäiskieli on englanti, koska kaikkia malleja ei ole käännetty suomeksi ja joidenkin termien kääntäminen vaatisi laajaa asiantuntijoiden käsittelyä. Mallit, jotka tässä esitellään, ovat seuraavat: SABSA, joka on kehys ja metodologia yrityksen tietoturvallisuusarkkitehtuurin luomiseen ja kehittämiseen sekä OSA, joka on toinen tietoturvallisuusarkkitehtuurimalli.

Muita, lähinnä vaatimuskokoelmia, ovat ISO 27000-standardiperhe, PCI DSS-standardi, Valtion tietoturvatasovaatimukset sisältyen varautumisvaatimuksiin (eVare), NIST800, COBIT ja ITIL.

3.1 SABSA

SABSA (Sherwood Applied Business Security Architecture) on John Sherwoodin ideasta Andrew Clarkin ja David Lynasin avulla kehitetty menetelmä. Alkuperäinen malli on kehitetty vuonna 1995. Vuonna 1998 alettiin käyttää Zachmanin yritysarkkitehtuurimallin termejä ja esitystä hyväksi, alkuperäinen perusajatus kuitenkin säilyttäen. SABSA-mallin ensimmäinen kirja julkaistiin vuonna 2005.

SABSA on malli ja metodologia riskilähtöisen yritystasoisen tietoturvallisuusarkkitehtuurin kehittämiseen [1]. Se tukee kriittiseen liiketoimintaan liittyvien tietoturvallisuusratkaisujen toteuttamista. Lähtöajatuksena siinä on, että kaikki tietoturvallisuusvaatimukset johdetaan liiketoimintavaatimuksista. Prosessi analysoi liiketoimintavaatimukset ja synnyttää jäljitettävän ketjun strategiatasolta toteutukseen sekä jatkuvat hallinnointi- ja mittaamisvaiheet [1].

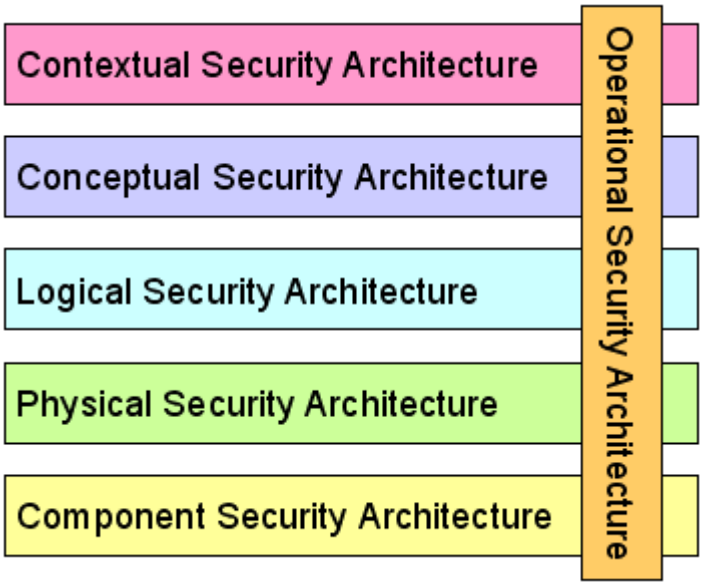
Malli koostuu kerroksista, joista ylin on liiketoiminnan vaatimusmäärittelytaso. Jokaisella alemmalla tasolla luodaan uusi abstraktion ja yksityiskohtien taso. Kerroksia on kuusi, joista jokainen kuvaa jotain yrityksen toiminnan näkökulmaa. Jokaisen kerroksen luomista tukee kuusi kysymystä, joiden vastaukset analysoimalla saadaan luotua vaatimuksia vastaava tietoturvallisuusarkkitehtuuri [1]. Kysymykset ovat mitä, miksi, miten, kuka, missä ja milloin. Esimerkkinä tietojärjestelmävaatimuksista: minkälainen tietojärjestelmä tarvitaan ja mihin sitä käytetään, miksi sitä käytetään, miten sitä käytetään, kuka sitä käyttää, missä sitä käytetään ja milloin sitä käytetään?

Business view	Contextual security architecture
Architect’s view	Conceptual security architecture
Designer’s view	Logical security architecture
Builder’s view	Physical security architecture
Tradesman’s view	Component security architecture
Facilities Manager’s view	Operational security architecture

Kuva 2. SABSA-arkkitehtuurimallin kerrosnäkökulmat [7].

Mallista muodostuu tällöin matriisi, joka liittää suojattavat kohteet, motivaation, prosessit, henkilöt, sijainnin ja ajankohdan edellä kerrottuihin tasoihin. Matriisia voidaan käyttää yrityksen tietoturvallisuusarkkitehtuurin kuvaamiseen ja kehittämiseen [1].

SABSA -malli on Sherwoodin [1] mukaan itsessään yleinen ja voi olla minkä tahansa yrityksen mallinnuksen pohjana, mutta analyysi- ja päätöksentekoprosessien edetessä ja tarkentuessa, siitä tulee yritykselle yksilöllinen malli. Sen muodostama yrityksen tietoturvallisuusarkkitehtuuri on keskeinen tietoturvallisuusstrategian onnistumiseksi. Alla olevassa kuvassa esitetään kuusi kerrosta toisella tavalla ryhmiteltynä. Tässä operatiivinen tietoturvallisuusarkkitehtuuri esitetään pystysuorassa muiden kerrosten yli ulottuvana. Tämä siksi, että operatiivisia tietoturvallisuuskysymyksiä nousee esiin kaikissa muissa tasoissa.



Kuva 3. SABSA-arkkitehtuurimallin kerrosten suhde toisiinsa [7].

SABSA -matriisissa käytetään kaikkien kuuden kerroksen tarkempaa analyysia varten jo aiemmin mainittuja kuutta kysymystä [1]:

1. MITÄ tällä tasolla yritetään tehdä? - Kohteet, joita tietoturvallisuusarkkitehtuurilla suojataan
2. MIKSI se tehdään? - Syy, miksi halutaan soveltaa tietoturvallisuutta, kunkin tason omien käsitteiden mukaisesti
3. MITEN se yritetään tehdä? - Ne toiminnot, joilla tämän tason tietoturvallisuus saavutetaan
4. KUKA liittyy tähän? - Ko. tason henkilö- ja organisaatioturvallisuusnäkohdat
5. MISSÄ tehdään? - Ko. tasolle merkitykselliset paikat, joissa tietoturvallisuutta sovelletaan
6. MILLOIN tehdään? - Ko. tasolle merkitykselliset aikariippuvaiset näkökohdat

Kun edellämainitut kysymykset on toistettu kaikilla kuudella tasolla, saadaan alla oleva 6x6 -matriisi, jonka solut edustavat tietoturvallisuusarkkitehtuurin koko mallia [1]. Jos kaikkien solujen esiin nostamat asiat on katettu, voidaan olla suhteellisen varmoja siitä, että tietoturvallisuusarkkitehtuuri on valmis, ja siinä on huomioitu yrityksen toiminnasta oleelliset asiat.

	Assets (WHAT)	Motivation (WHY)	Process (HOW)	People (WHO)	Location (WHERE)	Time (WHEN)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organization and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetime and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Nodes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management and Support	Security of Sites and Platforms	Security Operations Schedule

Kuva 4. SABSA-matriisi tietoturvallisuusarkkitehtuurin kehittämiseksi [7]

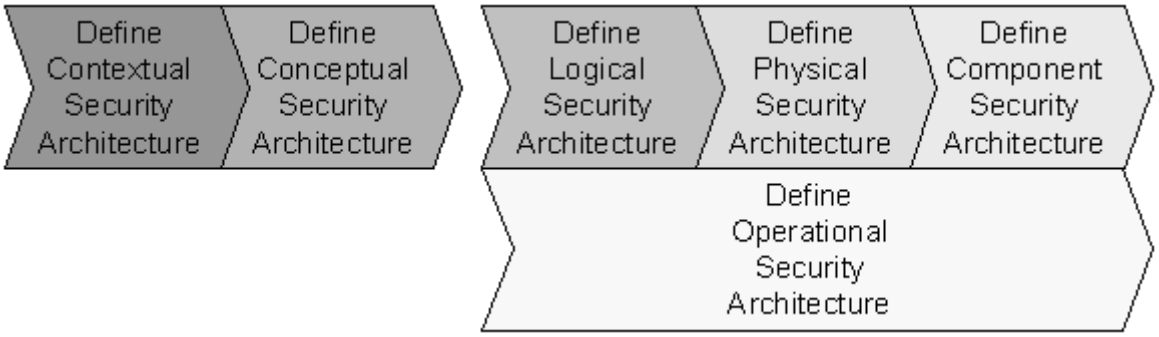
Tietoturvallisuuspalveluiden hallinta ja toiminnot hallitaan operatiivisen arkkitehtuuritason avulla. Ko. taso kuvataan osana kaikkia muita tasoja ja se varmistaa saumattoman ja kokonaisvaltaisen integraation valittujen standardien ja operatiivisten periaatteiden kanssa. SABSA ei vain takaa yhteensopivuutta

vaatimuskokoelmien kuten ITIL, BS15000 / AS8018, ISO 27000 ja CobIT, vaan SABSA tarjoaa keinot määrittää, miten nämä huomioidaan liiketoiminnan tarpeiden yhteydessä [7].

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	Business Requirements Collection; Information Classification	Business Risk Assessment; Corporate Policy Making	Business-driven Information Security Management Program	Business Security Organisation Management	Business Field Operations Program	Business Calendar & Timetable Management
Conceptual	Business Continuity Management	Security Audit; Corporate Compliance; Metrics, Measures & Benchmarks; SLAs	Change Control; Incident Management; Disaster Recovery	Security Training; Awareness; Cultural Development	Security Domain Management	Security Operations Schedule Management
Logical	Information Security; System Integrity	Detailed Security Policy Making; Policy Compliance Monitoring; Intelligence Gathering	Intrusion Detection; Event Monitoring; Security Process Development Security Service Management; System Dev Controls; Config Management	Access Control; Privilege & Profile Administration	Applications Security Administration & Management	Applications Deadline & Cut-off Management
Physical	Database Security; Software Integrity	Vulnerability Assessment; Penetration testing; Threat Assessment	Rule Definition; Key Management; ACL Maintenance; Backup Admin; Computer Forensics; Event Log Admin; Anti-Virus Admin	User Support; Security Helpdesk	Network Security Management; Site Security Management	User A/C Aging; Password Aging; Crypto Key Aging; Admin of Access Control Time Windows
Component	Product & Tool security & Integrity	Threat Research; Vulnerability Research; CERT Notifications	Product Procurement; Project Management; Operations Management	Personnel Vetting; Supplier Vetting; User Admin	Platform, Workstation & Equipment Security Management	Time-out Configuration; Detailed Security Operations Sequencing

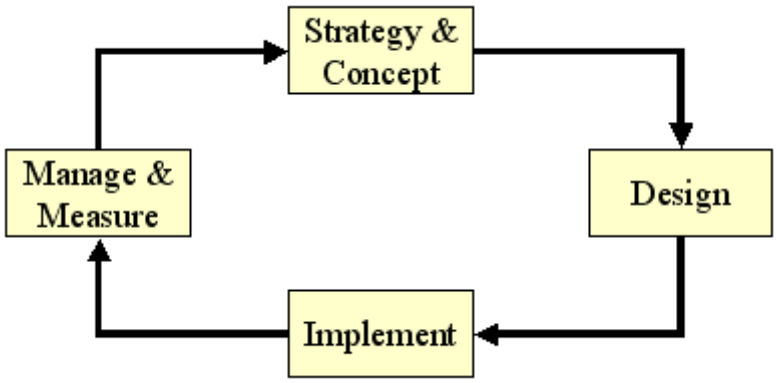
Kuva 5. SABSA -malli tietoturvallisuuspalveluiden hallintaan [7]

SABSA -malli tarjoaa siis pohjan arkkitehtuurin kehitysprosessiksi. Liiketoimintavaatimusten pohjalta luodaan lähtötaso. Suunnittelijat käyttävät sitä tarkan suunnitelman luomiseen, jota taas toimeenpanija käyttää järjestelmien rakentamiseen. Seuraavalla tasolla operoidaan valmista järjestelmää, mutta jos aiemmilla tasoilla ei ole huomioitu operatiivisia tarpeita, tässä vaiheessa tulee ongelmia järjestelmän elinkaaren aikana. Kehitysprosessi on esitetty karkealla tasolla allaolevassa kuvassa [7].



Kuva 6. SABSA kehitysprosessi [7]

SABSAn elinkaari on suunniteltu yhdenmukaiseksi IT-järjestelmien elinkaarihallinnan ja esimerkiksi ISO-standardeissa olevan kehityssyklin kanssa.



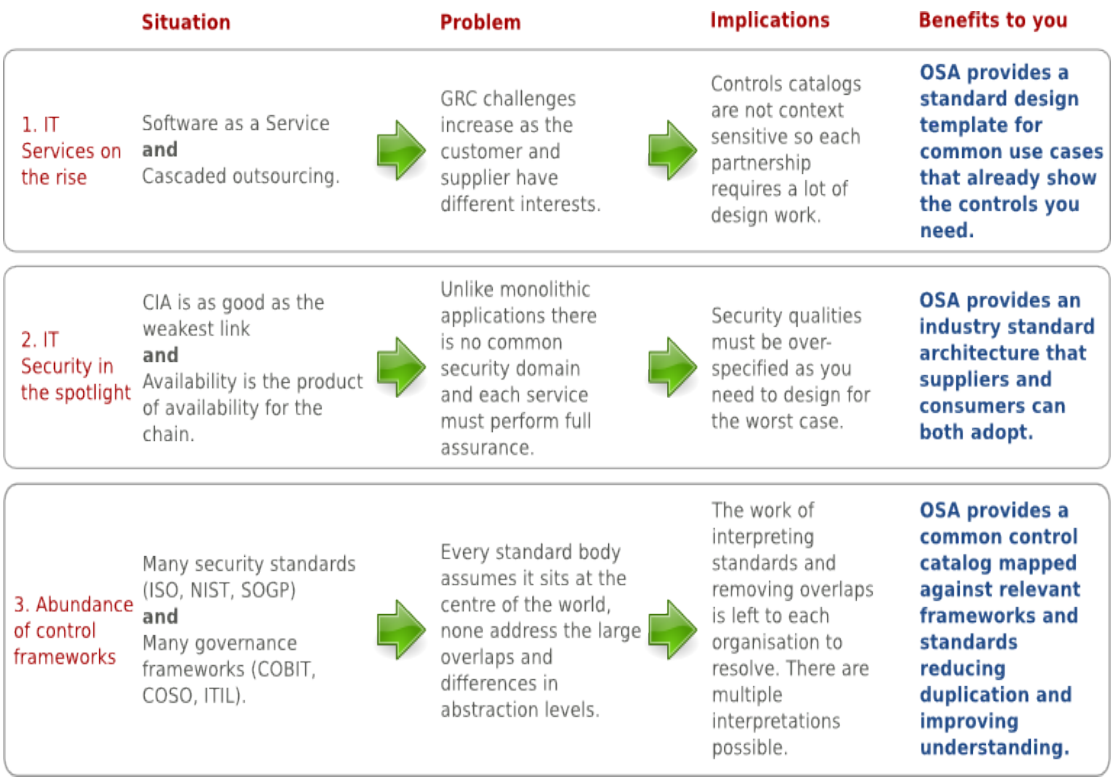
Kuva 7. SABSAn elinkaari [7]

SABSAn elinkaaressa kaksi ensimmäistä vaihetta on koottu aktiviteetiksi ‘Strategy & Concept’. Sitä seuraa ‘Design’ -vaihe, joka käsittää loogisen, fyysisen, komponentti- ja operatiivisen arkkitehtuurin suunnittelun. Kolmas vaihe on ‘Implement’ eli toteutus, jota seuraa ‘Manage and Measure’. Mittaamisen merkitys on se, että prosessissa asetetaan suoritustavoitteet [7].

3.2 OSA

OSA (Open Security Architecture) on toinen vaihtoehto määritellä yrityksen tietoturvallisuusarkkitehtuuri. OSA on opensource-yhteisö, jonka ensimmäiset malliversiot on julkaistu vuonna 2008. OSA perustuu yhtenäiseen Control Catalog -rakenteeseen, jonka avulla eri suunnista tulevat standardien, asiakkaiden, lakien ja määräysten vaatimukset voidaan yksinkertaistaa [5].

Allaolevassa taulukossa esitetään tulevaisuuden trendejä ja miten OSA:n käyttäminen voi auttaa [5]. IT-palveluiden merkitys on nykyään edelleen lisääntynyt liiketoiminnassa ja yritykset haluavat ostaa ne yhä useammin palveluina. Tietoturvallisuuden merkitys kasvaa tällaisessa hajautuneessa ja monimutkaisessa ympäristössä oleellisesti. Tietoturvallisuuden kokonaistaso on kuitenkin yhtä hyvä kuin sen heikoin lenkki.



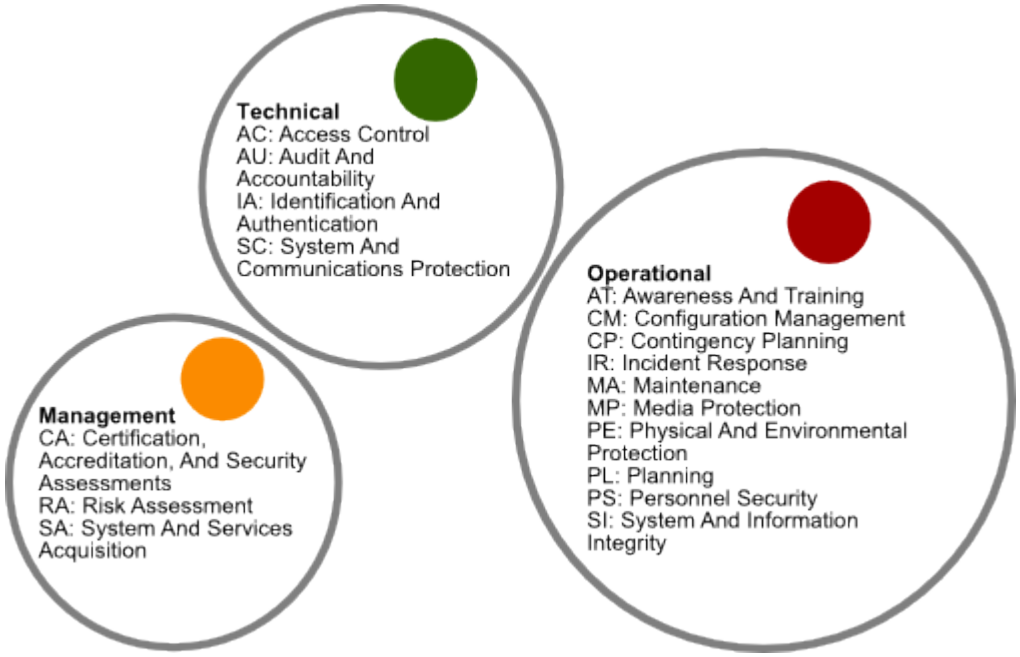
Kuva 8. Esimerkkejä OSA:n hyödyistä [5].

OSA tuo hyötyä käyttäjille, palveluntarjoajille ja toimittajille, sekä koko IT-yhteisölle etua ja laadunparannusta. IT-käyttäjien tarve on yhdistää useiden toimittajien eri arkkitehtuurit monimutkaisissa ketjuissa. OSA:n avulla käyttäjät voivat paremmin joko määrittää tai arvioida hankittavia palveluita ja parantaa sitä kautta laatua. Samalla voidaan vähentää riskiä, että koko arkkitehtuuri olisi vain toimittajan hallussa [5].

IT-sovellustoimittajat haluavat toimittaa mahdollisimman tehokkaasti tuotettuja palveluita mahdollisimman laajalle asiakaskunnalle. OSA:n avulla voidaan kehittää vaatimustenmukaisia järjestelmiä minimikustannuksilla mahdollisimman laajalle asiakaskunnalle. IT-palvelutoimittajat haluavat tukea tuotteita, jotka vastaavat markkinoiden tarpeisiin ja joilla on mahdollisimman pieni TCO. OSA:n avulla varmistetaan, että rakennetaan järjestelmiä, joissa on riittävät ja kunnolliset kontrollit [5].

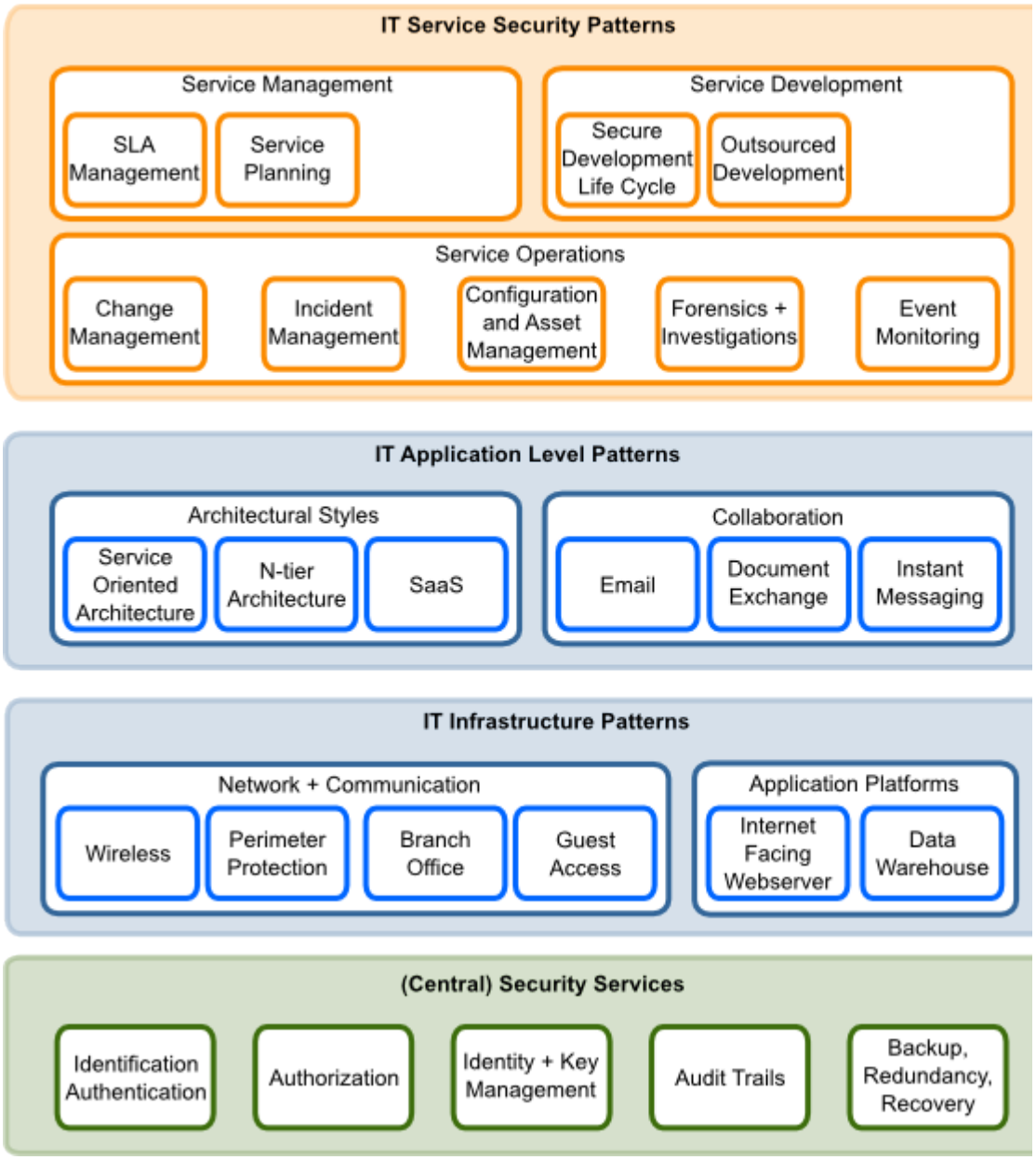
IT-järjestelmän tietoturvallisuus koostuu tietoturvallisuuden kolmesta perusnäkökulmasta; luottamuksellisuus, eheys ja käytettävyys. Tällöin on kyse järjestelmän kyvystä suojata käsiteltävän tiedon luottamuksellisuus ja eheys, järjestelmän ja tiedon käytettävyydestä, mutta lisäksi suoritettujen tapahtumien oikeellisuudesta ja varmuudesta, että järjestelmä toimii suunniteltujen tavoitteiden mukaisesti.

OSA koostuu osista nimeltään Control Catalog, Pattern Landscape ja Threat Catalog, joista viimeksi mainittu puuttuu toistaiseksi mallista kokonaan. Pattern Landscape eri erilaiset tietoturvallisuusarkkitehtuurit muodostuvat jatkossa alakohtaisiksi ja toisesta näkökulmasta uhkien mukaisiksi [5]. Control Catalog sisältää yksityiskohdat kaikista ohjausmenettelyistä, jotka tarvitaan luomaan tietoturvallisia ratkaisuja. Kontrollit on tarkoitus laajentaa aikaa myöden sisältämään testauksen, samoin kuin yhdistäminen muihin standardeihin, määräyksiin, lakeihin ja valtionhallinnon standardeihin. Ohjausmenettelykokonaisuudet on esitetty alla [5].



Kuva 9. OSA:n ohjausmenettelykokonaisuudet (control areas) [5].

OSA Pattern Landscape auttaa määrittelemään, missä osa-alueella on kehittämistä, priorisoimaan ja auttaa yritystä koordinoimaan kokonaisuutta. Alla on OSAn Pattern landscape [5]. OSA keskittyy IT-arkkitehtuuriin ja siihen liittyvään tietoturvallisuuteen.



Kuva 10. OSA:n Pattern Landscape -rakenne [5].

3.3 NIST

NIST800 -ohjeistuksessa lähestytään tietoturvallisuuden kokonaisuutta käsitteellä Information Security Governance [4]. Tähän kokonaisuuteen on sisällytetty yritysarkkitehtuuri. Sinällään NIST -ohjeistus on enemmän taktisen tason dokumentaatiota, eikä anna eväitä siihen, millä mallilla tietoturvallisuus-

arkkitehtuuri kannattaisi rakentaa. Tosin NIST:in ohjeissakin todetaan, että oleellista on riskien analysointi ja olennaisten kohteiden löytäminen, mutta kuvausmalli puuttuu. NIST800 -sarja on kokoelma hyviä dokumentteja, joka kuvaa USA:n valtionhallinnon tietoturvallisuuspolitiikkoja, menetelmiä ja ohjeita. NIST (National Institute of Standards and Technology) on USA:n puolustushallinnon yksikkö. Dokumentit kattavat ohjeet uhkien ja haavoittuvuuksien arviointiin ja riskejä pienentävien tietoturvallisuustoimenpiteiden toteutukseen.

Tietoturvallisuusarkkitehtuurin näkökulmasta dokumenteista arkkitehtuurin ylempiä tasoja käsittelee vain 'Information Security Handbook: A Guide for Managers', jossa arkkitehtuuriin liittyy kaksi lukua: Information Security Governance ja Information Security Strategic Planning. Dokumentissa on lisäksi kuvattu yritysarkkitehdin rooli, mutta ei selkeästi sen suhdetta tietoturvallisuusarkkitehtuuriin.

3.4 CobIT

CobIT (Control Objectives for Information and Related Technology) on enemmän tarkastajan ja IT-governancen kuin arkkitehtuurinäkökulma. Se on hyvä ja kattava kokonaisuus ICT:tä ajatellen, mutta ei sisällä arkkitehtuurin rakentamisnäkökulmaa. CobIT-mallia voidaan kuitenkin käyttää täydentävänä taustamateriaalina.

Tietoturvallisuus on Isaca:n mukaan kaikenkattava rakennekaavio tai malli, joka käsittää yrityksen tietoturvallisuuskäytännöt sisältäen liiketoiminnan vaatimukset, henkilöstön, prosessit, politiikat ja teknologian. Vankka liiketoiminnan tietoarkkitehtuuri on oleellinen tietoturvallisuustarpeiden ymmärtämiseen ja tietoturvallisuusarkkitehtuurin suunnittelun pohjaksi [6]. Yritys voi olla varma monitasoisen puolustautumisperiaatteen toteutumisesta silloin, kun eri arkkitehtuurit on kytketty dynaamisesti yhteen. Tarkan tason suunnittelu kuvaa, missä ja mitkä tietoturvallisuuskontrollit on tarpeen ja kuinka ne liittyvät IT-arkkitehtuurikokonaisuuteen. Yritystasoinen tietoturvallisuusarkkitehtuuri mah-

dollistaa tietoturvallisuuskyvykkyyden varmistamisen kattaen eri liiketoiminnat yhdenmukaisella ja kustannustehokkaalla tavalla ja mahdollistaa myös yrityksen olevan proaktiivinen tietoturvallisuusinvestointipäätöksissään.

Kuva 11. Tietoturvallisuuden liiketoimintamalli CobIT:n mukaan [6]

Kuten kuvassa on esitetty, malli avautuu parhaiten kolmiulotteisena pyramidirakenteena rakentuen neljästä toisiinsa linkitetystä elementistä, joita yhdistää kuusi dynaamista yhteyttä. Kaikki mallin näkökulmat vaikuttavat toisiinsa. Jos mikä tahansa mallin osa muuttuu, tai sitä ei hallita kunnolla, mallin tasapaino kärsii [6].

Mallin [6] neljä elementtiä ovat:

1. Organisaatio - suunnittelu ja strategia

Organisaatio on ihmisistä, kohteista ja prosesseista muodostuva verkko, jotka toimivat vuorovaikutuksessa määritellyissä rooleissa ja kohti yhteistä päämäärää. Yrityksen strategia määrittelee liiketoiminnan päämäärät ja tavoitteet kuten myös arvot ja missiot joihin pyritään. Strategia suhteutetaan ulkoisiin ja sisäisiin tekijöihin Resurssit (ihmiset, laitteet, osaaminen) ovat strategiasuunnittelun ensisijaista materiaalia. Suunnitteluvaiheessa määritellään kuinka organisaatio toteuttaa strategiaansa. Prosessit, kulttuuri ja arkkitehtuuri ovat tärkeitä suunnitelman määrittelyssä.

2. Ihmiset - elementti edustaa inhimillisiä resursseja ja niihin liittyviä turvallisuustekijöitä. Se määrittelee, kuka toteuttaa minkäkin osan strategiaa. Se edustaa ihmisryhmää ja siinä on huomioitava arvot, käyttäytyminen ja poikkeamat. On hyvin tärkeää, että tietoturvallisuuspäällikkö työskentelee henkilöstö- ja lakiosastojen kanssa ainakin seuraavissa asioissa:
- rekrytointistrategiat (pääsyt, taustatarkistukset, haastattelut, roolit ja vastuut)
- henkilöstöasiat (toimistojen sijainti, pääsyoikeudet työkaluihin ja dataan, koulutus ja tietoisuus, liikkuvuus yrityksen sisällä)
- työsuhteen päättyminen (syyt lähtöön, lähdön ajoitus, roolit ja vastuut, järjestelmien pääsyoikeudet, yhteydet muihin työntekijöihin).
Ulkoisesti asiakkaat, toimittajat, media, omistajat ja muut voivat omata yritykseen nähden vahvoja odotuksia, joita pitää tarkastella myös tietoturvallisuusnäkökulmasta.

3. Prosessi — sisältää muodollisia ja epämuodollisia mekanismeja, joilla asioita saadaan tehdyksi. Prosessit identifioivat, mittaavat, hallinnoivat ja kontrolloivat riskiä, käytettävyyttä, eheyttä, luottamuksellisuutta ja ne myös varmistavat vastuut. Ne johdetaan strategiasta ja ne toteuttavat organisaatioelementin operatiivisen osan. Ollakseen yritykselle hyödyllisiä, prosessien tulee:
- toteuttaa liiketoiminnan vaatimukset ja olla politiikan mukaisia
- tarkastella muutoksia ja sopeutua muuttuviin vaatimuksiin
- olla hyvin dokumentoitu ja kommunikoitu osallisille
- olla tarkastettu säännöllisesti tehokkuuden varmistamiseksi

4. Teknologia — elementit koostuvat kaikista työkaluista, sovelluksista ja infrastruktuurista, joilla prosesseja voidaan tehostaa. Kehittyvänä elementtinä, jossa tapahtuu jatkuvia muutoksia, teknologiassa on omat dynaamiset riskinsä. Tyypillisesti yritys on niin riippuvainen teknologiasta, että teknologia muodostaa yrityksen infrastruktuurin ytimen ja on yrityksen päämäärien saavuttamisessa kriittinen komponentti.

Riskien hallinta, joka on tietoturvallisuustyön perusta, vaatii riskitietoisuutta ylimmässä johdossa, selkeää näkemystä yrityksen riskienottokyvystä, ymmärrystä vaatimustenmukaisuudesta, merkittävien riskien läpinäkyvyyttä ja riskienhallintavastuiden määrittelyä organisaatiossa. CobIT:n mallin liiketoimintavaatimuksista viisi seitsemästä ovat tietoturvallisuusvaatimuksia; luottamuksellisuus, eheys, käytettävyys, vaatimustenmukaisuus ja luotettavuus [6].

3.5 ISO 27000

ISO 27000-standardiperhe kuvaa, miten yritykseen kehitetään tietoturvallisuuden hallintajärjestelmä. Kaksi ensimmäistä osaa, 27001 ja 27002 muodostavat kokonaisuuden kannalta oleellisen osuuden. Muut standardiperheen osat keskittyvät johonkin osakokonaisuuteen, kuten 27005 riskienhallintaan. Alla on listattu 27001:n ja 27002:n sisältö. Standardin rakenne on jätetty julkaisematta tässä, koska se edellyttäisi SFS:n lupaa, jota ei ole lähdetty pyytämään.

Hallintajärjestelmässä on luonnollisesti samoja elementtejä kuin arkkitehtuurissa, mutta hallintajärjestelmän näkökulma on erilainen kuin arkkitehtuurin. Lähinnä tietoturvallisuusarkkitehtuurimallia on valmisteilla oleva 27014 ’Information Security Governance’ ja se lupaa antaa viitteitä siitä, miten ISG viedään osaksi yritystason ja IT-hallintamalleja [10], mutta taas kerran arkkitehtuurimalli ja näkökulma puuttuvat. Sinällään hallintajärjestelmän rakenne toimii taustamateriaalina varmistamaan, ettei arkkitehtuurista jää mitään osioita pois.

3.6 PCI DSS

Tietomurtojen riski on Luottokunnan [13] mukaan erilaisissa tietojärjestelmissä on kasvanut ja tietoturvasta on tullut tärkeä osa yritysten arkea.

PCI DSS (Payment Card Industry Data Security Standard), eli lyhyesti PCI-standardi, on kansainvälinen maksukorttialan tietoturvastandardi, jossa ovat mukana Visa International, MasterCard Worldwide, American Express, JCB ja Discover Financial Services [13].

PCI-standardi lyhyesti [13]:

- Ohjaa maksukorttien tili- ja tapahtumatietojen vastaanottamista, käsittelyä, tallentamista ja välittämistä
- Standardin noudattaminen on pakollista kaikille korttitapahtumia vastaanottaville, välittäville tai tallentaville tahoille, kuten kaikille kauppiaille, jotka vastaanottavat maksukortteja sekä kaikille palveluntarjoajille, jotka käsittelevät maksukorttitapahtumia
- Vaatimukset koskevat lisäksi kaikkia järjestelmäkomponentteja. Tällaisia ovat kaikki verkkokomponentit, palvelimet ja sovellukset, jotka sisältyvät tai ovat liitettyinä kortinhaltijoiden tietoja sisältävään ympäristöön
- Tavoitteena turvata kortinhaltijoiden tilitiedot kaikissa olosuhteissa ja nostaa kaikkien korttitietoja käsittelevien tahojen tietoturvataso mahdollisimman korkeaksi
- Standardia hallinnoi kansainvälinen, korttijärjestöjen perustama riippumaton PCI Security Standards Council -toimielin

Standardin vaatimukset voi toki yleistää yrityksen näkökulman mukaisesti halutessaan myös ko. tapahtumien lisäksi muun tiedon käsittelyyn. PCI DSS esittää suhteellisen tarkan tason vaatimuksia tietoturvallisuudelle, joiden otsikkotaso on listattu alla. Arkkitehtuurinäkökulma siitäkin puuttuu.

Standardin pääkohdat [13]:

1. Suojaa tiedot asentamalla palomuuriratkaisu ja ylläpitämällä sitä.
2. Älä käytä ohjelmistotoimittajan määrittämiä oletussalasanoja tai muita tietoturva-asetuksia.
3. Suojaa tallennetut kortinhaltijatiedot.
4. Siirrä kortinhaltijoiden tiedot ja muut luottamukselliset tiedot julkisissa tietoverkoissa salattuina.
5. Käytä virustorjuntaohjelmistoa ja päivitä se säännöllisesti.
6. Kehitä turvallisia järjestelmiä ja sovelluksia sekä ylläpidä niitä.
7. Rajoita pääsy tietoihin koskemaan vain niitä, jotka tarvitsevat niitä liiketoiminnallisiin tarkoituksiin.
8. Luo jokaiselle tietojärjestelmän käyttäjälle yksilöllinen käyttäjätunnus.
9. Rajoita fyysinen pääsy kortinhaltijoiden tietoihin.
10. Seuraa ja valvo kaikkea verkkoresurssien ja kortinhaltijoiden tietojen käyttöä.
11. Testaa tietoturvajärjestelmät ja -prosessit säännöllisesti.
12. Luo työntekijöitä ja alihankkijoita koskeva tietoturvakäytäntö.

3.7 ITIL ja ISO 20000

ITIL on kokoelma parhaita käytäntöjä IT-palvelujen tarjoamiseen, joten siitä saa taustamateriaalia korkeintaan teknisen arkkitehtuurin tasolle. ISO 20000 on vastaava standardi. ISO 20000 koostuu kahdesta osasta, joista ISO 20000-1:2005 on spesifikaatiodokumentti ja määrittelee vaatimukset organisaatiolle IT-palveluiden toimittamiseen ja asiakkaiden hyväksymään laatutasoon. ISO20000-2:2005 on Code of practice ja kuvailee Palvelunhallintaprosessien parhaat käytännöt [9]. Tietoturvallisuus on osana prosesseja, kuten muutoshallintaa, mutta arkkitehtuurinäkökulma puuttuu tästäkin.

3.8 eVare ja TTT

Suomen valtionhallinto on viime vuosina kehittänyt omaa vaatimuskokoelmaansa Varautumis- ja Tietoturvatasovaatimusten kokonaisuudeksi. Vaatimukset on tarkoitettu valtionhallinnon palveluiden toteuttamiseen, joten ne koskevat useita IT- ja ICT-toimittajia. Vaatimukset jakautuvat eri kypsyystasoille ajatuksena sekä palvelun kriittisyys että kehityksen eteneminen. Vaatimukset voivat toimia samanlaisena lähteenä tietoturvallisuusarkkitehtuurille kuin muutkin edellä mainitut, mutta arkkitehtuurin kehittämiseen niistä ei tukea varsinaisesti saa. Vaatimusten osa-alueet ovat [11]

1. Johtajuus,
2. Strategiat ja toiminnan suunnittelu,
3. Henkilöstö,
4. Kumppanuudet ja resurssit,
5. Prosessit: ICT-jatkuvuuden hallinta ja
6. Mittaaminen.

Osa-alueet jakautuvat edelleen osiin, joihin liittyy eri kypsyystasojen vaatimuksia. Alemman tason vaatimukset on toteuduttava myös ylemmän tason toteutumiseksi.

Johtajuus jakaantuu osa-alueisiin [11]

- strateginen ohjaus,
- organisointi sekä
- yhteistyö, viestintä ja raportointi.

Strategiat ja toiminnan suunnittelu jakaantuu kahteen osaan [11]

- toiminnan suunnittelu riskien hallinnan avulla ja
- palveluiden jatkuvuuden suunnittelu.

Henkilöstövaatimusalueet ovat [11]

- osaamisen ja tietoisuuden kehittäminen sekä
- henkilöresurssien ja tehtävien hallinta.

Kumppanuudet ja resurssit-osio jakaantuu kahteen osioon [11]

- sopimustenhallinta ja
- toiminnan varmistaminen erityistilanteissa.

ICT-jatkuvuuden hallinnassa on osiot [11]

- ICT-johtaminen,
- ICT-palvelujen turvaaminen,
- tietojenkäsittely-ympäristön hallinta,
- tiedon turvaaminen ja
- häiriötilanteiden hallinta.

Viimeinen vaatimusosa-alue on mittaaminen [11].

Nämäkin toimivat vaatimuskokoelmana, jotka on sisällytettävä tietoturvallisuusarkkitehtuuriin tarvittaessa, mutta tukea arkkitehtuurinäkökulmaan niistä ei ole.

4 Tietoturvallisuusarkkitehtuurin kehittäminen

4.1 Yritysarkkitehtuurin merkitys ja hyödyt yritykselle

Yleisesti arkkitehtuurin merkitys yritykselle on se, että sen luomalla kehyksellä tai mallilla hallitaan monimutkaisuutta. Kun liiketoimintaympäristön monimutkaisuus kasvaa esimerkiksi ulkoistusten myötä, täytyy arkkitehtuurilla varmistaa liiketoimintaprosessien ja muiden toimintojen yhteentoimiminen. Tällöin varmistetaan palvelujen tehokas tuottaminen ja hallinta koko yrityksen, sen asiakkaiden ja yhteistyökumppaneiden verkostossa. Kun kyseessä on tietoturvallisuus, monimutkaisuuden hallintaa tehdään tietoturvallisuusarkkitehtuurilla.

Arkkitehtuuri (ja tietoturvallisuuden kohdalla tietoturvallisuusarkkitehtuuri) toimii myös ohjaavana dokumenttina projekteille ja kehyksenä, jonka puitteissa voidaan työskennellä yhteistä päämäärää kohti. Tällöin myös taktisella tasolla toteutetuilla järjestelmillä on suunta, jota kohti ne voivat jatkossa pyrkiä. Liian usein tästä kokonaisuudesta unohdetaan kuitenkin liiketoimintanäkökulma, ja tällöin esimerkiksi tietojärjestelmäarkkitehtuuri alkaa toteuttaa itseään huomioimatta liiketoiminnassa tapahtuvia muutoksia ja keskitytään liikaa teknisiin yksityiskohtiin, tietoturvallisuustyössä puhumattakaan.

Sherwoodin [1] ja OSA:n [5] mukaan arkkitehtuurin hyödyt saadaan siitä, että tuotetaan modulaarinen, uudelleenkäytettävä tekninen infrastruktuuri, tehokkaat toiminta- ja hallintaprosessit, ja tapa huomioida laaja kirjo liiketoimintavaatimuksia, kuten käytettävyys, yhteentoimivuus, integraatio, nopea ja kustannustehokas kehittäminen, skaalattavuus, uudelleenkäytettävyys sekä alhaiset operointi- ja hallinnointikustannukset. Tietoturvallisuusarkkitehtuurin hyödyt koskevat vastaavia tietoturvallisuusnäkökohtia.

4.2 Tietoturvallisuusarkkitehtuurin rooli

Yrityksen tietoturvallisuusarkkitehtuurin rooli on tukea ICT-arkkitehtuuria tietoturvallisuus- ja riskinäkökulmista. Joka ei tarkoita sitä, että huolehditaan kaikkien teknisten tietoturvallisuustuotteiden hankkimisesta ja asia on sillä ratkaistu. Tietoturvallisuusarkkitehtuurin hyöty tulee siitä, että asiaa katsotaan laajempana kokonaisuutena ja huolehditaan siitä, että kaikki turvallisuuskomponentit ovat olemassa, ne on erityisesti suunniteltu, hankittu, rakennettu ja hallittu toimimaan liiketoiminnan hyödyksi. Tällöin pitää huomioida, että kaikki komponentit ovat olemassa, ne toimivat yhteen, niistä muodostuu integroitu kokonaisuus, järjestelmä toimii häiriöttä, tiedämme että se on kunnolla asennettu, järjestelmä on kunnolla viritetty, sitä operoidaan oikein ja sitä ylläpidetään.

Tietoturvallisuusarkkitehtuurissa pitää huomoida, että teknologiakomponentit muuttuvat ajan myötä, liiketoimintatarpeet ovat dynaamisia ja riskit sekä niiden käsittelykyky vaihtelevat organisaation osasta toiseen. Tietoturvallisuus voidaan määritellä vain suhteessa liiketoiminnan arvoon ja riskiväittämiin. Tietoturvallisuusarkkitehtuuri varmistaa turvallisen organisaation tarkoittavan, että ratkaisuissa vastataan liiketoiminnan tarpeisiin, ne sopivat tarkoitukseensa, ne tuottavat mitattavan tietoturvatason, että tietoturvallisuus on varmasti kunnolla käsitelty ja tuottavat näkyvän tuoton investoinnille.

Tietoturvallisuustyön arvo on usein ymmärretty väärin välttämättömäksi kustannukseksi kun asiat menevät pieleen. Tällainen jälkijättöinen lähestymistapa ei mitenkään ehkäise ongelmia. Jotta tietoturvallisuus maksaisi itsensä takaisin, arkkitehtuuri on suunniteltava varmistamaan kattava proaktiivinen monitasoinen puolustusmekanismi, jossa huomioidaan ehkäisy, havaitseminen, suojaaminen ja toipuminen.

ICT-teknologian nopea eteneminen vaikuttaa alan kuin alan liiketoimintaan eri tavoin. Ne kaikki edellyttävät tietoturvallisuudelta strategista lähestymistapaa. Tuotteiden osana on yhä enemmän ICT-teknologiaa, tuotetuki on hyvin tietointensiivistä ja automatisoitua sekä yhä useammin tiedonvaihto onkin itse tuote. Asiakaspalvelu on kriittinen tekijä liiketoiminnan menestymiselle. Palvelun laatu ja tietoturvallisuus liittyvät läheisesti toisiinsa. Tietoturvallisuuskäytännöt voivat vaikuttaa merkittävästi jopa siihen, miten asiakkaat palvelun kokevat.

Liiketoimintasuhteet perustuvat luottamukseen, jota suojaamaan tarvitaan hyviä teknisiä tietoturvallisuusjärjestelmiä. Nykyaikaiset tietojärjestelmät ovat erittäin monimutkaisia ja tehokkaita, mutta niiden mukana tulee uuden sukupolven liiketoimintariskejä. Tuon ympäristön hallintaan tarvitaan hyvä kehys koko liiketoimintajärjestelmän elinkaaren ajan. Viime vuosina erilaiset Governance-vaatimukset ovat lisääntyneet kaikilla aloilla ja käytettävän kehysmallin on tuettava vaatimustenmukaisuuden toteutumisen osoittamista regulaation, asiakasvaatimusten ja teknisten standardien osalta.

4.3 Tietoturvallisuusarkkitehtuurin luominen

Tietoturvallisuusarkkitehtuuri on perinteisesti käsitetty teknisen tason ratkaisuina. Tietoturvallisuutta ei ole käsitetty liiketoimintaa kiinnostavaksi asiaksi eikä myöskään kovin yleisesti tietojärjestelmäasiaksi. Yleisimmin tietoturvallisuus on implementoitu jälkikäteen lukuun ottamatta joitakin erityisaloja, joissa on erittäin korkeat tietoturvallisuusvaatimukset. Nykyään kuitenkin sekä yleinen turvallisuus- ja siinä sivussa myös tietoturvallisuustyö on muuttunut teknisten ratkaisujen toteuttamisesta laajemmaksi kokonaisuudeksi, joka alkaa

strategiavalinnoilla ja niiden pohjalta tehtävillä valinnoilla tietoturvallisuusarkkitehtuuriksi ja kehityssuunnitelmaksi, joiden avulla strategiaa toteutetaan.

Erilaisia vaatimuskokoelmia on lukuisia edellä esitettyjen lisäksi, ja paras tapa muodostaa tietoturvallisuusarkkitehtuuri on ’noukkia rusinat pullasta', toisin sanoen ottaa mukaan oman yrityksen kannalta olennaiset vaatimukset, valita malli, jolla arkkitehtuuri luodaan ja luoda yrityskohtainen tietoturvallisuusarkkitehtuuri. Yrityksen kannalta olennaisten regulaation ja asiakasvaatimusten kohdalla pitää tietää, mitä suojataan ja miltä suojataan, onko kyseessä paljastumisen vai muuttumisen estäminen. Lisäksi on selvitettävä miten tiedetään, että suojaus on riittävä.

Tietoturvallisuusarkkitehtuuria luotaessa on mietittävä, miten mallin rakentaminen kannattaa aloittaa, miten edetään, miten malli strukturoidaan ja miten lopputulosta mitataan. Arkkitehtuurin on oltava riittävän helppokäyttöinen ja sille on määriteltävä elinkaari. Sen on oltava kuitenkin kattava, jotta se tukee yrityksen tietoturvallisuustyössä tavoitteiden saavuttamista. Muutokset liiketoiminnassa ja ympäristössä saattavat vaikuttaa arkkitehtuuriin, siksi on luotava prosessit, joilla muutokset tunnistetaan ja arkkitehtuuria voidaan muokata. On myös tunnistettava, milloin arkkitehtuurilinjaukset vanhenevat.

Tietoturvallisuudella on joskus huono maine, että on se vain liiketoiminnan esteenä. Tietoturvallisuusarkkitehtuurin avulla olisikin saatava aikaan ymmärrys siitä, että turvallisuus ja tietoturvallisuus sen osana suojaavat liiketoimintaa ja liiketoiminnan kannalta arvokkaita asioita. Suojatakseen aidosti liiketoimintaa, tulee tietoturvallisuuden aina olla liiketoimintariskeistä johdettua. Tietoturvallisuuden tarkoitus on laskea riski hyväksyttävälle tasolle. Tietoturvallisuus varmistaa myös lopputuloksen laadun omalta osaltaan. Siihen ei kuitenkaan riitä yksittäiset ratkaisut, vaan tarvitaan tehokas, riskienhallinnasta lähtevä tietoturvallisuusohjelma ja sitä tukemaan hyvällä rakenteella koostettu tietoturvallisuusarkkitehtuuri.

Toimiakseen kunnolla ohjaavana kehyksenä, tietoturvallisuusarkkitehtuuri on liitettävä yritysarkkitehtuuriin. Tällöin varmistetaan myös se, että tehdyt lin-

jaukset ovat yhteneviä. Tällöin arkkitehtuuri on myös mahdollista jalkauttaa yhtenä, ymmärrettävänä kokonaisuutena. Kannattaa myös hetki miettiä, mikä on arkkitehtuurin tarkoitus ylipäänsä: vastakohta pistemäisille ratkaisuille. Toisin sanoen, arkkitehtuuri on monimutkaisuuden hallintaa.

Tietoturvallisuusarkkitehtuurin haasteita ovat oman organisaation toiminnan lisäksi myös sidosryhmiltä tulevat vaatimukset. Asiakkailla, ainakin jos ovat turvallisuustietoisia, saattaa olla oman yrityksen tietoturvallisuustason ylittäviä vaatimuksia. Jos haluaa pitää asiakkaat, vaatimukset on syytä toteuttaa. Ne on kuitenkin samalla tuotava yrityksen tietoturvallisuusarkkitehtuuriin, koska erillisten saarekkeiden ylläpitäminen käy aikaa myöden mahdottomaksi.

Toisaalta yritysten keskittyminen ydinosaamiseensa ja sitä kautta tapahtunut ulkoistaminen ja verkostoituminen tuo omat haasteensa, miten alihankkijat tulee huomioida arkkitehtuurityössä. Sekä omien että sidosryhmiltä ja laeista tulevien vaatimusten pitää olla jalkautettavissa myös alihankkija- ja kumppaniverkostoon. Jos yritys tai sen kumppani toimii kansainvälisellä areenalla, on muiden maiden lait, kulttuuri, kieli ja yrityksen toimivaltuudet voitava huomioida arkkitehtuurimallissa.

Kattavia tietoturvallisuusarkkitehtuurimalleja ei ole kovinkaan montaa. Tietoturvallisuusarkkitehtuurimallin tulisi tukea tietoturvallisuuden liittämistä osaksi yritysarkkitehtuuria. Tämä on tärkeää myös siksi, että yritysarkkitehtuurimallit eivät yleensä ota lainkaan kantaa tietoturvallisuuteen. Edellä esitellyistä kehyksistä vain yksi ottaa kattavasti kantaa tietoturvallisuuden suhteeseen yrityksen muuhun toimintaan; SABSA, joka on aidosti malli ja metodologia yrityksen tietoturvallisuusarkkitehtuurin luomiseen ja kehittämiseen. OSA on toinen tietoturvallisuusarkkitehtuurimalli, joka ei vaikuta yhtä kattavalta. Se saattaa kuitenkin hyvinkin sopia pienimuotoisempaan toimintaan kuin SABSA. Toisaalta OSA on edelleen keskeneräinen.

Tukena arkkitehtuurityön taustalla kannattaa pitää esiteltyjä vaatimuskokoelmia (mm.ISO 27000-standardiperhettä, PCI DSS-standardia, Valtion tietoturvatasovaatimuksia) ja sovittaa ne osaksi tietoturvallisuusarkkitehtuuria. Lisäk-

si vastaavalla tavalla kannattaa lähestyä kunkin alan määräävää lainsäädäntöä ja niistä johdettuja määräyksiä. Muuta valittuun lähestymiskulmaan liittyvää taustamateriaalia saattaa olla mm. NIST800, COBIT, ITIL. Lopullinen valinta on tehtävä yrityksen näkökulmasta, ja lisäksi valituista taustamateriaaleista kannattaa valita vain omaa yritystä koskevat osiot ja muodostaa niistä hallittava kokonaisuus. Muutoin lopputuloksesta tulee helposti liian raskas ja laaja ylläpidettäväksi.

Kun tietoturvallisuusarkkitehtuuri on saatu määritellyksi ja se on osa yritysarkkitehtuuria sekä on luotu liiketoiminnan ohjauksessa, se on vielä saatava toimintaa ohjaavaksi. Haasteita tähän tuo paitsi yrityksen oman toiminnan piirteet, myös se kuinka paljon ja mitä toimintaa on ulkoistettu. Tietoturvallisuutta eivät yrityksessä toteuta tietoturvallisuusammattilaiset, vaan jokainen yrityksen työntekijä ja siksi tietoturvallisuusvaatimukset on jalkautettava jokaiselle, jokaiseen prosessiin ja organisaation osaan. Tietoturvallisuusammattilaiset luovat puitteet ja säännöt, eli arkkitehtuurit, politiikat ja ohjeistukset.

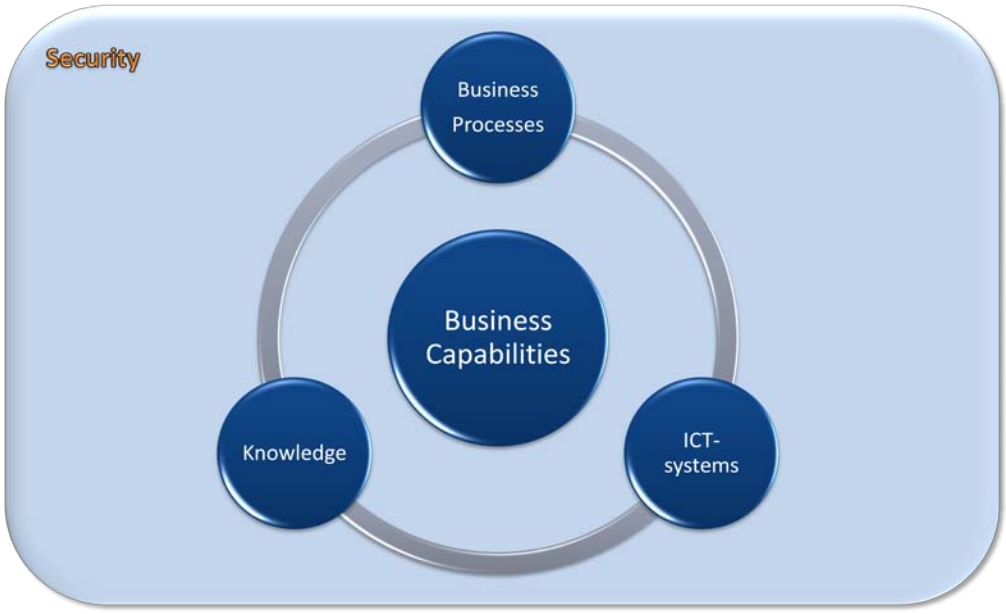
Tietoturvallisuuden kannalta tarvitaan läpinäkyvyys koko toimintayhteisöön alihankkijat ja toimittajat mukaan lukien. On siis tiedettävä, kuka käsittelee tietoja ja mitä alipalveluita yrityksen käyttämä palvelu käyttää. Oleellista on myös missä palvelut fyysisesti ja/tai loogisesti sijaitsevat, kuka niitä hallinnoi ja mitä alipalveluita pääpalvelu käyttää. Samoin fyysinen ja looginen pääsy palveluun on olennaista. Lainsäädäntö ja maiden tai maanosien rajat ylittävät palvelut on huomioitava erikseen ja varmistuttava, että tiedetään niiden vaikutukset.

On varmistuttava myös ennen tietoturvallisuusarkkitehtuurin jalkauttamista, että se kattaa kaikki yrityksen toiminnan osa-alueet ja arkkitehtuurin tasot. Siksi kannattaa käyttää tietoturvallisuusarkkitehtuurin luomisen apuna yhtä riittävän laajaa ja hyvää mallia, jolla voidaan varmistaa se, ettei mikään osa-alue jää huomiotta.

Tietoturvallisuusarkkitehtuurin osalta on päätettävä, missä tapauksissa se ehkä voidaan jättää kehittämättä tai valmis malli huomioimatta. Jos ollaan täysin varmoja siitä, että ratkaisu tai järjestelmä on erillinen, voidaan arkkitehtuuri

jättää huomiotta. Yleensä viimeistään silloin, kun pilotista tulee tuotantojärjestelmä, se liittyy yrityksen kokonaisuuteen niin kiinteästi, että sen tulee noudattaa tietoturvallisuusarkkitehtuuria. Joka tapauksessa tietoturvallisuusarkkitehtuuri kannattaa luoda, mutta vain sillä edellytyksellä, että on valmiuksia, mahdollisuuksia ja tahtotila sen ylläpitämiseen. Yleiset mallit ja kehykset auttavat ottamaan huomioon kokonaisuuden, eikä pyörää tarvitse keksiä uudelleen. Ja kannattaa valita tietoturvallisuusarkkitehtuurimalli pelkän vaatimuskokoelman sijasta, jolloin malli tukee sekä arkkitehtuurin kehittämisprosessia että kokonaisuuden huomioimista. Tällöin malli tukee myös kaikkien eri vaatimuskokoelmien sisällyttämistä lopputulokseen.

Yksi malli tietoturvallisuusarkkitehtuurin pohjaksi on seuraavassa esitetty Elisan Yritysarkkitehtuurimallin ylätaso. Organisaation kyvykkyys on ominaisuus tai resurssi, joka tuo lisäarvoa yritykselle, sen asiakkaille tai sidosryhmille. Sitä tukevat omista suunnistaan liiketoimintaprosessit, tietämys ja ICT-järjestelmät. Tietoturvallisuus on osa niistä jokaista, ja se miten, tarkennetaan tietoturvallisuusarkkitehtuurissa.



Kuva 12. Elisa Yritysarkkitehtuurin yleiskuva [Rajamäki,15].

Kuvassa olevaa mallia lähdetään tarkentamaan siten, että liiketoimintaprosessit koostuvat prosessikaavioista, moduleista ja konsepteista. Tietoturvallisuu-

den kannalta kuvataan, miten se liittyy edellämainittuihin, esimerkiksi mitkä tietoturvallisuusvaatimukset koskevat ja mitä prosesseja.

Tietämys koostuu tiedosta (information) ja datasta, joille löytyy niitä koskevat käsittely-, säilytys-, muuttumattomuus- ja saatavuusvaatimukset. Toisaalta, pitää tietää missä prosesseissa mitäkin tietoa käsitellään ja ketkä missäkin prosessissa työskentelevät, jotta se saadaan kattavasti huomioiduksi käytäntöönvientivaiheessa.

ICT-järjestelmät jakautuvat palveluihin, sovelluksiin ja infrastruktuuriin. Tässä osiossa korostuu tekniset vaatimukset eri teknologioille. Kaikkien kolmen osan täytyy toimia saumattomasti yhteen, ja arkkitehtuurimallin täytyy tukea sitä, jolloin muutostenhallinta ja toteutus ovat ylipäänsä mahdollisia. Toisin sanoen, pitää tietää, mitä tietoa käsitellään missäkin ICT-järjestelmissä ja missä prosesseissa ne ovat käytössä, jotta voidaan koostaa niitä koskevat tietoturvallisuusvaatimukse ja saadaan aikaan yksityiskohtainen, ylläpidettävä ja toimiva tietoturvallisuusarkkitehtuuri.

5 Tietoturvallisuusarkkitehtuurin käytäntöön vienti ja ylläpito

Kun tietoturvallisuusarkkitehtuuri on kertaalleen luotu ja on varmistettu, että se on osana yritysarkkitehtuuria, se on luotu liiketoiminnan ehdoilla ja siinä on huomioitu kaikki osa-alueet ja sidosryhmät, on aika miettiä, miten se viedään käytäntöön organisaatiossa ja miten arkkitehtuuria ylläpidetään niin, että se on aina ajantasainen.

Kokonaisuuden monimutkaisuus on vaikuttaa mallin valintaan, toisin sanoen se, kuinka suuresta yrityksestä on kysymys, kuinka monesta suunnasta vaatimuksia tulee, kuinka hajautunutta toiminta on fyysisesti ja loogisesti, tai onko toiminta kansainvälistä. Kannattaa varmistaa, että arkkitehtuurissa on tarpeellinen laajuus, mutta se ei ole liian laaja. Käytäntöön vienti on syytä tehdä sopivissa askelissa, ja jättää vaikka tarpeellisiakin osia pois aluksi, jotta organi-

saatiossa edistytään askel askeleelta. Käytäntöön vienti kannattaa kouluttaa sopivina annoksina, vuoropuheluna ja sovellettuna juuri kohdetoimintaan.

Tietoturvallisuuden toteutumista mitattaessa on todettu, että tietoturvallisuuskoulutus harvoin tuottaa toivotun lopputuloksen. Siksi myös tietoturvallisuusarkkitehtuurin koulutuksessa on avainasemassa kasvatustieteiden ja viestinnän oppien huomiointi. Toteuttajien käyttäytymisen parantamiseen on käytössä eri tapoja, esim. tietoisuuskoulutus, tietoisuuskampanjat, palkitseminen ja rangaistukset. Tutkimuksissa on todettu, että tiedon ja taidon lisäksi tietoturvallisuusvaatimusten toteuttamisasteeseen vaikuttaa henkilökohtaisella tasolla mm. motivaatio sekä organisaatioriippuvaiset asiat, kuten johtaminen ja politiikat [2]. Nämä reunaehdot on syytä ottaa huomioon, kun halutaan viedä tietoturvallisuusarkkitehtuuri käytäntöön.

Tätä työtä varten on haastateltu viittä tietoturvallisuusasiantuntijaa varsin erikokoisista ja eri aloilla toimivista yrityksistä. Jokaisella yrityksellä on jonkun alan vaatimukset huomioitavana, ja osana vaatimuksia joko tulee tietoturvallisuuteen vaikuttavia vaatimuksia tai tietoturvallisuusvaatimukset ovat omana kokonaisuutena. Yleisesti ottaen voisi sanoa, että mitä tiukemmat ovat alan vaatimukset, sitä selkeämmin ja tiukemmin ne on jalkautettu osaksi yrityksen prosesseja [18,19].

Asiantuntijoilta kysyttiin seuraavat kysymykset:

1. Onko yrityksessäsi tietoturvallisuusarkkitehtuuri?
2. Kuka/ketkä tietoturvallisuusarkkitehtuurin luovat?
3. Onko yrityksessäsi yritysarkkitehtuuri?
4. Onko tietoturvallisuusarkkitehtuuri osa yritysarkkitehtuuria?
5. Hyväksytetäänkö arkkitehtuurit organisaatiossa jollain tavalla?
6. Miten tietoturvallisuusarkkitehtuuri jalkautetaan?
7. Miten tietoturvallisuusarkkitehtuuria ylläpidetään?
8. Mihin viitekehykseen tietoturvallisuusarkkitehtuuri perustuu?
9. Mitä kokemuksia tietoturvallisuusarkkitehtuurin jalkauttamisesta on?

Kaikissa yrityksissä ei varsinaista tietoturvallisuusarkkitehtuuria ole, yleisesti ottaen on kuitenkin tietoturvallisuuspolitiikka, -ohjeistus ja jonkinlainen tietoturvallisuuden tietoisuusohjelma, jolla tietoturvallisuustasoa pyritään nostamaan ja pitämään yllä. Jos yritysarkkitehtuuri on olemassa, se pohjautuu johonkin yritysarkkitehtuurimalliin [17]. Jos lisäksi on tietoturvallisuusarkkitehtuuri, se liittyy yleensä tavalla tai toisella yritysarkkitehtuuriin siten, että yritysarkkitehtuuri ohjaa tietoturvallisuusarkkitehtuuria [17]. Yleensä tietoturvallisuus on pyritty toteuttamaan ainakin osana jotain muuta prosessia, onpa se sitten tuotekehitys-, tuotanto- tai IT-prosessi [17,18,19,20].

Tuotekehityksessä tietoturvallisuus saattaa olla laajimmillaan design-prosessin osana, jolloin syntyy tuotekohtainen tietoturvallisuusarkkitehtuuri [20]. Liitännät konsernitasoiseen tietoturvallisuusarkkitehtuuriin ovat löyhiä; yritystasolta tulevat tekniset ja toimintatapavaatimukset toteutetaan kyllä. Tietoturvallisuus voi olla myös osana IT-arkkitehtuuria, erityisesti silloin jos yritystasoista arkkitehtuuria ei ole. Tuotantoyrityksissä, erityisesti terveydenhuoltoalalla, yksi noudatettava vaatimuskokoelma on GAMP 5, jossa on samoja elementtejä kuin ISO 27000 standardissa [18]. GAMP 5 on kohtuullisen tiukka vaatimuskokoelma, kuten PCI DSS rahoitusalalta, mutta ne molemmat ovat vaatimuskokoelmia, jotka tulisi huomioida tietoturvallisuusarkkitehtuurissa. Kypsyysmalleja CMMI, ja esim. Cobitia ja Common Criteriaa on tutkittu taustaksi vaatimuksille, mutta yleensä on todettu, että joko menetelmä on liian raskas kokonaisuutena tai se on sen verran keskeneräinen suhteessa tarpeeseen tai näkökulma ei ihan istu, että ne on jätetty huomioimatta tai huomioitu vain oleellisin osuus [16,19]. Parhaiten tuntuvat toimivan alakohtaiset suhteellisen konkreettiset vaatimussetit, tai ainakaan niiden huomiotta jättäminen ei onnistu. Niiden implementointiin kannustaa esimerkiksi vuosittaiset tarkastukset [19].

Myös yrityskulttuuri, esimerkiksi se kuinka kauan on totuttu noudattamaan erilaisia vaatimuskokonaisuuksia, vaikuttaa tietoturvallisuusarkkitehtuurin käytäntöönvientiin [18,19]. Silloin, kun tietoturvallisuusvaatimusten toteuttamiseen on totuttu, voidaan odottaa liiketoimintayksiköiden suhtautuvan vaatimuksiin ymmärtäen kokonaisuus ja ne pystyvät suhteelliseen itsenäiseen käytäntöön-

vientiin ilman laajaa koulutusta tai vuoropuhelua. Tällöin voidaan keskittyä itse sisällön suunnitteluun.

Haastatteluiden perusteella syntyi vaikutelma, ettei tietoturvallisuusarkkitehtuuria ole kokonaisuutena lähes missään yrityksessä olemassa. Hyviä käytäntöjä ja vaatimuslistoja, joiden avulla täytetään yksi tai useampi ulkoinen vaatimuskokonaisuus, on kaikilla olemassa, mutta verrattaessa niitä SABSA-kokonaisuuteen, ne täyttävät vain osan sen malleista. Silloinkin kun hyvät käytännöt on hienosti integroitu osaksi tarvittavia prosesseja, kokonaisuusnäkökulma tuntuu puuttuvan. Se, mikä on hyvää, on kuitenkin se, että ainakin osittain on jo saatu johdon sitoutumista esitettyihin vaatimuksiin. Tietoturvallisuuskokonaisarkkitehtuurimalleihin on kuitenkin vielä matkaa. Se, missä kohdassa yrityksen johtoa tai liiketoimintaa vaatimukset hyväksytetään, vaihtelee sitten vaatimuslistan mukaan.

Silloin, kun yrityksessä on tietoturvallisuusarkkitehtuuri tai joitain muita tietoturvallisuuskäytäntöjä ja kaikilla haastatelluilla oli joitain malleja, sen suunnittelee yleensä tietoturvallisuusosasto, -päällikkö tai -arkkitehti, joskus myös yhdessä esim. tuotepäälliköiden kanssa. Taas tässäkin kohtaa suunnitteluvastuu riippuu siitä, onko tietoturvallisuus osa jotain muuta kokonaisuutta. Kokonaisuuden ylläpidosta voi olla vastuussa myös esim. laatupäällikkö tai riskienhallintapäällikkö [18]. Tai jos tietoturvallisuus on osa jotain arkkitehtuurimallia, tällöin yleensä nimetty arkkitehti on ylläpitovastuussa [16,17].

Tietoturvavaatimusten toteutumista prosesseissa, projekteissa tai tuotantolinjoissa on varmistamassa yleensä joku vastuullinen, joka voi olla security lead, tuotteen tai projektin tietoturvavastaava tai muu [16,19,20]. Hyvin toimintaan integroidut vaatimukset on kuvattu osana prosesseja, ja tällöin myös muutokset vaatimuksiin käydään prosessikohtaisesti läpi [19].

Lähtötiedot ylläpitotarpeeseen tulee yleensä joko asiakkaan tai regulaation kautta. Yhä vähemmän on vapauksia toteuttaa mitään best practise -tyyppistä vaatimuskokoelmaa. Jotkut yritykset tekevät säännönmukaista ylläpitoa vaatimuskokoelmalleen, esimerkiksi ohjeistuksen tarkastuksen kerran vuodessa

[19]. Toiset taas huomioivat muutokset projekteissa, joissa syntyvistä vaatimuksista kootaan yleisen tason uusi versio tarvittaessa [16].

Vaatimusten toteutuminen tarkastetaan auditoinneilla, validoinneilla, sisäisillä tarkastuksilla tai säännöllisillä haavoittuvuus- ja penetraatiotesteillä [18,19,20]. Vaatimusten käytäntöön vienti vaatii jatkuvaa hyötyjen argumentointia ja perusteluja asiantuntijoille [16,20]. Pakkokeinoista ei yleensä koeta olevan hyötyä, vaan käytäntöön vienti sitouttamisen kautta toimii paremmin.

Käytäntöön viennissä on havaittu, että turvaprosessin jalkauttaminen eli ajatus siitä, että tietoturvallisuusarkkitehtuurin vaatimukset toteutetaan, on se josta on eniten hyötyä. Teknologia kehittyy koko ajan ja tekniikoita on joka yrityksessä käytössä sen verran, että yksityiskohtaisten vaatimusten ajan tasalla pitäminen voi olla vaikeaa [17].

Haasteina koettiin jatkuvan vuoropuhelutarpeen lisäksi globaali ympäristö, riittävä verkostoituminen ja mentoroinnin tarve. Globaali ympäristö tuo haasteita luonnollisesti ihan jo kulttuurierojen ja vuorokausirytmin kautta [20]. Mentoroinnissa skaalautuvuus ei ole kovin hyvä ja mentoroinnin vaikutukset näkyvät vasta pitkällä tähtäimellä. Etämääräykset eivät turva-asioissa kuitenkaan toimi. Tietoisuuden kasvattamisen koettiin olevan avainasemassa, koska paitsi teknologian monimuotoisuus, joka vaikuttaa yksityiskohtaisen tason hajautumiseen, aina on myös uhkia, joita ei ole ehditty tai osattu viedä tietoturvallisuuskäytäntöihin, jolloin ainoa keino on implementoijan tietoisuus turvallisuustavoitteista yleisellä tasolla [20]. Johdon tuen näkivät kaikki hyvin oleellisena, jotta ylipäätään on olemassa edellytykset tietoturvallisuuden toteutukseen.

Vahvuutena nähtiin hyvä tasapainotus keskitetyn ja hajautetun tietoturvallisuusorganisoinnin välillä. Tällöin saadaan aikaan paitsi riittävä vuoropuhelu, voidaan olla suhteellisen varmoja, että arkkitehtuurivaatimukset toteutetaan riittävästi ja oikein [20].

Niissä yrityksissä, joissa tietoturvallisuusarkkitehtuuri on luotu, on positiivisina kokemuksina todettu, että arkkitehtuuri auttaa ymmärtämään ja hallitsemaan

kokonaisuuksia, standardoimaan rajapintoja, selvittämään riippuvaisuuksia sekä helpottaa toimittajien kanssa tekemistä ja niiden hallitsemista. Yleisenä ongelmana taas koettiin tietoturvallisuusarkkitehtuurien ja -politiikkojen ylläpidon haasteet yrityksen dynaamisessa toimintaympäristössä [17].

Haastattelutulosten lisäksi voisi yleisesti ottaen vielä todeta, että tietoturvallisuusarkkitehtuurin jalkautuksessa on huomioitava myös oman henkilökunnan ja alihankkijoiden erityyppiset roolit, mitä palveluita kukin rooli tuottaa ja missä prosessissa. Siitä saadaan selville, mitä tietoa tietoturvallisuusarkkitehtuurista ja sitä kautta tietoturvallisuuspolitiikoista ko. roolissa tai prosessissa tarvitaan. Tämän jälkeen voidaan suunnitella koulutusohjelmat, joissa tietoturvallisuusarkkitehtuuri huomioidaan. Koulutus voi tapahtua joko osana kokonaisarkkitehtuurikoulutusta, tietoturvallisuuskoulutusta, projektikoulutusta, prosessikoulutusta tai näiden yhdistelmänä. Valittu tapa riippuu organisaatiosta ja koulutettavasta kokonaisuudesta.

Alihankkijoiden ollessa kokonaiskuvassa mukana, tulee kokonaisuudesta entistä monimutkaisempi ja tarve ajantasaiseen arkkitehtuuriin on entistä suurempi. Keskeisten alihankkijoiden ja kumppaneiden kanssa kannattaa tehdä arkkitehtuurityötä yhdessä. Tällöin tavoitteet avautuvat tarkemmin ja paremmin molemmille osapuolille ja valvontatarve vähenee.

Mitä useampi rooli yrityksen toimintaan liittyy, sitä enemmän tarvitaan rooli- ja prosessikohtaista tietoturvallisuusarkkitehtuurin maanläheistämistä ja tarkempaa ohjeistamista. Kun tietoturvallisuuden tietoisuus kasvaa, ja sitä kautta tietoturvallisuuden kypsyystaso kasvaa, sitä enemmän voidaan jättää roolien ja prosessien omaan harkintaan tietoturvallisuusarkkitehtuurin tavoitteiden toteuttamistavat. Tällöin voisi uskoa, että ylläpitoprosessi kevenee. Alussa vaaditaan kuitenkin kovaa työtä ja prosessien ja roolien ymmärrettäviä esimerkkejä runsaasti. Tietoisuuskoulutus pitää myös toistaa määrävälein, jotta tavoitteet ja toteutus pysyvät linjassa.

Koska tietoturvallisuus on osallisena kaikessa yrityksen toiminnassa, on tietoturvallisuusarkkitehtuurin osa-alueiden ylläpitämisvastuu hyvä jalkauttaa hyvin

lähelle itse tuettavia toimintoja. Siellä on paras tietämys liiketoiminnan vaatimusten muuttumisesta ja täten parhaat edellytykset ylläpitää mallia oikea-aikaisesti. Tietoturvallisuusarkkitehtuurin kokonaisvastuun kannattaa sitten olla hieman kauempana operatiivisesta toiminnasta yhdessä paikassa organisaatiossa.

6 Yhteenveto

Monet yritykset tekevät tietoturvallisuuspäätöksiä vain taktisella tasolla. Tällöin ei ole varmuutta ratkaisujen yhteensopivuudesta. Usein ei ole myöskään laskettu ratkaisujen TCO:ta (total cost of ownership) ja on epäselvää, miten ratkaisu tukee liiketoimintaa.

Kuitenkin monella on myös enenevässä määrin ulkoa tulevia regulatiivisia tai asiakasvaatimuksia. Usein vaatimuskokonaisuuksia on useita, jotka kaikki pitää täyttää kokonaan tai osittain. Jotta tietoturvallisuustavoitteet toteutuvat, se on saatavat aidoksi osaksi yrityksen prosesseja ja toimintaa. Tämä ei onnistu ilman kunnollista kokonaisuuden suunnittelua; ja jotta toteutus suuntautuu oikein, on suunnittelu aloitettava strategiselta tasolta tarkentuen operatiivisiin menetelmiin ja työkaluihin.

Tietoturvallisuutta ei toteuteta tietoturvallisuuspäälliköiden ja/tai -asiantuntijoiden toimesta, vaan yrityksen koko henkilökunnan toimesta. Tietoturvallisuuden taso on yhtä korkea kuin sen heikoin lenkki. Tällöin jokaisella henkilökuntaan kuuluvalla on oltava selvillä se, mitä häneltä tietoturvallisuuden osalta odotetaan. Tavoitteet luodaan tietoturvallisuusarkkitehtuurin ja -politiikan avulla ja jalkautetaan koulutuksen, prosesseihin ja projekteihin viennin avulla koko henkilöstölle.

Näyttää siltä, että koko yrityksen kaikki toiminnot kattava tietoturvallisuusarkkitehtuuri on vielä suhteellisen harvinainen, eikä sen luomisessa ole käytetty ainakaan mitään tietoturvallisuusarkkitehtuurimallia hyödyksi, pikemminkin on luotu ohjeistuskokonaisuus, joka saatetaan osaksi muuta vaatimuskokonai-

suutta tai se viedään projekti- tai prosessikohtaisesti koulutuksen ja vuoropuhelun kautta asianosaisille. Mitään yhtä ja ainoaa tapaa toteuttaa tietoturvallisuusmalli ei selvästikään ole. Arkkitehtuuriliitäntä saattaa olla olemassa tai sitten ei. Niin tai näin, johdon sitoutuminen on todettu avainasiaksi, jota ilman on turha yrittää mallia viedä käytäntöön. Tärkeintä on siis ensimmäiseksi varmistaa johdon tietoisuus tietoturvallisuudesta ja siihen liittyvistä yritystä koskevista regulatiivisista ja asiakasvaatimuksista.

Arkkitehtuurimalliksi kannattaa valita malli, joka tukee kokonaisuuden nopeaa hahmotusta. Esitellyistä malleista ainoaksi sellaiseksi voidaan todeta SABSA, joka tukee myös arkkitehtuuriprosessia.

Arkkitehtuurin jalkauttamiseen kannattaa panostaa, eikä se onnistu ilman jatkuvaa vuoropuhelua liiketoiminnan kanssa, riittävää verkostoitumista sekä perusteluja hyödyistä. Tietoturvallisuustietoisuuden kasvattaminen on vuoropuhelussa avainasemassa, sen onnistuminen edellyttää motivoivaa ja viestinnän sekä kasvatustieteiden lainalaisuuksien huomiointia [2]. Toistuvuus ja eri viestintämenetelmien hyväksikäyttö takaa hyvän lopputuloksen.

Tavoitteiden toteutumista seurataan sitten tarkastuksin, jotka vaikuttavat ohjeistuksen ja vaatimusten ylläpitoon. Toisin sanoen, vanha tuttu plan-do-check-act on arvossaan.

Haluan vielä lopuksi kiittää työn ohjaajia, tietoturvapäällikkö Kimmo Helaskoskea ja palvelujohtaja Sami Rajamäkeä. Ilman heidän arvokkaita kommenttejaan ja apuaan tämän työn valmistuminen olisi ollut uhattuna.

7 Lähteet

1. Sherwood, J. , Clark, A. & Lynas, D. 2005. Enterprise Security Architecture - A Business Driven Approach. San Francisco, CA: CMP Books.

2. Puhakainen, Petri, A design theory for information security awareness Faculty of Science, Department of Information Processing Science, University of Oulu, Finland
Acta Univ. Oul. A 463, 2006, väitöskirja

3. Suomen Standardisoimisliitto, ISO/IEC 27001:fi: Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset, 2005

www-sivustot:
4. http://csrc.nist.gov/index.html [viitattu 28.1.2010]
5. http://www.opensecurityarchitecture.org/cms/ [viitattu 29.1.2010]
6. http://www.isaca.org/ [viitattu 30.1.2010]
7. http://www.sabsa-institute.org/ [viitattu 28.1.2010]
8. https://www.pcisecuritystandards.org/index.shtml [viitattu 30.1.2010]
9. http://www.isoiec20000certification.com/ [viitattu 2.2.2010]
10. http://www.27000.org/ [viitattu 2.2.2010]
11. http://www.vm.fi/ [viitattu 15.12.2009]
12. http://www.us-cert.gov/ITSecurityEBK [viitattu 20.2.2010]
13. http://www.luottokunta.fi/fi/pci/ [viitattu 27.2.2010]
14. http://en.wikipedia.org/wiki/Enterprise_information_security_architecture [viitattu 27.2.2010]

Haastattelut:

15. Andersin, Ari, Pääarkkitehti. Keskustelut 17.12.2009 ja 15.2.2010
16. Causton, Raymond, Tietoturvapäällikkö, CISSP, CISA, CISM. Haastattelu 19.2.2010
17. Oja, Kari, IT Security Manager. Haastattelu 24.2.2010
18. Ruusuvaara, Petri, Tietoliikenne- ja tietoturvapäällikkö, CISSP. Haastattelu 19.2.2010
19. Salminen, Helvi, Information Security Manager, CISA, CISSP, SCF, Master of Security. Haastattelu 22.2.2010
20. Waller, Gabriel, Head of Product Security. Haastattelu 17.2.2010