Jarkko Aalto

Organisaatioiden tietoturvamallit

Tietotekniikan pro gradu -tutkielma

27. heinäkuuta 2016

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Jarkko Aalto

Yhteystiedot: jarkko.t.aalto@student.jyu.fi

Ohjaajat: Isomäki Hannakaisa, Kurkinen Erkki ja Kärkkäinen Tommi

Työn nimi: Organisaatioiden tietoturvamallit

Title in English: Enterprise Security Patterns

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Ohjelmistotekniikka

Sivumäärä: 163+113

Tiivistelmä: Tutkielman tarkoituksena on selvittää löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien tai niiden piirteiden käyttöä. Tutkimuskysymyksiksi muodostuivat, miten tietoturvamallit näkyvät tutkittavissa organisaatioissa ja miten organisaatiot huolehtivat tietoturvasta. Tämä tutkimus suoritetaan korkeakouluorganisaatioihin. Aineston analyysimenetelmänä käytän laadullista ankkuroitu teoria -lähestymistapaa.

Avainsanat: Organisaatioiden tietoturva, IT-tietoturvamallit, Tietoturva, Maadoitettu teoria, Avoin koodaus, aksiaalikoodaus, valikoivakoodaus

Abstract: The purpose of this thesis is to find out whether enterprise security patterns or their features exist in the ways that educational organizations treat information security. The research questions are: How enterprise security patterns present themselves in the studied organizations? How do the organizations ensure data security? This research focuses on higher education organizations. The method used for analysis of the gathered material is the Grounded Theory approach.

Keywords: Enterprise Security Patterns, IT Security Patterns, Security, Grounded Theory, Open Coding, Axial Coding, Selective Coding

Termiluettelo

DNS	Domain Name server. Nimipalvelujärjestelmä, jolla muutetaan URL-osoitteet IP-osoitteiksi ja toisinpäin.
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jolla sallitaan verkkoon liittyvälle koneelle protokollan tietokannasta verkon käyttöön tarvittavat verkkoasetukset.
ERM	Entity Relationship Modeling. On käsitteellinen tapa kuvata tietokannan rakennetta.
IEC	International Electrotechnical Commission. IEC on kansainvälinen standardien ja vaatimustenmukaisuuden arviointilaitos kaikille sähköteknisille aloille.
ISC2	The International Information Systems Security Certification Consortium. Kansainvälinen tietoturvasertifiointiyhteenliittymä on voittoa tavoittelematon järjestö, joka on erikoistunut tietoturvakoulutukseen ja sertifikaatteihin.
ISO	International Organization for Standardization. ISO kehittää ja julkaisee kansainvälisiä standardeja.
ISMS	Information Security Management System. Tietoturvan hallintajärjestelmä, jolla kehitetään tietoturvaa vastaamaan muuttuvia organisaation toimintaa ja toimintaympäristöä.
LDAP	Lightweight Directory Access Protocol. LDAPn käyttötarkoitus on käyttäjätunnusten ja käyttöoikeuksien tarkastaminen.
LAN	Local Area Network. Lähiverkko, joka on organisaation sisäinen tietokoneverkko.
SSL	Secure Socket Layer. Tietoverkonsalausprotokolla, jolla suojata Internet-sovellusten tietoliikenne IP-verkkojen ylitse.
UML	Unifies Modeling Language. On yleiskäyttöinen graafinen notaatiotekniikka, jolla voidaan luoda havainnollistavia suunnittelumalleja.
VPN	Virtual Private Network. Virtuaalinen erillisverkko, joilla kaksi

	tai useampi erillisverkko voidaan yhditää julkisen verkon kautta.
WLAN	Wireless Local Area Network. Langaton lähiverkkotekniikka.
WWW	World Wide Web. Internet-verkossa toimiva hajautettu hypertekstijärjestelmä.

Kuviot

Taulukot

Sisältö

1 Johdanto

Organisaatioissa tietoturvan hoidon merkitys ja tärkeys aiheena muuttuu koko ajan tärkeämmäksi kaikissa yhteyksissä. Tässä pro gradu-tutkielmassa paneudutaan selvittämään sitä, löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien käyttöä tai niiden piirteitä. Aikaisempaa tutkimusta tietoturvamallien käytöstä koko organisaatioiden laajuisena tietoturvan hoidon välineenä ei ole merkittävästi tutkittu, mutta rajatumpia tutkimuksia on mm. toteutettu sovelluskehitykseen (ks. Lamminmäki 2008).

Tutkimusta tietoturvan hoidosta on tehty runsaasti. Tämän laaja-alaisen tutkimuksen tuloksen on syntynyt luvuissa 2.6 esiteltyjä kansainvälisiä standardeja ja 2.5 esiteltyjä kansainvälisiä ja kansallisia tietoturvan hoidon viitekehyksiä.

Tutkimusta tietoturvamallien käytöstä tietoturvan hoitoon apuna on tehty runsaasti ja se on ollut erittäin suosittu tutkimuksen kohde viimeisten 15 vuoden ajan. Eri yhteisöt ja tutkijat ovat luoneet luvussa 3.6 esiteltyjä mallikokoelmaluetteloita, joita on järjestelty tarkoituksen mukaisiin kokonaisuuksiksi luvussa 3.7 esitellyillä eri luokittelujärjestelmillä. Tietoturvamallien käyttöstä ohjelmistojen suunnitteluun ja niistä saatuja etuja tietoturvan hoitoon on tutkittu (ks. Yskout, Scandariato ja Joosen 2015).

Tutkimuksessani tarkastellaan kahta eri koulutusorganisaatiota, joista haastatteluun osallistuva kohdejoukko valittiin hyväksikäyttäen lumipallo-otantaa (engl. Snowball Sampling). Otannalla varmistuttiin, että haastateltavat olivat tutkimusongelman kannalta keskeisiä. Tutkielman toteutusmenetelmäksi vakioitui laadullinen tutkimus. Aineistonkeruun menetelmäksi valikoitui puolistrukturoitu teemahaastattelu ja analyysimenetelmänä käytän ankkuroitu teoria-lähestymistapaa (ks. Strauss ja Corbin 1998). Tietoturvan hoidon prosesseja tarkastellaan tutkimusongelman kannalta keskeiseltä kohdejoukolta saadusta raakadatasta, jota on analysoitu laadullisin menetelmin (ks. Strauss ja Corbin 1998, 10–11). Grounded Theory lähestymistapaa on hyödynnetty, jonkin verran tietoturvamallitutkimuksessa (ks. Smith 2012).

Analyysin tuloksena tutkielmassa nousi esille, etteivät koulutusorganisaatiot käytä tietoturvan hoidon apuna tietoturvamalleja. Organisaatiot hoitavat tietoturvaa johdon määritteämien periaatteiden mukaisesti siten, että organisaatioiden tietoturvan hoito on kustannustehokasta.

Tutkielman toisessa luvussa käsittelen tietoturvan teoreettista viitekehystä määrittelemällä sen keskeiset käsitteet, esittelen tietoturvan luokituksen määritelmät ja tarkastelen myös lyhyesti sen historiaa. Esittelen tietoturvaan vaikuttavien kansainvälisten ja kansallisten tietoturvan hallinnan viitekehyksiä ja tietoturvastandardeja. Käsittelen luvussa myös organisaatiotasolla tietoturvallisuuden kokonaisuutta luokittelemalla sen osa-alueet tutkielmassa käytettävän rajauksen mukaisesti organisaatio-, ohjelmisto- ja tietoverkkotasoille.

Kolmannessa luvussa käsittelen tietoturvamallien teoreettisia lähtökohtia, määrittelemällä keskeiset käsitteet ja tarkastelen myös lyhyesti sen historiaa. Esittelen tietoturvamallien hyötyjä organisaation tietoturvan hoitoon ja kuinka näiden mallien virheellistä soveltamista voidaan parantaa antimalleja lähestymistapaa hyväksikäyttämällä. Käsittelen myös tietoturvamalleille yleistä mallipohjaa ja sen tarkoitusta. Esittelen yksittäisten tutkijoiden tai yhteisöjen kehittämiä tietoturvamallipohjaluetteloita sekä niissä käytettyjä luokittelulähestymistapoja. Luvun viimeisessä kappaleessa kuvailen, kuinka tietoturvamalleja tulisi organisaatioissa käyttää.

Neljännessä luvussa käsittelen tutkimuksen toteuttamisen vaiheita, kuten tutkimuksen tehtävän ja tutkimuskysymysten asettelua, tutkimuksen kohdejoukon ja kohdeorganisaation valintaa sekä aineistokeruun toteutumista ja aineistoanalyysiä. Viidennessä luvussa käsittelen tuloksia. Pohdin analysointiprosessissa syntyneiden tuloksia ja läpikäyn tietoturvamallien näkyvyyttä ja tietoturvan hoitoa organisaatioissa. Lopuksi kuudennessa luvussa käsittelen analyysiprosessin tuloksia aikaisempiin tietoturvatutkimuksiin organisaatioiden tietoturvan ja tietoturvamallien osalta. Pohdin tutkielman validiteettia ja luotettavuutta sekä tutkielman käytännön sovellettavuutta ja jatkotutkimusaiheita organisaation tietoturvan ja tietoturvamallien osalta.

2 Tietoturva

Tässä luvussa käsitellään tietoturvan käsitteistöä. Ensimmäisessä alaluvussa käydään läpi tietoturvan määritelmän. Toisessa alaluvussa käsitellään pienimuotoisesti tietoturvan historiaa. Kolmannessa alaluvussa määritellään tietoturvan keskeiset käsitteet. Neljännessä alaluvussa käsitellään tietoturvan luokitusta (engl. Taxonomy). Viidennessä alaluvussa kuvataan tietoturvan kannalta tärkeitä hallinnan viitekehyksiä, joilla ei ole standardin asemaa. Sitten, kuudennessa alaluvussa kuvataan tietoturvaan vaikuttavia tietoturva standardeja ja lopuksi tietoturvan kokonaisuus pilkotaan organisaatiotasolla helpommin käsiteltäviin tietoturvan osa-alueisiin.

2.1 Tietoturvan määritelmä

Suomen lainsäädännössä (VAHTI 3/2007) *Tietoturvallisuuden tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan* tietoturvalla tarkoitetaan organisaation kaikkien järjestelmien sekä tietoliikenteen hallintaa ja suojaamista teknisillä sekä hallinnollisilla toimenpiteillä normaali- ja poikkeusolosuhteissa. Tavoitteena on luvussa 2.4 esiteltyjen tietojen luottamuksellisuuden, eheyden ja käytettävyyden mukainen säilyttämien kaikilta uhilta ja vahingoilta, päämääränä on turvata liiketoiminnan keskeytymätön toiminta. (ks. Andreasson ja Koivisto 2013, 29)

Organisaatioissa tietoturvan määritelmä on käsitteenä varsin laaja-alainen. Suppeimmillaan se voidaan määritellä organisaatioissa tietoturvasta huolehtimiseksi määriteltyjen lakien ja asetusten edellyttämien vähimmäisvaatimusten mukaisesti, vailla selkeitä suunnitelmia ja vastuita. Laajimmallaan se voidaan määritellä organisaation johdolle kuuluvaksi tehtäväkokonaisuudeksi. Kokonaisuudessa liiketoiminta ja tietohallinto nivoutuvat johdon tai johdon alaisuuteen nimeämän tietoturvapäällikön vastuulle, jonka toimenkuvaan sisältyy tietoturvan hallintokokonaisuus. (ks. Laaksonen, Nevasalo ja Tomula 2006, 115)

2.2 Tietoturvan historia

Varhainen tietokonejärjestelmien tietoturvan tutkimus keskittyi 1960-luvun puolivälissä keskuskoneessa olleeseen käyttöjärjestelmään Multics (Multiplexed Information and Computing Service), jonka General Electric (GE), Bell Labs ja Massachusetts Institute of Tecbology (MIT) yhdessä kehittivät. Multics oli ensimmäinen käyttöjärjestelmä, jossa turvallisuus oli integroitu sen ydintoimintoihin. Multics toteutti useita eri turvatasoja ja salasanasuojauksen.

1967 Advanced Research Projects Agency (ARPA) muodosti työryhmän tutkimaan prosessia, jolla haluttiin varmistaa turvaluokiteltuja tietojärjestelmiä. Työryhmän tuotoksena julkaistiin asiakirja RAND - raportti R-609.9 (ks. Willis 1970). Tämä asiakirja oli ensimmäinen julkaistu asiakirja, jossa tunnistetaan johdon rooli ja tietoturvan menettelytavat. Asiakirjassa todettiin, että laaja tietoverkkokomponenttien hyödyntäminen sotilaskäytössä aiheuttaa tietoturvariskejä, joita ei voida lieventää rutiinikäytäntein turvaamaan näitä järjestelmiä. Asiakirja laajensi tietoturvan koskemaan fyysisen sijainnin ja laitteistojen turvallisuutta tietojen turvaamiseksi sekä rajoittamaan satunnaista ja luvatonta pääsyä kyseisiin tietoihin ja jakamaan organisaatiotasolla henkilöstön useisiin tietoturvallisuustasoihin. (ks. Whitman ja Mattord 2011, 5-6)

1970-luvulla muistilaitteiden kehityksen myötä otettiin Yhdysvaltain ministeriöissä, suurissa organisaatioissa ja puolustuksen alalla käyttöön keskuskoneita (engl. Mainframe). Tällöin katsottiin tarpeelliseksi perustaa työryhmä, jonka tarkoituksena oli selvittää miten tilakonemallia varten voitiin luoda monitasoinen turvallisuuspolitiikka sen luottamuksellisille tiedoille. Tutkimusryhmä kehitti Bell-LaPadula (ks. Bell ja LaPadula 1973) tilakonemallin, joka vangitsi luottamuksellisuus näkökohtia kulunvalvontaan. Käyttöoikeudet oli määritelty läpi kulunvalvontamatriisin ja turvatason. Mallin toiminnallisena tarkoituksena oli ehkäistä tiedon virran kulkemisen alaspäin korkeammalta turvatasolta alhaisemmalle turvatasolle. Malli ottaa huomion tiedonkulun joka tapahtuu, kun kohde noudetaan tai kohdetta muutetaan. (ks. Gollman 2009, 7-9)

1980-luvulla ensimmäiset madot ja virukset eivät vielä saastuttaneet tietoverkkoja, vaan ne esiintyivät ensimmäisissä tutkimusraporteissa. Nämä madot kirjoitettiin Xeroxin Paso

Alton tutkimuskeskuksessa ja sen Ethernet-verkossa. (ks. Shoch ja Hupp 1982, 172–180) Tällöin tietokoneenkehityksen murroksesta huolimatta turvallisuustutkimus otti vielä mallia keskustietokoneaikakauden monitasoisen turvallisuuden ja ei-käyttöliittymiä tukevaa Bell-LaPadulan mallista. Vuonna 1985 julkaistiin Trusted Computer Security Evaluation Criteria (Orange Book) (ks. Brand 1985), joka vaikutti voimakkaasti yleisiin tietoturvakäsityksiin. Teoksessa korkea turvallisuuden varmuus ja monitasoinen turvallisuus kulkivat käsi kädessä. (ks. Gollman 2009, 4-6)

1987 kehitettiin Clark-Wilson malli (ks. Clark ja Wilson 1987) kaupallisten sovellusten turvallisuusvaatimuksiin. Tämän mallin vaatimukset olivat pääsiassa tiedon eheyteen liittyviä, eli kuinka estää luvaton tietojen muuttaminen, virheet ja petokset. Eheyttä koskevat vaatimukset on jaettu sisäiseen ja ulkoiseen johdonmukaisuuteen. Sisäisen johdonmukaisuudessa viitataan ominaisuuksiin järjestelmän sisäisessä tilassa, joita voidaan panna täytäntöön tietokonejärjestelmässä. Ulkoisessa johdonmukaisuudessa viitataan järjestelmän sisäisen ja ulkoisen maailmaa välillä olevaan tilaan ja tätä tilaa arvioidaan tietokonejärjestelmän ulkopuolelta. Mallissa käytetään ohjelmia välikerroksena subjektin ja objektin välillä. Subjektilla on lupa suorittaa sille ennalta määrättyjä ohjelmia. Tietoeriin pääsee käsiksi joukolla erityisohjelmia, jotka voivat saada tietyn tyyppisiä tietoja. (ks. Gollman 2009, 223–225)

Ensimmäinen laaja Internet-mato (engl. Morris worm) ilmestyi 1988 ja siinä hyödynnettiin useita tunnettuja haavoittuvuuksia, kuten raakaa voimaa (engl. brute force) salasanan arvaamiseksi etäkirjautumisessa, huonoa rakenteellisuutta sendmailin virheenkorjaustilassa ja puskurin ylivuotoa finger daemonissa. (ks. Gollman 2009, 5) Morris-madon ilmestymisen jälkeen National Computer Security Center (NCSC) järjesti sarjan kokouksia. Näiden kokousten tuloksena DARPA (entinen ARPA) ilmoittaa perustavansa uuden organisaation Computer Emergency Response Teamin (CERT). Organisaation tarkoituksena oli koordinoida vastauksia tietoturvahyökkäyksiin ja ilmoittaa tietoturvan haavoittuvuuksista, suorittaa turvallisuustutkimusta ja kouluttaa tietokoneen käyttäjiä turvallisuuskysymyksissä. Organisaation rahoituksesta ja käynnistämisestä vastaisi U. S. Defence Department, mutta DARPA oli aiemmin perustanut Software Engineering Institute (SEI) tutkimuskeskuksen. Tämän keskuksen tarkoituksena oli mukauttaa ohjelmistoinnovaatioita maanpuolustuksellisin sovelluksiin. Tämän takia DARPAn julkaisemassa CERTin perustamisajankohdan lehdistötiedottees-

sa todettiin, että jokainen tärkeä tietokoneyhteisö voisi päättää oman CERTin perustamisesta. Vaikka tämä oli suoranaisessa ristiriidassa alkuperäiseltä tarkoituksesta luoda keskitetty koordinointikeskus, niin CERT onnistui jo ensimmäisenä toimintavuotenaan raportoimaan kuusi erilaista haavoittuvuutta eri järjestelmien tietoturvallisuudessa. (ks. Leeuw ja Bergstra 2007, 685–686)

1989 ilmestyi Kiinalaisen seinän malli (engl. Chinese Wall Model) (ks. Brewer ja Nash 1989). Mallin turvallisuuspolitiikassa sovelletaan sääntöä, ettei saa olla olemassa tiedostopolkuja, jotka aiheuttaisivat eturistiriitoja. Mallin politiikassa yhdistyvät kaupallinen laillinen hankintavalta ja pakollinen valvonta. Malli sisältää Bell-LaPadula(BLP) ja Clark-Wilson mallien piirteitä. Mallin säännöt on luotu siten, että mikään subjekti ei voi käyttää suoraan objektin tietoja, vaan niihin päästään käsiksi ohjelmien kautta. Mallissa käyttäjäoikeuksien luovutuksen oletetaan olevan staattista ja käyttöoikeudet on jaettava uudelleen jokaisessa tilasiirtymässä. (ks. Gollman 2009, 221–222)

1990-luvulla alkoi Internetin aikakausi. Uudet tekniikat tulivat saataville, kun Cerneissä työskennelleiden Robert Cailliaun ja Tim Barners-Leen kehittämä http-verkkoprotokolla ja HTML-muodossa dokumentteja jakava WWW (World Wide Web) (ks. Berners-Lee 1989) otettiin käyttöön 1990. Internetin yleistyttyä yksittäiset tietokoneet eivät enää toimineet yksin tai kytkettynä lähiverkkoon LAN (engl. Local Area Network). Tällä oli kaksi suurta seurausta. Ensinnäkin järjestelmien omistajan eivät enää kyenneet ohjaaman, kuka pystyi lähettämään syötteitä heidän tietokoneesta, joten tämä sulki pois identiteettiin perustuvan elinkelpoisen suojamekanismin. Toiseksi hyökkääjät kykenivät lähettämään väärin muotoillun syötteen koneen avoimeen porttiin ja näin aiheuttivat puskuriylivuodon. Tahaton puskurinylivuoto voi kaataa ajettavan ohjelman, mutta tahalliset puskuriylivuodot voivat mahdollistaa hyökkääjän muokata turvallisuusjärjestelmien tietoja antamalla väärinmuotoillun arvon johonkin haluttuun muuttujaan. (ks. Whitman ja Mattord 2011, 7), (ks. Gollman 2009, 185)

2.3 Tietoturvan keskeiset käsitteet

Tietoturvan yleisiä keskeiset käsitteet ja määritelmät ovat (ks. Taulukko 1).

Otsikko	Selite
Pääsy(engl. Access)	Pääsy on aiheen tai objektin kyky käyttää, manipuloida, muokata tai vaikuttaa toiseen aiheeseen tai esineeseen. Valtuutetuilla käyttäjillä on asianomaiselta saatu laillinen lupa päästä järjestelmiin, kun taas asiattomilta tämä lupa on pyritty estämään. Tietojärjestelmissä järjestelmänpääsynvalvonnalla kyetään vaikuttamaan tähän. (ks. Whitman ja Mattord 2011, 9)
Riski (engl. Risk)	Todennäköisyys, jolla ei-toivottu tapahtuma toteutuu. Organisaation on määriteltävä riskitaso, jonka organisaatio on valmis hyväksymään. (ks. Whitman ja Mattord 2011, 11)
Uhka (engl. Threat)	Uhka muodostuu, kun esineitä, ihmisiä tai muita tahoja kohtaan esiintyy varaa, joka on aiheutettu tarkoituksenmukaisesti tai tahattomasti (ks. Whitman ja Mattord 2011, 11). Uhkan koostuu uhkan lähteestä, toiminnasta ja seurausosasta. Uhkan lähde käynnistää tapahtuman tai hyökkäyksen, joita voivat aiheuttaa ihmiset tai ympäristö. Toiminnallinen osa sisältää eri menetelmiä, joilla hyökkäys tai tapahtuma toteutetaan. Seuraus on tietoturvaloukkaus, joka on toteutunut ja aiheuttanut toteutuessaan vahinkoa. (ks. Schumacher ym. 2006, 115)
Varat (engl. Assets)	Varat ovat organisaation tai henkilön voimavaroja, jotka ovat suojattu. Tällaisia voimavaroja ovat esimerkiksi WWW-sivustot, tiedot ja varat jotka kohdistuvat ihmisiin, organisaation tietokonejärjestelmiin tai johonkin muuhun konkreettiseen esineeseen. (ks. Whitman ja Mattord 2011, 9)

... jatkuu seuraavalla sivulla

Otsikko	Selite
Hyökkäys (engl. Attack)	Hyökkäys on tahallinen tai tahaton teko, jolla voidaan aiheuttaa vahinkoa tai muuten muuttaa sellaista tietoa, joka on tärkeää. Kohdistetut hyökkäykset voivat olla tahallisia, aktiivisia, tahattomia, suoria, epäsuoria tai passiivisia. Tahallinen tai aktiivinen hyökkäys on asiattoman käyttäjän tunkeutuminen tietojärjestelmään. Tahattomana hyökkäyksenä voidaan pitää ympäristöstä aiheutuvia uhkia. Suoralla hyökkäyksellä tarkoitetaan asiattoman käyttäjä tunkeutumista tietojärjestelmään. Epäsuorat hyökkäykset ovat järjestelmän toimintahäiriöitä tai työntekijöiden aiheuttamia uhkia. Passiiviseksi hyökkäykseksi luokitellaan arkaluonteisen tiedon käyttöön saattaminen. Esimerkiksi ohimennen lukemalla saadaan sellaista tietoa, mikä ei ole tarkoitettu nähtäväksi. (ks. Whitman ja Mattord 2011, 9)
Hyödyntäminen (engl. Exploit)	Hyödyntäminen on tekniikan aiheuttama uhka, joka vaarantaa järjestelmän. Tätä tekniikkaa käyttävät asiattomat lähteet, jotka haluavat hyödyntää järjestelmiä tai muuta tietoa. Hyödyntämisessä käytetään olemassa olevia ohjelmistotyökaluja tai tehtävää varten räätälöityjä ohjelmistokomponentteja. (ks. Whitman ja Mattord 2011, 10)
Tappio (engl. Loss)	Tappiolla tarkoitetaan organisaatiolta varastettuja, vaurioitettuja tai muutettuja tietoja, joita on luovutettu tahattomasti tai tahallisesti. (ks. Whitman ja Mattord 2011, 10)
Haavoittuvuus (engl. Vulnerability)	Haavoittuvuus on vika tai heikkous suojamekanismeissa tai järjestelmässä, joka altistaa sen vahingolle tai hyökkäykselle. (ks. Whitman ja Mattord 2011, 11)

Taulukko 1: Tietoturvan keskeiset käsitteet

2.4 Tietoturvan osa-alueet

Tietoturva määritellään perinteiseen ja laajennettuun tietoturvan luokitukseen (engl. Taxonomy). Perinteinen määritelmä pitää sisällään luottamuksellisuuden, käytettävyyden ja eheyden. Laajennettuun määritelmään on lisätty kiistämättömyys, pääsynvalvonta ja autenttisuus. (ks. Hakala, Vainio ja Vuorinen 2006)

Luottamuksellisuudella (engl. Confidentiality) tarkoitetaan tietojärjestelmätietojen olevan vain niihin oikeutettujen käyttäjien käytettävissä. Luottamuksellisuudella pyritään suojaamaan tietojärjestelmien laitteistot ja tiedontallennusvarastot riittävän suojauksen omaavilla käyttäjätunnuksilla ja salasanoilla. Arkaluonteisia ja arvokkaita tietoja pyritään mahdollisuuksien mukaan suojaamaan eri salakirjoitusmenetelmin. (ks. Hakala, Vainio ja Vuorinen 2006, 6-7) Tällaisia tietoja ovat esimerkiksi henkilöiden palkkatiedot ja organisaatiossa käytettävien sovelluksien tiedot. Tietojen luottamuksellisuus saavutetaan kolmella strategialla, varastoinnin luottamuksellisuudella (engl. Storage Confidentiality), siirron luottamuksellisuudella (engl. Transmission Confidentiality) ja valtuutuksella. (ks. Scandariato ym. 2008, 6-7)

Saatavuus (engl. Availability) antaa valtuutettujen henkilöiden ja tietokonejärjestelmien käyttää järjestelmiä. Saatavuudella pyritään takaamaan laitteistojen ja ohjelmistojen soveltuvuus tietojärjestelmiin riittävällä tehokkuudella ja saatavuudella. Nykyaikaisissa tietojärjestelmissä pyritään tiedonhankinta automatisoimaan siten, että tietoja tarvitsevat saavat haluamansa tiedot nopeasti, heille sopivassa muodossa. (ks. Hakala, Vainio ja Vuorinen 2006, 4-5), (ks. Whitman ja Mattord 2011, 12)

Eheydellä (engl. Integrity) pyritään ohjelmistoteknisin ratkaisuin vaikuttamaan tietojärjestelmien sisältämien tietojen paikkansapitävyyteen ja siihen, että ne eivät sisältäisi tahattomia tai tahallisia virheitä. Eheyttä pyritään ylläpitämään sovelluksin, jotka voidaan ohjelmoida tarkastamaan tallennus- ja tiedonsiirto-operaatioita varmistussummin tai tiivistein. Sovellusten halutaan rajata käyttäjien syötteitä halutuin syöttörajoittein tai syötteiden tarkastuksin. Laitteistotasolla eheyttä pyritään varmistamaan käyttämällä virheitä korjaavia väyliä tai muisteja. Tietoliikenneratkaisuissa käytetään virheiden tunnistus- ja korjausmekanismeilla varustettuja laitteita ja protokollia. Eheyttä voidaan ylläpitää myös eri ohjelmistoilla, joilla tiedot voidaan salakirjoittaa. (ks. Hakala, Vainio ja Vuorinen 2006, 5)

Kiistämättömyydellä (engl. Non-Repudiation) tarkoitetaan järjestelmäkäskyjä, joilla tunnistetaan ja tallennetaan järjestelmää käyttävien henkilöiden tiedot. Kiistämättömyydellä varmistutaan tiedon alkuperästä ja estetään olemassa olevan tietojen luvaton käyttö. (ks. Hakala, Vainio ja Vuorinen 2006, 4-5)

Pääsynvalvonnalla (engl. Access Control) tarkoitetaan menetelmiä, joilla pyritään estämään ulkopuolisia ja henkilöstöä käyttämästä organisaation laitteita omiin tarkoituksiinsa. Tämä saattaa kuormittaa tietoliikenneverkkoja ja täten heikentää käytettävyyttä. (ks. Hakala, Vainio ja Vuorinen 2006, 4-5)

Autenttisuus (engl. Authentication) tarkoittaa tietojärjestelmää käyttävien toimijoiden kuten ihmisten ja järjestelmän laitteiden luotettavaa tunnistamista. Autenttisuus liittyy yksistään tai yhdessä johonkin, mitä henkilö on, tietää tai mitä hänellä on. Tietoverkossa käyttäjän tunnistetaan salasanoin ja järjestelmän laitteet tunnistetaan esimerkiksi digitaalisin tunnistein. (ks. Kettula 1999, 95–96)

2.5 Tietoturvan hallinnan viitekehykset

Organisaation tietoturvan hallintaan on kehitelty liiketoimintaa tukevia erilaisia toimintamalleja eli viitekehyksiä. Näissä toimintamalleista käsitellään organisaation tietoturvaa sen liiketoiminnan kokonaisuutena. Toimintamallit pitävät sisällään järjestelmien tai liiketoiminnan tärkeimpiä osa-alueita, kontrolleita tai prosesseja. Nämä toimintamallit eivät kuitenkaan ole saavuttaneet standardin asemaa. (ks. Laaksonen, Nevasalo ja Tomula 2006, 92) Tässä tutkielmassa viitekehyksistä esitellään Trusted Computer System Evaluation Criteria, GAISP, Suomessa julkiselle sektorille valtionvarainministeriö on laatinut Vahti-ohjeistukset (ks. Valtionvarainmisteriö 2013b) ja Suomessa 7.1.2015 kumottu ISO/IEC 17799 standardi tietoturvallisuuden hallintaa koskeva viitekehys (ks. SFS 2006). Nämä viitekehykset on esitelty tämän kappaleen alaluvuissa.

2.5.1 Trusted Computer System Evaluation Criteria

Tietoturvan yleisiä kriteereitä (engl. Evaluation Criteria) kehitettiin 1980-luvun alusta alkaen. Tarkoituksena oli luoda kansainvälisesti yleishyödyllisiä arviointiperusteita informaa-

tioteknologian käyttöön. Ensimmäisiä tietoturvan arviointiperusteita käsitelevä teos Trusted Computer System Evaluated Criteria (TCSEC) kehitettiin Yhdysvalloissa 1985 (ks. Brand 1985). Teoksessa käsiteltiin tyypillisiä turvallisuusvaatimusmalleja, jotka olivat olemassa, kun kriteerit laadittiin. Tietyt varmuuden ja turvaominaisuusvaatimukset on määritelty arvioinnin luokkiin. Luokat on jaettu neljään turvallisuusosastoon ja seitsemään turvallisuusluokkaan. Turvallisuusluokat on määritelty asteittain ja kaikki vaatimukset alemmasta luokasta sisältyvät automaattisesti turvamekanismein ylempiin luokkiin. Korkeammat turvallisuusluokat tarjoavat paremmat turvamekanismit ja suuremman varmuuden. Turvallisuusosastot on esitelty (ks. Taulukko 2). (ks. Gollman 2009, 4-6)

Turvallisuusosasto	**Turvallisuusluokka**
D	Vähäinen suojaus
C	Harkinnanvarainen suojaus 'Hyvä tietää' C1: Harkinnanvarainen tietoturvasuojaus C2: Harkinnanvarainen pääsynhallinta
B	Pakollinen suojaus (perustuen 'luokitukseen') B1: Merkitty tietoturvasuojaus B2: Turvallisuus verkkotunnukset
A	Vahvistettu suojaus A1: Vahvistettu suunnittelu

Taulukko 2. Tietoturvan ominaisvaatimuksien mukainen turvaluokitus eri tasoittain

Ensisijaisena tavoitteena lähestymistavassa on osittaa, että arvioitava järjestelmä täyttää sille asetetun turvallisuustason. Vaatimuksina ovat tietyt suojamekanismit ja täytäntöönpanon oikeellisuus. Haittapuolena arviointiperusteissa on, että se keskittyy luvussa 2.6.2 esitettyihin yksittäisiin arvioinnin tasoihin (engl. Target of Evaluation (TOE)). Järjestelmältä odotettavien vaatimusten täyttäminen on kallista ja aikavievää, koska arviointiprosessin läpivienti on erittäin monimutkaista ja vaatii paljon tietoturvaosaamista. Lisäksi kaikkien järjestelmän TOE:n ajan tasalla pitäminen on erittäin vaikeaa. (ks. Schumacher ja Roedig 2001, 3)

2.5.2 GAISP

GAISP (engl. Generally Accepted Inforfmation Security Principles) viitekehyksen tarkoituksena on toimia tietolähteenä tietojärjestelmien ja laitteiden käyttäjille. GAISP on päivitetty version GASSPista (engl. Generally Accepted System Security Principles), jossa System nimi on korvattu kattavammalla Information sanalla. Tämä viitekehys perustuu 1990 Yhdysvaltain kansallisen turvallisuuskeskuksen julkaisemaan teokseen Computer at Risk (ks. Sciences 1991). Nykyistä GASSPia kehittää ja ylläpitää ISSA (Internaltional System Security Association) järjestö, jonka tukena toimivat standardoimisorganisaatio ISO ja kansainvälinen tietoturvasertifiointiyhteenliittymä ISC2. (ks. Laaksonen, Nevasalo ja Tomula 2006, 100)

GAISP:n tarkoituksena on toimia tietoturvan hoidon viitekehyksenä riippumatta siitä, mitä tietoturvastandardeja, periaatteita tai menetelmiä organisaatiossa halutaan käyttää. Viitekehys jakautuu yleisiin, yleisluontoisiin ja yksityiskohtaisiin periaate osa-alueisiin siten, että koko organisaation tietoturva tulisi täytetyksi. Yleiset periaatteet on tarkoitettu organisaation johdon toteutettavaksi, sisältäen kaikki organisaation perusperiaatteet esimerkkinä mainittakoon eettisyyden ja vastuunjaon periaatteet. Yleisluontoiset periaatteet on tarkoitettu operatiivisen johdon toteutettavaksi ja ne kuuluvat johdon määrittelemien yleisten periaatteiden alaisuuteen ja tarkoituksena niillä on olla kuvailevampia, esimerkkinä mainittakoon tietoturvapolitiikkaa ja tiedonhallinta. Yksityiskohtaiset periaatteet ovat suunnattu tietoturvan toteuttamisesta vastaavalle henkilöstölle. Nämä periaatteet antavat yksityiskohtaisia ohjeita ylemmäntason periaatteiden toteuttamiseksi. (ks. Laaksonen, Nevasalo ja Tomula 2006, 100–103)

2.5.3 VAHTI-ohjeet

Vahti-ohjeet ovat valtioneuvoston ja valtionvarainministeriön luoma erittäin kattava yleinen tietoturvaohjeisto, joka sisältää valtionhallinnon tietoturvallisuutta koskevia säädöksiä, suosituksia ja ohjeita sekä muita tietoturvallisuuden linjauksia.Ohjeistuksen tarkoituksena on ohjata tietoturvallisuuteen liittyvässä päätöksenteossa. Ohjeistuksen toiminnallinen tarkoitus on parantaa valtionhallinnon päätösten ohella julkisyhteisöjen tietoturvallisuutta. (ks.

Valtionvarainmisteriö, 2008b) Suomalaisten organisaatioiden kannattaa huomioida Vahti-ohjeistus tietoturvan suunnittelussa, koska kansallisia standardeja ei vielä ole olemassa ja Vahti-ohjeistus noudattaa kansainvälisiä standardeja. (ks. Hakala, Vainio ja Vuorinen 2006, 46) Vahti-ohjeistus on kokonaisuudessaan saatavissa osoitteesta `https:www.vahtiohje.fi/web/guest/home`.

2.5.4 Tietoturvallisuuden hallintaa koskeva viitekehys

Tietoturvallisuuden hallintaa koskevassa viitekehyksessä otetaan kantaa opastuksen keinoin organisaation tietohallinnan käyttöönoton, ylläpidon ja tavoitteiden parantamiseen. Ohjeistuksen käytäntöjen pohjalta voidaan organisaatioissa kehittää tietotuvallisuushallinnan tavoitteita ja tehostamaan käytäntöjä joilla voidaan lisätä yhteistyökumppaneiden välistä luottamusta.

Viitekehyksessä esitellään tietoturvan valvonnassa tarvittavia yhtälöitä, joita tarvitaan riskinarvioinnissa sekä riskien käsittelyssä. Viitekehys on jaettu eri tietoturvan aihealueisiin ja nämä jakautuvat tarkentaviin ala-aiheisiin (ks. SFS 2006). Viitekehyksen aihealueita ovat:

- **Turvallisuuspolitiikka**. Organisaation johdon tuki tietoturvallisuuden toteuttamiselle sen liiketoiminnantavoitteiden ja asiaankuuluvien lakien ja asetusten mukaisesti. (ks. SFS 2006, 28)
- **Tietoturvallisuuden järjestäminen**. Organisaation johdon hyväksymän tietoturvapolitiikan mukaisen hallintarakenteen toteuttamista siten, että siihen käytetään organisaation sisäistä tai ulkopuolista tietoturva-asiantuntemusta. (ks. SFS 2006, 32)
- **Suojattavien kohteiden hallinta**. Organisaatiotasolla suojattavilla kohteilla on riittävä suojaus ja ylläpito siten, että kohteet on lueteltu ja dokumentoitu ja niiden hoitamiseksi on nimetty vastuuhenkilöt. (ks. SFS 2006, 50)
- **Henkilöstöturvallisuus**. Tällä varmistetaan, että kaikki toimijat organisaatiossa ovat tietoisia tietoturvallisuuteen kohdistuvista uhkista ja niiden merkityksestä sekä velvollisuuksistaan ja vahinkovastuista. (ks. SFS 2006, 62)
- **Fyysinen ja ympäristön turvallisuus**. Organisaatio estää toiminnoillaan ja sijoittelulla luvattoman tunkeutumisen organisaation toimitiloihin ja tietoaineistoihin. Toi-

mintoina voi olla turvasulut ja kulunvalvontalaitteistot, joilla luodaan suojattuja turva-alueita. Tietotoaineistojen kuluu sijoittaa siten, että ne suojataan luvattomalta käytöltä, vahingoilta ja häirinnältä. (ks. SFS 2006, 68)

- **Tietoliikenteen ja käyttötoimintojen hallinta**, joilla varmistetaan tietojenkäsittelypalvelujen asianmukainen ja turvallinen käyttö, siten että käyttötoimintaan määritellään ohjeistus ja velvollisuudet. (ks. SFS 2006, 80)
- **Pääsyoikeuksien hallinta**. Organisaation tulisi laatia pääsynvalvontasäännöstöt, joissa määritellään pääsy organisaation tietoihin, tietojenkäsittelypalveluihin ja liiketoimintaprosesseihin turvallisuus- ja liiketoimintavaatimuksien mukaisesti. (ks. SFS 2006, 122)
- **Tietojärjestelmien kehitys**. Tavoitteena on varmistaa, että organisaation tietojärjestelmiin kuuluvat infrastruktuuri, käyttöjärjestelmät, liiketoimintasovellukset, palvelut kehitetään turvalliseksi. (ks. SFS 2006, 152)
- **Tietoturvahäiriöiden hallinta**. Tavoitteena on, että organisaation tietojärjestelmiin ja tietoturvatapahtumiin liittyvistä heikkouksista raportoidaan riittävän nopeasti niistä vastaaville tahoille. Tällöin varmistetaan se, että korjaaviin toimenpiteisiin voidaan ryhtyä riittävän ajoissa. (ks. SFS 2006, 176)
- **Liiketoiminnan jatkuvuuden hallinta**. Tavoitteena on ehkäistä organisaation liiketoiminnan keskeytyminen sekä suojata kriittisiä liiketoimintaprosesseja tietojärjestelmien merkittävien häiriöiden tai onnettomuuksilta ja tällöin taata prosessien toimita. Hallinnan tulisi sisältää riskien tunnistamisen turvamekanismit, joilla rajoitetaan vahingollisia tapauksia ja taataan liiketoimintaprosessien käytettävyys. (ks. SFS 2006, 184)
- **Vaatimustenmukaisuus**. Tavoitteena on kaikkien lakien, säännösten ja turvallisuusvaatimusten ja sopimusten noudattaminen, sekä organisaation tietojärjestelmien suunnitteluun, käyttöön kohdistuvien säädösten ja asetuksiin perustuvien turvallisuusvaatimuksien noudattaminen. (ks. SFS 2006, 192)

2.6 Tietoturvastandardit

ISO/IEC-tietoturvastandardit on pääsääntöisesti tarkoitettu ja suunniteltu yksityissektorin käyttöön, mutta niitä voidaan soveltaa myös julkishallinnon organisaatioissakin. Nämä kansainväliset standardit eivät välttämättä aseta tietoturvalle vaatimuksia, vaan ne ovat erittäin hyödyllisiä suunnittelussa syntyville dokumenteille, antaen esitettäville tuloksille sisällön ja hyödyllisen muodon. (ks. Hakala, Vainio ja Vuorinen 2006, 46)

2.6.1 ISO/IEC 27000 Standardisarja

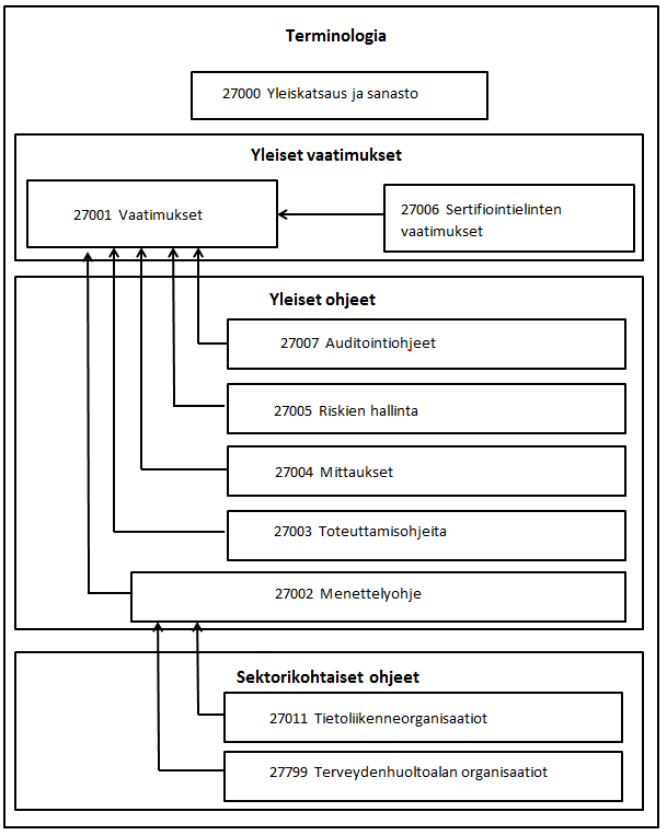
ISO/IEC 27000-standardisarjaa hyväksikäyttämällä organisaatiot kykenevät kehittämään ja toteuttamaan tietoturvan hallinnan perustason ja valmistelemaan riippumattomia tietotuvan ulkoisen arvioinnin tietoturvanhallintajärjestelmälle. 27000-standardisarja pitää sisällään terminologian, yleiset vaatimukset, yleiset ohjeet ja sektorikohtaiset ohjeet (ks. Kuvio 1). Nämä tasot on esitelty myöhemmin tässä kappaleessa. Sarja soveltuu kaupallisille ja ei-kaupallisille yrityksille sekä julkisille organisaatioille. Hyötyinä standardien käytöstä on tietoturvariskien pienentyminen. Ne myös auttavat luomaan toimintamallin riskienhallintaan sekä tarjoavat yhteisen kielen ja käsitepohjan, mikä helpottaa saavuttamaan liikekumppanien luottamuksen. (ks. Suomen Standardisoimisliitto, 2009a)

Terminologia

ISO/IEC 27000:2009-standardissa määrittää tietoturvan hallintajärjestelmä ISMS (engl. Information Security Management System). Tietoturvallisuuden hallintajärjestelmää luodessa organisaation on tunnistettava tieto-omaisuus ja siihen liittyvät turvallisuusvaatimukset, arvioitava tietoturvariskit, valittava asianmukaiset turvamekanismit ja tarkkailtava, ylläpidettävä sekä parannettava niitä. (ks. Suomen Standardisoimisliitto, 2009a)

Yleiset vaatimukset

ISO/IEC 27001-standardissa käsitellään tietoturvallisuuden hallintajärjestelmän luomista ja käyttöä koskevia vaatimuksia sekä turvamekanismeja, joiden avulla voidaan hallita ja lieventää tieto-omaisuuteen liittyviä riskejä. Nämä riskit sisältävät informaation, ohjelmistot (tieto-



Kuvio 1. 27000-standardin viitekehys

koneohjelmisto), fyysiset kohteet (tietokone), palvelut, ihmiset (pätevyys, taito ja kokemus) ja aineettomat kohteet (maine ja julkiskuva). (ks. Suomen Standardisoimisliitto, 2009a)

Tietoturvallisuuden hallintajärjestelmän vaatimuksissa esitettyjen valvonnantavoitteiden ja turvamekanismien kattavan tunnistuksen jälkeen organisaatio voi hakea auditointia ja sertifiointia. Standardin mukaan tietoturvan hallinta ja johtaminen on jatkuvassa muutostilassa oleva prosessi, jota hallintajärjestelmällä kehitetään. Tämän prosessimainen toimintatapa perustuu suunnittele-toteuta-arvio-toimi PDCA-mallin (engl. Plan-Do-Check-Act). Suunnittelussa asetetaan tavoitteet ja laaditaan suunnitelmat. Toteutusvaiheessa toteutetaan nämä suunnitelmat. Arvioinnissa mitataan saadut tulokset. Toiminnan vaiheessa korjataan ja parannetaan suunniteltuja toimintoja. (ks. Suomen Standardisoimisliitto, 2009a)

Yleiset ohjeet

ISO/IEC 27002 standardi menettelyohje sisältää tietoturvastandardeja ja tietoturvallisuuden hallintakäytänteitä koskevia ohjeita riskien huomioimiseksi. Standardi pitää sisällään 14 hallintaa liittyvää pääkohtaa, jotka on jaettu 35 pääturvallisuusluokkaan ja nämä sisältävät yhteensä 114 hallintakeinoa. Nämä kaikki pääkohdat eivät ole pakollisia, vaan niitä sovelletaan silloin kun organisaatio on tunnistanut niiden olemassaolon. Pääturvallisuusluokkia ovat tietoturvapolitiikka, tietoturvallisuuden organisointi, henkilöturvallisuus, suojattavan omaisuuden hallinta, pääsynhallinta, salaus, fyysinen turvallisuus, ympäristön turvallisuus, käyttöturvallisuus, viestintäturvallisuus, tietoturvahäiriöiden hallinta, vaatimustenmukaisuus, liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia, suhteet toimittajiin sekä järjestelmien hankkiminen, kehittäminen ja ylläpito. (ks. Suomen Standardisoimisliitto 2013)

ISO/IEC 27003 standardi toteuttamisohjeet sisältää tietoturvallisuuden hallintajärjestelmän projektin aloittamisen, suunnittelun ja määrittelyn. Hallintajärjestelmän suunnittelu pitää sisällään vaiheet, joita ovat 1) Johdon hyväksyntä ISMS-projektille, 2) ISMS järjestelmän kattavuuden, rajoitteiden ja toimintaperiaatteiden määrittelemisen 3) Tietoturvallisuusvaatimusten analysoinnin 4) Riskien arvioinnin ja riskien käsittelyn suunnittelun 5) ISMS-järjestelmän suunnittelun. (ks. Suomen Standardisoimisliitto 2010)

ISO/IEC 27004 mittaukset sisältää mittaustoimintojen lähtötietojen ja tulosten suhdetta. Tietoturvamittakusilla on ISMS-järjestelmässä suunnittele-toteuta-arvioi-toimi kaavion mukaiset tavoitteet. Suunnitteluvaiheessa valitaan tavoitteet ja turvamekanismit määriteltyjen riskien käsittelyyn. Toteutus vaiheessa toteutetaan valitut turvamekanismit, määritellään miten valittuja turvamekanismien vaikutusta mitataan ja varmistutaan että turvamekanismien vaatimukset on täytetty. Arviointivaiheessa johdon toimesta katselmoidaan hallintajärjestelmän vaikuttavuutta, arvioidaan riskejä sekä jäännösriskin ja riskitason suhdetta. Toiminta vaiheessa parannetaan päätetyt parannustoimenpiteet, joita on löydetty arviointi kohdassa. (ks. Suomen Standardisoimisliitto, 2009b)

ISO/IEC 27005 standardi tietoturvariskien hallinta sisältää organisaation tietoturvariskien hallintaprosessin ja siihen liittyvien toimintojen kuvauksen. Tietoturvavaatimukset ja tietoturvallisuuden hallintajärjestelmän edellyttää tietoturvariskien hallintaa. Tämän hallintajär-

jestelmän toimintamallin olisi sovittava organisaation toimintaympäristöön ja se olisi oltava linjassa määritellyn riskienhallinnan kanssa. (ks. Suomen Standardisoimisliitto, 2011a)

ISO/IEC 27007 standardi tietoturvallisuuden hallintajärjestelmän auditointiohjeet sisältää vaatimukset tietoturvahallintajärjestelmän auditoinitohjelmien hallinnan, auditointien suorittamisen ja auditoijen pätevyysvaatimukset. Auditointiohjelmien hallinnalla tarkoitetaan tavoitteiden määrittämistä, joita tarvitaan auditoinnin suunnittelu ja toteutusvaiheessa, jotta voidaan varmistua siitä, että auditointiohjelmaa kyetään toteuttamaan onnistuneesti. Auditoinnin suoritus onnistuu, jos hallintajärjestelmän tallenteet ovat katselmoitavissa. Auditoijien pätevyysvaatimuksissa määritellään tiedot ja taidot joita auditoijalta vaaditaan. (ks. Suomen Standardisoimisliitto, 2011b)

Sektorikohtaiset ohjeet

ISO/IEC 27011 standardi tietoliikenneorganisaatiot sisältää tietoturvahallintajärjestelmän ohjeistusta. Tarkoituksena on antaa tukeva ohjeistus tietoturvallisuuden hallinnan toteuttamiseen tietoliikennealan organisaatioissa. (ks. Suomen Standardisoimisliitto, 2009a)

ISO/IEC 27799 standardi terveydenhuoltoalan organisaatiot sisältää terveydenhuollon organisaatioiden tietoturvaa ja muille terveydenhuolloin palveluntarjoajille tiedonhankinnan ohjauksen. (ks. Suomen Standardisoimisliitto, 2008a)

2.6.2 ISO/IEC 15408 Tietoturvan arviointiperusteet

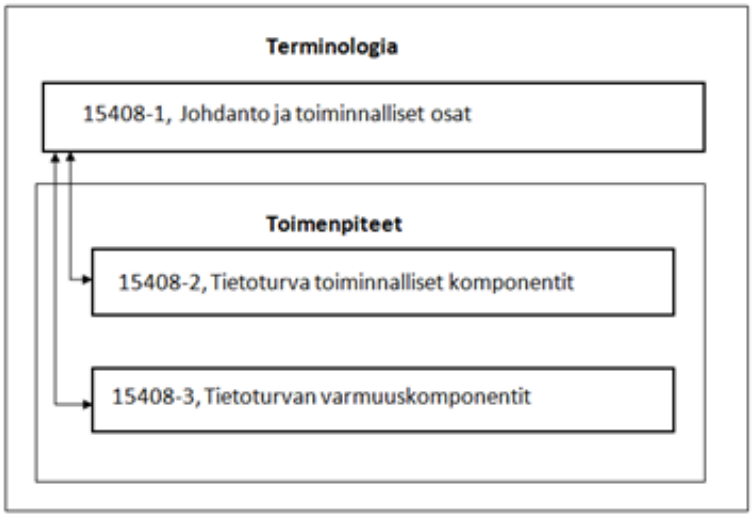
Tietoturvan arviointiperusteiden (engl. Common Criteria) pohjana toimii Yhdysvalloissa 1985 julkaistu ja luvussa 2.5.1 esitelty Trusted Computer System Evaluated Criteria (TCSEC). Tämän teoksen ilmestymisen jälkeen useat eri yhteisöt kehittivät arviointiperusteita. Merkittävimpiä julkaisuja ovat Euroopan komission 1991 julkaisema Information Tecnology Evaluation Criteria (ITSEC) Versio 1.2 (ks. Communities–Commission ym. 1991), Kanadassa 1993 julkaistu The Canadian Trusted Computer Product Evaluation Criteria (ks. Newstaff 2013) ja Yhdysvalloissa 1993 julkaistu Federal Criteria for Information Tecnology Security (FC) versio 1.0 (ks. Standards, (NIST) ja (NSA) 1992) ja vuonna 1999 julkaistu ISO/IEC 14508 Common Criteria standardisarjan ensimmäinen painos. (ks. Gollman 2009, 238–244)

ISO/IEC 15408-standardisarja on jaettu kolmeen tarkoituksenmukaiseen osaan ja siinä määritellään kolme pääkäyttäjäryhmään. Ryhmät ovat kuluttajat (engl. Consumers), kehittäjät (engl. Developers) ja arvioijat (engl. Evaluators). Kuluttajien kannalta standardisarjalla varmistetaan, että arvioinnilla täytetään kuluttajien, kuluttajaryhmien, eturyhmien sekä riippumattoman rakenteen täytäntöönpanon arvioinninsuojausprofiilit (engl. Evaluation of Protection Profiles (PP)) siten, että niitä voidaan käyttää tai niillä voidaan seurata vastaavatko arvioinnin tulokset organisaatioissa laadittujen riskianalyysin ja politiikka dokumentteja. Lisäksi tuetaan kehittäjien mahdollisuuksia valmistella ja avustaa arvioinninkohteesta (engl. Target of Evaluation (TOE)) ja tunnistamaan arvioinninkohteen turvallisuusvaatimukset, jotka sisältävät toteutuskohtaiset turvallisuuden tavoitteet (engl. Security Targets (ST)). Standardi sisältää kuvauksen yleisistä toimista, joita arvioitsijoiden on suoritettava. (ks. ISO, 2008b, 20–21)

Standardisarja sisältää kolmeen eri julkaisuun. Ensimmäinen osa on johdanto ja toiminnalliset osat (engl. Introduction and General Model) (ks. ISO 2009), jossa määrittää standardisarjassa käytettävät yleiset käsitteet ja periaatteet tietoturvan arviointiin. Lisäksi esitetään yleisen malli arvioinninkohteesta. Toinen osa on tietoturvan toiminnalliset osat (engl. Security Functional Components) (ks. Suomen Standardisoimisliitto 2008c), luetellaan joukko toiminnallisia komponentteja ja järjestellään ne luokiksi. Kolmas osa on tietoturvan varmuuskomponentit (engl. Security Assurance Components), jossa luetellaan joukko varmuuden komponentteja ja järjestetään ne luokkiin ja määritellään arvioinninsuojausprofiilit (engl. Evaluation of Protection Profiles (PP)) ja esitellään turvallisuuden tavoitteet (engl. Security Targets (ST)) ja ennalta määritellyt varmuuden paketit (engl. Evaluation Assurance Levels (EALS)) (ks. Kuvio 2). (ks. ISO, 2008b, 22–23)

2.7 Tietotuvan toteutus organisaatiossa

Organisaatiotasolla tietoturva voidaan jakaa kahdeksaan eri osa-alueeseen, jotta kokonaisuutta olisi helpompi hallita. (ks. Andreasson ja Koivisto 2013, 52) Kirjallisuudessa esiintyy useita eri tapoja eritellä organisaation tietoturvaa. Tässä tutkielmassa se jaetaan perinteisellä organisaatioiden käyttämällä tavalla ja tutkielman rajauksen (ks. Kuvio6) mukaisesti.



Kuvio 2. ISO/IEC 15408-standardisarjan viitekehys

- Organisaation turvallisuus
  - Hallinnollinen turvallisuus
  - Henkilöstöturvallisuus
  - Fyysinen turvallisuus
  - Laitteistoturvallisuus
  - Tietoaineturvallisuus
  - Käyttöturvallisuus
- Ohjelmistoturvallisuus
- Tietoliikenneturvallisuus

2.7.1 Organisaation tietoturva

Hallinnollinen turvallisuus

Hallinnollisella turvallisuudella tarkoitetaan organisaation tietojärjestelmien tietoturvan eri osa-alueiden johtamista. Tavoitteena on varmistaa, että tietoturvan ohjaus ja kehitys ovat riittävän hyvällä tasolla. Tämän tavoitteen varmistamiseksi laaditaan tietoturvapolitiikka ja tietoturvasuunnitelma. Näiden kahden dokumentin erona on, että tietoturvapolitiikassa esitellään jokaisesta kohdasta yleisluontoinen kuvaus, kun taas tietoturvasuunnitelmassa jokainen

kohta määritellään yksityiskohtaisesti. (ks. Ruohonen 2002, 5-6)

Tietoturvapolitiikka on organisaation johdon selkeä kannanotto tietoturvallisuuden laajuudesta (ks. Laaksonen, Nevasalo ja Tomula 2006, 145). Tietoturvapolitiikan sisältöön vaikuttavat viitekehykset, tietoturvastandardit, Suomen lainsäädäntö ja valtionhallinnon Vahti-ohjeistus, johon on sisällytetty organisaation tietoturvapolitiikka dokumentin runko ja laatimisohje. Tietoturvapolitiikan voidaan määritellä myös samansisältöisesti ISO/IEC 27000-standardisarjan mukaisesti, jolloin organisaation voi sertifioida omat tietoturvatoimintonsa tämän vaatimusstandardin mukaisesti. (ks. Andreasson ja Koivisto 2013, 33-35)

Tietoturvasuunnitelman laatimisella varmistetaan tietojärjestelmien tietoturvallisuuden riittävän tehokas suojaaminen siihen kohdistuviin riskeihin nähden (ks. Ruohonen 2002, 6). Suunnitelman laatimisen vaiheita ovat:

- Tavoitteiden määrittäminen siten, että organisaation johto tai turvallisuudesta vastaaman nimetyn työryhmän määrittämä tietoturvan tason. Taso määräytyy asetettujen tavoitteiden mukaisen suurimman sallitun riskin asettamisesta tasolle, joka on mahdollista saavuttaa kohtuullisilla kustannuksilla.
- Tietoturvakerrosten määrittäminen siten, että tietojärjestelmä on suojattu usealla tietoturvakerroksella siten, ettei yhden suojakerroksen ohittaminen anna suoraa pääsyä suojattuihin tietoihin tai tietojärjestelmän ulkopuolella toimivien hakkereiden aiheuttamia uhkia organisaation tietojärjestelmille.
- Riskianalyysin tavoitteena on tietojärjestelmään kohdistuvien riskien ja riskin toteutumisen aiheuttamia kustannuksia. Analyysissa tulisi ottaa huomioon sisäiset ja ulkoiset uhkat, tahattomat vahingot ja ennalta arvaamattomat tilanteet.
- Toimenpiteissä määritellään kaikki tekniset määräykset ja käytännön ohjeet, joista käy ilmi toimenpiteet, miten valitut tavoitteet pyritään saavuttamaan.
- Vastuut määritellään organisaatiotasolla tarkasti kenen työn toimenkuvan vastuualueeseen tietyt tietoturvan osa-alueet kuuluvat.
- Toipumissuunnitelman tavoitteena on kertoa, kuinka mahdollisen hyökkäyksen kohteeksi joutunut tietojärjestelmä palautetaan toimintakuntoon mahdollisimman nopeasti. Suunnitelmassa on esitelty toimenpiteet, kuinka toimitaan, kun tietojärjestelmässä on havaittu tietomurron yritys tai onnistunut tietomurto.

Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan valtionhallinnon VAHTI-ohjeistuksen, *Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta* (VAHTI 2/2008), määritelmän mukaan henkilöstöön liittyvien käytettävyys-ja salassapitoriskien ennalta ehkäisevää hallinta siten, että salassapitovaatimus sekä saatavuuden ja eheyden vaatimukset täyttyvät. Vaatimuksien on täytyttävä, kun henkilöstö käsittelee vastaanottamalla, muokkaamalla, tallentamalla, välittämällä ja tuhoamalla organisaation tietoja, lisäksi henkilöstöllä on keskeinen rooli organisaation tietovarastojen ja järjestelmien ylläpitäjänä. (ks. Valtionvarainministeriö, 2008a, 11–12)

Henkilöstöturvallisuutta voidaan myös tarkastella organisaatiotasolla työtehtäviä täytettäessä sekä työnkuvan kannalta ja henkilöstöhallinnon näkökulmista. Työnkuvan kannalta työntekijän on sovelluttava työtehtävään ja oltava luotettava sekä nuhteeton, sekä työtehtävien toimenkuvat ovat selkeitä ja vastuualueet on rajattu selkeästi. Henkilöstöhallinnon prosessin pitää sisällään työntekijän tai yhteistyökumppanin elinkaarimallin, joka pitää sisällään taustaselvitykset, työsopimuksen allekirjoituksen, työtehtävissä tapahtuvat muutokset ja työsuhteen päättymisen. (ks. Laaksonen, Nevasalo ja Tomula 2006, 143–144)

Fyysinen turvallisuus

Fyysisen turvallisuuden tavoitteena on estää fyysisten vahinkojen syntyminen. Organisaation fyysisellä turvallisuudella, *Valtionhallinnon tietoturvasanaston* (VAHTI 8/2008) mukaan tarkoitetaan henkilöiden, laitteiden, toimitilojen ja varastojen suojelemista tuhoilta ja vahingoilta. (ks. Andreasson ja Koivisto 2013, 52)

Fyysisen turvallisuuden kannalta ihmisten aiheuttamia uhkia ovat ilkivalta ja murrot. Ympäristön aiheuttamia uhkia ovat erimerkiksi tulipalot, tulvat sekä infrastruktuuriset ongelmat, kuten sähkö-, vesi-, viemäröinti- ja lämmitysjärjestelmien toimintahäiriöt. Näitä uhkia voidaan minimoida huolehtimalla rakennusten ja tilojen ylläpidosta siten, että niistä huolehtivat vartiointi ja kiinteistönhuollon ammattilaiset, kun taas tietohallinnon ammattilaiset osallistuvat palvelintilojen suojaukseen ja ylläpitoon. Tavoitteena toimilla on ehkäistä luvaton pääsy tiloihin ja fyysisten vahinkojen syntyminen. (ks. Hakala, Vainio ja Vuorinen 2006, 304–307)

Yksi keskeisimmistä käsitteistä on termi tilaturvallisuus. Termillä tarkoitetaan organisaation henkilöstön, tiedon ja materiaalin suojaamista rakenteellisin ja valvonnallisin keinoin. Rakenteellisina toimina tarkoitetaan kaikkia mekaanisia ja paloturvallisuuteen vaikuttavia ratkaisuja, ja valvonnallisilla keinoilla tarkoitetaan kulunvalvonta-, tunkeutumisen ilmaisu- ja olosuhdevalvontajärjestelmiä. (ks. Andreasson ja Koivisto 2013, 53)

Laitteistoturvallisuus

Organisaation laitteistoturvallisuudesta vastaa pääsääntöisesti tietohallinto. Laitteistoturvallisuuden piiriin kuuluu tietokoneiden ja muiden tietojärjestelmiin kytkettyjen laitteiden tarkoituksenmukainen mitoitus, toiminnallinen testaus, huoltaminen sekä laitteistojen kulumisen ja vanhentumisen seuranta ja kätöstä aiheutuvien vaaratekijöiden arviointi, kuten esimerkiksi sähköiskut ja muut vaaratekijät. (ks. Hakala, Vainio ja Vuorinen 2006, 308-314) *Valtionhallinnon tietoturvasanaston* (VAHTI 8/2008) laitteistoturvallisuuteen kuuluu edellä mainittujen asioiden lisäksi ulkoisten palveluntarjoajien kanssa sovittujen tukipalvelujen ja–ylläpidon määrittämineen palvelusopimuksin. Palvelusopimuksessa voidaan määrittää vasteajan pituus, jolla voidaan vaikuttaa organisaatiossa määritetyn tietoturvatason ylläpidettävyyteen ja ulkoistettujen tärkeiden laitteiden, käyttöjärjestelmien ja ohjelmistojen asetusten ja varmuuskopioiden säilytykseen ja ottotiheyteen. Laitteistoturvallisuuden kannalta ylläpidon pitäisi varautua siihen, että tärkeiden laitteiden käyttöjärjestelmät, ohjelmistojen asetukset ja niiden sisältämät tiedot voidaan palauttaa välittömästi poikkeamasta toipumisen yhteydessä mahdollisimman tuorein varmuuskopioin. Ylläpidon tulisi testata järjestelmien tietoturvapäivitykset toiminnallisuus ennen niiden asentamista tuotantojärjestelmiin, sekä varmistua, että tietokoneiden BIOS-tason (engl. Basic Input-Output System) ja laitteiden käyttöjärjestelmien tietoturvaominaisuuksia käytetään hyväksi. (ks. Andreasson ja Koivisto 2013, 65)

Tietoaineturvallisuus

Tietoaineturvallisuudella tarkoitetaan tietoaineistojen suojausta ja käsittelyä. Tietoaineistolla tarkoitetaan paperisia tai digitaalisessa muodossa olevien asiakirjojen yksittäistä tietojenkäsittelyä sekä määritellään tietoaineiston turvallinen kopiointi, säilytys ja suojaus. Tietoaineis-

ton käsittelyyn organisaatiotasolla vaikuttavat sähköisen viestinnän tietosuojalaki ja organisaation omat tietoaineluokittelussa määrittelemät käytänteet luottamukselliselle tietojenkäsittelylle. (ks. Laaksonen, Nevasalo ja Tomula 2006, 67)

Tietoaineturvallisuus pitää sisällään asiakirjanhallinnan. Asiakirjanhallinnan tietoturvallisuuden kehittäminen on ensimmäinen tärkeää organisaation toimintaprosesseissa. Asiakirjanhallinnalla on liitäntäpiste koko organisaation toimenpidealueisiin. Asiakirjojen sisällön turvaamisella pystytään takaamaan tietoihin kohdistuva laadulliset vaatimukset. Asiakirjahallinnan tietoturvallisuus toteutetaan asiakirjojen metatietoelementtien ja niiden arkistolaitos SÄHKE-määrityksen ja arkistolaitoksen määrityksien mukaisesti. (ks. Valtionvarainministeriö 2006)

Käyttöturvallisuus

Käyttöturvallisuuden tarkoituksena on mahdollistaa ja ylläpitää toimintaolosuhteet, jossa tietotekniikan käyttö on turvallista. Toimenpiteinä mainitaan tietojärjestelmiin kohdistuvien ohjelmistotuen-, ylläpidon-, kehittämis- ja huoltotoimenpiteiden toteuttaminen siten, että ylläpidon ja järjestelmän omistajien välillä on selkeästi määriteltyinä sopimusdokumentteina menettelytavat ja toimenpiteet toimintatavoista kaikissa tilanteissa. Lisäksi soveltaa järjestelmien käyttöoikeuksien, käytön ja järjestelmän keräämien lokien valvonnan toteuttamisesta siten, että poikkeaviin tapahtumiin puututaan heti tai niistä lähetetään automaattinen hälytys asianosaisille työajan ulkopuolella. Tietojärjestelmät tulisi suojata kaikilta haittaohjelmilta. (ks. Valtionvarainministeriö 2007, 65–68)

Kerättävät lokitiedostot ovat tiedostoja, joihin tiedot tallentuvat automaattisesti ja aikaleimalla varustettuna järjestelmien tapahtumista ja virhetilanteista. Tietojärjestelmät keräävät lokia omiin tietokantoihinsa. Näiden tarkoituksena on, että niistä voidaan seurantaa ja valvontaa tehdä luontevasti ja nämä dokumentit käyvät rikkeiden näytössä todisteina. Yksittäinen ohjelmisto tai järjestelmä voi kerätä käyttölokia, muutoslokia, luovutuslokia ja virhelokia. (ks. Andreasson ja Koivisto 2013, 127)

2.7.2 Ohjelmistoturvallisuus

Ohjelmistojen tietoturvaan voidaan vaikuttaa ohjelmistokehityksen ja muiden teknisten keinojen avulla. Ohjelmistokehityksen keinoin ohjelmistojen turvallisuuteen vaikuttavia tekijöitä ovat käytetyt prosessit, käytetyn ohjelmisto- ja ohjelmistoalustan asetukset sekä ohjeistukset. Muin teknisin keinoin voidaan ohjelmistoa käyttöä ja sen sisältämän tiedon saantia rajoittaa parantamalla ohjelmaympäristön tietoturvallisuutta turvapäivityksin sekä rajoittamalla tietoverkon näkyvyyttä. Tietoturvallisuutta voidaan parantaa määrittelemällä minkälaisen tietoturvavaatimusten mukaisesti hanketta tai uutta tietojärjestelmää ollaan rakentamassa. Tällöin on syytä määrittää projektin alussa tärkeysluokitus, turvallisuustarpeet ja -taso, joilla järjestelmän elinkaaren aikaisiin muutoksiin reagoidaan. (ks. Valtionvarainministeriö 2007, 69–71)

Ohjelmistoturvallisuudella tarkoitetaan tietojärjestelmässä käytettävien ohjelmistojen lisenssien ylläpitämistä ja suojaamista luvattomalta käytöltä. Lisenssien ylläpidolla varmistutaan, ettei tietojärjestelmissä käytetä laittomia ohjelmistoja, ja varmistutaan täten siitä, että ohjelmistot toimivat kuten on suunniteltu ja niihin saadaan ohjelmistotoimittajien päivitykset. (ks. Ruohonen 2002, 4)

Oman ohjelmistotuotannon tietoturvan testausvaiheessa perustuu toiminnallisuuden varmistamiseen, jolloin siitä haetaan tietoturva-aukkoja. Korkealla tasolla vaaditaan lähdekoodikatselmointia. Ohjelmistotuotannon hyväksymistestaus tehdään tuotantoa vastaavassa ympäristössä. (ks. Valtionvarainmisteriö 2013a, 57)

2.7.3 Tietoliikenneturvallisuus

Valtionhallinnon tietoturvasanaston (ks. Valtionvarainministeriö, 2008b) määrittää tietoverkkojen tietoturvan siirtoyhteyksien käytettävyydeksi, tiedonsiirron suojaamiseksi ja salaamiseksi sekä sellaisiksi turvallisuustoimenpiteiksi, joilla kyetään tietoverkkojen käyttäjät tunnistamaan ja takaamaan organisaation tietoliikenteen turvallisuus. (ks. Andreasson ja Koivisto 2013, 69)

Ennen verkon suojaamisen suunnittelua on otettava huomioon organisaation tietoverkon rakenne. Rakenteellisessa suunnittelussa on otettava kantaa kaapelointijärjestelmiin, aktiivi-

laitekokoonpanoon. Tietoverkon suojaamista ja tietoverkon rakennetta esitellään tarkemmin liitteessä A. Suojaamisessa tarvitaan ennen kaikkea päätökseen siitä, miten laaja verkoista on tarkoitus rakentaa. Tietoverkoista tulisi laatia aina ajantasainen dokumentaatio. Dokumentaation pitäisi sisältää tietoverkon suunnittelu- ja suojausdokumentit, fyysisen arkkitehtuurikuvan, loogisentason arkkitehtuurikuvan ja laitelistan. Suunnittelussa tulisi huomioida kaikkien yhteyksien kahdentaminen siten, ettei tietoverkko ole riippuvainen yksittäisen komponentin toiminnasta ja varayhteydet tulisi suunnitella siten, etteivät kaapelit tulisi samassa maalinjassa organisaation tiloihin ja kaapelit olisivat suojattu ilkivallalta ja häirinnältä. Fyysisen arkkitehtuurikuvan tulisi sisältää kaapeloinnin, verkkoliitäntöjen ja aktiivilaitteiden tarkat sijainnit sekä niiden verkko-osoitteet. Loogisen tason arkkitehtuurikuvasta tulisi selvitä eri verkkoalueiden ja virtuaaliverkkojen tarkat sijainnit. Laitelistasta tulisi selvitä kaikkien aktiivilaitteiden tarkat tiedot, sisältäen asennusajan, takuun sekä käyttötarkoituksen. (ks. Andreasson ja Koivisto 2013, 71)

Seuraavassa luvussa tarkastellaan organisaation tietoturvan hoitoa helpottamaan luotujen tietoturvamalli dokumenttien tarkoitusta ja sen erityistä tapaa ratkaista tietty tietoturva ongelma tai sen osa-ongelma.

3 Tietoturvamallit

Tässä luvussa käsitellään organisaatioiden tietoturvan hoidon avuksi kehitettyjä tietoturvamalleja. Ensimmäisessä alaluvussa määritellään tietoturvamallit. Toisessa alaluvussa käydään läpi tietoturvamallien kehityshistoriaa. Kolmannessa alaluvussa käydään läpi tietoturvamallien tarkoitusta. Neljännessä luvussa esitellään antimallilähestymistapaa, joka tarjoaa lähestymistavan luetteloida ja tarkastella eri epäonnistumisia. Viidennessä alaluvussa esitellään tietoturvamalli dokumentin mallipohja. Kuudennessa alaluvussa käydään läpi yksittäisten tutkijoiden tai yhteisöjen tuottamia tietoturvamallikokoelmia. Kuudennessa alaluvussa kuvataan tietoturvamallien luokittelua, jotta tietoturvamalleja kyettäisi järjestämään tarkoituksenmukaisiin kokonaisuuksiin. Lopuksi käydään läpi miten organisaatiossa tietoturvamalleja tulisi käyttää.

3.1 Tietoturvamallien määritelmä

Tietoturvamalleista ei ole oikeaa yksikäsitteistä määritelmää, koska tietoturvamalleja käyttävät eri kohderyhmät, kuten kehittäjät, arkkitehdit ja toimitusjohtajat. Kehittäjien ensisijainen mielenkiinto voivat olla mallit, jotka kuvaavat ohjelmistotason objekteja. Arkkitehtien näkökulmasta mallit ovat järjestelmätason, kuten esimerkiksi tietoverkon malleja, ja toimitusjohtajien näkökulmasta ne voisivat olla malleja, jotka kuvaavat yrityksen luottamussuhdetta muihin organisaatioihin. (ks. D. Kienzle ym. 2002, 5)

3.2 Tietoturvamallien historia

Malliajattelun alkuperäinen idea tulee ohjelmistokehityksen ulkopuolelta. Alkuperäisen idean ohjelmistomalleihin antoi kaupunkiarkkitehti Christopher Alexander, hän esitteli keskeiset suunnittelumallien käsitteet kirjoissaan Pattern language: Towns, Building, Construction (ks. Alexander, Ishikawa ja Silverstein 1977) ja The Timeless Way of Building (ks. C. Alexander 1979). Kirjoissa Alexander esitteli hänen keksimäänsä lähestymistapaansa arkkitehtuuriin ja kaupunkisuunnitteluun, jossa kaapataan jo olemassa olevien ratkaisujen olennaisimmat tiedot ja tarjotaan näitä menetelmiä uuden ongelman ratkaisumalliksi. Mallit vaihtelivat ai-

na korkeantason (rakennusten sijoittelu) ja matalan tasonmalleihin (yksitäinen huone). (ks. Schumacher ym. 2006, 10–12)

Tämä lähestymistapa mahdollisti nykyisten ohjelmisto- ja tietoturvamallien kehityksen, kun Peter Coad (ks. Coad ja Yourdon 1991) osoitti, että Alexanderin suunnittelumalleja voidaan soveltaa ohjelmistoarkkitehtuurin korkeampaan abstraktioon. Tämän takia niitä voidaan käyttää koko organisaation järjestelmätasolla (ks. Schumacher 2003, 11–12), (ks. Hafiz ja Johnson 2006, 3). Ohjelmistomalleihin kiinnitettiin enemmän huomiota, kun 1995 ilmestyi teos Desing Patterns- Elements of Reusable Object Oriented Software (ks. Gamma ym. 1995), jossa määriteltiin eri ohjelmistosuunnittelumalleja. Ohjelmistokehittäjille tämä teos antoi uusia ideoita ja toivoa siitä, että mallit auttaisivat ratkomaan ohjelmistokehityksessä ilmeneviä ongelmia. (ks. Schumacher ym. 2006, 1-2) Ohjelmistomallien menestymisen syynä on, että ne ovat matalantason aloitteen tekijöitä, jolloin niiden avulla voidaan rakentaa ja hyödyntää ammattitaitoisten suunnittelijoiden kokemuksia uudelleen esiintyviin ongelmiin, joita he ovat onnistuneet ratkaisemaan jo aiemmin. (ks. Schumacher ym. 2006, 10–12)

Tietoturvan kannalta ensimmäiset kokoelmat suunnittelumalliajattelusta esiteltiin 1970- luvulla, mutta nämä mallit sisälsivät yleisiä mallinnuksen ohjeita kehittää tietoturvaratkaisuja ja niiden tulkintoja siten, että niiden tulkinta ja hyväksyntä jäi tietoturvallisuusinsinöörien asiantuntemuksen varaan (ks. Willis 1970). Nykyisin käytettävistä tietoturvamallisesta ensimmäiset artikkelit ilmestyivät 1997 (ks. J. Yoder ja J. Barcalow 1998), kun kyettiin osoittamaan, että oliomalleja voidaan käyttää tietoturvamallien esittämiseen. Näitä mallipohjia ei vielä tässä vaiheessa kutsuttu tietoturvamalleiksi, koska niissä käytettiin vielä ohjelmistomallien standardimallipohjia. (ks. Schumacher ym. 2006, 10–12)

3.3 Tietoturvamallien tarkoitus

Tietoturvamallin tarkoituksena on esitellä luotettava ratkaisu, joka korjaa tietyn ongelman. Mallien tulisi kaapata organisaation järjestelmäasiantuntijoiden käytäntöjä ja kokemuksia, joiden avulla kokemattomampi työntekijä voi toimia suuremmalla luottamuksella ja tiedolla. Yksittäinen tietoturvamalli keskittyy itsenäiseen ratkaisuun yhteen erityiseen ongelmaan, mutta niiden välillä on hienostuneisuus. Malli ratkaisee tietyn ongelman, mutta se voi myös

auttaa ympärillään olevia malleja ratkaisemaan osa-ongelmia alkuperäisestä ongelmasta, eli harvoin löytyy yksittäistä tietoturvamallin käyttöä. Tietoturvamallin tulisi myös esittää sen käytöstä ilmenevät hyödyt ja haitat, jolloin haastateltavien vastauksen myös esittäisivät kerronnallisessa dialogissa näitä hyötyjä ja haittoja. Sen tulisi myös keskustella ongelman ratkaisun seurauksista ja esittää ongelmaan yksiselitteinen ratkaisu. (ks. Schumacher ym. 2006, 31-34)

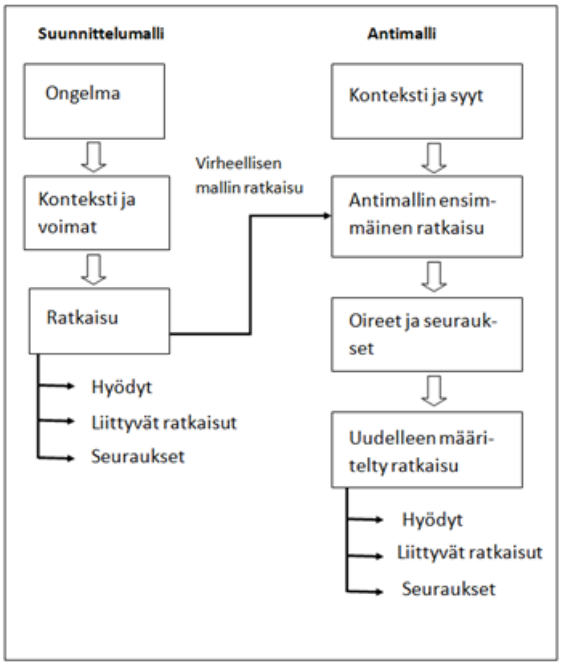
Mallien tulisi olla uudelleenkäytettäviä, eikä tarjota teorioita tai spekulaatioita kuinka ongelma tulisi ratkaista (ks. Heyman ym. 2007). Tietoturvamallien käytöstä organisaatioiden tulisi saada kolme tärkeää etua. Ensinnäkin niiden tarjoamat ratkaisut ovat tunnettuja, koska niiden toiminnallisuus on jo testattua. Toiseksi niiden hyödyt ja haitat tiedetään etukäteen, joten niiden vaikutus voidaan huomioida jo kehitysvaiheen aikana ja kolmanneksi ne luovat yhtenäisen sanasto, joka helpottaa viestintää eri sidosryhmien välillä. (ks. Yskout ym. 2008, 1)

Tietoturvamallit mielletään yleensä ohjelmistosuunnittelumalleiksi, joten niiden tulisi kuvata toimintaansa graafisella UML-mallinnuskaaviolla (engl. Unified Modeling Language) ja niiden tulisi sisältää lähdekoodia. Tietoturvamallien esitys tässä muodossa on jossain tapauksissa liian rajoittunutta, koska on olemassa menettely- ja arkkitehtuurimalleja, joiden esittäminen tässä muodossa on liian rajoittunutta. (ks. Kienzle ja Elder 2002). Esimerkkinä tällaisesta tilanteesta on roolipohjaisen kulunvalvontajärjestelmän (engl. Role-Based-Access) kuvaamiseen tarkoitettu tietoturvamalli, koska tällainen tietoturvamalli ei sisällä lähdekoodia tai sitä on hankala esittää graafisella mallinnuskaaviolla. (ks. Kodituwakku S., Bertok ja Zhao 2001, 2-3)

Organisaatiossa ylläpidettävä tietoturvamallijärjestelmä tarjoaa yhteysketjun eri tietoturvamallien välille. Riippuvuussuhdetta voidaan tarkastella kokonaisvaltaisesti ja siitä saatava hyöty on se, että asiantuntijat voivat tunnista, nimetä ja keskustella tietoturvaongelmista ja ratkaista ne jäsennellysti. (ks. Schumacher 2003, 2). Tietoturvamallien käytössä tulisi huomioida, että niiden jälkiasentaminen toimiviin järjestelmiin, joiden suunnittelussa ei ole huomioitu tietoturvaa voi olla hyvin vaikeaa tai jopa mahdotonta. (ks. J. Yoder ja J. Barcalow 1998, 27)

3.4 Antimallit

Antimallilähestymistavassa dokumentoidaan ohjelmistokehityksen ja tietoturvallisuuden yleisiä virheitä. Tällaisia virheitä esiintyy arkkitehtuurissa, ohjelmistotuotannossa ja yleisessä toteuttamisessa. Antimalli tarjoavat lähestymistavan luetteloida ja tarkastella eri epäonnistumisia. (ks. D. Kienzle ym. 2002, 3) Antimallilla kuvataan yleisesti esiintyviä ongelman kielteisiä ratkaisuja, jotka voivat johtua tietoturvamallin virheellisestä soveltamisesta tai johtajan, arkkitehdin tai kehittäjän tietotaidon puutteesta tai riittämättömästä kokemuksesta ratkaista esiintyviä ongelmatilanteita. Antimallilla määritellään yhteinen ammattisanasto viallisille prosesseille ja toteutuksille, jotta toimenpiteitä voitaisiin kuvata tehokkaasti esimerkiksi (ks. Kuvio 3). Näillä toimenpiteillä voidaan parantaa tehokkaasti ohjelmistojen suunnittelun, hallinnan ja kehityksen eri osa-alueita. Mallit sisältävät ongelman ja ratkaisuosuuden, mutta antimallissa on kaksi eri ratkaisua. Ensimmäinen ratkaisu on ongelmallinen, koska se tuottaa useimmin ei halutun ratkaisun. Toinen yleensä esittää menetelmän, jolla kyetään ongelma ratkaisemaan ja muuttamaan ratkaisu haluttuun muotoon. (ks. Mowbray, Brown ja McCornnick III 1998, 4-5)



Kuvio 3. Suunnittelumallien ja antimallin ongelman ratkaisun esittely

3.5 Tietoturvamallipohja

Tietoturvamalleille on nykyisin olemassa runsaasti erilaisia mallipohjia, kuten esimerkiksi (ks. Bandara ym. 2010), (ks. Schumacher ym. 2006), (ks. A. Alvi ja M Zulkernine 2011) ja (ks. D. Kienzle ym. 2002). Tutkielmassa esitellään yleinen mallipohjan (ks. Taulukko 3), jonka tarkoituksena on antaa käyttäjilleen kaikki tieto mallien soveltamisesta ja siitä aiheutuvista seurauksista käytettävään järjestelmään (ks. Schumacher ym. 2006, 9-11).

Otsikko	Selite
Nimi	Käytettävä nimi ja tiivistelmä tietoturvamallin tarkoituksesta.
Tunnetaan myös nimellä	Tietoturvamallista käytettävät muut tunnetut nimet.
Esimerkki	Todellinen esimerkki, jolla osoitetaan mallin tarpeellisuus. Esimerkin avulla esitellään mallin tarjoama ratkaisu ja täytäntöönpanoon, jos se on tarpeen ja hyödyllistä.
Tausta	Tilanteet, joissa mallia voidaan soveltaa.
Ongelma	Ongelma johon malli on tarkoitettu ja esitellään myös vastavoimat jotka vaikuttavat ongelmaan.
Ratkaisu	Tarkka ja perusteellinen ratkaisu jonka malli tarjoaa.
Rakenne	Yksityiskohtainen erittely mallin rakenteellisiin näkökohtiin.
Dynamiikka	Kuvataan mallin ajonaikainen käyttäytyminen.
Täytäntöönpano	Mallia koskevia ohjeita, joita voidaan muuttaa, jos ilmenee erilaisia, ylimääräisiä tai yksityiskohtaisempia uudelleen järjestelyjä. Sovellettavuus voidaan esittää UML-kaavion muodossa, jossa havainnollistetaan mallin mahdollista toteutusta.
Esimerkki ratkaisu	Esimerkit kaikista tärkeistä näkökohdista, jotka eivät sisälly osioihin ratkaisu, rakenne, dynamiikka tai toteutus.
Eri vaihtoehdot	Lyhyt kuvaus vaihtoehtoisista varianteista tai erikoisalojen malleista.
Tunnetut käyttötavat	Esimerkkejä mallin käytöstä nykyisessä järjestelmässä.

... jatkuu seuraavalla sivulla

Otsikko	Selite
Seuraukset	Hyötyjen esittely ja mallin mahdolliset aiheutuvat haittavaikutukset.

Taulukko 3: Tietoturvamallipohjadokumentin tietokentät

3.6 Tietoturvamallikokoelmat

Tietoturvamalliluetteloista voidaan tehdä organisaatiolle sopivia, käyttämällä niihin eri työkaluja. Tärkeimpiä työkaluja ovat huolto, luokittelu, mallinnus ja päättely. Organisaatiot voivat huoltaa tietoturvamalleja luomalla ja muokkaamalla niitä itse, osallistumalla tietoturvamallien julkaisutoimintaan, lukemalla muiden luomia tietoturvamalleja. Käyttämällä tietoturvamalleihin sopivaa luokittelumallia tai järjestelmää, niin tällöin organisaatio voi mallintaa niitä omiin järjestelmiin ja arkkitehtuuriin. Mallintamisen jälkeen pystytään päättelemään paras ratkaisu esiintyvä ongelma. (ks. Schumacher ja Roedig 2001, 8)

Tietoturvamalleista esiintyy kirjallisuudessa ja Internetissä eri tutkijoiden ja yhteisöjen ylläpitämiä mallikokoelmaluetteloita. Näissä yksittäisissä tietoturvamallikokoelmissa esiintyvissä malleissa esiintyy huomattavaa päällekkäisyyttä, koska saman toiminnallisuuden omaavia malleja on nimetty eri nimillä ja niitä on käsitelty eri lähestymistavalla. Haittapuolena tästä on, ettei tietoturvamallien kirjoittaja ja käyttäjä voi vertailla vaihtoehtoisia ratkaisuja ongelmiinsa. (ks. Hafiz ja Johnson 2006) Esittelen tässä tutkielmassa muutamia kirjallisuudessa ja Internetissä esiintyviä tietoturvamallikokoelmia.

Yoder ja Barcalow julkaisivat 1997 seitsemän tietoturvamallin kokoelman, jossa he käsittelivät ohjelmiston tietoturvaa (ks. J. Yoder ja J. Barcalow 1998).

Fernandez ja Pan julkaisivat 2001 artikkelin jossa esiteltiin 4 ohjelmistotason mallia (ks. Fernandez ja Pan 2001).

Kienzle ja Edler julkaisivat 2002 luettelokokoelman 26 tietoverkkotason malleista (ks. D.M. Kienzle ym. 2002).

Open Group on julkaissut 2004 teoksen Technical guide: Security Design Patterns (ks. Blakley ja Heath 2004) ja yksittäinen tietoturvamalliarkiston (ks. D.M. Kienzle ym. 2002), jossa he esittelevät 26 tietoturvamallia ja luokittelujärjestelmän liitteessä B.4 esitellyn rakenteellinen -ja menettelymalli (engl. Structural and Procedural model) mukaisesti.

Marcus Schumacher ja hänen työryhmänsä julkaisi 2006 teoksen Security Patterns: Integrating Security and System Engineering, jossa esitellään 46 tietoturvamallia. Mallit käsittelevät organisaatioiden tietoturvaratkaisuja, riskien hallintaan, tunnistamista, todentamista, kulunvalvontaa, kirjanpitoa, palomuuriarkkitehtuuria ja turvallisia Internet-sovelluksia. (ks. Schumacher ym. 2006)

Software Engineering Institute julkaisi 2009 mallikokoelman, joka pitää sisällään 6 toteutus-, 3 arkkitehtonista ja 6 suunnittelutason ohjelmisto tietoturvamallia (ks. Dougherty ym. 2009).

OSA on IT-alalla toimiva tietoturva-arkkitehtuuriyhteisö, joka tarjoaa avoimen lähdekoodin Creative Common Share -lisenssin periaatteella turvallisempia tietojärjestelmiä. Yhteisö tarjoaa kattavan turvallisuusmalliluettelon. Mallipohjien luetteloinnissa käytetään liitteessä B.3 esitellyn vaatimuksen mukaisella arkkitehtuurilla luotuja tietoturvamalleja. Yhteisö tarjoaa visuaalisen kehyksen, johon asiakas voi koota tarvitsemansa tietoturvamallikokonaisuudet. (ks. SecurityArchitecture) 2013)

3.7 Tietoturvamallien luokittelujärjestelmät

Tietoturvamallien kirjoittajat ja käyttäjät tarvitsivat tietoturvamallien hallintaan luokittelua. Luokittelun hyötynä olisi se, että tällöin tietoturvamallit voitiin järjestää tarkoituksenmukaisiin kokonaisuuksiin. Järjestettyjen tietoturvamallien vertailu ja vaihtoehtoisten ratkaisujen löytäminen olisi helpompaa. (ks. Kienzle ja Elder 2002, 6)

Tietoturvamallien ensimmäisissä luokittelumallinnuksissa tutkijat pyrkivät luokittelemaan tietoturvamallit yhteen yhteiseen luokitteluun. Tämän jälkeen luoduissa luokittelumalleissa mallit on jaettu eri osioihin, mutta käyttö on osoittanut, että ne ovat liian yleisiä ollakseen

hyödyllisiä. (ks. Hazif, Adamczyk ja Johnson 2007, 52) Tämän takia tietoturvamallien luokitteluun on esitetty eri lähestymistavalla tehtyjä luokitteluja. (ks. A. Alvi ja M Zulkernine 2011) Tutkielmassa esittelen näistä luokittelujärjestelmiä niiden ilmestymisvuoden mukaisesti. Esittelen lyhyen yhteenveto tässä luvussa ja tarkempi kuvaus on esitelty tämän tutkielman liitteessä B.

Zachmanin kehys (engl. Zachman framework) esiteltiin 1987. Kehys perustuu taulukkomuotoiseen esitystapaan, jossa rivit kuvaavat tietomallien tasoja ja sarakkeet kuvaavat arkkitehtuurin näkemyksiä. Tietoturvamallien luokittelun Zachmanin kehystä on käytetty vuodesta 2002, jolloin alkuperäiseen kehykseen lisättiin tietoturvamallien tarpeisiin turvallisuuden näkymä sarake. Luokittelulla on tarkoitus käsitellä koko organisaation tietoturvamalleja. (ks. Hafiz ja Johnson 2006, 7-8) Kehys on kuvattu tarkemmin liitteessä B.1.

McCumber kuutio (engl. McCumber Cube (aka. CSNN Security model)) esiteltiin 1991. Kuutio esitellään Rubikin kuutiomaisena rakenteena. Luokittelun mekanismissa tarkastellaan tietoturvaa tiedon tilan yhteydessä. Mallissa tunnistetaan tiedon kulku järjestelmän, jäsennetään tiedonkulku järjestelmässä ja tietoturvaa koskeva ympäristö. Kuutiossa on määritelty tietoturvanalueet joihin on puututtava, jotta nykyaikainen tietojärjestelmä kyetään turvaamaan. Päätarkoituksena on suojata tietojen koskemattomuutta niiden säilytyksen aikana. (ks. Crowley 2003) Luokittelu on esitelty tarkemmin liitteessä B.2.

CIA-malli (engl. CIA-Model) esiteltiin 1991. Luokittelumallin lähestymistavassa kuvataan tietoturvaan luottamuksellisuuden, eheyden ja saatavuuden näkökulmaan. Päätarkoituksena on parantaa järjestelmän ohjelmistojen ja tietojärjestelmien turvallisuutta. (ks. Hafiz ja Johnson 2006, 16) Luokittelua on esitelty tarkemmin liitteessä B.3.

Rakenteellinen ja menettelymalli (engl. Structural and Procedural Model) esiteltiin 2002. Luokittelumallin tarkoituksena on jakaa tietoturvamalliarkiston mallit kahteen eri pääluokkaan, niiden toiminnallisuuden perusteella. Rakenteelliset mallit voidaan toteuttaa lopputuotteissa. Menettelymallien käytön tarkoituksena on parantaa turvallisuuskriittisiä ohjelmistoja. (ks. D. Kienzle ym. 2002) Luokittelua on esitelty tarkemmin liitteessä B.4.

Suojatun ja saatavilla olevan järjestelmän mallit (engl. The Available and The Protected System Model) esiteltiin 2003. Luokittelumallissa tietoturvamallit jaetaan saatavilla oleviin ja

suojattuihin malleihin. Saatavilla olevat järjestelmämallit sisältävät rakennesuunnittelumalleja. Suojatut järjestelmämallit helpottavat suojaamaan järjestelmän arvokkaita resursseja. Suojatut ja saatavilla olevat mallit pitävät sisällään toiminnallisen sekvenssin, joka määrittelee järjestyksen tietoturvallisuusnäkökohdille. (ks. Blakley ja Heath 2004, 13-15) Luokittelua on esitelty tarkemmin liitteessä B.5.

Moniulotteinen lähestymistapa (engl. A Multi-Dimenssion Approach) esiteltiin 2003. Lähestymistavan tarkoituksena on käyttää hyväksi ohjelmistosuunnittelun tarkoitus ja soveltamisalan mukaista luokitusta. Tietoturvamallit luokitellaan näiden määriteltyjen lähestymistapojen mukaisesti. Moniulotteisella tavalla yhdistetään arkkitehtuuri, suunnittelu ja toiminta kerroksellisuuden mukaisesti. (ks. Schumacher 2003, 16–17) Luokittelua on esitelty tarkemmin liitteessä B.6.

Soveltuvuuteen perustuva luokitus (engl. Classification based on applicability) esiteltiin 2004. Luokitusjärjestelmässä tietoturvamallit jaetaan ohjelmistoarkkitehtuurin mukaisesti kahteen eli suljetun ja avoimen järjestelmät pääluokkaan. Suljetun järjestelmän tieto omaisuudenmenetelmän tarkoitus on suojella arvokkaita resursseja luovuttamiselta ja muuttamiselta. Avoimissa järjestelmissä keskeytymätön palvelu ja resurssien käyttö on tärkeintä. (ks. Hafiz ja Johnson 2006) Luokittelua on esitelty tarkemmin liitteessä B.7.

Tietoturvallisuusmallien kartoitus ydin ja ei-ydin malleihin (engl. Security Patterns inventory Core and non-core patterns) esiteltiin 2007. Luokitusjärjestelmän tarkoituksena on jakaa tietoturvamallit ydinmalleihin, jolloin ne voidaan jakaa järjestelmä tai ohjelmistosovellustasolle. Ei-ydinmallit jakautuvat täytäntöönpanotasolle. (ks. Yskout ym. 2006) Luokittelua on esitelty tarkemmin liitteessä B.8.

STRIDE (engl. Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege) esiteltiin 2007. Mallin nimitys tulee sen elementtien englantilaisten nimen alkukirjaimista, joita ovat: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege and (All)). "All"on lisätty jälkikäteen, kun on haluttu luokitella tietoturvamalleja. Luokittelumallin tarkoituksena on luokitella mallit seitsemään eri elementtiryhmään. (ks. Shostack 2008, 4-5), (ks. Hazif, Adamczyk ja Johnson 2007, 58) Luokittelua on esitelty tarkemmin liitteessä B.9

Taulukkomuotoinen luokittelujärjestelmä malleille (engl. Tabular Classification Scheme for Patterns) esiteltiin 2004. Luokitusjärjestelmän on taulukkomuotoinen esitystapaan, jonka tarkoituksena on auttaa tietoturvamallikirjoittajia järjestämään organisaatiossa käytössä olevia malleja ja tunnistamaan järjestelmästä dokumentoimattomia alueita. (ks. Trowbridge ym. 2004) Luokittelujärjestelmää on esitelty tarkemmin liitteessä B.10.

Six-Sigma luokittelulähestymistapa tietoturvamalleille käyttäen toivottavia ja ei toivottavia ominaisuuksia (engl. Six-Sigma Approach for the Classification of Security Patterns Using the Desirable and Undesirable Properties) esiteltiin 2006. Luokituslähestymistavan tarkoituksena on ehdottaa toivottavia ominaisuuksia, joilla etsitään tietoturva- ja suunnittelumalliluetteloista puutteita. (ks. Laverdière ym. 2006) Luokitusta on esitelty tarkemmin liitteessä B.11.

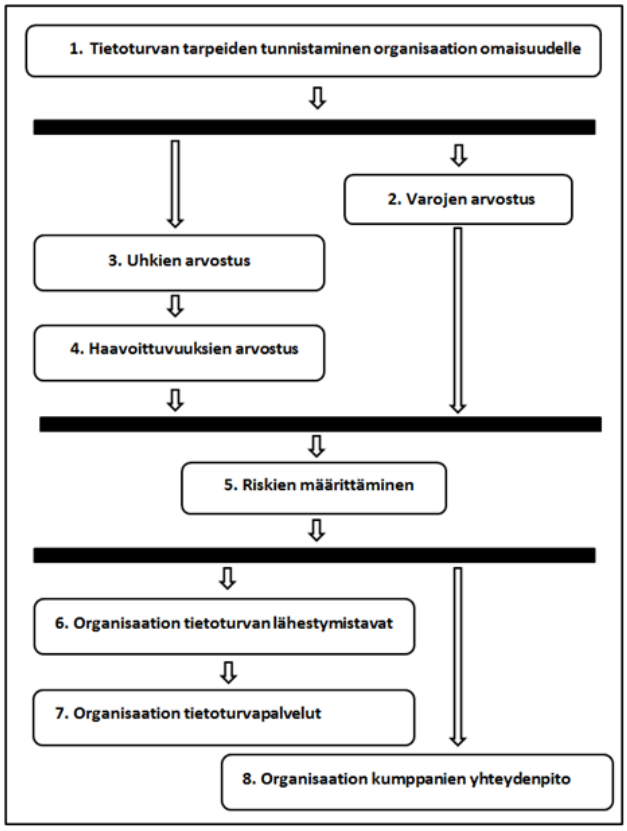
Oikean tietoturvamallin valitseminen käyttäen tekstiluokitusta (engl. Selecting Proper Security Pattern Using Text Classification) esiteltiin 2009. Luokitus perustuu koneoppimisentekniikkaan, joka parantaa tarkkuutta ja automatisoi tietoturvamallien valinnan sekä menetelmä kykenee tunnistamaan samankaltaisuuksia tietoturvamalleista. (ks. Hasheminejad ja Jalili 2009, 1-5). Luokitusta on esitelty tarkemmin liitteessä B.12.

3.8 Tietoturvamallien käyttö organisaatiossa

Tässä kappaleessa kuvataan kuinka organisaatiossa tietoturvamalleja tulisi käyttää. Tässä tutkielmassa esiteltävät tietoturvamallirakenne ei ole täydellinen vaan tarkoituksena on esitellä vain esimerkinomaisesti eri organisaatio-, ohjelmisto-, ja tietoverkkotason tietoturvamalleja. Edellä mainittujen tasojen tietoturvamalleja esitellään tarkemmin seuraavissa alaluvuissa.

3.8.1 Organisaatiotason tietoturvamallit

Organisaatiotasolla turvallisuus ja riskienhallinta tietoturvamallien käytöllä otetaan kantaa koko organisaation turvallisuuskysymyksiin siten, että mallien laajuus pitää sisällään tietoturvapolitiikan ja rajoituksia, joilla on vaikutus kaikkiin organisaation järjestelmiin ja toimintoihin. Organisaatiotason tietoturvamallien järjestys on seuraavanlainen (ks. kuvio 4). (ks. Schumacher ym. 2006, 60).



Kuvio 4. Organisaatiotason tietoturva ja riskienhallinnan tietoturvamallit

Tietoturvatarpeiden tunnistaminen organisaation varoille

Tietoturvatarpeiden tunnistaminen organisaation varoille (engl. Security Needs Identification for Enterprise Assets) on juurisolmu organisaation tietoturvalle. Mallin tarkoituksena on selvittää minkä tasoista ja minkä sisällöistä tietoturva organisaation tulisi soveltaa. Malli ottaa kantaa koko liiketoimintasuunnitelmaan, koska organisaatio voi joutua täydentämään tai suunnittelemaan uusiksi tietoturvasuunnitelman, tietoturvapolitiikan tai IT-järjestelmiä määriteltyjen tietoturvallisuuden tarpeiden mukaan. Mallin rakenne kuvaa yleisiä varojen, liiketoiminnan tekijöiden ja tietoturva ominaisuuksien välisiä suhteita. Mallia on esitelty tarkemmin liitteessä C.1. (ks. Schumacher ym. 2006, 89-103)

Varojen arvostus

Mallin tarkoituksena on auttaa organisaation määrittämään sellaisia omaisuuseriä, joita organisaatio omistaa ja hallinnoi. Omaisuuserien katoaminen tai vaarantuminen aiheuttaa organisaatiolle kustannuksia. Omaisuuserien määrittämisen on keskeisin osa riskinarvioinnissa. Ilman tätä määritystä organisaatio ei voi tunnistaa se varoihin kohdistuvia riskejä. Organisaation riskinarvioinnin määrityksessä tulisi tunnistaa tietoturvan, rahallisen ja liiketoiminnallisten arvojen vaikutus liiketoimintaan. Tunnistetut riskit ja uhat voidaan luokitella kuuteen eri luokkaan niiden laadun mukaan korkean tai matalan välille. Malli on esitelty tarkemmin liitteessä C.2. (ks. Schumacher ym. 2006, 103-112)

Uhkan arviointi

Uhkan arviointimallissa uhkan todennäköisyys tai mahdollisuus organisaation määrittelemille varoille tai esineille, joita tulisi suojella vaarallisilta tapahtumilta. Organisaation tulisi tunnistaa nämä uhkat ja määritellä todennäköisyys niiden esiintymille. Malli on esitelty tarkemmin liitteessä C.3. (ks. Schumacher ym. 2006, 113-124)

Haavoittuvuuden arviointi

Haavoittuvuuden arviointimallissa määritellään organisaation järjestelmissä ilmeneviä heikkouksia, joita voidaan hyödyntää. Tämä hyödyntämisen uhka vaarantaa organisaation tietoturvan, joilla se suojellee sen varoja. Haavoittuvuuden arvioinnin tarkoituksena on tunnistaa niiden vakavuus, jos haavoittuvuutta hyödynnetään. Malli on esitelty tarkemmin liitteessä C.4. (ks. Schumacher ym. 2006, 125-136)

Riskien määrittäminen

Riskein määrittäminen on viimeinen vaihe riskien arviointiprosessissa ja sisältää varojen arvostuksen, uhkan ja haavoittuvuuden arvioinnin. Käyttämällä näitä tietoturvamalleja organisaatio kykenee arvioimaan ja priorisoida riskit sen varoille. Malli on esitelty tarkemmin liitteessä C.5 . (ks. Schumacher ym. 2006, 125-136)

3.8.2 Ohjelmistotason tietoturvamallit

Ohjelmistotietoturvamalleista esittelen ohjelmistojen tietoturvatavoitteiden dokumentoinnin (engl. Document the Security Goals) ja vastuiden jakamisen turvallisuudelle (engl. Share Responsibility for Security) tietoturvamallit. Malleissa otetaan kantaa ohjelmistosuunnittelun ristiriitaisten menettelytapojen ja sopimattomien mekanismien poistamiseen sekä miten ohjelmistokehittäjät saadaan rakentamaan vastuullisia turvallisia järjestelmiä.

Tietoturvatavoitteiden dokumentointi

Jotta ohjelmistokehittäjät voisivat tehdä yhdenmukaisia, älykkäitä ja tietoturvallisia valintoja heidän on ymmärrettävä koko järjestelmän tavoitteet ja sen takana olevat liiketoimintamallit. Jos tietoturvatavoitteita ei dokumentoida tai annettu kaikkien tietoon, niin tällöin tulkinnat voivat johtaa ristiriitaisiin menettelytapoihin ja sopimattomiin mekanismeihin. Malli on esitelty tarkemmin liitteessä D.1. (ks. D.M. Kienzle ym. 2002)

Vastuiden jakaminen tietoturvalle

Vastuiden jakaminen tietoturvalle yrittää saada kaikki kehittäjät rakentamaan vastuullisia turvallisia järjestelmiä. Tietoturva on enemmän kuin vain salaus, antivirusohjelmisto tai palomuuri. Jokainen järjestelmäelementti voi olla turvallisuusnäkökohta ja järjestelmäkehittäjien on ymmärrettävä ja käsitellä näitä näkökohtia. Käyttämällä tätä mallia vältetään ongelmaa, jossa tietoturvatiimi kääntyy muita kehitystiimejä vastaan. Malli on esitelty tarkemmin liitteessä D.2. (ks. D.M. Kienzle ym. 2002)

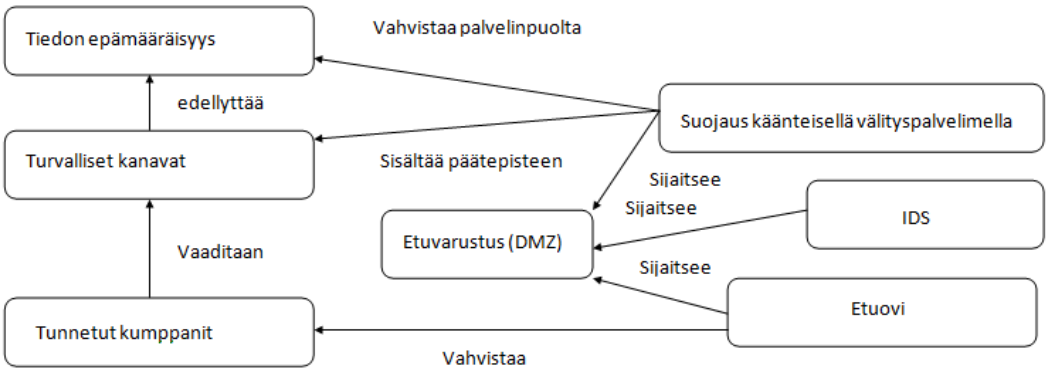
3.8.3 Tietoverkkotason tietoturvamallit

Tietoturvamallin näkökulmasta tietoverkkotopologian tarkoituksena on opastaa ja esitellä organisaatiolle tietoturvaa parantavan rakenteellinen kuvaus. Mallien tarkoituksena on vaihtoehtojen kautta opastaen mallin käyttäjää löytämään tarvitsemansa ratkaisu tai auttaa parantamaan olemassa olevan tietoverkon tietoturvaa.

Vaihtoehtona on tarjota tietoverkkoon tietoverkkotopologia, jota kutsutaan etuvarustukseksi

(engl. Demilitarized Zone (DMZ)) tämän mallin ratkaisu on esitelty kaaviokuvauksena (ks. Kuvio 5), jossa keskeinen tietoturvamalli on etuvarustus. Tämä tietoturvamalli itsessään pitää sisällään suojauksen käänteisellä välityspalvelimella (engl. Protection Reverse Proxy), etuoven (engl. Front Door), tunkeutumisen havaitsemisjärjestelmä (engl. Intrusion Detection (IDS)) ja VPN-palvelimen. Nämä tietoturvamallit on esitelty tarkemmin alaluvussa ja liitteessä E.

Etuvarustukseen kuuluvia tietoturvamalleja tunnetut kumppanit (engl. Known Partners), turvalliset kanavat (engl. Secure Channels) ja tiedon epämääräisyys (engl. Information Obsecurity) toimivat täydentävinä, tietoturvaa parantavina malleina, edellä mainittujen mallien kanssa (ks. Schumacher ym. 2006, 78-80). Näitä malleja ei käsitellä tässä tutkielmassa.



Kuvio 5. Tietoverkkotopologia esitettynä tietoturvamallien näkökulmasta

Etuvarustus

Etuvarustus tietoturvamallin tarkoituksena on tarjota ratkaisu siihen, kuinka tietoverkon järjestelmät voidaan erotella ulkoisille sekä sisäisille käyttäjille tarjottaville toiminnoille ja tiedoille. Etuvarustukseen tulisi sijoittaa Web-palvelimet, jotka pitävät sisällään muuttumattoman eli staattisen sisältöä ja sovelluspalvelimet joiden tehtävänä on liiketoiminnallisten ja muuttuvien eli dynaamisten Web-sisältöjen säilytys ja luominen tulisi sijoittaa sisäverkkoon. Tarkoituksena on tehdä tietoverkosta kerroksellinen, jotta siihen olisi vaikeampi hyökätä. Malli on esitelty tarkemmin liitteessä E.1. (ks. Schumacher ym. 2006, 449-456)

Suojauksen käänteisellä välityspalvelimella

Suojaus käänteisellä välityspalvelimella (engl. Protection Reverse Proxy) tarkoituksena on suodattaa verkko kaikilta tulevilta palvelinpyynnöiltä. Suojaus käsittää suodatuksen, jotta vain useimmiten vaarattomimmat asiakkaiden palvelupyynnöt pääsevät käyttämään Web-, FTP-, IMAP- ja SMTP-protokollia. Mallissa käydään läpi etuvarustukseen sijoitettavista erillisistä tai useammasta tietokoneesta/palvelimista suodattamaan edellä mainittujen palvelimien käyttämiä protokollia. Malli on esitelty tarkemmin liitteessä E.2. (ks. Schumacher ym. 2006, 457-464)

Etuovi

Etuovi (engl. Front Door) tietoturvamallin tarkoituksena on opastaa kuinka järjestelmään voidaan luoda yhden kirjautumispisteen ratkaisu. Ratkaisu tukee käyttäjien tunnistamista. Syntyvät keskeiset tiedot voidaan tallentaa keskeiseen lokiin. Mallissa keskustellaan mahdollisuudesta asentaa etuvarustukseen useampi etuovi, koska tällöin tietoverkon autentikoinnit voidaan jakaa tarvittaessa taustapalvelimille, Extranetille ja Intranetille. Malli on esitelty tarkemmin liitteessä E.3. (ks. Schumacher ym. 2006, 473-480)

Tunkeutumisen havaitsemisjärjestelmä

Tunkeutumisen havaitsemisjärjestelmä (engl. Intrusion Detection (IDS))Mallin tarkoitukena on kuvata kuinka organisaatio voi monitoroida tietoverkon kautta kulkevaa liikennettä sekä kuinka sitä voidaan analysoida. Mallissa kuvaillaan tunkeutumisen havainnoinnissa tarvittavien palomuurien toimintaa, tulevien palvelupyyntöjen tarkkailua ja tunkeutumisen estojärjestelmän toimintaa. Malli on esitelty tarkemmin liitteessä E.4. (ks. Kumar ja Fernandez 2012)

TSL VPN

Etuvarustukseen sijoitettavan VPN-palvelimen tarkoituksena on tarjota käyttäjilleen mahdollisuus kirjautua organisaation sisäverkossa oleville palveluille. Tämä yhteys on toteutettu esiladattavien VPN-ohjelmisen mahdollistama suojattu tunneli toimipisteverkkojen välille,

jossa tiedot kulkevat salatusti. Malli on esitelty tarkemmin liitteessä E.5. (ks. Fernandez-Buglioni 2013)

Seuraavassa luvussa tarkastellaan menetelmiä, kuinka tutkimus tehtiin eli tutkimuksen asiakokonaisuuteen vaikuttavien asiakokonaisuuksien, kuten tiedon hankinnan keinoja ja vaiheta, valintojen perusteluita, aineiston kuvaamisen sekä aineisto analyysin tekniikoita.

4 Menetelmä

Tässä luvussa käsitellään miten tutkimus tehtiin. Ensimmäisessä alaluvussa käydään läpi tutkimuksen toteutusta. Toisessa alaluvussa esitellään tutkimuksen tehtävä ja tutkimuksen kannalta keskeiset tutkimuskysymykset. Kolmannessa alaluvussa käydään läpi tutkimuksen kohdejoukko. Neljännessä alaluvussa käydään läpi aineistokeruun toteutusta ja lopuksi aineistoanalyysi alaluvussa käydään läpi aineistoanalyysin kulkua.

4.1 Tutkimuksen toteutus

Tutkielmani toteutusmenetelmäksi valikoitui kvalitatiivinen eli laadullinen tutkimus. Laadullisella tutkimuksella tarkoitetaan tutkimusta, joka tuottaa havaintoja. Havainto voi tarkoittaa henkilöiden tai organisaatioiden kokemuksien, tuntemusten, käyttäytymisen, sosiaalisten liikkeiden, kulttuurillisten ilmiöiden tutkimista tilastollisin tai muita määritysrajan keinoja hyväksikäyttäen. Tutkimusta voidaan tehdä haastattelun avulla ja raakadatasta saatuja havaintoja voidaan analysoida laadullisin menetelmin. (ks. Strauss ja Corbin 1998, 10–11) Mielestäni laadullinen tutkimusote soveltui tutkimusmenetelmäksi, koska käsiteltävä aihealue ja sen laaja-alaisuus oli tiedossa ennen tutkimuksen aloittamista. Laadullisesta analyysistä puhuttaessa ei puhuta pelkästään tietojen määrästä vaan tarkoituksena on löytää käsitteitä ja suhteita raakadatasta ja tämän jälkeen tiedot järjestetään osaksi teoreettista selventävää mallia (ks. Strauss ja Corbin 1998, 10–11). Nähdäkseni tutkimuksellinen tarkastelu käyttävätkö koulutusorganisaatiot tietoturvan hoidossa tietoturvamalleja on ollut vähäistä, vaikka tietoturvan merkitys aiheena ja sen tärkeys kaikissa yhteyksissä muuttuu kokoajan yhä tärkeämmäksi.

4.2 Tutkimuksen tehtävä ja tutkimuskysymykset

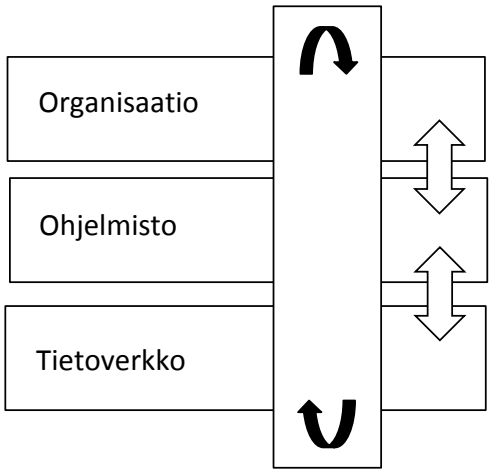
Pro gradu-tutkielmani ei sisälly mihinkään hankkeeseen, vaan toteutin sen Jyväskylän yliopiston tietotekniikan laitokselle. Tutkimustehtävänä oli selvittää löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien käyttöä tai piirteitä. Organisaation tietoturvan laaja-alaisuudesta johtuen, tietoturvan tarkastelu jaettiin organisaatio-, ohjelmisto- ja

tietoverkkotasojen mukaisesti (ks. Kuvio 6).

Tutkimuskysymykseni muotoutuivat seuraavanlaisiksi:

1. Miten tietoturvamallit näkyvät tutkittavissa organisaatioissa?

    a) Organisaatiotasolla
    b) Ohjelmistotasolla
    c) Tietoverkkotasolla
2. Miten organisaatiot huolehtivat tietoturvasta?



Kuvio 6. Tutkielman organisaatiotason rajaukset

4.3 Tutkimuksen kohdejoukko

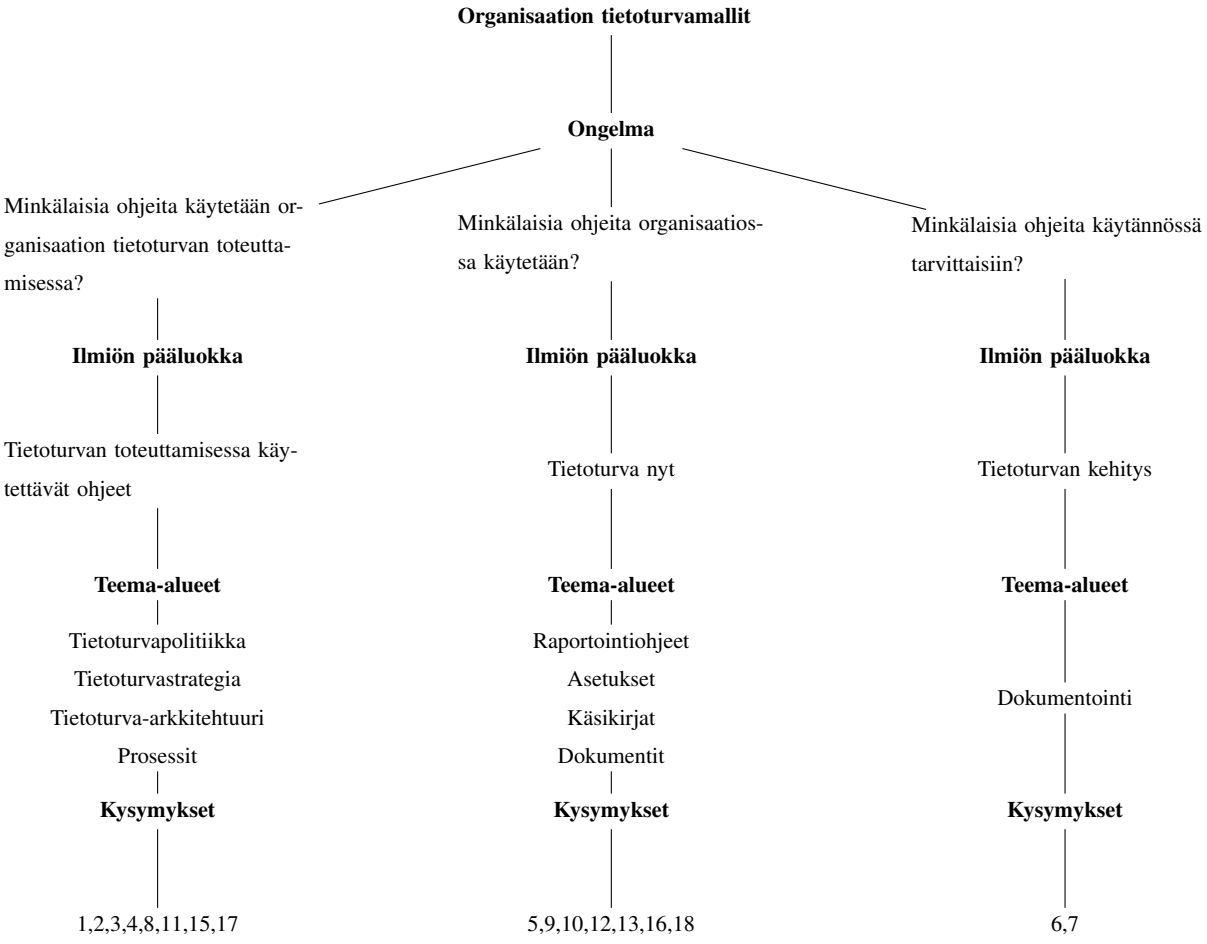
Haastateltaviksi organisaatioiksi valikoitui jo tutkimukseni aiheen valinnan yhteydessä, että tutkimushaastattelut kohdistettiin vain koulutusorganisaatioihin. Lähestyttäviksi organisaatioiksi valittiin Jyväskylän yliopisto (JYU) ja Jyväskylän ammattikorkeakoulun (JAMK), koska tiedettiin, että koulutusorganisaatioihin on ylipäätään mahdollisuus päästä tekemään tietoturva-aiheista tutkimusta. Tutkimuksen haastatteluun osallistuva kohdejoukko valittiin heidän ammatillisen sekä työtehtävien perusteella, joten luonnollisin menetelmä haastateltavien valinnalle oli hyväksikäyttää lumipallo-otantaa (engl. Snowball Sampling). Otannassa haastateltavia avainhenkilöitä pyydettiin viimeisenä kysymyksenä ehdottamaan muita haas-

tateltavia (ks. Hirsjärvi ja Hurme 2011, 59–60). Tämä lähestymistapa varmisti sen, että sain haastatteluun sellaisia henkilöitä, jotka olivat varmasti tutkimusongelman kannalta keskeisiä.

4.4 Aineistokeruun toteutus

Aineistokeruumenetelmäksi valikoitui puolistrukturoitu teemahaastattelu. Tarkoituksena oli, että haastateltava saivat kertoa aiheesta omin sanoin, jolloin he saattavat täydentää puheillaan jo saatua tietoa. Haastattelut toteutettaisiin yksilöhaastatteluin, koska tällöin haastattelutilanteen luonne olisi vapautunutta ja luontevaa. (ks. Hirsjärvi ja Hurme 2011, 60)

Laadin haastattelun kysymysrungon teema-alueiden mukaisesti teema-alueluettelo muotoon. Tutkimuksen teema-alueiden kysymyksiä lähestyttiin tutkimuskysymys - ja rajausnäkökulmasta, koska nämä olivat pääasiallisia teoria taustasta heränneitä kysymyksiä, jolloin ne muodostivat teoreettisten pääkäsitteiden, eli tutkielman teoreettisen tarkastelun lukujen tietoturva 2 ja tietoturvamallit 3 sisällöstä. Kysymysrungossa ongelma jakautui kolmeksi kysymyksenomaiseksi luokaksi. Näissä luokissa halusin selvittää: Minkälaisia ohjeita käytetään organisaation tietoturvan toteuttamisessa, eli näkyykö dokumenteissa mallimaisuutta. Ilmiön pääluokat muodostivat ns. ennen-nyt-tuleva lähestymistavasta, jonka tarkoituksena on tukea yläluokkaa. Teema-alueiksi valikoitui organisaation tietoturvaa käsittelevien dokumenttien sisältö ja olemassa olevien dokumenttien sisällöllisten puutteiden selvittäminen. Tutkimusongelman kysymysten tarkoituksena oli olla pelkistettyjä pääaiheita käsitteleviä kysymyksiä, joiden päätarkoituksena oli toimia muistilistana ja keskustelua ohjaavana elementtinä. (ks. Hirsjärvi ja Hurme 1991, 41–44) Luettelon (ks. Kuvio 7) kysymykset ovat numeroitu ja niiden vastaavuudet on esitelty (ks. Taulukko 4).



Kuvio 7. Haastattelun kysymysrungon hahmottelu

Kysymys
1. Kuinka kauan olette työskennelleet organisaation palveluksessa?
2. Mikä on toimenkuvasi, eli mitä teet täällä?
3. Millä tavalla organisaatio kouluttaa työntekijöitä?
4. Oletko ollut koulutuksessa?
5. Kuinka organisaatiossanne on otettu kantaa turvallisuuskysymyksiin eli millaisia dokumentteja käytätte?
6. Päivitetäänkö tietoturvaohjeistusta säännöllisin väliajoin?
7. Luetteloidaanko ohjeistuksissa ilmeneviä puutteita?
8. Mitkä ovat pääasiallisia keinoja, kun tietoturvan hoidossa ilmenee ongelmia?
9. Kenelle raportoit ilmenevät ongelmat?
10. Onko mahdollista, että kokematon työntekijä joutuu vastamaan kriittisistä toiminnoista?
11. Onko työntekijällä mahdollisuus turvautua ongelmatilanteissa ohjeistukseen?
12. Minkälaisia dokumentteja käytätte ongelmatilanteiden yhteydessä?
13. Kirjataanko uusien ongelmatilanteiden ratkaisuja muistiin dokumentaatioon?
14. Ovatko ohjeistusdokumentaatiot mielestäsi yhdenmukaisia?
15. Miten organisaatiossanne varmistutaan ohjelmistojen tietoturvasta?
16. Miten organisaatiossanne varmistutaan siitä, että käytettävät ohjelmistot ovat turvallisia?
17. Miten organisaatiossanne määritellään tietoverkkojen tietoturva?
18. Millaisia dokumentteja organisaation tietoverkoista on olemassa?
19. Keitä muita henkilöitä voitaisiin haastatella tutkimukseen liittyen? (vain avainhenkilöt)

Taulukko 4. Haastattelukysymysrunko

Haastateltavien hankinta alkoi siten, että lähestyin sähköpostitse Jyväskylän yliopiston (JYU) ja Jyväskylän ammattikorkea koulun (JAMK) avainhenkilöitä ja pyysin heiltä lupaa haastatella heitä ja mahdollisesti neljää tietohallinnon työntekijää. Viestissä kerroin tällöin pro gradu-tutkielmani nimen, tutkimuskysymysaihe-alueen, tutkielman ohjaajat sekä ettei tutkielmani kuulunut mihinkään hankkeeseen. Annoin tässä vaiheessa esitietoina seikat, joita olivat: haastattelun kesto noin 2 tuntia, haastattelut suoritettaisiin heidän työpaikoilla, jotta haastattelulle löytyisi rauhallinen paikka, sekä haastattelut tulisi voida nauhoittaa. (ks. Hirsjärvi ja Hurme 1991, 61–62)

Avainhenkilöt vahvistivat sähköpostitse heidän suostumuksensa, joten sain suorittaa tutkimushaastattelut heidän organisaatioissaan. Tämän jälkeen sovin heidän kanssaan puhelimitse haastatteluun sopivan ajankohdan. Lumipallo-otannasta johtuen, sain tietää muiden haastateltavien nimet vasta haastateltuani avainhenkilöt. JYU:n avainhenkilö nimesi kolme ja JAMK:n avainhenkilö neljä sopivia haastateltavaa. Lähestyin ensin heitä kaikkia sähköpostitse ja tiedustelin heidän halukkuuttaan osallistua haastatteluun. Kukaan nimetyistä henkilöistä ei tässä vaiheessa kieltäytynyt haastattelukutsusta. Tämän jälkeen olin heihin kaikkiin yhteydessä puhelimitse ja tiedustelin heidän halukuuttaan osallistua haastatteluun ja sovin heidän kanssaan haastatteluajankohdasta sekä paikasta. En myöntynyt lähettämään heille tutkimuskysymyksiä etukäteen. Ainoastaan yksi mahdollista haasteltavista kieltäytyi tässä vaiheessa haastattelusta sekä yksi haastateltavista ei suostunut nauhoitettuun haastatteluun. Tutkimukseen osallistuneet henkilöt eivät olleet minulle entuudestaan tuttuja.

Haastattelun suoritusta haittasi alussa se, etten alkuperäisen suunnitelman mukaisesti kyennyt testaamaan teemahaastattelurunkoa ja sen toimintaa esihaastatteluissa vaan, esihaastattelu toteutui vasta ensimmäisten haastatteluiden yhteydessä. Suunnitelmaa muutti se, että eräs tutkielman ohjaajista oli sitä mieltä, että esihaastattelun voi korvata hänen tarkalla teoreettisella selostuksella. Tästä huolimatta totesin haastattelurungon pääosin toimivaksi, mutta muutin hieman tarkentavienkysymysten painotusta, koska haastattelukysymysrunko toimii haastattelutilanteissa haastattelijan muistilistana ja keskustelua ohjaavana dokumenttina (ks. Hirsjärvi ja Hurme 2011, 66).

Tutkimukseni aineistonkeruun haastattelut toteutettiin syksyn 2013 loka- ja marraskuun aikana. Haastatteluissa käsiteltävän aiheiden arkaluonteisuudesta johtuen esitin jokaiselle haas-

teltavalle ennalta laaditun tieteellisen tutkimuksen rekisteriselosteen, joka täyttää henkilötietolain 10§ ja 14 § pykälät (ks. Oikeusministeriö 1999).

Haastatteluiden tallennusvälineistönä käytin kynää ja paperia sekä digitaalista tallenninta, josta haastattelunauhoitteet saatiin helposti siirrettyä USB-kaapelia käyttäen tietokoneelle. Ennen haastattelutilaisuutta tarkistin, että haastateltavat ovat niitä, joiden kanssa olin haastattelun sopinut. Haastattelut suoritettiin sovitusti haastateltavien työpaikoilla siten, että haastateltavat olivat varanneet haastattelulle kokoushuoneen tai työhuoneen. Tällä kyettiin varmistamaan että haastatteluympäristö oli mahdollisimman häiriötön. (ks. Hirsjärvi ja Hurme 2011, 74) Haastattelujen yhteydessä havainnoin kielellisen tietojen ohessa ei-kielellistä ns. kehon kielellistä tietoa. Tein pieniä muistiinpanoja haastateltavista haastatteluiden aikana ja kirjoitin niistä lyhyen kuvauksen haastateltavasta heti haastattelun jälkeen, jotta kykenisin myöhemmin tarkistamaan sanallisen tiedon luotettavuutta. (ks. Hirsjärvi ja Hurme 1991, 50)

Haastatteluiden kestot olivat lyhyimmillään 21 minuuttia ja pisimmillään 56 minuuttia. Kaiken kaikkiaan haastatteluaineistoa kertyi 5 tuntia 4 minuuttia ja 25 sekuntia. Taulukossa ilmenee eri haastattelutilanteet (ks. Taulukko 5). Taulukon ensimmäinen sarake sisältää henkilön numerona, koska henkilöiden nimet on poistettu tutkimusmateriaalista ennen analysointia. Toinen sarake kertoo ajankohdan milloin haastattelu suoritettiin ja kuinka kauan se kesti. Kolmas sarake ilmaisee työskentelyorganisaation. Neljäs sarake sisältää haastattelutilanteessa esitellyt kysymykset, nämä kysymykset pitävät sisällään muistilistassa olevat ja haastateltavalle esitetyt tarkentavat kysymykset. Viides sarake sisältää aineistolitteroinnin sivumäärän kyseisestä haastattelutilanteesta. Viimeinen sarake pitää sisällään tiedon sukupuolesta, työtehtävä nimikkeen sekä kuinka kauan tutkimusotos on työskennellyt organisaation palveluksessa.

Haastattelun jälkeen nauhoitettu materiaali litteroitiin eli auki kirjoitettiin sellaisella sanatarkkuudella, että täytesanoja ei litteroitu. Litterointi kesti noin kaksi kuukautta haastattelujen aloittamisesta. Litteroinnin valmistuttua kirjoitettua aineistoa kertyi 52 sivua (fontti 12, Font as default, 1,5 riviväliillä). Litterointi suoritettiin Notepad++ tekstinkäsittelyohjelmalla, koska tietokoneavusteisella Atlas.ti- analyysiohjelmistolla (engl. The Qualitative Data Analysis & Research Software) tiedostot, jotka olivat .txt-päätteisiä toimivat varmasti ilman

No	Aika & kesto	Org.	Kysymykset	Sivut	Sukupuoli / nimike / työsuhteen kesto
v01	29.10.2013, 56 min	JAMK	40 kpl	13	M / Tietohallintopäällikkö / 5,5 v.
v02	30.10.2013, 38 min	JYU	102 kpl	10	M / Tietoturvapäällikkö / 10 v.
v03	6.11.2013, 36 min	JYU	42 kpl	9	M / Levypalvelut, Alustapalvelut, Työpöytäympäristö ja Web-palvelut / 17 v.
v04	7.11.2013, 50 min	JAMK	35 kpl	9	M / Ylläpito ja ATK-tuki / 27 v.
v05	11.11.2013, 27 min	JAMK	46 kpl	6	M / Järjestelmäsuunnittelija / 17 v.
v06	12.11.2013, 21 min	JYU	47 kpl	6	M / Identiteetinhallinta, Postipalvelut ja Verkkopalvelut / 15 v.
v07	19.11.2013, 32 min	JAMK	54 kpl	8	M / Tekninen asiantuntija / 10 v.
v08	20.11.2013, 40 min	JAMK	23 kpl	3	N / Tietohallinnon suunnittelija / 4 v.

Taulukko 5. Haastattelujen toteutus

yhteensopivuusongelmia.

4.5 Aineistoanalyysi

4.5.1 Aineistoanalyysin toteutuksen valinta

Grounded Theory eli ankkuroitu teoria on lähestymistapa laadulliseen tutkimukseen. Menetelmän kehittivät Glaser ja Strauss (ks. Glaser ja Strauss 1967). Grounded Theory jakautui kehittäjien (Glaser ja Strauss) riitauduttua tutkimusmenetelmän analyysistä 1990 Glaserilaiseen ja Staussilaiseen lähestymistapaan. Tämä riita alkoi siitä, kun Strauss ja Corbin keskittyivät kehittämään teoriasta hieman analyyttisemman lisäämällä siihen välitason eli aksiaalistason sekä sisällyttämään ohjauksen aloitteleville tutkijoille. Glaserilainen lähestymistapa noudatti alkuperäistä luotua analyysimallia, joka pitää sisällään sisällöllisen (engl. Substantive Coding) ja teoreettisen (engl. Theoretical Coding) koodausvaiheen. Sisällöllinen koodaus on tietoriippuvaista, jolloin siitä tulee entistä abstraktimpia. Tällöin tiedot voidaan teoreettisen koodausvaiheen aikana uudelleen luokittaa, jolloin tiedot voidaan integroida syntyneeseen uuteen teoriaan. Straussilaista lähestymistapa taas pitää sisällään kolmitasoisen hermeneuttisen analyysitekniikan, joka koostuu avoimen koodauksen (engl. Open Coding), aksiaalisen koodauksen (engl. Axial Coding) ja selektiivisen koodauksen (engl. Selective Coding) vaiheesta. Eroina voidaan myös mainita, että Glaserilaisessa tulkinnassa ilmiöllä voidaan tarkoittaa useaa eri asiaa (koodia) samanaikaisesti, mutta Staussilaisessa lähestymistavassa näin ei voi olla. (ks. Heath ja Cowley 2004, 141–146)

Valitsin tutkimukseni aineistoanalyysiksi Grounded Theory analyysitekniikka, koska tämä laadullisen tutkimuksen lähestymistapana tuo parhaan vastaukseen selvitettäviin tutkimuskysymyksiin. (ks. Hirsjärvi, Remes ja Sajavaara 2013, 224) Etenkin Straussilainen kolmitasoinen hermeneuttinen analyysitekniikka sopii parhaiten, koska se sisältää kolme eri mekaanista vaihetta avoimen koodauksen (engl. Open Coding), aksiaalisen koodauksen (engl. Axial Coding) ja selektiivisen koodausvaiheen (engl. Selective Coding) ja tässä lähestymistavassa luokalle annetaan vain yksi tarkoitus. Tämä oli mielestämme tärkeää, koska tutkimuksen alussa organisaation tietoturvan laaja-alaisuudesta johtuen, se jaettiin organisaatio-, ohjelmisto- ja tietoverkkotasoihin (ks. Kuvio 6)

4.5.2 Avoin koodaus

Tämän aineistoanalyysivaiheen tarkoituksena on harjoittaa tutkimalla, vertailemalla, käsitteellistämällä sekä luokittelemalla tutkimuksen aineisto. Tällä tarkoitetaan joko lauseita, lausetta tai kohtia, joka antaa erilliselle tapaukselle idean, nimen tai jotain joka edustaa ilmiötä. Nämä kysymykset auttavat tunnistettavien käsitteellisten ilmiöiden kategorioiden ryhmittelyssä analysoinnin ensimmäisen vaiheen aikana, jolloin menettelyssä tunnistettujen ilmiöiden käsitteitä voidaan luokitella kuuluvaksi samaan luokitukseen. Luokituksen nimeäminen tapahtuu suoraan aineistosta löytyvien käsitteiden mukaisesti, jolloin varmasti tiedetään niiden tarkka merkitys. (ks. Strauss ja Corbin 1990, 63–65)

Tutkielman tässä vaiheessa otin käyttöön Atlas.ti analysointiohjelmiston. Aluksi perehdyin litteroituun haastatteluaineistoon lukemalla sen useaan kertaan läpi hyvän käsityksen aikaansaamiseksi. Ensimmäisellä analysointikerralla etsin aineistosta ilmiöitä, joille kykenin antamaan käsitteellisen nimen ja jatkoin tällä tavalla läpi koko aineiston.

Aloittaessani aineiston koodaus sovimme että käytän (ks. Kuvio 6) rajauksen mukaisia indikaattoreita (engl. Indicator) luokkien nimissä, jotta pystyisin jatkossa erottamaan mihinkä rajauksen mukaiseen kategoriaan kukin tagi kuuluu. Tämä jako säilytettiin sotkematta kokoa aineistoanalyysin ajan, myös muissa koodausvaiheissa vaikka muissa koodauksen vaiheissa yläluokille tulisi eri nimi. Tässä merkinnässä ensimmäinen osa on indikaattori ja toinen osa on luokan nimi, ne ovat muotoa:

- **Organisaatiotaso:** OR:<merkitys>
- **Ohjelmistotaso:** OH:<merkitys>
- **Tietoverkkotaso:** TV:<merkitys>

Ensimmäiset tämän koodausvaiheen aikana syntyneet luokat olivat joko liian abstrakteja tai tarkkoja, koska käytin alussa vain mikroanalyysin virkeanalyysiä, joka on rivi-riviltä analyysi. Tämän takia syntyi useita iteraatiokierroksia, joista usea päättyi käsitteiden ja luokkien uudelleen muodostamiseen, koska suoritimme näistä tutkielman ohjaajien kanssa laadullista analyysia katselmointien yhteydessä. Vaikeutena oli luokkien nimeäminen niiden ominaisuuksien ja ulottuvuuksien mukaan. Muutimme tässä vaiheessa aineistoanalyysilähestymistapaa ja otin käyttöön myös "In Vivo"-koodauksen, jossa nimesin suoraan eli käsitteellistin

tutkimusaineistosta vastaajien antamia avainsanoja. (ks. Strauss ja Corbin 1990, 63–65) Jatkaessani vertailua joidenkin ilmiöiden selittäminen tavalliseen tapaan ei onnistunut, tällöin käytin tarvittaessa tarkempaa järjestelmällisen vertailun analyysiä, jolloin suoritin vertailun löydöksen ja kirjallisuuden tietoja, koska muuten nämä ilmiöt olisivat jääneet huomioimatta (ks. Strauss ja Corbin 1998, 93–94). Kirjoitin nämä tiedot Atlas.ti ohjelman tageihin muistiin myöhempää luokittelua ja analysointia varten.

Avoimen koodauksen tuloksena syntyi yhteensä 321 tagia (ks. Taulukko 6). Käsitteellistämisen eli ilmiöiden tunnistamisen jälkeen päällekkäiset ilmiötä jakautuivat yhteiseen luokkarakenteeseen niiden yhteisten ominaisuuksien mukaisesti (ks. Strauss ja Corbin 1998, 103). Luokitellessani näitä tageja kirjoitin myös luokan nimen yhteyteen muistion, johon lisäsin tiedon siitä mitä olin luokan nimeä tehdessäni miettinyt. Nämä muistiot auttoivat minua, kun luokittelin tageja järjestykseen niiden ominaisuuksien ja ulottuvuuksien mukaan. Tämä vaihe kesti useita viikkoja. Käsitteellistämisen tuloksena syntyi 61 luokkaa, jotka jakautuivat työn rajauksen mukaisten indikaattorien alaisuuteen siten, että niitä oli organisaatiotasolla 41, ohjelmistotasolla 12 ja tietoverkkotasolla 9 kappaletta.

Taulukko 6. Avoimen koodauksen luokat

Avoinkoodaus	Tagien lkm.	Avoinkoodaus	Tagien lkm.
OH: Päivitys	5	OR: Tietoturvaohjeistuksen päivittäminen	10
OH: Käyttöönoton tarkastukset	6	OR: Tietoturvaohjeistuksen puutteiden luettelointi	11
OH: Lokitiedot	4	OR: Tietoturvaohjeistuksen saatavuus	8
OH: MST Ohjelmistotuki	4	OR: Tietoturvaohjeistuksen sisältö	9
OH: MST ohjelmistot	4	OR: Tietoturvaohjeistuksen yhdenmukaisuus	5
OH: MST testaus	8	OR: Tietoturvaongelman tapahtuma analyysi	12
OH: MST tietoturva	7	OR: Tietoturvaongelmien havaitseminen	5
OH: OST ohjelmistot	2	OR: Tietoturvaongelmista tiedottaminen	5
OH: OST riskit	2	OR: Tietoverkkojen käyttösäännöt	5
OH: OST testaus	5	OR: Tietoverkonsuunnittelu	2
OH: Päivityksien testaus	8	OR: Toimenkuva	11
OH: Testiympäristö	3	OR: Toimintapolitiikan ja -strategian muutokset	3
OR: Asiakirjahallinnan tietoturva	3	OR: Toimintapolitiikka ja –strategia	3
OR: Asiakirjahallinta	4	OR: Työn ohessa kouluttautuminen	4
OR: Hiljainen tieto	5	OR: Uhkista raportointi	8
OR: Järjestelmän käyttö-ohjeistus	6	OR: Yleisoheistuksen yhdenmukaisuus	6
OR: Käyttäjätunnustenhallinnan uudistaminen	3	OR: Yleisohjeistuksen haku	3
OR: Käyttäjätunnustenhallinta	3	OR: Yleisohjeistuksen päivittäminen	2
OR: Kokematon työntekijä	10	OR: Yleisohjeistuksen puutteiden kirjaaminen	7
OR: Kouluttautuminen	5	OR: Yleisohjeistuksen sisältö	7
OR: Koulutuksesta saadun tiedon jakaminen	3	TV: Dokumentaatio	11
OR: Koulutusmahdollisuus	11	TV: Hallinnanvalvontajärjestelmä	2
OR: Koulutusmuodot	7	TV: Palomuuri	4
OR: Laitteiden käyttö-ohjeistus	4	TV: Palvelinlaitteisto	1
OR: Laitteiden valvonta	2	TV: Rakenteellinen tietoturva	6
OR: Nykyinen työkokemus	9	TV: Rakenteelliset puutteet	2
OR: Palvelujen ostaminen	3	TV: Sisäverkko	2
OR: Rekrytointi - Aiempi työkokemus	8	TV: Varmuuskopio	1
OR: Sisäinen koulutus	5	TV: VPN-yhteys	2
OR: Tapahtumanhallintajärjestelmä	4		
OR: Tietohallinnon tehtävät	5		
OR: Tietohallinnon vahvuus	3		
OR: Tietoturvanhallinta	3	Yhteensä	321

4.5.3 Aksiaalinen koodaus

Aksiaalisen koodauksen tarkoituksena on koota tutkimusaineisto luokkiin ja alaluokkiin niiden ominaisuuksien ja ulottuvuuksien mukaan (ks. Strauss ja Corbin 1998, 123). Siirryin tässä analyysin vaiheessa käyttämään tukena Excel-taulukkolaskentaohjelmaa Atlas.tin ohessa, koska avoin koodaus sisälsi huomattavan määrän luokkia ja Atlas.ti ohjelma mielestäni peitti kategorialistat ja haittasi luokkien kokoamista.

Aksiaalikoodausen alkuvaiheessa, kun analyysi oli edennyt siihen pisteeseen, että luokat ja alaluokat alkoivat muodostua, suoritin niille paradigma-analyysin, jossa alaluokat vastaavat kysymyksiin kuka? milloin? miksi? miten? ja mitä seurauksia? Nämä vastaukset paljastavat luokkien väliset suhteet. Tämä analyysi on vain tietynlainen näkökulma dataan, auttaen liittämään rakenteen ja prosessin integroinnin systemaattisesti. (ks. Strauss ja Corbin 1998, 127)

Aloitin analyysin tekemällä taulukon ja täyttämällä avoimen koodauksen luokan lauseilla taulukon kentät siten, että jos alaluokista löytyi saman sisällöllinen vastaus jätin ne käyttämättä. Tämän induktion ansiosta kykenin myös tarkastelemaan ja uudelleen luokittelemaan heikosti kehittyneitä luokkia. Vastausta ilman jääneet kysymyskohdat jätettiin tyhjäksi. Analyysissä kenttään kuka suuraakkosin lisätty tieto on tutkija lisäämä. Taulukkokentissä vastaus on lainausmerkeissä ja sen jälkeen on vastaaja. Esimerkkeinä analyysin vaiheesta ovat organisaatiotason luokka Hiljainen tieto (ks. Taulukko 7), ohjelmistotason luokka (MTS) Muualla tuotettujen sovellusten ohjelmistotuki (ks. Taulukko 8) ja tietoverkkotason luokka rakenteelliset puutteet (ks. Taulukko 9).

Luokka	**Kuka?**	**Milloin?**	**Miksi?**	**Miten?**	**Mitä seurauksia?**
OR: Hiljainen tieto	TIETOHALLINTO	"Meillä on myös paljon käyttäjien tai järjestelmien ylläpitäjien päässä olevaa hiljaista tietoa. tämä hiljainen tieto pitäisi saada tuonne dokumentteihin." -v07 "Ohjeistuksien toiminnot myös leviävät keskustelujen kautta, jos joku muu törmää myös samaan asiaan. Tällöin voidaan kertoa mitenkä asia hoidetaan ja mitenkä tämä nyt menikään." -v04	"No, ne ovat suullisia ohjeita, koska ne tulevat/ muodostuvat omiksi käytänteiksi, siten että joku asia jota pitää tehdä, niin se selvitetään, mutta siitä ei tehdä mitään erillistä ohjetta."-v04	"Niistä ei ole mitään kirjattu ylös, ne ovat lähinnä tällaisia keskusteluja, joissa asiat selvitetään ja käydään läpi. Tietystihän meille tulee, ne kaverit jotka asentelevat ja tekevät näitä hallintajärjestelmiä, niin onhan meillä näistä semmoisia esittelytilaisuuksia, joissa käydään näitä ajoittain läpi. " -v04	"Väkisinhän sitä jonkin verran syntyy ja jää sinne, mutta ainakin pääpiirteittäin hiljainen tieto pitäisi saada järjestelmien osalta, eli se tieto millä tavalla se on konfiguroitu, mitä ne järjestelmät ovat ja mitkä päivitykset sinne on ajettu." -v07

Taulukko 7. Paradigma analyysi organisaatiotason luokalle

Luokka	**Kuka?**	**Milloin?**	**Miksi?**	**Miten?**	**Mitä seuraksia?**
OH: MTS Ohjelmistotuki	TIETOHALLINTO	"Ohjelmistojen tietoturvaa seurataan useista kanavista, mitä tietoturva-aukkoja löytyy vastaavista järjestelmäympäristöistä mitä meillä on."-V06	"Seurataan maailmalla tapahtuvia reaktioita, kun toiset käyttäjät asentavat näitä päivityksiä, jos niissä on jotain ongelmia, niin silloin maailmalle tulee hirveästi tietoa mitä niissä päivityksissä on ja miten ne ovat menneet." – V04	"Meillä on skanneriohjelmistoja joilla voimme tietysti löytää sellaiset tyypilliset puutteet ja se että ohjelmistot pidetään ajan tasalla." – V01 "Mitä tulee näiden muiden tuotteiden ohjelmistosovelluksiin mitä otetaan meillä käyttöön, niin niihin perehdytään ennen käyttöönottoa konfiguraatio tasolla ja luetaan hyvät käytännöt miten niitä on tarkoitus käyttää ja miten niitä käytetään." -v03	"Näihin aukkoihin reagoidaan nopeasti tai hitaasti riippuen tietoturva-aukon kriittisyydestä." – V06

Taulukko 8. Paradigma analyysi ohjelmistotason mallille

Luokka	**Kuka?**	**Milloin?**	**Miksi?**	**Miten?**	**Mitä seurauksia?**
TV: Rakenteelliset puutteet	TIETOHALLINTO	"Tällä hetkellä melkein kuka tahansa voi tulla kannettavan tietokoneen kanssa ja varastaa IP-osoitteen kytkemällä sen vapaaseen pistorasiaan." -V06	"Tähän ollaan miettimässä keinoja, joilla kytkeytymiset voitaisiin estää." – V06	"Jos vain seinässä oleva rasia on kytketty verkkoon, niin tällöin pitää löytää meidän verkosta vapaa IP-osoite, niin tällöin meidän Intranet on käytettävissä. Eli tällöin tunkeutujan pitää löytää vapaa IP-osoite, hän ei voi muuten kytkeytyä." – V06	-

Taulukko 9. Paradigma analyysi tietoverkkotason luokalle

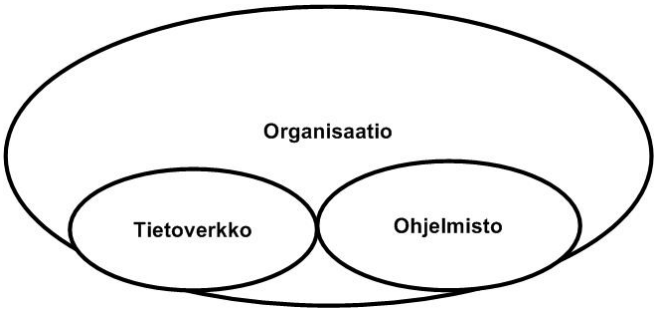
Aksiaalikoodauksen analyysissä etsin vastausta kysymyksiin miksi? tai miten? Näiden kysymysten avulla voidaan luoda sarjan olosuhteita tai tapahtumia, jossa henkilöt tai ryhmät voivat olla. Etsimällä aineistosta vastausta kysymyksiin kuka? ja miten? Nämä kysymykset voivat antaa vastauksen toimita/vuorovaikutussuhteisiin, siitä miten nämä henkilöt tai ryhmät vastaavat toiminta/vuorovaikutus tilanteisiin. (ks. Strauss ja Corbin 1998, 124–128) Toteutin tämän vaiheen induktion ja päättelyn keinoin. Keräsin aineistosta tunnistamista tiedoista inhimillisiä tekijät ja mahdolliset vääristävät merkitykset vertailemalla niitä omien tulkintojeni kautta. Kirjoitin nämä tiedot aksiaalistason luokan muistoon. (ks. Strauss ja Corbin 1998, 137).

Aksiaalikoodauksen aikaisen paradigman selityksen tulee sisältää mikro - ja makrotason ehtoja, sekä tiedot siitä miten nämä leikkaavat toisiaan (ks. Strauss ja Corbin 1998, 131–133). Tässä tutkimuksessa mikrotasolla tarkoitetaan koulutusorganisaatioita itseään ja makrotasolla sen ulkopuolista maailmaa eli yhteistyökumppaneita, laitteistotoimittajia, ohjelmistotoimittajia ja tietoturvaa.

Aksiaalikoodauksen aikaisen paradigma-analyysin tuloksena syntyi SWOT nelikenttämenetelmällä luotu kaavio. Nämä kaaviot on esitelty luvussa tulokset yhteenveto alaluvussa (ks. luku 5.4). Sen tarkoituksena oli kuvata toiminta/vuorovaikutuksen ja olosuhteiden tilaa mikrotasolla. Tämä tapahtui siten, että koulutusorganisaation tietoturvanhoidossa tutkimusaineistossa ilmenneitä vahvuuksia kuvattiin (+)-merkillä ja heikkouksia, eli tietoturvaa heikentäviä uhkia/toimia (-)-merkillä. Ulkopuolisen maailman suhteita eli tietoturvaa parantavia asioita kuten ohjelmisto- ja laitteistotoimittajien päivitykset, tietoturvaohjeet, lait ja standardit sekä tietoturvaa parantavat viitekehykset (+)-merkillä ja ulkoiset uhat (-)-merkillä. Tässä analyysissä kuvataan alaluokkien suhdetta luokkaan. (+)-merkki tarkoittaa että se vie alaluokkaa kohti pääluokkaa ja (-)-merkki vie alaluokkaa poispäin tutkittavasta luokasta. Näimä kaaviot ilmentävät (ks. luvussa 5.2) kuinka organisaatiot huolehtivat tietoturvasta. (ks. Strauss ja Corbin 1998, 184–185)

Selektiivinen koodaus on viimeinen analyysivaihe integraatiossa yläluokan käsitteiden ympärille ja se täyttää luokkia, jotka tarvitsevat elelleen kehittämistä ja tarkentamista. Ensimmäinen askel tässä integraatiossa on löytää keskeiset pääluokat, jotka edustavat tutkimuksen pääteemaa eli asetettuja tutkimuskysymyksiä ja rajauksia. (ks. Strauss ja Corbin 1998, 146)

Aloitin lähestymisen integraatioon kirjoittamalla muistioihin juonen "Mitä näyttää olevan tekeillä?" ja ydinkategoriat, joihin muut luokat liittyvät, vahvistui. Syntyi siis yksi keskeinen ydinkategoria organisaatio ja sitä täydentävät ohjelmisto ja tietoverkko (ks. Kuvio 8)



Kuvio 8. Selektiivisen koodauksen luokkarakenne

Seuraavassa luvussa tarkastellaan tutkimuksen tuottamien tulosten antia ja niitä esitellään tutkimusongelmittain.

5 Tulokset

Tässä luvussa käsittelemme tutkimuksen tuottamia tuloksia. Kolmessa ensimmäisessä alaluvussa tarkastellaan asetettuja tutkimusongelmia ja lopuksi yhteenveto alaluvussa esitän vastaukset esiteltyihin tutkimuskysymyksiin.

5.1 Miten tietoturvamallit näkyvät tutkittavissa organisaatioissa?

Aineistoanalyysi tuloksena tarkentuivat tutkimuksen alussa määritellyt ydinkategoriat, jotka jakavat organisaation organisaatio-, ohjelmisto- ja tietoverkkotasoille. Nämä muodostuneet kategoriat ovat vahvasti sidoksissa toisiinsa organisaation sisällä. Organisaatiotaso toimii kaiken organisoivana yksikkönä, jonka kaikki toiminnot heijastuvat heikentävästi tai vahvistavasti muiden tasojen hoitoon. Organisaatiotaso pitää sisällään organisaation kaikki suunnittelu ja toteutusmääritelmät. Ohjelmisto- ja tietoverkkotaso ovat toteuttamisen tasoja. Ohjelmistotasolla sovelletaan organisaatiotasolla päätettyjen suunnitelmien ja toteutusmääritysten mukaisten järjestelmien ohjelmistojen toiminnallisuus ja niiden tietoturvallisen toiminnallisuuden varmistaminen. Tietoverkkotasolla sovelletaan organisaatiotasolla tehtyjen suunnitelmien ja toteutusmääritysten verkon rakenteellisen toiminnallisuuden varmistamiseen.

Organisaatiotaso

Organisaatiotason rakenne ja sen tietoturvan hoitaminen oli odotetusti haastattelujen keskeisin taso koko organisaation toiminnan ja tietoturvan kannalta. Tässä kappaleessa käsittelen sitä, miten tietoturvamallit näkyvät organisaatiotason tilassa. Seuraavassa taulukossa (ks. Taulukko 10) esittelen ne luokittelukohdat aineistosta, jotka koskevat organisaationtasoa haastateltavien antamissa merkityksissä.

Luokka	Alaluokka
Tietoturvataso	OR:Toimintapolitiikka ja -strategia OR:Toimintapolitiikan ja - strategian muutokset OR:Tietoturvan hallinta OR:Tapahtumanhallintajärjestelmä
Tietoturvapoikkeamatilanteiden hallinta	OR:Tietoturvaongelman tapahtuma-analyysi OR:Tietoturvaongelmien havaitseminen OR:Tietoturvaongelmista tiedottaminen OR:Tietoturvauhista raportointi
Pääsynhallinta	OR:Käyttäjätunnustenhallinta OR:Käyttäjätunnustenhallinnan uudistaminen
Tietoturvan toteutuminen	OR: Laitteiden valvonta OR:Uhkista raportointi
Tietoturvaohjeistus	OR:Tietoverkkojenkäyttösäännöt OR:Tietoturvaohjeistuksen sisältö OR:Tietoturvaohjeistuksen saatavuus OR:Tietoturvaohjeistuksen yhdenmukaisuus OR:Tietoturvaohjeistuksen puutteiden luettelointi
Yleisohjeistus	OR: Yleisohjeistuksen yhdenmukaisuus OR:Yleisohjeistuksen haku OR:Yleisohjeistuksen päivittäminen OR:Yleisohjeistuksen puutteiden korjaaminen OR:Yleisohjeistuksen sisältö

Taulukko 10: Tietoturvamallien näkyvyys organisaatiotasolla

Organisaation tietoturvasuunnitelmien muoto tulee olla sellainen, että ammattilaiset voivat

ymmärtää niiden sisällön. Niiden luonteena on olla julkinen dokumentti ja tämän takia niiden ei kuitenkaan tulisi olla yksityiskohtaisia tietoja sisältävä dokumentti. Tämä rajoite suojaa organisaatioita, jotta dokumentit eivät anna mahdollisuutta hyökkäyksien tai tietomurtojen suunnitteluun. Haastateltavat kuvaavat organisaatioiden ylimmän johdon tietoturvasuunnittelussa hyväksymiä käytänteitä, joiden tarkoituksena on saavuttaa haluttu tietoturvan taso tietojärjestelmissä. Organisaation toimintapolitiikka ja -strategiadokumentin tallennustapaa kuvaa eräs haastateltava seuraavasti:

> " *Itse asiassa, ne johdon tekemät strategiat ovat minun mielestä viety Intaraan ja niiden pitäisi löytyä meidän Intrasta, mutta tietoturvapäälliköllä on joitain dokumentteja, joita ei ole viety edes Intraan jostain syystä.-v06*"

Muistio aiheesta: Haastateltava kuvaa ilmeisesti tietoturvapolitiikka ja -strategiadokumenttien liitetiedostoja, joissa on kuvattu käytänteitä ja teknisiä ratkaisuja. Nämä liitteet sisältävät sellaista tietoa, joka antaisivat mahdollisuuden haitallisen toiminnan suunnittelulle ja toteuttamiselle.

Toimintapolitiikka ja-strategia dokumenttien sisältäviä suunnitelmia tulisi kehittää keskipitkällä aikavälillä ja eräät haastateltavat kuvaavat niitä seuraavasti:

> " *Sitten tuli tarkennuksia tuohon Katakri-standardiin ja tähän liittyen on auditointi tuolla IT-dynamon puolella. laboratorioihin tulee tiettyjä vaatimuksia tietohallinnolle ja koko organisaatiolle. Näissä dokumenteissa on otettu huomioon mitä se Katakri-standardi vaatii.-v07*"

> " *Jos nyt totta puhutaan niin kyllä. Emme olisi ihan noin raskaasti lähetty liikenteeseen. Tietysti tarkastuksia olisi tehty muutenkin, tämä on vähän turhan tämä Katakri, koska tehdään vain paljon paperia, ne jätetään sitten vain noihin mappeihin pölyyntymään. Näillä resursseilla se on vähän turhan raskas prosessi.-v05*"

Muistio aiheesta: Työntekijöiden näkemykset standardimaisen tietoturvasuunnittelun vaatimustason tuomista muutoksista ovat suuria. Heidän mielestään vaatimustaso vaikuttaa haittaavasti rutiinityöskentelyyn ja täten päivittäisten työtehtävien suorittamiseen. Heidän mie-

lestään näiden muutosten vaikutus järjestelmätasolla ei ole kovin suuri ja se vaatii hyötyyn nähden erittäin suuren dokumentaation.

Organisaation tietoturvasuunnitelmat sisältävät myös tapahtumanhallintajärjestelmän. Tämän dokumentin tarkoituksena on suunnitella miten haitalliset havaitut tapahtumat, jotka sisältävät poikkeamia, kirjataan tietohallinnon ylläpitämään tapahtumanhallintajärjestelmään. Eräs haastateltava kuvaa tämän dokumentin rakennetta ja kehittämistä seuraavasti:

> " *Se jatkuvampi dokumentaatio on sitten siellä tapahtumahallintajärjestelmässä tai jos me otetaan vaikka järjestelmäversio. [–] Saattaa olla, että versiohallinasta luodaan tiketti hallintajärjestelmään tai versiopäivitys luodaan tapahtumanhallintaan omana tikettinä. Eli tällöin tapahtumat käsitellään sitten tiketissä, jolloin tämä tieto ei koskaan päädy alkuperäiseen asennusdokumentaatioon. Elikkä se jää vain olemaan, eli se pitää osata sieltä sitten katsoa, mitä tehtiin ja miksi se tehtiin.-V03*"

Muistio aiheesta: Tietoturvamallin tarkoituksena on tiivistää tehtävän toimenpiteen tarkoitus, sen tuomat hyödyt ja haitat järjestelmän toimintaan tai vaikutukset ympäristön muihin toimintoihin. Kuvattu järjestelmä ei tue laadukkaiden tai luotettavien ratkaisujen mukaista toimintatapaa.

Organisaation tietoturvasuunnitelmat sisältävät myös tietoturvallisuuden hallintajärjestelmän. Eräs haastateltava kuvaa sen tarkoitusta ja toimintaa seuraavasti:

> " *Hallintajärjestelmä on ollut tällainen projekti, missä me olemme systemaattisesti tarkastelleet eri osa-alueita ja viemme eteenpäin tietoturvakysymyksiä kehitettäväksi ja sitä kautta tietoturva asiat tulevat henkilöstölle tutuksi.-v01*"

Muistio aiheesta: Haastateltavat sekoittavat tietoturvanhallintajärjestelmän ja tapahtumahallintajärjestelmän tai sitten heillä on tarkoitus jakaa tietoturvanhallintajärjestelmä kahdeksi eri dokumentaatioksi. Tietoturvamallin näkökulmasta tietoturvanhallintajärjestelmissä tulisi määrittää vain todelliset uhkat ja niiden haavoittuvuudet varoille. Muiden uhkien määrittäminen tekee tietoturvan toteuttamisesta vain kalliimpaa.

Organisaation tietoturvallisuuden hallintajärjestelmän tarkoituksen on olla prosessi, jossa

toiminnan tai ympäristön muutoksia kehitetään niiden noudattamisen, seurannan ja arvioinnin keinoin. Prosessin lähtökohtaiset vaiheet ovat suunnittele, tee, tarkasta ja toimi. Eräs haastateltavat kuvaa sitä seuraavasti:

> " *Kuten jo aikaisemmin sanoin, meillä on tietoturvahallintajärjestelmäprojekti menossa, niin siellä tähän dokumentaatioon on jonkin verran elinkaarisuunnittelua ja toipumissuunnitelmaa, sekä tämmöiseen perusdokumentaatioon liittyviä asioita mietimme tarkkaan. Voisi ajatella, että mitä meillä ollaan viemässä eteenpäin, on ehkä tällainen systemaattisempi tapa listata meidän hallinnassa olevia asioita ja niiden perustietoja. Kuten esimerkiksi kuka järjestelmän omistaa, kuka on tekninen pääkäyttäjä, mikä on järjestelmä laskennallinen arvo, kuka sen hallinnollinen omistaja on, kuinka usein otetaan backup-tietoja ja kuka on sen järjestelmän toimittaja.-v01*"

Tietototurvapoikkeamatilanteiden hallinta osoittautui tärkeäksi aiheeksi haastateltavien keskuudessa. Poikkeamatilanteita varten organisaatioiden tulisi luoda etukäteissuunnitelmat sille, kuinka heidän tulisi säilyttää häiriötilanteiden tai poikkeusolojen aikana toimintakykynsä. Eräät haastateltavat kuvaavat näitä käytänteitä seuraavasti:

> " *Niin tämä asia hoidetaan sitten sen prosessin mukaisesti tai jos se ei maailman kiireellisin asia olisi, jos siten nähdään selkeästi ja varmasti joka sitten aistii että jotain on nyt pielessä, niin aika paljon pallo on sitten hänellä kuinka hän reagoi ja mihin päin ottaa yhteyttä. Olivatpa ne se sitten raportti, dokumentti tai yleisesti tekemistä niin reagoitaisiin siihen mahdollisimman pian ja korjattaisiin asia kuntoon. Tietoturvaongelmissa tietysti pienistä asioista voi kuitenkin syntyä isoja tai kerralla voimme kokea laajana uhkana, mutta tietysti tässä kun meillä ei ole hirveästi kokemusta, koska tällaisia tapauksia ei ole oikeastaan ollut lainkaan matkanvarrella, niin ainahan se tietysti varautuminen on sitten haasteellista.-v01*"

> " *Pääasiallisia keinoja ovat, tunnetaan omat järjestelmät. Pysytään uutisvirrassa ajan tasalla, jotta tiedetään mitä tapahtuu. Osataan tämän kautta sopeutetaan omia järjestelmiä, koska tällöin havaitaan ongelmakohdat, jotka koskevat*

meidän omia järjestelmiä ja ollaan aktiivisesti päivittämässä järjestelmiä heti kuin mahdollista. Nämä ovat ne pääasialliset keinot, eli ollaan valppaana. On tärkeää, että ylläpitäjä tuntee nämä Certi-fi listat ja totta kai käyttöjärjestelmien valmistajat, jos ajatellaan näitä kahta päähaaraa, eli Linux ja Windows järjestelmiä.-v02"

Muistio aiheesta: Haastateltavien työtehtävät vaikuttavat suoraan siihen, kuinka he mieltävät näiden etukäteissuunnitelmien sisällön. Toiset haastateltavat odottavat tietoa tapahtuneesta tietoturvapoikkeamasta ja rupeavat toimimaan suunnitelmien mukaisesti. Toiset haastateltavista ajattelevat, että jatkuva varautuminen on paras puolustus.

Vaikka organisaatiot ovat luoneet etukäteissuunnitelmia sille, kuinka heidän tulisi toimia tietoturvapoikkeamatilanteissa, olivat haastateltavat kuitenkin hieman epävarmoja suunnitelmien toiminnallisesta sisällöstä:

" *Onko tämä henkilö kenties meidän tietoturvapäällikkö vai ottaako joku muu asian hoitaakseen.-v06*"

" *Elikkä tulee tällainen tietoturvahäiriö. Meillä ei ole käytössä mitään varsinaisia kriteerejä sitä, miten lähdettäisiin tekemään. Mutta luulen, että sitä lähdetään tekemään tietoturvallisuuden hyvien käytänteiden mukaisesti.-v07*"

Muistio aiheesta: Organisaatiot ovat luoneet etukäteissuunnitelmat, kuinka heidän tulisi toimia häiriötilanteissa. Nämä etukäteissuunnitelmat ovat vieraita henkilöstölle. Suunnitelmiin ei ole nähtävästi poimittu organisaation sisällä syntyneitä työrutiineita, joista on tullut ajan kuluessa käytänteitä. Onko näitä etukäteissuunnitelmia testattu käytännössä? Eikö organisaatioissa ole vielä ilmennyt häiriötilanteita? Onko häiriötilanteista toteutettu suunnitelmien vaiheiden mukaisesti? Ovatko vastuuhenkilöt soveltaneet mielensä mukaisesti ohjeistusta tilanteen mukaan lieventäen?

Haastateltavat ottivat kantaa siihen, kuinka heidän organisaatioissaan toimitaan, kun havaitaan tai on aiemmin havaittu tietoturvaongelmia:

" *No kyllähän se varmaan on minun lähimmät työkaverit ensimmäisenä, joille asioista raportoidaan, koska he ovat sellaisia joilla on mahdollisuus tehdä*

joitakin toimenpiteitä tälle asialle.-v04"

" *Ongelmia on hyvin vähän ollut koko työurani aikana. Käytännössä mitä sitten on ollut, ovat olleet sitä tasoa, että olemme olleet poliisiin yhteydessä suoraan. Näissä tapauksessa on rikottu lakeja, meidän käytänteet menevät tällä tavoin.-v05*"

Haastateltavat kuvaavat, kuinka organisaatiossa on suunniteltu tietoturvauhkista raportointi. Haastateltavien mielestä järjestelmien käyttäjät harvoin tai koskaan raportoin tietoturvauhkista, vaan yleensä ne ovat peruskäyttöön liittyviä ongelmia. Eräät haastateltavat kuvasivat tilanteita seuraavasti:

" *Ei tietoturvapuolella ongelmia siellä raportoinut kukaan tai ottanut kantaa näissä tiketeissä. Nämä asiat liittyvät ihan peruskäytännön ongelmiin ja sellaisiin tapauksiin tai jotain täytyy saada luotua jonnekin järjestelmään ikään kuin tällaisia pyyntöjä.-v04*"

" *Siis, mitä Helpdeskiin tulee, niin ne ovat loppukäyttäjien ongelmia, joko itse aiheutettuja pääsääntöisesti. Tai sitten, jos on ollut vikatilanteita, jossain esimerkiksi laitteita hajonnut tai jotain tällaista, tämä on normi Helpdesk lähituki toimintaa pääsääntöisesti.-v05*"

Organisaation työntekijöiden havaitsemia tietoturvauhkia ovat enimmäkseen kirjautumisiin liittyvät ongelmat ja eräs haastateltava kuvaa niitä seuraavasti:

" *Nämä tapaukset ovat sellaisia, että tunnuksen aktiivisuus on sellaista, mitä ei normaalisti millään tunnuksella ole. Tällöin tulee kirjautumisia useita päivässä sellaisista paikoista, missä käyttäjä tuskin tällä hetkellä on liikkumassa.-v06*"

Eräs haastateltava kuvaa tietohallinnon käytänteitä havaittuun tietoturvauhkaepäilyyn seuraavasti:

" *Nämä epäilyt kirjataan suoraa APUSE-palveluun jonoon ja jos tietoturvapäällikkö on paikalla, niin voin käydä vielä sanomassa henkilökohtaisesti tietoturvapäällikölle, että tällainen homma on menossa ja voiko katsoa tätä. Jos tieto-*

turvapäällikkö ei ole paikalla, niin tällöin pitää katsoa kuka on tuolla APUSEn puolella paikalla, niin tällöin käyn sanomassa että viitsisittekö katsoa tätä tapausta.-v06"

Tietoturvan poikkeustilanteiden hoitoon kuuluu myös organisaation häiriötilanteesta toipuminen. Toipumisen jälkeen, myös muita yhteistyökumppaneita tai toimijoita tulisi varoittaa ilmenneestä uhkasta tarvittaessa. Haastateltavat kuvaavat näitä toimia seuraavasti:

" *Ja jos nähdään, että on hyvin tärkeä tai merkittävä asia kyseessä, niin totta kai johdon tulee olla siitä tietoinen. Turvallisuusvastaava, joka talossa on tai turvallisuuspäällikkö, joka on toimitilapalveluissa sijainnillisesti, niin hänen kanssaan yhteistyössä jos siihen liittyy jotain isompaakin uhkaa tai nähtäisi uhkakuvia laajemmin ottaen, niin voisimme ottaa siihen paremmin kantaa. Kun olemme Jyväskylän kaupungin konsernia, niin tietoturvapolitiikassa on kyllä määritelty jo vähän senkin suuntaista asiaa, jos me nähdään että on sensuuntaista tietoturvauhka ongelma tai vastaava niin myös ilmoitettaisiin tästä jyväskylän kaupungille.-v01*"

" *Tämän lisäksi ilmoittaisimme siitä myös laajemmin CERT-FIlle tai vaikka nyt Jyväskylän yliopistolle. Mutta tavallisemmin ilmoituksen saaja olisi ammattioppilaitos tai toisen asteen oppilaitos kuntayhtymässä, koska me olemme samassa verkkomaailmassa heidän kanssaan.-v01*"

" *Jolloin asia katsottaisiin, minkälainen se on ja millä tavalla sitä lähdetään tiedottamaan. Tiedotus koskisi niitä käyttäjiä ketä se koskee ja sitten mitä nyt on tapahtunut, niin voivatko he tehdä sille asialle jotain. Tämän jälkeen kun tiedämme mitä asia koske, niin voimme lähteä lieventämään sitä vahinkoa ja estämään jatkossa sen syntymistä.-v07*"

Haastateltavat kuvaavat organisaation pääsyn- ja käyttäjätunnustenhallinnan valvontamekanismien käyttöä. Pääsynvalvontaan tarvitaan tietojärjestelmien ja muiden laitteiden hyväksyttävän käytön määrittämistä. Määritys voidaan tehdä koko organisaatiota koskevana tai sitten työtehtävien mukaan. Käyttäjätunnusten hallinta on tietoturvan perustavoitteita täydentävä toimi. Tällä halutaan varmistua, että organisaatio kykenee kiistatta todistamaan tietojen

luojan tai käyttäjän henkilöllisyyden. Haastateltavat kuvaavat näitä määrityksiä seuraavasti:

> " *Järjestelmällinen tunnusten käsitteleminen tarvitsee tiedon, milloin henkilö on tullut tiettyyn tehtävään ja muutenkin kun henkilö tulee taloon. Tähän liittyy myös paljon muita asioita eri tietojärjestelmissä. Sen takia, koska hänen pitäisi saada rahaa ja kaikkea muuta tällaista asioita, eli kuka on hänen esimies.-v04*"

> " *Käyttö-oikeuksilla ja asiakirjahallintajärjestelmien sisällä käyttäjätunnuksia ei anneta ryhmiin automaattisesti. Tietojenhallinnassa kun käyttäjä poistuu, niin tilanne päivitetään välittömästi.-v08*"

Haastateltavat toivat aiemmin esiin organisaation tarpeen tarkastella vanhojen tietoturvasuunnitelmien käytänteiden tasoa suhteessa haluttuun tietoturvatason heidän tietojärjestelmissään. Tämän toiminnan tuomia muutoksia pääsy- ja käyttäjätunnustenhallinnan vaatimuksia kuvaa eräs haastateltava seuraavasti:

> " *No, itse asiassa se on sen seurannan parantaminen, ettei vaan oteta vain henkilöä töihin ja anneta hänelle tunnuksia. Sitten tämä henkilö heiluu täällä ja ehkä siihen laitetaan jokin raja-aika hänen tunnukselle. Tarkoituksena olisi saada henkilöhistoriat hallintaan siten, että meillä ihan siitä päivästä käyttäjä tulee meille aina siihen päivään kun hän lähtee. Meidän olisi hyvä tietää keitä on talon järjestelmissä ja missä hommissa ja mahdollisesti kuinka kauan hän on palveluksessa.-v04*"

Haastateltavat kertovat, kuinka organisaatiot huolehtivat tietopääomaan eli järjestelmien sisältämien tietojen lisäksi myös laitteisto- ja fyysisestä turvallisuudesta. Organisaation varmistavat fyysisen omaisuuden toimivuudesta ja saatavuudesta seuraavasti:

> " *Seuraamme ettei tietokoneita varasteta ja sitä, että tietokoneita kohdellaan hyvin ja sitä, että tietokoneet ovat käyttökuntoisia. Sitten taas kun perinteinen virastoaika päättyy ja talossa on vielä tämän jälkeenkin paljon ihmisiä paikalla, niin ilta-aika on aikalailla vahtimestarien vastuulla, koska kun he ilta-aikaan kiertelevät ja katselevat esimerkiksi vähän mitä ihmisiä täällä liikkuu ja mitä meidän tietokoneilla tehdään. Vahtimestarit omalta osaltaan ja henki-*

löstö omalta osaltaan ja vastaavalla tavalla IT-tuki seuraa työasemien käyttöä ja miten opiskelijat istuvat noiden tietokoneiden ääressä ja mitä noilla koneilla tehdään.-v01"

Haastateltavat kuvaavat organisaation johdon määrittelemiä, käyttäjille tarkoitettuja teknisiä tietoturvaohjeistuksia. Näiden dokumenttien tulisi olla toimintaa edistäviä ja ylläpitäviä asiakirjoja. Nämä asiakirjat on tarkoitettuja tietojärjestelmistä vastaaville ja tietojärjestelmiä käyttäville henkilöille. Nämä dokumentit ovat yleensä katsottavissa tietoverkon välityksellä, joko julkisena tai rajoitetusti tietylle asiakaskunnalle. Eräät haastateltavat kuvaavat näkyvyyttä seuraavasti:

" *Toinen on tämmöinen kuin tietoverkon käyttösäännöt ja toinen on tietoverkon ylläpitosäännöt ja nämä ovat sellaisia niin kuin, varsinkin tietoverkon käyttösäännöt että ne ovat julkisia ihan meidän Helpdesk sivustoilta löytyviä. Sitten ne ovat niin kuin henkilöstö Intrassa ja sitten on opiskelija Intrassa nämä säännöt ja sitten on arkistoitu tuohon meidän dokumentinhallintajärjestelmä, jolloin niillä on tietty säilytysaika sitten siellä niin kuin dokumenttityypin mukaisesti. Tietoverkon ylläpitosäännöt koskevat taas meidän ylläpitohenkilöstöä. Tietoturvan sisälle kuuluvan tietoverkkojen käyttösäännöissä, niin otettiin kantaa valvontaan, seurantaan ja siihen ketkä sitä tekevät. Nämä asiat ovat lähtökohtaisesti samalla ajatuksella tehty, kun kuinka toimitiloja seurantaan ja valvotaan.-v01*"

" *Verkonkäyttösäännöt tällaiset yleisesti saatavat kaikille henkilökunnalle ja opiskelijoille ja ne on sijoitettu Intraan. Kun opiskelijat hyväksytään koulutukseen, niin heille lähetetään verkonkäyttösäännöt, missä on tietoa tietoturvaan liittyen. Opiskelijat hyväksyvät nämä käyttösäännöt samalla, kun tulevat opiskelemaan.-v07*"

Tietoverkon ylläpitosääntöjen sisältä haastateltavat kuvaavat seuraavasti:

" *Konfiguraatiot on dokumentoitu ja ne ovat tarkoitettu asiansa osaaville, niin kuin tuota myös jatkuvuusdokumentaatiota ylläpitäjille.-v02*"

" *Ohjeistus pitää sisällään täsmällisiä ohjeita. Yleiset ohjeet ovat mielestäni ihan kunnossa, mutta vähän täsmällisemmät toimintaohjeet ovat vähän leväperäisiä, joten niitä pitäisi parantaa. No, mielestäni missään ei ole tällaista salasanapuolta, mitenkään ohjeistettu ei ole mitenkään dokumentoitu miten se oikeasti pitäisi toimia. En ole koskaan nähnyt tästä minkäänlaista paperista ohjeistusta missään, jossa olisi ollut toimintatapa.-v06*"

Haastateltavat kuvaavat ylläpitosääntöjen sisällön lisäksi niiden muotoa ja saatavuutta seuraavasti:

" *Oikeastaan kun Hepldesk-järjestelmään menee, niin laitavalikossa on jo tietoturvaasiat, että sieltä löytyy aika kattavasti semmoista hyvää tietoa tietoturvaan liittyen. Kyllä meillä on semmoiset sopivan tason dokumentaatiot on varmasti olemassa ja että ne on sijoitettu siten, että niihin pääsy on rajoitettu.-v01*"

" *No tikettinä, Wiki-dokumentteina, omina teknisinä muistiinpanoina ja sittenhän järjestelmät totta kai osaavalle henkilölle ne dokumentoivat itse itsensä, ne ovat selittäviä dokumentoijia, niin totta kai sieltä katsellaan mitenkä ne ovat toimineet.-v03*"

Muistio aiheesta: Tietoturvaohjeistuksen muoto vaihtelee suuresti ja se ei vastaa säännönmukaista tietoturvamallimaista dokumentaatiota. Nämä dokumentit ovat tarkoitettu teknisille asiantuntijoille itselleen, kun taas tietoturvamallit järjestelmien ylläpidosta ja hoidosta vastaaville henkilöille.

Haastateltavat kuvaavat ylläpito-ohjeistuksen yhdenmukaisuutta. Heidän mielestä dokumenttimallipohjasta huolimatta niiden sisällöllinen tarkkuus vaihtelee tekijän mukaan. Osa haastateltavista oli tyytyväisiä ja osa ei, riippuen kenen tekemiä dokumentteja he lukevat. Eräät haastateltavat kuvaavat näitä seuraavasti:

" *Kyllä meillä on tämmöinen Wiki tyyppinen järjestelmä mihin voidaan laittaa kaikkien osalta ne esille. Joidenkin työntekijöiden osalta ne eivät mene sinne ja toisten osalta ne menevät sinne. Se on vähän ylläpitäjistä kiinni itsestään. Se on niin kuin vakioitua pakotettua käyttöä.-v03*"

" *Minun mielestäni ohjeistus on yhdenmukaista ja johdonmukaista.-v04*"

" *Oheistus saisi olla parempaa, joten tällä hetkellä siihen ei pysty paljoa turvautumaan.-v06*"

Muisto aiheesta: Organisaation johdon tehtäviä on antaa tarvittaessa koulutusta myös asianmukaisen dokumentaation tekemiseen. Dokumenttien laatimisen ja ylläpidon vastuu kuuluu järjestelmän ylläpidon rutiineihin, koska puutteellisten dokumenttien selvitystyö vie enemmän aikaa kun niiden kunnollinen laatiminen.

Organisaation tulisi luetteloida tietoturvaohjeistuksessa ilmeneviä puutteita dokumenttien tarkasteluvälin aikana. Haastateltavat kuvaavat organisaatioiden käytänteitä niiden luettelointiin.

" *On ainakin aikaisemmin luetteloitu. En muista tämän viimeisimmän päivityksen yhteydessä olleita puutteita, mutta aikaisemmin on luetteloitu. Jos viimeisimmässä päivityksessä ei ole luetteloitu, niin minun mielestäni huono homma, mutta veikkaan ettei tällä hetkellä ole puutteita luetteloitu. Mielestäni ohjeistuksessa puuttuvia uhkia on luetteloitu, mutta puutteita ei ole.-v06*"

" *Ei luetteloida. Jos muutoksia tapahtuu, mutta ohjeistusta pidetään ajan tasalla sitä mukaan, kun yksiköt ilmoittavat puutteellisista tiedoista. Ei sammallailla kuin tietojärjestelmistä, tietojärjestelmien ollessa kyseessä ilmenevät puutteet luetteloidaan välittömästi tikettijärjestelmässä. Ideana on, että ihminen ilmoittaa mahdollisista virheistä. Tietohallinto tutkii asiaa ja ilmoittaa päätöksestä, josta jää myös merkintä järjestelmään. Järjestelmään ilmoitetuista puutteista, jotka eivät aiheuta toimienpinteitä, jää myös merkintä järjestelmään.-v08*"

Tietoturvaohjeistuksessa ilmenneiden puutteiden luetteloinnin jälkeen ne tulisi käsitellä ja niiden luonteesta riippuen ohjeistusta tulisi päivittää sen ajan tasalle saamiseksi. Haastateltavat kuvaavat näitä käytänteitä seuraavasti:

" *Sitä päivitetään, mutta ei säännöllisesti. Meillä on tällainen, jos ajattelet tietoturvaohjeistusta sellaista niin kuin, niille jotka käyttää tätä meidän järjestelmiä. Niin meillä on nettisivusto siihen, mutta sitä ei ole vuositarkastusta sille sään-*

nöstölle vaan tarpeen mukaan.-v02"

" *Tietoturvaohjeet niminen dokumentti on olemassa, sitä päivitetään varmaan säännöllisesti, mikäli viiden vuoden sykli voidaan pitää säännöllisenä, mutta tuota sanotaan vaikka näin hirveen aktiivista se ei ole. Sen nimisenä kuin se tietoturvaohjeistuksena ole, mutta totta kai nämä ylläpitokäytänteet on tällainen juokseva rutiini niin sitä mukaan kun se päivittyy, niin onhan sekin osaltaan tietoturvaohjeistusta ja ylläpitokäytänteitä. Ihan tuollaisena tietoturvaohjeistus nimistä pumaskaa ei ole verkossa ole aktiivisesti päivitettynä.-v03*"

Muistio aiheesta: Tietoturvaohjeistuksen tietosisältö ja dokumenttien rakenne ei vastaa tietoturvamallien määritelmää.

Organisaation järjestelmä asiantuntijoiden tulisi kirjoittaa dokumentaatiot muille järjestelmäylläpitäjille, jotta he voisivat tukeutua ongelmatilanteissa näihin dokumentteihin. Eräät haastateltavat kuvaavat dokumentointi käytänteitä seuraavasti:

" *Elikkä, jos joku nyt huomaa jossain että pitäisi dokumentoida joku asia ja päivittää ohjeistusta. Parhaimpana tapana näen, koska järjestelmienylläpitäjät ja kehittäjät istuvat työpaikalla vierekkäin tai ainakin vierivieressä, niin näen että vuoropuhelu on syntynyt ja joku huudahtelee tai ottaa asian esille kahvipöytä tai käytävä keskusteluissa, palvelupisteissä tai sähköposteissa tai milloin missäkin linkeissä.-v01*"

" *Jos tekisimme valtavan määrän dokumentaatiota ja pitäisimme se ajantasaisena. Meillä on hirveä määrä järjestelmiä ja jos kaikesta kirjoitettaisi kaikki tarkasti auki, niin tästä syntyisi sellainen määrä sivuja, ettei kukaan ylläpitäjä lukisi niitä. Muutamat asiat ovat nyt olleet sellaisia, että niistä on kirjoitettu raportit vain raportoinnin vuoksi. Tuntuu että tähän vain tulee byrokratiaa tähän touhuun, jos näin pienellä porukalla mitä meillä on ihmisiä, niin tarvittavan dokumentaation tuottaminen ja muu.-v01*"

" *Muutamat asiat ovat nyt olleet sellaisia, että niistä on kirjoitettu raportit vain raportoinnin vuoksi. Tuntuu että tähän vain tulee byrokratiaa tähän touhuun, jos*

näin pienellä porukalla mitä meillä on ihmisiä.-v05"

Haastateltavat kuvaavat organisaation johdon määrittelemiä käyttäjille tarkoitettuja teknisiä yleisohjeistusdokumentteja. Näiden dokumenttien sisällöllisen tiedon tuottaminen on tietohallinnon asiantuntijoiden tehtävä ja niiden tarkoitus on olla käyttäjille tukevia teknisiä asiakirjoja, joiden ohjauksen avulla käyttäjien tulisi selvitä normaaleista tietojärjestelmien tuottamista ongelmatilanteista. Haastateltavat kuvaavat näiden dokumenttien sisältöä seuraavasti:

" *En tiedä onko meillä itse asiassa kuinka kattava, se on hirveän vähän esillä yleensä, siis meillähän on esimerkiksi opiskelijoita varten ja tietysti henkilökuntaakin varten Intrassa Helpdesk. Siellä on tietoturva-asioita, mutta en tiedä kuinka syvälle menevää se on. Se saattaa olla tällaista yleistä, että pitää olla huolellinen, miten minä nyt sanoisin, omiin asioihin liittyvien asioiden kanssa, siis kaikki työasemat ja käyttäjäsalasanat, siis pitää noudattaa sellaista etiikkaa, että se on aina esillä esimerkiksi uusien opiskelijoiden näissä aloitustilaisuuksissa.-v04*"

" *Meillä on tuo Helpdesk järjestelmässä tiketti järjestelmä, jonne me sitten kirjoitamme niitä ratkaisuja. Sinne jää jollain tasolla ylös, mutta sitäkään ei ole mitenkään tarkasti ohjeistettu, mitä kaikkea sinne pitäisi kirjoittaa. Osa näistä ratkaisuista on tosi hyviä ja sitten osa on pelkkiä ok tyylisiä ratkasuja.-v07*"

" *No, voihan siellä jonkun ohjeen kirjoitta joku toinen, joten tiettyä mallia näihin ohjeistuksiin ei ole sen asian kuvauksissa, joten ohjeissa saattaa näkyä jokaisen ihmisen persoonallinen tyyli, miten se on laitettu sinne www-sivulle ja kuka sen sinne päivittää.-v04*"

Muistio aiheesta: Asiantuntijoiden tekemät ohjeistukset ovat Wiki-muotoisia ohjeistuksia, joiden sisältö ei ole säännönmukaista. Näiden ohjeiden tulisi olla pikemminkin tietojärjestelmistä vastaaville työntekijöille kun peruskäyttäjille.

Ohjeistus on julkaistu Web-sivuilla tiettyjen otsikoiden alla, jolloin käyttäjien tulisi löytää ratkaisu tiettyyn ongelmaan yleisellä hakusanalla. Haastateltavat kuvaavat Web-sivun oh-

jeistuksen avainsanakäytänteitä seuraavasti:

> " *Kyllä löytyy, eli pystyy hakemaan hakusanalla. Mutta tällöin sieltä pitää osata hakea. Koska, jos hakee jonkun otsikon mukaisesti niin, pitää ymmärtää, että käyttäjät tekevät nämä tiketit, niin tällöin ne voivat olla otsikoiltaan ihan mitä vain. Kukaan ei kirjoita mitään tarkempia metatietoja näihin tapauksiin. Se on kyllä ihan toimiva, sieltä on löytynyt monesti ratkaisuja, siten että asiat nopeutuvat.-v07*"

Organisaation tulisi pitää ohjeistukset ajantasaisena aina kuin käytettäviin järjestelmiin tai ohjelmistoihin tulee muutoksia. Haastateltavat kuvaavan käytänteitä seuraavasti:

> " *En muista milloin näitä julkisia ohjeistuksia on päivitetty, mutta tämä ohjeistus on myös sellaista, joka pitäisi päivittää vuosittain.–v06*"

> " *Tällaista toiminnallisuutta ei ole meidän tuotteessa, joten Intran sekä julkisen puolen WWW-sivustot kirjoitetaan erikseen käsin.-v06*"

> " *Sanotaan, että se mikä on julkinen ja mitä on Intrassa, niin näissä ohjeistuksissa on pieniä ristiriitoja. Ne mitkä ovat Intrassa, niin niissä on tiukempia ohjeistuksia, kun niissä jotka ovat tuolla julkisella puolella kaikkien nähtävänä. Julkisissa ohjeistuksissa sallitaan vähän enemmän kuin Intrassa olevissa ohjeissa.-v06*"

Tietojärjestelmiä käyttävät henkilöt testaavat ohjeistuksen ja käytännön paikkansapitävyyttä ja ehdottavat ohjeistukseen korjauksia ja muiden puutteiden korjaamista. Haastateltava kuvaavat tilannetta seuraavasti:

> " *Kyllä nämä jäävät muistiin ja yleensä joku muistaa, että hei tämä on tuttu juttu ja käykääpä katsomassa tuolta tiketti trakkeristä. Sieltä löytyy miten aikaisemmin vastaavassa tilanteessa on toimittu. Tarpeeksi monta kertaa joku asia tulee ilmi, niin sitten joku kirjoittaa sen auki, eli miten tilanteessa toimitaan.-v06*"

> " *Puutteet kirjataan dokumentaatioon, asian tärkeydestä riippuen, viimeistään kerran vuodessa. Dokumentaatio käydään läpi palaverimuistioiden pohjalta ja*

ryhmän sisällä käydään läpi tulkintaongelmallisia tapauksia, jotta asiakirjat olisivat mahdollisimman tarkkoja.-v08"

Muistio aiheesta: Yleisohjeistuksen tietosisältö ja dokumenttien rakenne ei vastaa tietoturvamallien määritelmää.

Ohjelmistotaso

Ohjelmistotason rakenne ja sen tietoturvan hoitaminen tietoturvamallien avulla jäi odotetusti haastatteluissa vähemmälle huomiolle koko organisaation tietoturvan hoidon kannalta. Tarkoituksenani oli tarkastella miten tietoturvamallit näkyvät tutkittavassa organisaatiossa. Tietoturvamallin tulisi esitellä laadukas luotettava ratkaisu, joka auttaa työntekijöitä ratkaisemaan tietyn tietoturvaongelman asiantuntijoiden kehittämissä suurissa ja monimutkaisissa järjestelmissä. Tässä kappaleessa käsittelen sitä, miten tietoturvan piirteet näkyvät ohjelmistotasolla. Seuraavassa taulukossa (ks. Taulukko 11) esittelen ne osat luokitellusta aineistosta, jotka koskevat organisaation ohjelmistotasoa haastateltavien antamissa merkityksissä.

Luokka	Alaluokka
Sovelluskehityksen hallinta	OH: Käyttöönoton tarkastukset
	OH:MST testaus
	OH:MST tietoturva
	OH:MST Ohjelmistot
	OH:OST ohjelmistot
	OH:OST riskit
Testausprosessi	OH:Testiympäristö
	OH:Oman sovellustuotannon testaus
Päivitykset	OH:Päivityksien testaus
	OH:Päivitys
Käytönvalvonta	OH:Lokitiedot

Taulukko 11: Tietoturvamallien näkyvyys ohjelmistotasolla

Haastateltavat kertovat organisaation sovelluskehityksen hallinnasta, jolloin näiden sovellusten käyttöönotossa on huomioitava niiden sopiminen olemassa olevan infrastruktuurin tietoturvaratkaisuihin ja tasoon. Tällöin infrastruktuuri voi asettaa vaatimuksia uudelle tai päivitettävälle sovellukselle tai voi olla että uusi sovellus asettaa tiukempia tietoturva vaatimuksia olemassa olevalle infrastruktuurille. Haastateltavat kuvaavat tätä suhdetta seuraavasti:

> " *Näistä ohjelmista pitäisi olla rekisteriselosteet ja tietosuojaselosteet kirjoitettuna, jotka näitä lokitiedostoja ja varsinkin henkilötietoja käyttää tai käsittelee. Sen kyllä pidämme vaatimuksena, että näistä on kaavanmukaiset tiedot ja nämäkin tiedot säilytettäisi tuolla dokumentinhallintajärjestelmissä. Tämä puoli pitäisi olla hallinnassa, jos sen nyt kaikki muistaa tehdä ja huolehtia kuntoon.-v01*"

Muistio aiheesta: Organisaatiolla tulee olla suunnitelmat, joissa otetaan huomioon vaatimukset käyttöönotettavalle sovellukselle. Näihin määriteltyihin kriteereihin voidaan vaativat tietyt etukäteisdokumentaatiot. Ohjelmistojen tietoturvamallit ottavat kantaa näihin suunnitelmiin.

> " *Hyvällä tuurilla. Järjestelmistä ei ole etukäteistarkistusta tai saatikka sitten tuota niin kuin jossain ohjelmistoprojekteissa taikka ohjelmistohankinnoissa ei ole tämmöistä aluetta mukana.-v02*"

Muisto aiheesta: Sovelluksen tietoturvan huomiotta jättäminen aiheuttaa organisaatioille hallinnollisia ja teknisiä tietoturvahaasteita. Vaikka ohjelmistoprojektit olisivat koulutusorganisaation sisäisiä, niin tämä ei takaa että sovelluskehitystä opettavat koulutusorganisaatiot opettaisivat näissä tietoturvan huomioonottamista.

> " *Kyllä, ohjelma tarkistetaan ennen käyttöä ja sitten sen jälkeen se tarkistetaan tuotantojärjestelmään liittämisen jälkeen, että kaikki toimii niin kuin pitääkin.-v06*"

> " *Itse en ole nähnyt ainakaan mitään ohjeistusta tai mitään tarkastuslistaa olleen*

kenelläkään käytössä. Nehän voi taas olla käytänteitä mitkä on heillä itsellään. He ovat tehneet työtään vuosia ja heille omasta päästään, joten ei ainakaan yleistesti ole mitään tarkastuslistaa.-v07"

Organisaatiot määrittävät suunnitteluvaiheessa minkälaisia ohjelmistoja he tulevat järjestelmissään käyttämään. Heidän tulee ottaa huomioon olemassa olevien lakien ja asetusten vaatimukset sekä organisaation periaatteet ja ohjeet, jotka vaikuttavat sovelluksien vaatimuksiin. Organisaatiot voivat tukeutua räätälöityihin tai valmiisiin sovelluksiin. Eräät haastateltavat kuvaavat sovelluskokonaisuuksia seuraavasti:

" *Näen, että käytämme ja olemme valinneet sen tyyppisiä teknologioita, etteivät ne ole kovin eksoottisia. Ne ovat aikalailla markkinoilla yleisesti käytössä olevia ja toisinpäin ne ovat taas semmoisia järjestelmiä ja teknologioita jotka ovat yleisesti tunnettuja, joten niihin ei niin helposti tietoturvauhkia kohdistu ulkopuolelta. Toisaalta helposti myös saadaan päivityksiä ja korjauksia taas valmistajilta. Me olemme lähteneet siitä, että pääsääntöisesti yrittäisimme mahdollisimman paljon tukeutua valmiisiin tuotteisiin tai että tuotteita räätälöidään ohjelmistotalo kumppanin kanssa ja tehdään heidän kanssaan kehitysyötä. Semmoinen, tavallaan eliminoidaan sillä tavalla sitä riskiä ja taas sitten toisaalta henkilöitymistä, jotta ei olisi niin sanottuja yhden miehen ohjelmistoja tai järjestelmiä.-v01*"

" *On pyritty siihen, että kaupallisesti tuettuihin systeemeihin, mutta onhan niintä tyyliin käyttöhallinnan puolella ja tommoisissa olemassa. Siinä mielessä, mutta jos ajatellaan tätä minun omaa tonttia elikkä infrapuolta, niin täällä menemme kaupallisilla ratkaisuilla, mutta nämä opintohallinnon järjestelmät ja ratkaisut ovat aika paljon räätälöityjä.-v03*"

Yhteistyökumppanien tai kolmansien osapuolten valmistamien ohjelmistojen tietoturvan tasosta vastaa viimekädessä ja ainoastaan järjestelmän omistaja eli organisaatiot. Heidän tulisi läpikäydä esitutkintavaiheessa ohjelmistolta vaadittavat tietoturvavaatimukset ja käyttöönottovaiheessa heidän tulisi varmistua testaamalla, että ohjelmiston tietoturva vastaa organisaation vaatimustasoa. Haastateltavat kuvaavat kuinka organisaatiot testaavat näiden ohjelmis-

tojen tietoturvan seuraavasti:

> " *Ei tällaisia asioita pysty sellaisella tasolla testaamaankaan, että voisi sanoa, mutta tässä on vain luotettava siihen, jos me ostamme jotain eksoottisempia ohjelmistoja. Se joka tällaisia ohjelmistoja tarvitsee, on vähän niin kuin itse otettava selvää, että kyseinen ohjelmisto on sellainen mitä ohjelmisto väittää se olevan.-v05*"

> " *Tämän tyyppisillä ohjelmistoilla, mutta lähtökohtaisesti olemme tietojärjestelmien ja ohjelmistojen toimittajien armoilla ja joudumme luottamaan siihen että he ovat ohjelmoineet ja toteuttaneet ne turvallisesti.-v01*"

Organisaation tulisi testata yhteistyökumppaneiden tai kolmansien osapuolten ohjelmistojen yhtyeensopiminen nykyiseen järjestelmän muiden ohjelmistojen kanssa siten, että häiriötilanteita ei syntyisi. Eräät haastateltavat kuvaavat näitä testejä seuraavasti:

> " *Ainoa testaus, mikä tehdään on se, että rikkooko asennettava uusi päivitys mitään toimintoja järjestelmästä.-v06*"

> " *No, ensin testataan tuolla IT-palveluissa joku ylläpitäjä sillä ohjelmistolla, joka kokeilee sen. Sitten testataan miten se toimii paketin muiden järjestelmien kanssa.-v07*"

> " *Windows puolelta voidaan sanoa, että kaikki kriittisimmät tietoturvapäivitykset pääsetetään levitykseen testaamatta, koska tällaiset päivitykset auttavat meidän järjestelmien tietoturvallisuutta. Testauksia tehdään sen mukaisesti mitä keritään. Uudet ohjelmistoversiot testataan lähes kaikki, jotain ihan pienempiä triviaaleja päivityksiä ei testata. Koska näistä tiedetään, etteivät ne voi mitään hajottaakaan.-v06*"

> " *Lähtökohtaisesti ne ovat ohjelmistojen valmistajien armoilla. Kun me käytämme ohjelmistoja, niin silloin toki tarkkailemme verkkoliikennettä, sillä tasolla millä se on teknisesti mahdollista tehdä, näitä keinoja ovat valvonta, seuranta ja puuttuminen.-v01*"

Oman ohjelmistotuotannon ohjelmistojen tietoturvan tasosta vastaa viimekädessä ja ainoastaan järjestelmän omistaja eli organisaatiot. Heidän tulisi läpikäydä esitutkintavaiheessa ohjelmistolta vaadittavat tietoturvavaatimukset ja käyttöönottovaiheessa heidän tulisi varmistua testaamalla, että ohjelmiston tietoturva vastaa organisaation vaatimustasoa, jos heillä on omaa sovellustuotantoa, kuten eräs haastateltava kertoo:

> " *Lähtökohtaisesti minun on hyvä todeta se, että emme itse täällä koodata järjestelmiä eikä tehdä, niin kuin yliopisto maailmassa saattaa olla ja yritysmaailmakuvioissa on sisäisiä ohjelmistokehitysyksiköitä tai osastoja järjestelmien tekemiseen.-v01*"

Haastateltavat kuvaavat oman ohjelmistotuotannon riskitekijöitä seuraavasti:

> " *Sehän tässä olisi, jos me ohjelmoisimme itse tai tekisimme itse omat ohjelmistot. Niin tällöin tämä olisi suurempi ongelma, jos meiltä tällainen henkilö lähtisi talosta yhtä äkkiä tai sanoisi huomen aamulla, että hän tästä lähtee. Tällöin voisi jäädä vaikka viiden vuoden ohjelmointityö meille tuohon pöydälle ja siitä kukaan ei välttämättä ottaisi enää selvää, mitä ohjelmistossa tapahtuu ja miten se on tehty.-v01*"

> " *Toki onhan niissäkin sitten alustana, jos ajatellaan vaikka Korppi, niin siellä kaupallisesti tuettu Redhatin Postgre-tietokanta on alustana ja tällaiset tonkerit ja muut on millä itse alusta asti itse tehtyinä järjestelminä mene, joten ne on vain itse tehtyjä vain sisällön puolesta. Mutta totta kai niissäkin pystyy ampumaan itseään jalkaan, jos kirjoittaa huonoa koodia.-v03*"

Organisaation tulisi testata oman ohjelmistontuotannon ohjelmistojen yhtyeensopiminen nykyisen järjestelmän muiden ohjelmistojen kanssa siten, että häiriötilanteita ei syntyisi. Eräät haastateltavat kuvaavat näitä testejä seuraavasti:

> " *Se on projektin tehtävä se.-v02*"

> " *Tämä asia jätetään kokonaan sinne kehittämispuolelle. Emme me enää sitä koodia katsella, vaan me tarjoamme täältä palvelinalusta ja sanomme, että laittakaa tuonne se pyörimään. Oletetaan, että heillä on siellä jonkinlainen koodi-*

katselmus prosessi. Siellä tietääkseni varmistutaan sillä tavalla, että tunnetaan se softa ja kovetetaan sitä sen mukaan kun on tarve. Ollaan yleisistä periaatteista selvillä, että miten turvallisia sovelluksia luodaan.-v03"

Organisaation ohjelmistosovellusten testausympäristön tulisi vastata organisaation tuotantojärjestelmää tai ainakin kriittisiltä osiltaan sen tulisi olla vastaava. Eräät haastateltavat kuvaavat heidän testiympäristöään ja sen tarkoitusta seuraavasti:

" *Tämä siksi, että varmistutaan, että nämä päivitykset aiheuttavat jotain ongelmia ja kaikista kriittisistä järjestelmistä on olemassa testiympäristöjärjestelmät, joissa me teemme aina ensin testaukset. Kokeillaan käyttäytyykö se päivityksen jälkeen siten kuin oli tarkoitus ja sen jälkeen vasta kun se on todettu turvalliseksi, niin laitetaan se vasta kriittiseen järjestelmään.-v03*"

" *En minä tiedä tästä testipenkistä, koska ei meillä tällaista testipenkkiä oikeastaan ole olemassa. Se on lähinnä kokemusten perusteella.-v04*"

Haastateltavat kuvaavat organisaatioiden käytänteitä järjestelmäpäivitysten käyttöönottoon.

" *Kyllä, tulevat päivitykset testataan ennen tuotantoon siirtämistä ja päivityksien mukana tulevat erodokumentit ja julkaisudokumentit luetaan lävitse ennen kuin päivitykset asennetaan. Tietenkään mihinkään lähdekoodiin asti me emme lähde lukemaan vaan totta kai pitää luottaa siihen, kun kaupallinen toimija päivityspaketin laittaa ulos se on siltä osin turvallinen, mutta kaikki nämä toiminnalliset dokumentaatiot jotka tulevat päivitysten mukana luetaan lävitse ennen kuin pätsejä ajetaan.-v03*"

" *Niin valmistajilta tulee enemmänkin tätä päivitys ja tietoturvavirtaa jatkuvasti. Kaikki tämä luetaan kyllä ja laitetaan toimeksiannoksi, jos on tarvetta. Väittäisin, että on aika aggressiivinen tämä meidän päivityspolitiikka. Eli kaikki ajetaan heti kun vain on mahdollista.-v03*"

" *Ei, ellei sitten ole ihan tietoisesti päätetty ja nähty etukäteen, että nyt on tulossa tuollainen, joten tämä on syytä testata tai tätä päivitystä ei pistetä kaikille*

jakoon. Joitakin päivityksiä ajetaan siten, että ne asennetaan pienemmälle porukalle ensin käyttöön, mutta pääsääntöisesti kaikki niin työasemien kuin palvelimillekin kaikki päivitykset menevät automaattisesti.-v05"

Haastateltavat kuvaavat heidän organisaatioiden tapaa tarkastaa asennettavista uusista ohjelmistoista, mitä lokitiedostoja he tulevat keräämään käytönvalvonnan yhteydessä.

" *Kyllä tällaiset tarkastukset tehdään, mutta ei sellaisia tietoja ole missään paperilla.-v07*"

Lokitiedot ovat oleellinen osa organisaatioiden tietoturvallisuuden valvontaa. Lokien analysoinnin tulisi perustua ennalta määriteltyjen järjestelmien ja toimintatapojen mukaisesti. Järjestelmien omistajan roolissa organisaation tulee varmistua siitä, ettei nämä kerää turhaa tietoa käyttäjän toimista, joiden kerääminen on kansallisten lakien vastaisia. Nämä tiedot voivat sisältää käyttäjien tietosuojan piiriin kuuluvia tietoja. Eräät haastateltavat kuvaavat lokeja ja järjestelmiä joista niitä kerätään seuraavasti:

" *Joo, aika pitkälle on omia tapoja tallentaa lokia ja esimerkiksi näiden palvelimien tai tietokantapalvelimista on ihan omanlaisensa tiedosto nimet ja rakenteet millä tavalla lokeja kierrätetään ja minkä nimisinä niitä luodaan. Kyllä niin kuin pyritään saattamaan ne sellaiseen muotoon, että niistä on helppo lukea ja niitä muokataan tarpeen mukaisesti. Vähän riippuu tietysti softasta, mutta niin kuin kyllä niitä lokeja käytetään elikkä jos niistä konfiguroidaan sellaisia, että ne ovat luettavissa.-v03*"

" *Lähinnä tulee mieleen sähköpostin välityslokit tai tällaiset autentikointi tiedot tai tämän kaltaiset. Ei niitä oikeastaan tule mieleen sellaisia lokeja, jotka keräisivät tällaisia tietoja. Mutta joka tapauksessa kun meillä on sellaiset vehkeet, jotka keräävät lokitietoja, niin ne tutkitaan konfiguroidessa. Eli, kun lokeja tarkastellaan niiden keräämät tiedot on tunnettuja tietoja, eivätkä täten lokit pidä sisällään haluamatonta tietoa.-v03*"

Tietoverkkotaso

Tietoverkkotason rakenne ja sen tietoturvan hoitaminen tietoturvamallien avulla jäi odotetusti haastatteluissa vähemmälle huomiolle koko organisaation tietoturvan hoidon kannalta. Tarkoituksenani oli tarkastella miten tietoturvamallit näkyvät tutkittavassa organisaatiossa. Tietoturvamallin tulisi esitellä laadukas luotettava ratkaisu, joka auttaa työntekijöitä ratkaisemaan tietty tietoturvaongelma asiantuntijoiden kehittämissä suurissa ja monimutkaisissa järjestelmissä. Tässä kappaleessa käsittelen sitä, miten tietoturvan piirteet näkyvät tietoverkon tilassa. Seuraavassa taulukossa (ks. Taulukko 12) esittelen ne osat luokitellusta aineistosta, jotka koskevat organisaation tietoverkkotasoa haastateltavien antamissa merkityksissä.

Yläluokka	**Alaluokka**
Verkon suunnittelu ja palautus	TV: Dokumentaatio TV: Varmuuskopio
Verkon rakenne	TV: Palomuuri TV: VPN-yhteys TV: Sisäverkko

Taulukko 12: Tietoturvamallien näkyvyys tietoverkkotasolla

Haastatteluissa tulee esiin verkon suunnittelussa ja palauttamisessa organisaatioiden tietoverkon dokumentoinnin tärkeys tietoverkon toiminnallisuuden ja sen tietoturvan kannalta. Dokumentaatio on tietoturvan ylläpidon ja edistämisen ehdoton edellytys, vaikka yleensä haastateltavat kuvasivat dokumentaatiota yleisluonteisesti. Organisaatiot ovat jo suunnitteluvaiheessa määritelleet tietoverkon dokumentaatiota Tietoturvakontrolleista haastatteluissa esiintyi yksi tärkeimmistä kontrolleista eli varmuuskopiointi. Eri kontrolleiden tarkoituksena on määritellä, kuinka organisaation tulisi toipua menetyksistä ja kärsimistään vahingoista, jotka aiheutuvat laiterikoista, varmuuskopiointia hyväksikäyttäen. Eräät haastateltavat kuvaavat dokumentaatiota sisältöä seuraavasti:

" *Meidän verkot on rakennettu pitkään perinteenä olleen tavan mukaisesti, ehkä*

se osaltaan varmistaa ettei tietoverkkomme ole kovinkaan haavoittuva. Olemme laajentaneet tietoverkkoamme pala palalta muuttamatta sen rakennetta.-v01 "

" *Sanotaan, että sieltä löytyy erittäin kattavat dokumentaatiot meidän tietoverkosta. Nämä meidän verkkoihmiset ovat sen verran pikkutarkkoja ihmisiä ja niiltä kyllä löytyvät aivan loistavat dokumentaatiot.-v06*"

" *Elikkä tällaiset, jos tietoverkoista puhutaan edelleen kuten porttikaaviot, topologiakaaviot ja kaikki tämmöiset aina kuin niihin muutoksia tulee, niin kyllä ne tietääkseni piirretään uudelleen ja nämä järjestelmät varmaankin dokumentoi itse itsensä.-v03*"

Muistio aiheesta: Dokumentaation laatuun ja sisältöön vaikuttaa myös se, käytetäänkö niissä tarkoitukseen sovittua tai valittua mallipohjaa. Mallipohjaa käytettäessä dokumenteissa ilmenee samansisältöisyys. Tietoverkkokomponenttien toimittajat ovat tuoneet markkinoille ohjelmistoja, jotka automatisoivat dokumenttien ylläpidon, vain harva tietohallinnossa todellisuudessa ylläpitää näitä dokumentteja. Tietoturvamallien käytöstä dokumentaatiossa ilmenisi tyypillinen täytäntöönpanomalli, jossa kerrotaan kuinka ongelmiin voidaan puuttua. Tämän jälkeen mallin tulisi kuvata mahdollisia erilaisia ratkaisuja ja lopuksi pitäisi kuvata kompromissit eri ratkaisuvaihtoehdoille. Tietoturvamallien dokumentaatiot pitäisivät olla muutakin kuin pelkkä luetelma dokumenteista.

Dokumentaation tarkoituksellisena luonteena tulisi kuitenkin olla tietoverkon teknisen ylläpidon ja tietohallinnon työtehtävien tukeminen. Kuten eräs haastateltava kuvailee:

" *Kaikki kerroskaapit ja kytkimet löytyvät piirroksista, eli mitä kaapelointeja on olemassa ja kuinka kaapelit on merkattu. Tällaiset perusasiat ovat kunnossa.-v01*"

Muistio aiheesta. Ammattitaitoinenkaan tietoverkon ylläpitäjä ei kykene hoitamaan tehokkaasti työtehtäviään, jos kerroskaappeja, kytkimiä tai kaapelointia ei ole merkattu kaapelitasolla tai dokumentaatioihin.

Dokumentaatiota tulisi päivittää jo suunnitteluvaiheesta lähtien, jolloin laitehankinnat ja verkon tila olisi ajan tasalla tapahtuvista muutoksista huolimatta. Haastateltavat toivat esille

myös dokumentoinnissa ilmeneviä puutteita. Kuten eräs haastateltava kuvailee:

> " *Langattomien verkoista löytyy kattavuuskartat, mitä tosin eivät ole tällä hetkellä ajan tasalla, koska olemme joutuneet heittelemään meidän tukiasemia aika paljon pois. Sanotaan, että puolivuotta sitten ollut tilanne löytyy vielä.-v06*"

Muistio aiheesta. Tietoturvamallin mukaan tietohallinnon suunnitteluohjeistuksessa tulisi olla määritelty vastuuhenkilöt eli asiantuntijat, jotka vastaisivat siitä, että dokumentit valmistuvat ajallaan.

Haastatteluista käy ilmi, että organisaatiot ovat ottaneet kantaa suunnitteludokumentaatioissaan toiminnan jatkuvuutta koskeviin suunnitelmiin. Tietoturvamallien mukaan yksi osa suunnittelua on palautumisen valvonta. Valvonnan tarkoituksena on varmistaa, kuinka organisaatiot aikovat toipua ei-toivottujen tapahtumien menetyksistä ja vahingoista. Varmuuskopioinnin järjestäminen on yksi osa tätä suunnitelmaa. Varmuuskopioiden tulisi sisältää käyttäjä- ja järjestelmätason tiedot sekä suojata kaikilta uhkilta. Varmuuskopiot tulisi sijoittaa ja säilyttää turvallisessa paikassa. Eräs haastateltu kuvaa käytänteitä seuraavasti:

> " *Yleisesti on topologiat verkosta. Siellä on, en tarkkaan tiedä mitä sieltä on. Kai kaikista konfiguraatioista on dokumentit tallessa, ne ovat ainakin tallessa kassakaapissa, jos jotain sattuu ja ne päästään helposti sitten palauttamaan. No itse asiassa en ole ihan varma ovatko ne ihan kassakaapissa, koska emme ole joutuneet palauttamaan mitään, mutta ainakin se sama konfiguraatio on muualla verkossa tallessa ja sitten se on palautettu kytkimeen tai reitittimiin. Ne on kyllä testattu, mutta sellaista yleistä palauttamisen testausta meillä ei ole, että sitä vuosittain testattaisi.-v07* "

Muistio aiheesta: Kuten haastateltavakin huomauttaa, organisaatiot huolehtivat varmuuskopioinnista. Pelkästään varmuuskopioiden ottaminen ja niiden säilyttäminen turvallisessa paikassa ei välttämättä riitä. Niiden sisältämien tietojen palauttamisen testausmielessä tulisi tietoturvamallin mukaan myös harjoitella säännöllisin väliajoin.

Organisaation tietoverkon rakenteen suunnittelussa tulee ottaa huomioon verkon rakenteellinen toiminnallisuus. Toiminnallisuuteen vaikuttaa siihen lisättävä laitekanta ja millaista tie-

toa tietoverkossa tullaan siirtämään. Näillä keinoilla tietoverkoista voidaan rakentaa tietoturvallinen ja sen laajentaminen sekä hallinta on myöhemmin helppoa. Eräät haastateltavat kuvaavat tietoverkon rakennetta seuraavasti:

> " *Pidämme tietoverkon toiminnassa tärkeimpinä asioina, että se toimii, tuottaa palveluja käyttäjille ja että palvelujen käyttäjät kokevat tietoverkon turvalliseksi ja käyttökelpoiseksi arkipäiväisessä käytössä.-v01*"

> " *Voidaan sanoa, että meillä on myös yksinkertaisuutta, joka tulee esiin siinä, että tietoverkkojen perusrakenne yritetty rakentaa siten, että se olisi selkeä ja helposti hallittava. Siten, että perusrakenne olisi sopivasti toiminnallisuudeltaan rajattu, siten että ulkoverkko ja sisäverkko ovat selkeästi eroteltu.-v01*"

Suunnitelmissa tulisi ottaa myös kantaa järjestelmän tietoturvallisen toiminnallisuuden varmistamiseen. Tämä pitää sisällään liikenteellisten heikkouksien karsimisen ja suunnitelmat sille, kuinka organisaation tärkeät varat kuten tiedot ja palvelut suojataan, jotta verkkoon tunkeutuminen ei olisi helppoa.

Haastatteluissa ilmenee yksi tehokas keino turvata organisaation tietoverkko.

> " *Tietoverkko on suurin piirtein avoin verkko, palomuurit sentään on ja joitain estoja on asetettu ulkomaailmaan päin, mutta kuitenkin ollaan vielä aika avoin verkon. Suurimmat estot ovat tuolla meidän palvelimien puolella. Siellä on tehty kaksi DMZ ja sitten on märitelty julkinen ja ei julkinen alue.-v06*"

Keinona on erotella sen toiminnalliset osat keskenään etuvarustusta (DMZ) hyväksi käyttäen. Toteutuksessa erotetaan Web-palvelimet ja organisaation suojattava liiketoiminnallinen toiminnallisuus ja tieto erilleen, rakentamalla tietoverkosta kerroksellinen. Kerrosten määrä riippuu organisaation koosta ja tarpeesta suojata tieto-omaisuutta. Eräs haastateltava kuvaa rajapintojen turvallisuusmekanismeja seuraavasti:

> " *En tiedä mitenkä se määritellään, mutta sitä toteutetaan, niin kuin palomuurilla jakamalla tietoverkko eri alueisiin ja sitten tuota siellä on verkkoalueiden välillä olemassa oletuksena kaikki linjat kiinni ja ne avataan vain jos on tarve.-v03* "

Palomuurit sijoitetaan yleensä jokaisen kerroksen rajapintaan, koska tarkoituksen on ohjata saapuva liikenne niiden kautta. Niiden toiminnallisena tarkoituksena on suodattaa saapuvasta liikenteestä sallittu ja kielletty liikenne ja täten pitää loitolla hyökkääjien tuottama toiminta.

Haastateltavat kuvaavat organisaation sisäverkon tietoturvan varmistamiseksi sisäverkon laitteille, kuten palvelimilla ja muilla kiinteillä verkkolaitteilla tulisi olla. Kiinteät IP-osoitteet helpottavat vikojen ja tietoturvapoikkeamien selvittämistä. Haastateltava kuvaa kuinka langattomien verkkojen käyttöä on rajoitettu tiettyjen menettelyjen avulla

> " *Ei ole mahdollista. Sisäverkkoon voi päästä vain niillä koneilla jotka ovat meidän tiedossa. Kaikki muut, kun meillähän on paljon opiskelijoita joilla on omat läppärit, niin nämä menevät vierailijaverkkoon kaikki.-v04*"

,jolloin vieraat koneet eivät pääse sisäverkon palvelimiin käsiksi. Organisaatioilla on erilaiset käytänteet sisäverkon suojauskäytäntöihin. Eräät haastateltavista kuvaillee tilaa

> " *Tällä hetkellä melkein kuka tahansa voi tulla kannettavan tietokoneen kanssa ja varastaa IP-osoitteen kytkemällä sen vapaaseen pistorasiaan. Tähän ollaan miettimässä keinoja, joilla kytkeytymiset voitaisiin estää.-v06* "

Muistio aiheesta: Organisaatiot pitävät tärkeänä estää tietoturvamalleissa ilmenevää tarvetta suojata Internetistä käsin tulevien haitallisten pyyntöjen suodatuksen. Toisaalta malleissa otetaan kantaa myös sisäverkon pyyntöjen suodatukseen. Organisaatiot luottavat liikaa verkon valvonnan tai tietoverkon laitemäärityksillä tehtävään suodatukseen suojautuakseen sisältäpäin tulevilta hyökkäyksiltä.

Haastateltava tuovat esiin organisaation tavan rakentaa heidän palvelinalustansa.

> " *Palvelinkonesalin, jossa on palvelimista reilut sata olisikohan satakolmekymmentä, tai sataviisikymmentä palvelinta. Palvelimet ovat nykyään virtualisoituja palvelimia ja niissä ylläpidetään tietojärjestelmiä, joita meillä on.-v01* "

On eri tapoja rakentaa palvelinkonesalit. Palvelimet voidaan rakentaa vain tiettyjä erityistoimintoja varten, jolloin palvelinkonesalissa on useita eri palvelimia, jotka suorittavat suunniteltuja tehtäviä. Toinen vaihtoehto on rakentaa järeä palvelinlaitteisto, jonne palvelut keski-

tetään. Kolmas vaihtoehto on virtuaalipalveluita, jolloin yhdessä järjestelmässä voidaan ajaa useita palvelimia samaan aikaan, jolloin saavutetaan edellä mainittujen ratkaisujen parhaat ominaisuudet.

Useat haastateltavat toivat esiin organisaation tukevan VPN-yhteyden käyttöä organisaation toimipisteiden yhdysverkkona tai etätyön teko mahdollistamisen kotitoimistosta käsin. Yleensä Internetin kautta kulkeva liikennettä pidettiin tietoturvariskinä. Näitä riskejä voidaan minimoida käyttämällä VPN-yhteyttä, jossa liikenne voidaan rakentaa salasanasuojatun tietoturvallinen tunneli etäkäyttöpalvelimen ja yksittäisen koneen välille. Eräät haastateltavat kuvaavat yhteyttä:

> " *Tähän on myös tullut hyvin toimivia tietoturvallisia ratkaisuja ja ne ovat tällaiseen turvalliseen etäkäyttöyhteyteen, eli kuinka meidän verkkopalveluihin päästään käsiksi etäyhteyttä hyväksikäyttäen. Eli näillä mahdollistetaan yhteydet, jotka eivät ole saatavilla muilla verkkoteknisillä ratkaisuilla.-v01*"

> " *Meillä on käytössä tällainen Sitrix-yhteys miten se tehdään ja miten siellä toimitaan. Se on aika yksinkertainen asia, mutta ainahan voi sattua jotain.-v04*"

5.2 Miten organisaatiot huolehtivat tietoturvasta?

Aineistoanalyysin tuloksena hahmottui kolme ydinkategoriaa, jotka jakavat organisaation kolmeen eri osaan. Keskeisimmiksi kategorioiksi hahmottui organisaatio-, ohjelmisto- ja tietoverkkotasot. Nämä muodostuneet kategoriat ovat vahvasti sidoksissa toisiinsa organisaation sisällä. Organisaatiotaso toimii kaiken organisoivana yksikkönä, joka kaikki toiminta heijastuu heikentävästi tai vahvistavasti kaikkien tasojen hoitoon. Organisaatiotaso pitää sisällään organisaation kaikki suunnittelu ja toteutusmääritelmät. Ohjelmisto- ja tietoverkkotaso ovat toteuttamisen tasoja, jossa sovelletaan organisaatiotasolla päätettyjen suunnitelmien ja toteutusmääritysten täytäntöönpanoa. Ohjelmistotasolla sovelletaan organisaatiotasolla tehtyjen suunnitelmien ja toteutusmääritysten mukaisesti järjestelmien ohjelmien toiminnallisuus ja niiden tietoturvallisen toiminnallisuuden varmistaminen. Tietoverkkotasolla sovelletaan organisaatiotasolla tehtyjen suunnitelmien ja toteutusmääritysten mukaisesti verkon rakenteellisen toiminnallisuuden varmistaminen.

Organisaatiotaso

Toinen tutkimuskysymykseni koski tietoturvaa ja lähdin etsimään vastausta kysymykseen miten organisaatiot huolehtivat tietoturvasta? Haastateltavien keskusteluista kävi odotetusti ilmi, että aineiston sisältö kasautuu organisaatiotason tietoturvaan. Seuraavissa taulukoissa (ks. Taulukko 13) esittelen ne osat luokitellusta aineistosta, jotka koskevat organisaatiotasoa haastateltavien antamissa merkityksissä.

Luokka	Alaluokka
Tietohallinto	OR:Tietohallinnon tehtävät OR:Tietohallinnon vahvuus
Tietoturvataso	OR:Toimintapolitiikka ja – strategia OR:Toimintapolitiikan ja -strategian muutokset OR:Tietoturvanhallinta OR:Tapahtumanhallintajärjestelmä
Arkistoinnin toteutus	OR:Asiakirjahallinnan tietoturva OR:Asiakirjahallinta
Turvallisuusosaamisen ylläpito	OR:Rekrytointi - Aiempi työkokemus OR:Nykyinen työkokemus OR:Toimenkuva OR:Kokematon työntekijä OR:Kouluttautuminen OR:Koulutusmahdollisuus OR:Koulutusmuodot OR:Sisäinen koulutus OR:Työn ohessa kouluttautuminen OR:Koulutuksesta saadun tiedon jakaminen OR:Hiljainen tieto
Tietoturvapoikkeamatilanteiden hallinta	OR:Tietoturvaongelman tapahtuma-analyysi OR:Tietoturvaongelmien havaitseminen

... jatkuu seuraavalla sivulla

Luokka	Alaluokka
	OR:Tietoturvaongelmista tiedottaminen OR:Tietoturvauhkista raportointi
Pääsynhallinta	OR:Käyttäjätunnustenhallinta OR:Käyttäjätunnustenhallinnan uudistaminen
Tietoliikenneturvallisuus	OR:Tietoverkonsuunnittelu
Tietoturvan toteutuminen	OR:Laitteiden valvonta OR:Uhkista raportointi

Taulukko 13: Organisaatiotason tietoturvasta huolehtiminen

Organisaation johdon on sitouduttava tukemaan laadittuja tietoturvallisuuden tavoitteita ja käytännön tietoturvan huolehtia toimenpiteitä. Haastateltava kuvasi heidän organisaation tietohallinnon henkilöstövahvuutta ja eri työtehtäviä seuraavasti:

> " *. . . no meitä on noin, onkohan meitä kaksikymmentäkaksi vai kaksikymmentäviisi henkeä.-v05* "

> " *Tietohallinto tarjoaa työasematukea ja järjestelmähallintaa. Tällaisia ovat opintohallinnon järjestelmät, oppimisympäristöt, taloushenkilöhallinto, Intra, julkaisujärjestelmä, julkiset WWW-sivustot ja monenlaista muuta sähköpostia ja kalenteria. Nauhoitamme luentotilaisuuksia ja sitten studio olosuhteissa tehdään ihan tämmöisiä oppimateriaaleja, niin kuin videolle.-v01* "

Tietohallinnon vastuulle kuuluu myös organisaatioiden tietojärjestelmistä ja laitteista huolehtiminen. Eräs haastateltu kuvasi niitä seuraavasti:

> " *Palvelinkonesali jossa on palvelimia reilut sata olisikohan satakolmekymmentä, tai sataviisikymmentä palvelinta. Palvelimet ovat nykyään virtualisoituja palvelimia ja niissä ylläpidetään tietojärjestelmiä, joita meillä on.-v01* "

" *Sähköpostiin liittyvät asiat ja tietysti ohjeistukset ja sääntöjä, jos henkilö on vaikka sairaana tai tapahtuu nopea kuoleman tapaus tai joku muu, niin kuinka me pääsemme tällaisen henkilön sähköpostiin käsiksi, niin meillä on laadittu ohjeistus kyllä. Eli missä tapauksessa työntekijän sähköpostista voidaan hakea ja avata. Meillä on eri tilanteita varten olemassa erilaisia dokumenttipohjia ja tuota tukimateriaalia kuinka tällaisissa tilanteissa tulisi toimia ja ketkä ihmiset siinä tilanteessa on mukana.–v01* "

Organisaation johto määrittelee organisaation tietoturvatason ja näkemykset tietoturvasuunnitteluun pääosin ajantasaistettavissa dokumenteissa, jotka ovat julkisia dokumentteja. Eräs haastatelluista kuvaa niiden näkyvyyttä seuraavasti:

"*Itse asiassa, ne johdon tekemät strategiat ovat minun mielestä viety Intaraan ja niiden pitäisi löytyä meidän Intrasta. Mutta tietoturvapäälliköllä on joitain dokumentteja, joita ei ole viety edes julkaisuun jostain syystä.-v06*"

Muistio aiheesta: Haastateltava kuvaa ilmeisesti tietoturvasuunnitelmien liitetiedostoja, jotka sisältävät teknisiä toimintaohjeita ongelmatilanteiden hallintaan.

Tietoturvasuunnitelmiin kohdistuvista muutoksista eräs haastateltava kertoo seuraavasti:

"*Nämä liittyvät IT-dynamoon, koska täällä on tämä kyberturvallisuus kokonaisuus, niin he haluavat sinne Katakri auditoinnin, että he voivat sitten käsitellä sen suojaluokan tietoja. Nämä tiedot asettavat että organisaatiolla on Katakri standardinmukaiset toimintatavat koko organisaatiolla tietojenkäsittelyltä.-v07*"

Organisaation tietoturvasuunnitelmat sisältävät myös tapahtumanhallintajärjestelmän. Tämän dokumentin tarkoituksena on että havaitut tapahtumat, jotka sisältävät poikkeamia, kirjataan tietohallinnon ylläpitämään tapahtumanhallintajärjestelmään. Eräs haastateltava kuvaa sitä seuraavasti:

"*Hallintajärjestelmä on ollut tällainen projekti, missä me olemme systemaattisesti tarkastelleet eri osa-alueita ja viemme eteenpäin tietoturvakysymyksiä kehitettäväksi ja sitä kautta tietoturva asiat tulevat henkilöstölle tutuksi.–v01*"

Eräs haastateltu löysi syyn, miksi organisaatiossa ei käytetä hallintajärjestelmää.

> "*No siinä on vähän järjestelmä esteitä ja sitten se toimintakulttuuri esteitä myös.–v03*"

Organisaatioiden asiakirjanhallinnalla on liitäntäpiste kaikkiin organisaation toimenpidealueisiin. Tuotettujen asiakirjojen sisällön turvaaminen pyritään takaamaan tietoihin kohdistuvilla laadullisilla tietoturvavaatimuksilla. Haastateltavat kuvaavat niitä seuraavasti:

> "*Meillä on ihan ihminen sitä varten tietohallinnossa, joka näistä asioista vastaa, kehittää ja on pitkään tätä maailmaa tehnyt, jopa ennen tähän taloon tuloakin ja on siten hyvää asiantuntemus ja on myös toteuttanut dokumentinhallintajärjestelmän nämä luokitukset.-v01*"

> "*Arkistosääntö määrittää sisäisten salassa pidettävien asiakirjojen hallintaa. Asiahallintajärjestelmässä asiakirjat ovat luokiteltu ja vain määrätyt henkilöt saavat käyttää tietoja.-v08*"

> "*Ulkoverkosta ei voida olla yhteydessä asiakirjahallinta dokumentaatioon, vaan yhteys voidaan muodostaa vain sisäverkosta. Kaikista toiminnoista kerätään loki-tiedot, joista voidaan tarkistaa toiminta. Järjestelmien sisällä tietojen ja asioiden käyttöoikeudet näkyvyyttä voidaan rajoittaa ryhmiä muuttamalla. Ryhmiä muuttamalla voidaan poistaa, josta raportoidaan tietohallintopäällikölle.-v08*"

Muistio aiheesta: Arkistoinnin sisältämät dokumentit ovat tietoturvaltaan organisaation tärkein omaisuuserä. Palvelimen näkyvyyttä on rajattu ja käyttöoikeuksia voidaan rajata helposti.

Organisaation johdon on huolehdittava tietojenkäsittelytehtävissä ja etenkin tietoturvallisuuden hallintajärjestelmän asiantuntijatehtävissä toimivien henkilöiden osaamisesta sekä koulutuksesta. Tietohallinnon on myös varmistuttava siitä, että työntekijöillä on vaadittava pätevyys, joka voi syntyä koulutuksen, työkokemuksen tai harjoittelun tuloksena. Tällä pätevyydellä on vaikutus myös tietoturvan tasoon, joten on tärkeää kyetä määrittämään mitä työtehtäviä voidaan tarjota kokemattomalle työntekijälle. Eräät haastatelluista kuvaavat koulutusmahdollisuuksia seuraavasti:

"*Organisaatio kouluttaa, siten että me käymme kaupallisilla kursseilla, konferensseissa ja seminaareissa. Se on oikeastaan kiinni työntekijästä itsestään, kummanko vaihtoehdon hän valitsee mieluiten. Haluaako hän kartuttaa kirjallisuuden kautta tai haluaako hän käyttää Wepinaareja vai haluaako mennä kursseille. Tässä on niin erilaisia tapoja oppia, mikä onkaan se oikeanlainen tapa saada se.-v03*"

"*Pitää itse olla aktiivinen ja hakea näihin koulutuksiin. Pitää olla sitä omaa halukkuutta. Sitten katsotaan siihen toimenkuvaan liittyviä järkeviä koulutuksia.-v07*"

"*No, ei ole, niin kuin sanoin se ei ole mitenkään systemaattista. Koulutusta ei jatkuvasti päivitetä, siinä on vähän tietysti sitä vastuuta viety omille siten, että oman ammattitaidon ylläpidon osalta.–v01*"

Muistio aiheesta: Organisaation johdon on huolehdittava asiantuntijatehtävissä toimivien henkilöiden osaamisesta ja koulutuksesta. Haastateltavien kuvauksista käy ilmi että kouluttautumismahdollisuudet perustuvat vain teoriaan.

Esimerkkinä haastatellut kuvaavat heidän omaa toteutunutta koulutustaan seuraavasti:

"*Ehkä tämä kouluttautuminen on jäänyt sen takia, koska aina ei tiedä mitä kaikkea meidän tulisi tietää.-v04*"

"*Missä minä olen käynyt, ne ovat suunnattu tähän tietoturvaan, ei ole laiteesittelyjä. Tietystihän ne ovat mieluusti mukana kaikki tuota F-Secure, Stonesoft ja vastaavat, mutta kuitenkin kunnossa.-v02*"

"*Minulla itselläni koulutuksena on vain ITIL koulutus maksullisena koulutuksena. Se oli meillä sellainen koulutus, joka tuli meidän tietohallintoon, kaikki tietohallinnosta suoritti tämän koulutuksen.-v07*"

Muistio aiheesta: ITIL-koulutuksen tarkoituksena on kuvata kuinka IT-palveluiden ja niiden tuottamisen prosesseja voidaan johtaa tehokkaasti. Organisaation tietoturvasuunnitelmat perustuivat ennen Katakri- standardiuudistusta ITIL:n sisältämään tietoturvan parhaiden käy-

tänteiden viitekehyksiin.

Koska kaikki halukkaat eivät pääse koulutuksiin, kuvaavat eräät haastatelluista koulutuksesta saadun tiedon jakamista seuraavasti:

> "*Tämä menee siten, että muutama kaveri käy kursseilla, jossa pystytetään järjestelmä. Järjestelmän pystytyksestä ja ylläpidosta järjestelmää sitten työpajoja, näille jotka hyödyntävät järjestelmää. Tämä on sellaista tiedon valuttamista, se on pääasiallista kouluttamista.–v03*"

> "*No ei varsinaisesti kouluta, mutta he valuttavat sitä tietoutta sitten muille. Voihan sitä periaatteessa koulutukseksi sanoa, kun kerrotaan asioita eteenpäin, eli miten kannattaa asioita tehdä. Mutta ei ehkä, en nyt sanoisi sitä koulutukseksi, nämä tilanteet ovat sellaista ohjeistusta.-v06*"

Muistio aiheesta: Koulutuksesta saadun tiedon jakaminen on hyvä keino "valuttaa uutta tietoa", koska tällöin käsitellään lisäksi "hiljaista tietoa" työntekijöiden keskuudessa. Tiedon valuttaminen auttaa myös organisaatiota arvioimaan kouluttajien asiantuntijuuden merkitystä ja siten auttaa organisaatioita valitsemaan parhaat kouluttajat. Tämä parantaa työntekijöiden ammattitaitoa, joka parantaa organisaation tietoturvaosaamista.

Organisaatioilla on käytänteet uusille tai kokemattomille työntekijöille. Voidaanko heitä sijoittaa työskentelemään yksin, vaikka heillä olisi tarvittavaa työkokemusta? Haastattelija esitti kysymyksen "*Onko mahdollista, että kokematon työntekijä joutuu vastaamaan kriittisistä toiminnoista?*". Haastateltavat kuvaavat käytänteitä seuraavasti:

> "*Ainakaan tässä meidän ympäristössä, kyllä me hyvin tarkkaan mietimme etenkin kun meillä on täällä työharjoittelijoitakin, niin mietitään mitä me voimme heillä teettää.-v04* "

> "*Tähän voisi lyhyesti sanoa että ei. Ajatellaan meidän palvelinhallintaa, niin ei me sinne kokemattomia ihmisiä päästetä ja sama liittyy kaikkeen kulkuun, koska laitetilat ovat vain kaikkineen lukkoineen tiettyjen henkilöiden käytössä.-v01* "

> "*Totta kai, jos meille tulee jotain uusia kavereita, niin heitä ajetaan sisään, sit-*

ten että heille annetaan ohjeistusta joitakin päiviä, mutta periaatteessa sellaista sisäistä koulutusta ei muuten ole olemassa.-v06 "

"*Ei. Työntekijä käy asiakirjahallinnan koulutuksen ja sen jälkeen hänet opastetaan työtehtäviin. Arkistovastuu ja lähituki ulottuvat yksilötasolle.-v08* "

Muistio aiheesta: Yhteenveto haastateltujen vastauksista: Organisaatioiden palkkaamilla uusilla työntekijöillä on oltava vankka työkokemus työtehtävistä. Tämän lisäksi he työskentelevät aluksi kokeneemman työntekijän parina jonkin aikaa.

Organisaatioiden sisällä suullisista ohjeista muodostuu ajan kuluessa omia käytänteitä nk. "hiljaista tietoa", joka määrää miten organisaatiossa toimitaan ja asioita hoidetaan. Haastateltavat kuvaavat tätä tietoa seuraavasti:

" *No ne ovat suullisia ohjeita koska ne tulevat/muodostuvat omiksi käytänteiksi, siten että joku asia jota pitää tehdä. Se selvitetään mutta siitä ei tehdä mitään erillistä ohjetta.-v04* "

"*Meillä on myös paljon käyttäjien tai järjestelmien ylläpitäjien päässä olevaa hiljaista tietoa. Tämä hiljainen tieto pitäisi saada tuonne dokumentteihin.-v07* "

Eräs haastateltu kuvaa organisaatioiden pääasiallisina keinoina torjua ja hallita ilmeneviä tietoturvan poikkeamatilanteita seuraavasti:

"*Pääasiallisia keinoja ovat, että tunnetaan omat järjestelmät. Pysytään uutisvirrassa ajan tasalla, jotta tiedetään mitä tapahtuu. Osataan tämän kautta sopeutetaan omia järjestelmiä, koska tällöin havaitaan ongelmakohdat, jotka koskevat meidän omia järjestelmiä ja ollaan aktiivisesti päivittämässä järjestelmiä heti kuin mahdollista. Nämä ovat ne pääasialliset keinot, eli ollaan valppaana. On tärkeää, että ylläpitäjä tuntee nämä Certi-fi listat ja totta kai käyttöjärjestelmien valmistajat, jos ajatellaan näitä kahta päähaaraa, eli Linux ja Windows järjestelmiä.-v03* "

Tietoturvaongelmien havaitseminen tapahtuu organisaatioiden johdon hyväksymän suunnitteludokumentin mukaisten toimien määräämällä tavalla. Eräät haastateltavat kuvasivat, kuin-

ka heidän organisaatioissaan tämä on ohjeistettu, seuraavasti:

> "*Se on vähän mistä se vyyhti lähtee purkautumaan tai kuka sen havainnoi, jos ajatellaan sitten vaikka miten me toivoisimme kriittisten hälytysten tulevan. Kriittiset lähdöt voivat tulla puhelinsoittona suoraan minulle tai ne voivat tulla asiantuntijalle, johdolle tai riippuen vähän kuka ja millä lailla ne havainnoidaan. Yksi asia tietysti olisi helpoin meille, että miten selkeimmin homma lähtisi jotenkin hallittavasti ja rekisteriin olisi meidän Helpdesk järjestelmä.-v01* "

> "*No, tietoturvapäällikölle ja meillä on tietoturva-asiantuntijalle [–]. Häntä voisi nimittää tietoturva-asiantuntijaksi ja hän pääsee tekemään asialle heti jotain. Tämän jälkeen koko Infratiimille, jolloin asia menee kaikkien tietoon. Mutta ensisijainen on tietoturva / tietohallintojohtaja.–v07* "

Tietoturvaongelman tapahtuma-analyysi tapahtuu heti, kun tiedetään havaitun ongelman laajuus. Eräät haastelluista kuvasivat niitä seuraavasti:

> "*Jos jotain on ilmennyt, niin ne totta kai tärkeintä on aina reagointi siihen ja löytää ne oikeat ihmiset, jotka lähtevät asiaa tarvittaessa selvittämään asiaa. Niin tämä asia hoidetaan sitten sen prosessin mukaisesti tai jos se ei maailman kiireellisin asia olisi, jos siten nähdään selkeästi ja varmasti joka sitten aistii että jotain on nyt pielessä, niin aika paljon pallo on sitten hänellä kuinka hän reagoi ja mihin päin ottaa yhteyttä.–v01* "

> "*Elikkä jos meillä havaitaan tällainen pienimuotoinen tietoturvapoikkeama, niin siihen on tällainen prosessikäsittely. tällöin tietoturvapoikkeamat kulkevat Nabuse-ryhmän kautta.-v02* "

> "*Joo, sitten tuota tässä niin kuin otetaan tällainen virkamieslähestymistapa, eli meillä on tässä tällainen tiketti, jota ruvetaan hoitamaan eli siihen etsitään se asiantuntija jos on sen laatuinen että meillä on epäilys että on murrettu joku.–v02* "

Muistio aiheesta: Onko organisaatio testannut toimintasuunnitelmiaan poikkeustilanteiden

varalle? Tulee sellainen tunne, että organisaatiot ovat luoneet dokumentaation kuinka tällaisessa tilanteessa toimitaan, mutta sitä ei ole koskaan testattu tai tarvinnut käyttää vielä käytännössä.

Tietoturvaongelmista tiedottaminen tapahtuu sen jälkeen, kun havaittu ongelma on saatu selvitettyä ja havaitaan tarve viestiä siitä organisaation sisäisesti. Eräs haastatelluista kuvaa tätä seuraavasti:

> "*Hierarkia on olemassa, eli heti jos tällainen tapaus tulee ilmi, niin tapaus laitetaan Apuse jonoon ja sen jälkeen ilmoitus trakkeriin ja kolmantena ilmoitetaan tietoturvapäällikölle tai ilmoitus APUSE porukan jäsenelle, jos tietoturvapäällikkö ei ole paikalla.–v06* "

Havaitusta tietoturvauhkasta lähdetään raportoimaan julkisesti, kun ongelma on todennettu johtuvan ulkopuolisesta lähteestä ja havaitaan sen olevan erittäin kriittinen. Eräs haastateltava kuvaa tätä toimintaa seuraavasti:

> " *Tämän lisäksi ilmoittaisimme siitä myös laajemmin CERT-FIlle tai vaikka nyt jyväskylän yliopistolle. Mutta tavallisemmin ilmoituksen saaja olisi ammattioppilaitos tai toisen asteen oppilaitos kuntayhtymässä, koska me olemme samassa verkkomaailmassa heidän kanssaan.-v01* "

Käyttöoikeudet edellyttävät, että käyttäjillä on organisaation myöntämä henkilökohtainen tunnus. Tunnus sisältää myös ryhmät, joihin hän voi työtehtäviensä mukaan kuulua. Käyttäjä voi myös kuulua useisiin eri oikeuksia omaaviin ryhmiin. Tämä tunnus voi myös sisältää muutakin tietoa käyttäjistä. Eräät haastateltavat kuvaavat tätä seuraavasti:

> " *Järjestelmällinen tunnusten käsitteleminen tarvitsee tiedon, milloin henkilö on tullut tiettyyn tehtävään ja muutenkin kun henkilö tulee taloon. Tähän liittyy myös paljon muita asioita eri tietojärjestelmissä. Sen takia, koska hänen pitäisi saada rahaa ja kaikkea muuta tällaista asioita, eli kuka on hänen esimies.-v04*"

> " *Käyttö-oikeuksilla ja asiakirjahallintajärjestelmien sisällä käyttäjätunnuksia ei anneta ryhmiin automaattisesti.-v08*"

Organisaatiot myös ajanmukaistavat käyttöoikeuksien hallintaa. Eräs haastatelluista kuvasivat tätä seuraavasti:

> "*Meillä on projekteja tietoturvan parantamiseen, meillä on tällainen projekti, jossa ruvetaan vääntämään tarkemmin meidän käyttäjätunnuksia ja valvontaa tehostetaan ja täten meidän tunnustautumista parannetaan. Tarkoituksena olisi saada henkilöhistoriat hallinnassa siten, että meillä ihan siitä päivästä käyttäjä tulee meille aina siihen päivään kun hän lähtee. Meidän olisi hyvä tietää keitä on talon järjestelmissä ja missä hommissa ja mahdollisesti kuinka kauan hän on palveluksessa.-v04*"

Tietoliikenneturvallisuuden tarkoituksena ovat tiedonsiirron suojaaminen ja salaaminen sekä sellaiset turvallisuustoimet, jotka takaavat tietoliikenteen turvallisuuden eri verkkojärjestelmissä. Tietoverkosta tulee olla rakenteellinen fyysinen ja looginen arkkitehtuurikuva. Fyysisestä kuvasta ilmenee rakenne ja loogisesta kuvasta eri verkkoalueet ja virtuaaliverkot. Eräät haastatelluista kuvasivat niitä seuraavasti:

> "*Remonteissa olemme tehneet yhteistyökumppaneiden kanssa sähkösuunnittelua ja laajemmin työasemien sijoittelua, eli mihinkä verkkoliitäntöjä asennetaan tai mietitään langattoman verkon toimivuutta, eli miten laajalti langattoman verkon tulisi kampusalueella toimia ja tällä tasolla varmasti suunnitellaan niiden määriä, paikkoja, sijainteja ja kaapelointia. Fyysinen tekeminen ja verkon aktiivilaitteiden konfikurointi on sitten osaltaan, eli sanotaan että se verkon lähtö- ja ristikytkennät tulee huomioiduksi kerroskytkimille.-v01*"

> "*Tietoverkot näkyvät yhtenä osana sähkösuunnitteludokumenteissa, eli sähkösuunnittelijoiden piirroksissa näkyvät sähkövedot ja ATK-pistokkeiden vedot ja tarpeiden ja määrien dokumentointi.-v01*"

Fyysiseen turvallisuuteen kuuluu tilojen ja laitteiden valvonnan toteuttaminen. Eräs haastateltava kuvasi valvonnan toteutumista seuraavasti:

> "*Seuraamme ettei tietokoneita varasteta ja sitä, että tietokoneita kohdellaan hyvin ja sitä, että tietokoneet ovat käyttökuntoisia. Sitten taas kun perinteinen vi-*

rastoaika päättyy ja talossa on vielä tämän jälkeenkin paljon ihmisiä paikalla, niin ilta-aika on aikalailla vahtimestarien vastuulla. Koska kun he ilta-aikaan kiertelevät ja katselevat esimerkiksi vähän mitä ihmisiä täällä liikkuu ja mitä meidän tietokoneilla tehdään.–v01"

"*Vahtimestarit omalta osaltaan ja henkilöstö omalta osaltaan ja vastaavalla tavalla IT-tuki seuraa työasemien käyttöä ja miten opiskelijat istuvat noiden tietokoneiden ääressä ja mitä noilla koneilla tehdään.–v01*"

Käyttäjille on varattu mahdollisuus raportoida havaitsemiaan puutteita. Eräs haastateltu kuvasi sitä seuraavasti:

"*Meillä on vikailmoitus raportointi tai voi kirjata raportin toimintahäiriöistä tai mistä nyt ihmiset kirjoittavat tietotekniikkaan liittyvistä asioista. Tähän on olemassa netissä semmoinen kenttä, johon he saavat kuvailla sen ongelman ja sitten se tulee meidän järjestelmään tikettinä ja me sitten puramme näitä tikettejä järjestelmästä.–v04*"

Ohjelmistotaso

Ohjelmistotason tietoturvan huolehtiminen jäi odotetusti haastatteluissa vähemmälle huomiolle koko organisaation tietoturvan hoidon kannalta. Tarkoituksenani oli tarkastella miten organisaatiot huolehtivat tietoturvasta. Tässä kappaleessa käsittelen sitä, miten organisaatiot huolehtivat ohjelmistotason tietoturvasta. Seuraavassa taulukossa (ks. Taulukko 14) esittelen sen osan luokitellusta aineistosta, joka koskee organisaation ohjelmistotasoa haastateltavien antamissa merkityksissä.

Luokka	Alaluokka
Käytönvalvonta	OH:Lokitiedot
Sovelluskehityksen hallinta	OH:OST ohjelmistot OH:OST riskit OH:MTS ohjelmistotuki OH:MTS tietoturva OH:MTS ohjelmistot OH:Käyttöönoton tarkastukset
Testausprosessi	OH:Testausympäristö OH:OST testaus OH:MTS testaus
Päivitykset	OH:Päivitys OH:Päivityksien testaus

Taulukko 14: Ohjelmistotason tietoturvasta huolehtiminen

Organisaatioiden tulee määrittää jokaiselle ohjelmistokehityksen osa-alueelle vastuuhenkilö. Sovellustuotannosta voidaan osa siirtää toteutettavaksi kolmannelle osapuolelle, mutta tietoturvallista sovelluskehitystä ei voi pelkästään jättää kolmannen osapuolen vastuulle. Organisaation tulee itse varmistua ohjelmiston tietoturvasta. Eräs haastateltu kuvasi oman sovellutustuotannon ohjelmistoja seuraavasti:

> "*Me olemme lähteneet siitä, että pääsääntöisesti yrittäisimme mahdollisimman paljon tukeutua valmiisiin tuotteisiin tai että tuotteita räätälöidään ohjelmistotalo kumppanin kanssa ja tehdään heidän kanssaan kehitysyötä. [–] eliminoidaan sillä tavalla sitä riskiä ja taas sitten toisaalta henkilöitymistä, jotta ei olisi niin sanottuja yhden miehen ohjelmistoja tai järjestelmiä.-v01*",

> "*Näen, että käytämme ja olemme valinneet sen tyyppisiä teknologioita, etteivät ne ole kovin eksoottisia. Ne ovat aikalailla markkinoilla yleisesti käytössä*

olevia ja toisinpäin ne ovat taas semmoisia järjestelmiä ja teknologioita jotka ovat yleisesti tunnettuja, joten niihin ei niin helposti tietoturvauhkia kohdistu ulkopuolelta. Toisaalta helposti myös saadaan päivityksiä ja korjauksia taas valmistajilta.-v01"

Eräs haastateltu kuvasi muualla tuotetuiden sovellusten ohjelmistoja seuraavasti:

"*Mitä näitä tietojärjestelmiä on taloon tullut, niin niiden toimittajia ovat ulkopuoliset kumppanit. Osatamma valmiin tuotteen tai sitten ostetaan tekijät, jotka sitten toteuttavat sen.-v05*"

Organisaatiot voivat tarkkailla tietojärjestelmien tilaa ja suorittaa ohjelmistoille tarkastuksia ja seurantaa siihen tarkoitukseen suunniteluilla ohjelmistoilla tai muita keinoja hyväksikäyttäen. Eräät haastateltavat kuvasivat käyttöönoton tarkastuksia seuraavasti:

"*Meillä on skanneri-ohjelmistoja joilla voimme tietysti löytää sellaiset tyypilliset puutteet ja se että ohjelmistot pidetään ajan tasalla.-v01*"

"*Ohjelmistojen tietoturvaa seurataan useista kanavista, mitä tietoturva-aukkoja löytyy vastaavista järjestelmäympäristöistä mitä meillä on. Näihin aukkoihin reagoidaan nopeasti tai hitaasti riippuen tietoturva-aukon kriittisyydestä.-v06*"

"*Seurataan maailmalla tapahtuvia reaktioita, kun toiset käyttäjät asentavat näitä päivityksiä, jos niissä on jotain ongelmia, niin silloin maailmalle tulee hirveästi tietoa mitä niissä päivityksissä on ja miten ne ovat menneet.-v04*"

Riskeinä sovellustuotannossa ovat sen toiminnalliset, hallinnolliset ja tekniset haasteet tietoturvan toteutumiselle. Eräs haastateltu kuvasi niitä seuraavasti:

"*Toki onhan niissäkin sitten alustana, jos ajatellaan vaikka Korppi, niin siellä kaupallisesti tuettu RedHatin Postgre-tietokanta on alustana ja tällaiset tonkerit ja muut on millä itse alusta asti itse tehtyinä järjestelminä mene, joten ne ovat vain itse tehtyjä vain sisällön puolesta. Mutta totta kai niissäkin pystyy ampumaan itseään jalkaan, jos kirjoittaa huonoa koodia. Ymmärtääkseni ohjelmoijat ovat koulutettuja osaajia, että eivät he sutta ja sekundaa sillä suunnalla*

tee.–v03"

Hyväksymistestaukset tulisi aina suorittaa tuotantojärjestelmää vastaavassa testausympäristössä. Testauksen tulisi olla suunnitelmallista ja perustua etukäteen laadittuun testausaineistoon. Eräät haastatellut kuvasivat kuinka heidän testausympäristönsä on toteutettu seuraavasti:

> "*Meidän testiympäristö ei ihan välttämättä ole aivan samanlainen, kun meidän tuotantoympäristö.-v06*"

> "*En minä tiedä tästä testipenkistä, koska ei meillä tällaista testipenkkiä oikeastaan ole olemassa. Se on lähinnä kokemusten perusteella.-v04*"

Oma ohjelmatestaus jätetään yleensä projektien huoleksi tai siihen ei ole varattu tarvittavia resursseja. Syy voi myös olla liian korkeat kustannukset. Eräät haastatellut kuvaavat ohjelmistotestausta seuraavasti:

> "*Tämä asia jätetään kokonaan sinne kehittämispuolelle. Emme me enää sitä koodia katsella, vaan me tarjoamme täältä palvelinalusta ja sanomme, että laittakaa tuonne se pyörimään. Oletetaan, että heillä on siellä jonkinlainen koodikatselmus prosessi.-v03*"

> "*Veikkaan kuitenkin, että meidän kehitystiimimme testaavat tulevat ohjelmistot ennen niiden julkaisua, varsinkin meidän Korpin osalta.-v06*"

Eräs haastateltu kuvasi muualla tuotettujen sovellutusten testausta seuraavasti:

> "*Ei tällaisia asioita pysty sellaisella tasolla testaamaankaan, että voisi sanoa, mutta tässä on vain luotettava siihen, jos me ostamme jotain eksoottisempia ohjelmistoja. Se joka tällaisia ohjelmistoja tarvitsee, on vähän niin kuin itse otettava selvää, että kyseinen ohjelmisto on sellainen mitä ohjelmisto väittää se olevan.-v01*"

Käyttöjärjestelmien ja ohjelmistojen päivityksistä julkaistaan tietoturva- ja ohjelmistopäivityksiä sekä korjauspäivityksiä. Nämä voivat aiheuttaa muutoksia ohjelmistojen ja järjestelmien toimintaan. Päivitykset tulisi testata ennen käyttöönottoa. Eräät haastateltavat kuvaavat

päivitysten testauksesta seuraavasti:

> "*Pääsääntöisesti, vaikka Microsoftin päivitykset, niin nehän menevät käytännössä automaattisesti kaikki, jos näissä ilmenee ongelmia, niin rullataan takaisinpäin.-v05*"

> "*Kyllä, tulevat päivitykset testataan ennen tuotantoon siirtämistä ja päivityksien mukana tulevat erodokumentit ja julkaisudokumentit luetaan lävitse ennen kuin päivitykset asennetaan.-v03*"

Ohjelmistopäivityksen jälkeen voi ilmetä ongelmia joidenkin ohjelmien yhteensopivuuden kanssa. Eräs haastatelluista kuvasi tällaista ongelmaa seuraavasti:

> "*Ohjelmistopäivitysten kanssa joudutaan niin kuin kikkailemaan. Huomataan yhtä äkkiä että tämä ei tuekaan uutta Java-versiota tai jotain muuta kilkettä. Tällaisia yllätyksiä välillä tulee, vaikka meillä muuten pystyttäisiin käyttämään näitä ohjelmia, niin joku saattaa lakata toimimasta. Yleensä kyllä päivitykset katsotaan aika tarkkaan kannattaako ne asentaa ja päätetään milloin ne kannattavat asentaa.-v04* "

Tietoverkkotaso

Tietoverkkotason tietoturvan huolehtiminen jäi odotetusti haastatteluissa vähemmälle huomiolle koko organisaation tietoturvan hoidon kannalta. Tarkoituksenani oli tarkastella miten organisaatiot huolehtivat tietoturvasta. Tässä kappaleessa käsittelen sitä, miten organisaatiot huolehtivat tietoverkkotason tietoturvasta. Seuraavassa taulukossa (ks. Taulukko 15) esittelen sen osan luokitellusta aineistosta, joka koskee organisaation tietoverkkoa haastateltavien antamissa merkityksissä.

Luokka	Alaluokka
Verkon suunnittelu ja palautus	TV:Dokumentaatio TV:Varmuuskopio
Verkonrakenne	TV:Palomuuri TV:Palvelinlaitteisto TV:Rakenteellinen tietoturva TV:VPN-yhteys TV:Sisäverkko TV:Rakenteelliset puutteet
Turvallisuuden hallintajärjestelmät	TV:Hallinnanvalvontajärjestelmä

Taulukko 15: Tietoverkkotason tietoturvasta huolehtiminen

Verkon suunnittelussa on erittäin tärkeää tietää, mitä laitteita tietoverkkoon on kytketty. Tämän takia verkon dokumentointi jo suunnitteluvaiheesta lähtien on välttämätöntä. Verkosta tulisi olla fyysinen arkkitehtuurikuva, kaapeloinnit, kaavio aktiivilaitteista ja laitelista. Eräät haastatelluista kuvasivat tietoverkon suunnitteludokumentaatiota seuraavasti:

> "*Siis, siellä on ihan fyysistä dokumentaatiota itse verkon rakenteesta. Palomuureista ja niiden säännöistä löytyy kattavat dokumentit. Reitittimien paikalliset konfiguratiot. Suuremmat topologiakuvat ja talokohtaiset topologiakuvat ja sieltä löytyy kaikenlaisia dokumentaatioita laidasta laitaan.–06*"

> "*Kaikki kerroskaapit ja kytkimet löytyvät piirroksista, eli mitä kaapelointeja on olemassa ja kuinka kaapelit on merkattu. Tällaiset perusasiat ovat kunnossa.-v01*"

Esimerkkinä tietoverkon suunnitteludokumentaation nopeasta vanhenemisesta esitti eräs haastateltu kuvasi tätä seuraavaa:

"*Langattomista verkoista löytyy kattavuuskartat, mitä tosin eivät ole tällä hetkellä ajan tasalla, koska olemme joutuneet heittelemään meidän tukiasemia aika paljon pois. Sanotaan, että puolivuotta sitten ollut tilanne löytyy vielä.-v05*"

Poikkeaman sattuessa tietohallinnon tulisi varautua siihen, että verkkolaitteiden sisältämät tiedot tulisi voida nopeasti palauttaa poikkeamasta toipumisen aikana tuorein varmuuskopioin. Eräs haastateltu kuvasi tietoverkon varmuuskopioiden tilaa seuraavasti:

"*No itse asiassa en ole ihan varma ovatko ne ihan kassakaapissa, koska emme ole joutuneet palauttamaan mitään, mutta ainakin se sama konfiguraatio on muualla verkossa tallessa ja sitten ne on palautettu kytkimiin ja reitittimiin. Ne on kyllä testattu, mutta sellaista yleistä palauttamisen testausta meillä ei ole, että sitä vuosittain testattaisi.-v07*"

Organisaatioiden tietoliikenneverkon perustehtävänä on ylläpitää verkon käytettävyyttä ja luottamuksellisuutta. Ennen kuin verkon rakennetta voidaan ylläpitää suunniteltava verkon rakenne. Suunnittelussa tulee huomioida kaapelointijärjestelmä ja käytettävät aktiivilaitteet. Eräs haastateltu kuvaa koulutusorganisaatioiden verkkorakennetta seuraavasti:

"*Meidän verkot on rakennettu pitkään perinteenä olleen tavan mukaisesti, ehkä se osaltaan varmistaa ettei tietoverkkomme ole kovinkaan haavoittuva. Olemme laajentaneet tietoverkkoamme pala palalta muuttamatta sen rakennetta. Pidämme tietoverkon toiminnassa tärkeimpinä asioina, että se toimii, tuottaa palveluja käyttäjille ja että palvelujen käyttäjät kokevat tietoverkon turvalliseksi ja käyttökelpoiseksi arkipäiväisessä käytössä.-v01*"

Organisaation johto määrittelee tietoturvastrategiassa palomuuripolitiikkadokumentin, jossa määritellään palomuurien vastuut. Eräs haastateltava kuvaa palomuuripolitiikkaa seuraavasti:

"*Sitten on tämä palomuuri juttu tietysti olemassa, ihan päätöstasoinen asia tämmöinen palomuuripolitiikka on luotu, siitä on kyllä jo aikaa varmaan 3-4 vuotta.–v02*"

" *Se oli tuota, sen aikaisen Atk-keskuksen johtokunnan vahvistama toimintatapa.-*

v02"

Verkon palveluiden ja itse verkon käyttämistä voidaan rajoittaa palomuurein. Palomuurin tarkoituksen on eristää organisaation tietoverkko Internetistä sekä erotella suunnitellusti sisäverkon osia toisistaan siten, että ei-haluttujen pakettien pääsy näiden verkkojen välillä estetään. Palomuurin avulla voidaan myös kontrolloida mitä liikennettä sallitaan eri verkon osien ja laitteiden välillä. Erääät haastateltavat kuvaavat palomuurien käyttöä seuraavasti:

> "*Tietoverkko on suurin piirtein avoin verkko, palomuurit sentään on ja joitain estoja on asetettu ulkomaailmaan päin, mutta kuitenkin ollaan vielä aika avoin verkon. Suurimmat estot ovat tuolla meidän palvelimien puolella. Siellä on tehty kaksi DMZ ja sitten on märitelty julkinen ja ei julkinen alue.-v06*"

> "*En tiedä mitenkä se määritellään, mutta sitä toteutetaan niin kuin palomuurilla jakamalla tietoverkko eri alueisiin ja sitten tuota siellä on verkkoalueiden välillä olemassa oletuksena kaikki linjat kiinni ja ne avataan vain jos on tarve.-v03*"

Sisäverkko eli Intranet on tietoverkko, joka toimii samalla periaatteella kun Internet. Erotuksena niiden välillä on, että Intranetiin voi kirjautua sisään vain luvan saaneet käyttäjät. Tietoturvan kannalta sisäverkon riskinä pidetään haittaohjelmia, laiterikkoja, ohjelmistovirheitä sekä ulkopuolisen käyttäjän kytkeytymistä verkkoliitännän kautta sisäverkkoon. Luvaton sisäverkon käyttö voidaan estää 802.1X-standardilla eli porttiperustaisella autentikoinnilla. Eräs haastateltava kuvaa sisäverkon tietoturvaa seuraavasti:

> "*Sisäverkkoon voi päästä vain niillä koneilla jotka ovat meidän tiedossa. Kaikki muut, kun meillähän on paljon opiskelijoita joilla on omat kannettavat tietokoneet, niin nämä menevät vierailijaverkkoon kaikki.-v04*

Esimerkki sisäverkon tietoturva rakenteellisesta puutteesta:

> "*Tällä hetkellä melkein kuka tahansa voi tulla kannettavan tietokoneen kanssa ja varastaa IP- osoitteen kytkemällä sen vapaaseen pistorasiaan. Tähän ollaan miettimässä keinoja, joilla kytkeytymiset voitaisiin estää. – v06* "

Organisaatioissa on sallittu etäyhteydenotot organisaation verkon ulkopuolelta. Etäyhteyden

voi muodostaa niin sanotun suojatun tunnelin avulla eli VPN-yhteyden avulla. Eräs haastateltava kuvaa VPN-yhteyden käyttöä seuraavasti:

> "*Tähän on myös tullut hyvin toimivia tietoturvallisia ratkaisuja ja ne ovat tällaiseen turvalliseen etäkäyttöyhteyteen, eli kuinka meidän verkkopalveluihin päästään käsiksi etäyhteyttä hyväksikäyttäen. Eli näillä mahdollistetaan yhteydet, jotka eivät ole saatavilla muilla verkkoteknisillä ratkaisuilla. – v01* "

Organisaatioilla on mahdollisuus tarkkailla verkon turvallisuutta aktiivilaitteiden valmistajien tuottamilla työkaluilla. Niillä kyetään lukemaan kytkinten, reitittimien ja tukiasemien asetukset. Näillä työkaluilla kyetään myös poistamaan mahdolliset haavoittuvuudet. Eräät haastateltavat kuvasivat tietoverkkojen hallintajärjestelmiä seuraavasti:

> "*Meidän verkon hallinnanvalvonnan puolella määritellään kuinka eri kiinteistöjen verkkoihin ja muihin päästään käsiksi, sekä miten valvotaan niiden verkkoliikennettä ja laitteiden toimintaa.-v01* "

> "*Meillä laitteet ovat valvontajärjestelmissä, josta laitteet näkyvät ihan suoraan.-v05* "

5.3 Löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien käyttöä tai niiden piirteitä?

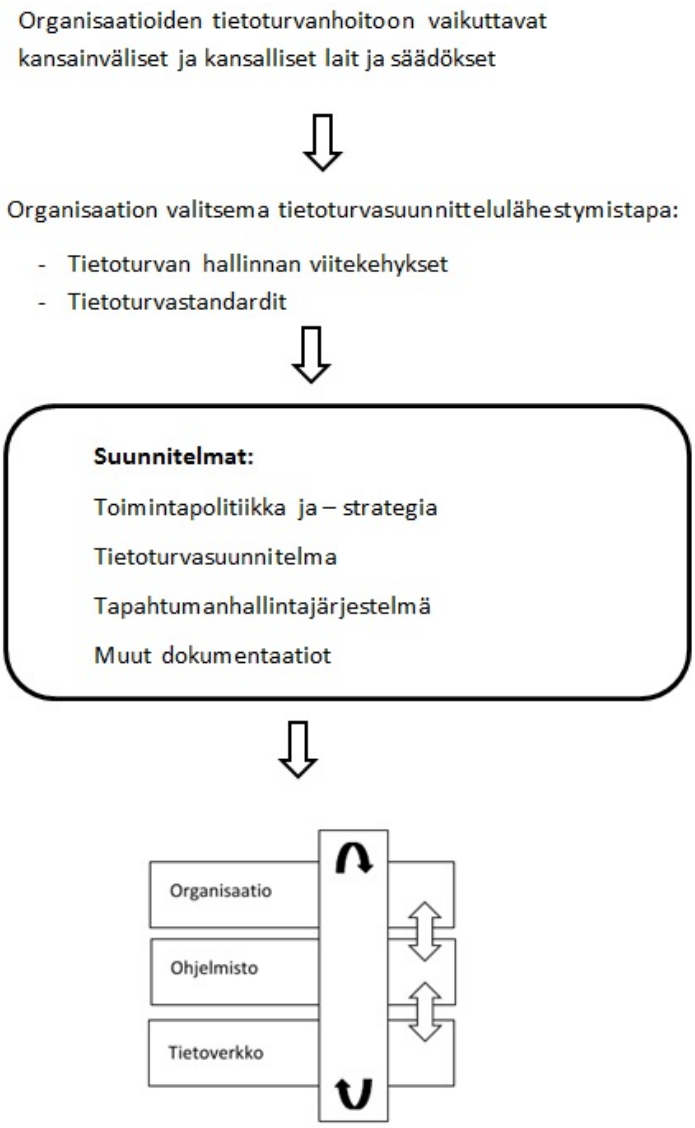
Kolmas tutkimuskysymykseni tarkasteli löytyykö koulutusorganisaatioiden tietoturvanhoidosta tietoturvamallien käyttöä tai niiden piirteitä. Vastaan tutkimuskysymykseen aikaisemmin tässä luvussa 5.1 ja 5.2 yhteenvedossa esiteltyjen tutkimuskysymysten ratkaisuja, jotka vastasivat osin tähän tutkimuskysymykseen. Seuraavassa kuviossa (ks. Kuvio 9) esittelen ne osat aikaisempien tutkimuskysymysten luokitellusta aineistosta, jotka vastaavat tähän tutkimuskysymykseen. Kuten ensimmäisen tutkimuskysymyksen vastauksesta 5.1 käy ilmi, ettei tietoturvamallit näy tutkittavien organisaatioiden tietoturvanhoidossa, joten niiden käyttökin on miltei mahdotonta.

Aineistoanalyysin tuloksena tarkentui organisaation tietoturvan hoidossa ilmenevien piir-

Luokka	Alaluokka	Luokka	Alaluokka
Organisaatiotaso	Tietohallinto	Ohjelmistotaso	Käytönvalvonta
	Tietoturvataso		Sovelluskehityksen hallinta
	Arkistoinnin toteutus		Testausprosessi
	Tietoturvallisuuden ylläpito		Päivitykset
	Tietoturvapoikkeamatilanteiden hallinta	Tietoverkkotaso	Verkon suunnittelu ja palautus
	Pääsynhallinta		Verkonrakenne
	Tietoliikenneturvallisuus		Turvallisuuden hallintajärjestelmät
	Tietoturvan toteutuminen		
	Tietoturvaohjeistus		
	Yleisohjeistus		

Kuvio 9. Tietoturvan hoidossa ilmenevät piirteet

teiden (ks. Kuvio9) vaikutus tietoturvamallien piirteisiin (ks. Kuvio10). Organisaatiotasolla esiintyviin Arkistoinnin toteutukseen, tietohallintoon ja tietoturvatasoon vaikuttavat kansalliset lait ja säädökset. Tietoturvamalli lähestymistavassa oletetaan, että tietoturvatasoon vaikuttavat suunnitteludokumentit on toteutettu aikaisemmin tai sitten ne luodaan tietoturvamallien käyttöönoton yhteydessä. Ohjelmistotasolla organisaatiot ovat siirtäneet tai siirtämässä ohjelmistokehityksen ja testauksen kokonaisvastuun ohjelmistotaloille.



Kuvio 10. Organisaatioiden tietoturvamallien piirteisiin vaikuttavat tekijät

5.4 Yhteenveto

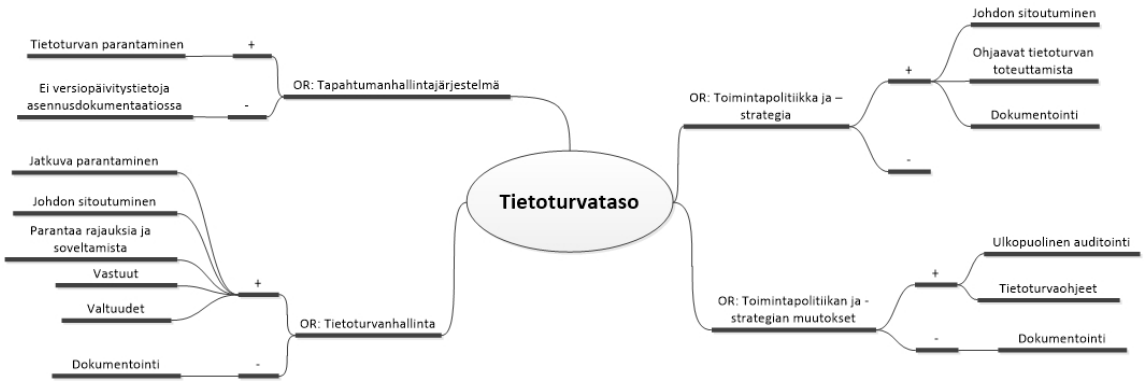
Ensimmäinen tutkimuskysymykseni tarkasteli miten tietoturvamallit näkyvät tutkittavissa organisaatioissa. Vastaan ensimmäiseen tutkimuskysymykseen aineistoanalyysin ja paradigma-analyysin keinoin tietoturvamalleista haastateltavien kertomana. Tarkoitukseni oli analysoida kaikkien tässä luvussa esiteltyjen luokkien ja niiden alaluokkien tietoturvavelvoitteiden toteutumista ja saada vastaus tutkimuskysymykseen.

Paradigma-analyysiä käytetään osa-analyysinä ja siinä kuvataan muodostuneiden alaluokkien suhdetta pääluokkaan, joten tämä on vain osa keino analysoida tuloksia. (+)-merkki tarkoittaa sitä, että alaluokassa ilmenee tietoturvanhoidon piiteitä, joten se vie kohti pääluokkaa eli tietoturvan hoidossa on otettu kantaa tähän piirteeseen ja (-)-merkki vie alaluokkaa poispäin tutkittavasta luokasta eli tietoturvan hoidossa on vähemmän otettu kantaa tähän piirteeseen. Seuraavaksi läpikäydään organisaatio-, ohjelmisto- ja tietoverkkotason tietoturvamalleihin näkyvyyteen vaikuttavat osatekijät hyväksikäyttäen tietoturvahoidon piirteistä dokumenttien ilmenemismuotoja, joilla voidaan tarkkailla käyttävätkö organisaatiot tietoturvamalleja dokumentaatioissaan.

Organisaatiotaso

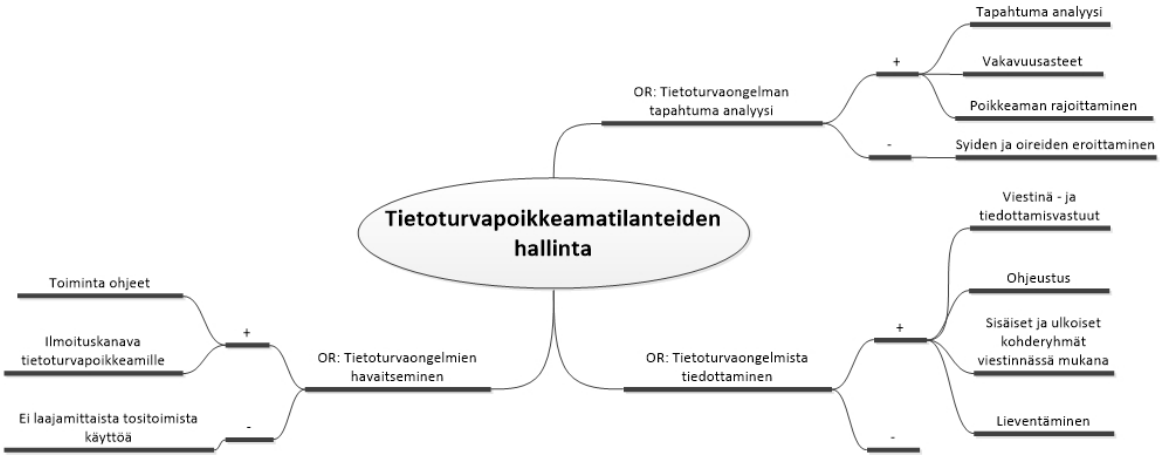
Organisaatiolla tulee olla laadittuna tai on laadittava tietoturvahallinnalliset suunnitteludokumentit, jos he aikovat käyttää tietoturvamalleja (ks. Kuvio11). Tällaisia tietoturvanhallinnallisia dokumentteja ovat toimintapolitiikka ja -strategia sekä tapahtumanhallintajärjestelmä dokumentit. Dokumentit kuvaavat organisaatioiden ylimmän johdon suunnittelussa hyväksymiä käytänteitä, joilla saavutetaan haluttu tietoturvan taso organisaatiossa. Suunnitelmia tulisi kehittää ja tarkastella keskipitkällä aikavälillä ja johdon tulisi nimetä vastuuhenkilö näiden dokumenttien ylläpitämiseen. Päätetty tietoturvataso määrittää käytettävien organisaatiotason tietoturvamallien tarpeen.

Tietoturvapoikkeamatilanteiden hallintaan tarvitaan etukäteissuunnitelmat tai analysoida etukäteen, kuinka toimintakyky säilytetään häiriötilainteiden tai poikkeusolojen aikana (ks. Kuvio 12). Tietoturvaongelmien havaitsemiseen on laadittu auttava toimintaohjeistus ja ilmoituskanava, jotta havaittuihin poikkeamatilanteisiin puututaan mahdollisimman nopeasti. Tietoturvaongelmien tapahtuma-analyysissä on määritelty vastuualueet, joiden avulla selviää



Kuvio 11. Tietoturvataso mikro- ja makrotasojen vuorovaikutussuhteilla

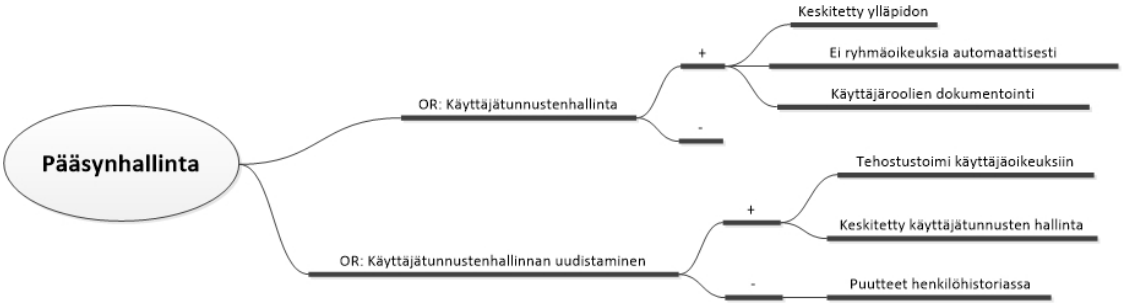
tarvittavat vastuut. Analyysissä on otettu kantaa tapahtuneen poikkeaman rajoittamiseen ja sen poistamiseksi. Heikentävän tekijänä on, ettei ohjeistuksessa ole kyetty erottamaan syitä ja oireita.



Kuvio 12. Tietoturvapoikkeamatilanteiden hallinta mikro- ja makrotasojen vuorovaikutussuhteilla

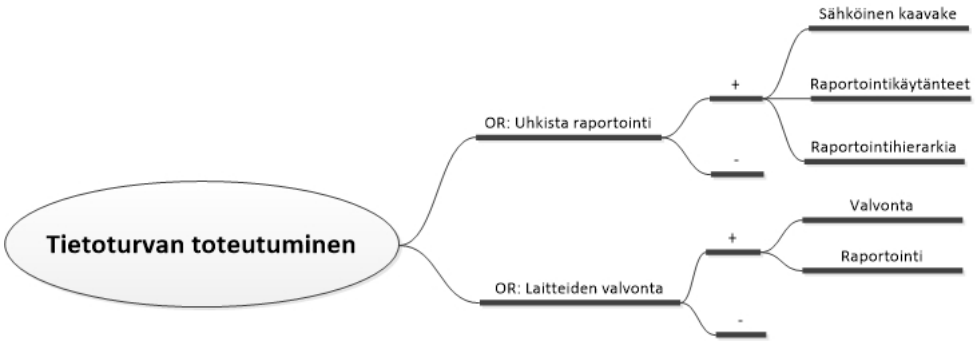
Koulutusorganisaatioiden pääsynhallintaan on dokumentoitu. Dokumentaatiossa otetaan kantaa käyttäjätunnusten keskitettyyn ylläpitoon ja kuinka käyttäjäroolit on dokumentoitu (ks. Kuvio 13). Käyttäjätunnusten hallinnan uudistuksessa voidaan tarkentaa dokumentaatiossa määritellyn tunnuksen sisällä pitämien tietojen laajuutta.

Koulutusorganisaatioiden sisällä kaikkien sidosryhmien velvollisuus on raportoida tietoturvauhkista (ks. Kuvio14). Dokumentaation tulisi määrittää keskeisten toimintojen ja järjes-



Kuvio 13. Pääsynhallinta mikro- ja makrotasojen vuorovaikutussuhteilla

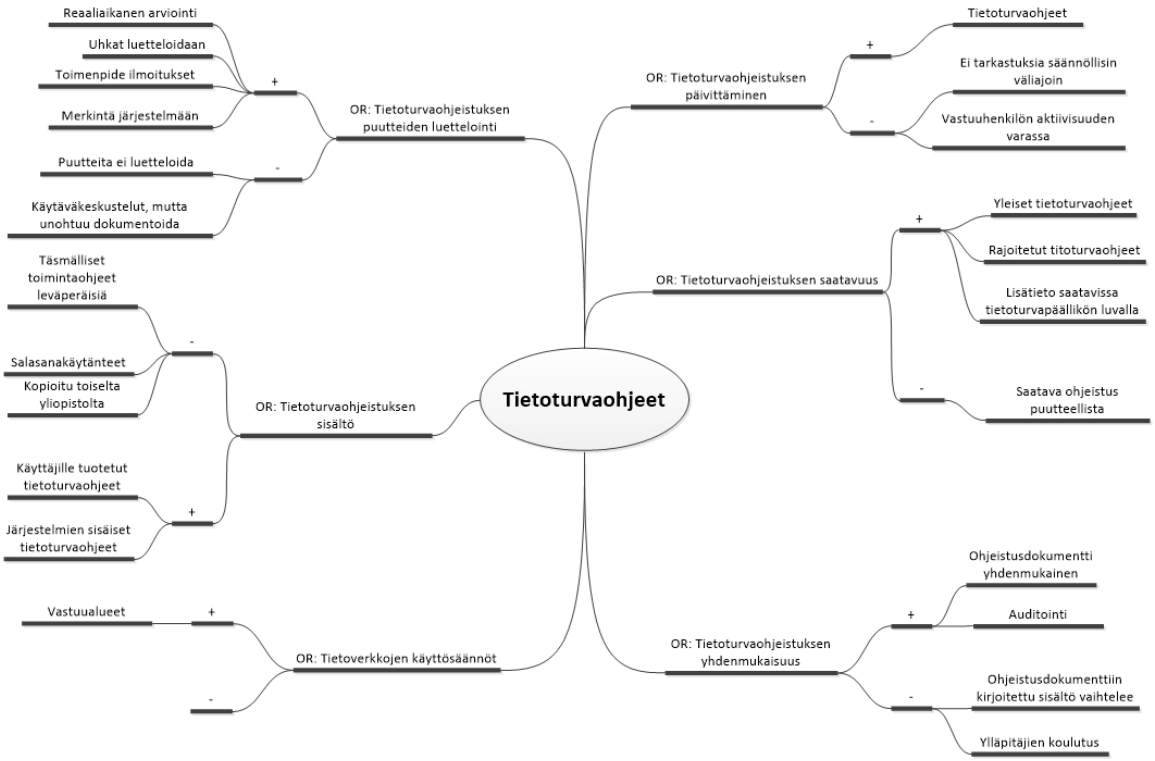
telmien raportointikäytänteet eri aiheiden ja tilanteiden mukaisesti. Laitevalvonnan ja raportoinnin tulisi tukea tilanteiden kuvausta siten, että resurssit osattaisiin kohdentaa tärkeisiin kohteisiin.



Kuvio 14. Tietoturvantoteutuminen mikro- ja makrotasojen vuorovaikutussuhteilla

Organisaation tietohallinnon vastuulla on ylläpitää henkilöstölle ja käyttäjille ajantasaista tietoturvaohjeistusta (ks. Kuvio 15). Laadittujen tietoturvaohjeistuksien yhdenmukaisuuteen on parannettu dokumentaatiopohjaa uudistamalla. Heikentävänä tekijänä yhdenmukaisuusvaatimukselle on, että dokumentaatioon päättyvä sisältö vaihtelee niiden tekijöiden persoonallisuuden mukaan. Ohjeistus on saatavilla pääsääntöisesti tietoverkon välityksellä, mutta kaikkea ei ole julkaistu. Tietoturvaohjeistusta ei päivitetä säännöllisin väliajoin ja niiden päivitys on vastuuhenkilön aktiivisuuden varassa. Ohjeistuksen toimintaohjeistuksen sisällöllinen anti on osoittautunut käytännössä epätarkoiksi. Ohjeistuksen puutteellisuuksia ei luetteloida, vaikka ne tulevat esiin käytäväkeskusteluiden yhteydessä.

Yleisohjeistuksen eli käyttäjien toimintaohjeistus on keskitetty tietoverkkoon (ks. Kuvio 16), mutta siihen tulevia muutoksia ei päivitetä säännöllisesti. Ohjeistuksen hakutoimintoihin vai-



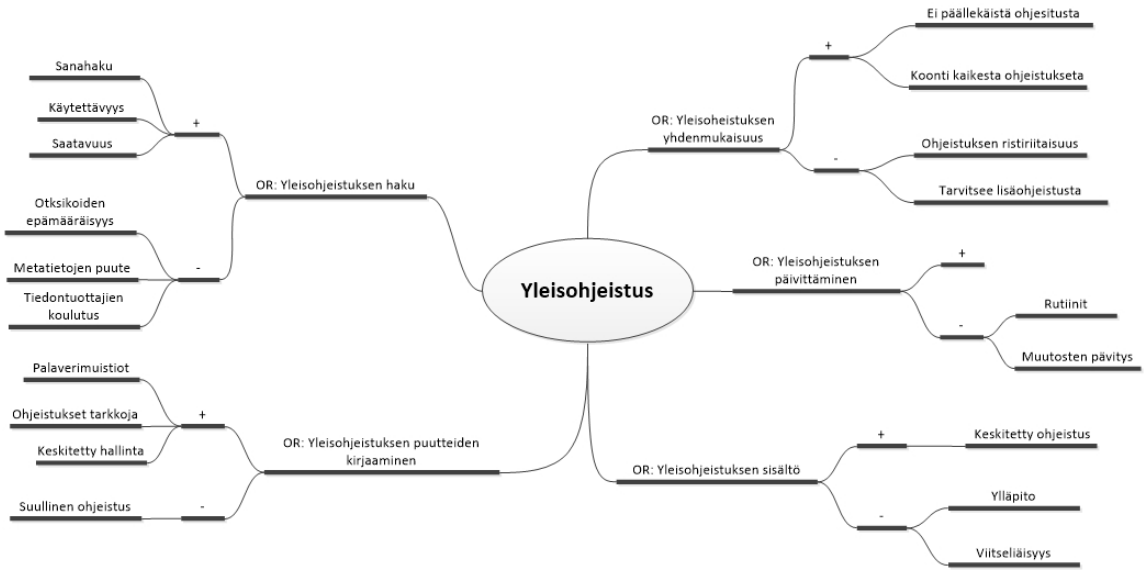
Kuvio 15. Tietoturvaohjeet mikro- ja makrotasojen vuorovaikutussuhteilla

kuttavat metatiedot ovat puutteellisia, joten hakijan pitää tietää tarkka hakusana, joilla tieto on saatavilla. Ohjeistuksen puutteellisuuteen puututaan keskitetyn hallinnan ja palaverimuistioiden huomioiden perusteella, mutta kaikki puutteet eivät saavuta näitä viestikanavia.

Ohjelmistotaso

Ohjelmistojen sovelluskehityksen hallinnassa otetaan kantaa omaan ja muuallatuotettujen sovellusten tuotannollisiin kysymyksiin (ks. Kuvio 17). Ohjelmistojen suunnitteluvaiheesta tulisi ottaa huomioon ohjelmistojen soveltuvuus olemassa olevaan infrastruktuuriin tietoverkkoratkaisuihin ja tasoon. Suunnitteludokumenttien validius tulisi toteutua käyttöönoton yhteydessä suoritetussa käyttöönotto tarkastuksissa. Haittapuolena uusien ohjelmien käyttöönotossa on, että ne voivat myös asettaa uusia tiukempia vaatimuksia infraksruktuurissa olemassa oleville sovelluksille tai itse järjestelmille.

Omassa ohjelmistotuotannossa riskeinä ovat, ettei organisaatio osaa vaatia sovellusprojektilta tietoturvatavoitteita tai vaadi ammattitaitoisia sovelluskehittäjiä sekä testaajia. Muualla



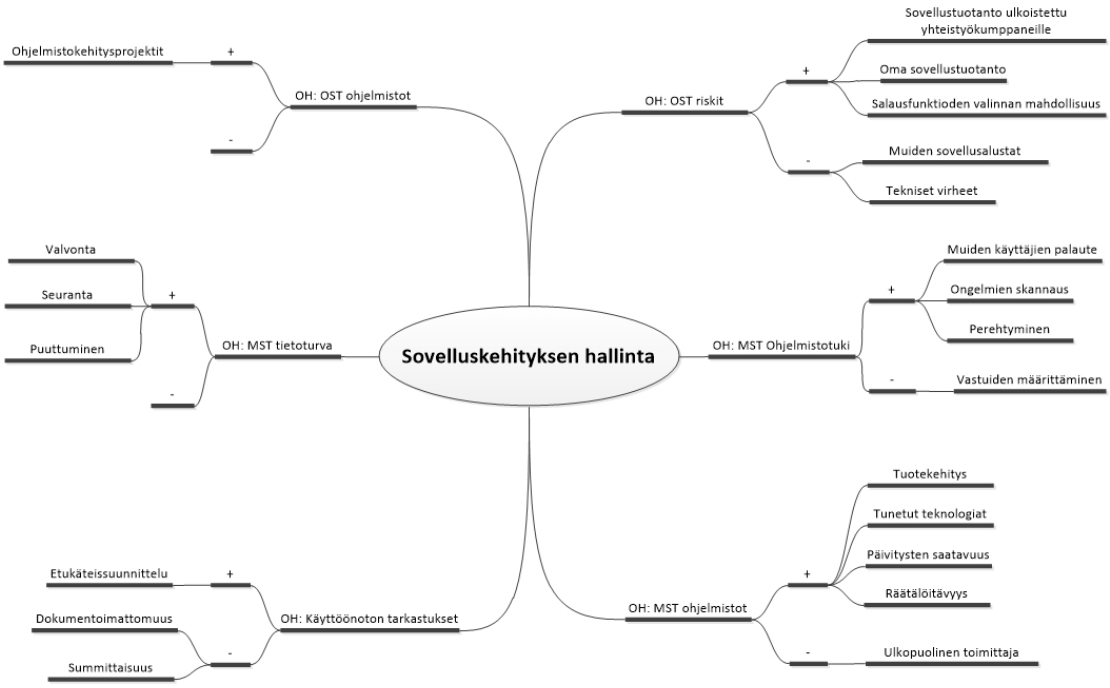
Kuvio 16. Yleisohjeistus mikro- ja makrotasojen vuorovaikutussuhteilla

tuotetussa sovellustuotannossa yleensä on resurssit tehdä tarvittavat ohjelmistopäivitykset ja heillä on resurssit tehdä tarvittavia ohjelmistomuutoksia.

Organisaation tietohallinto vastaa yleensä testausprosesseista (ks. Kuvio 18). Näiden testausympäristöjen tarkoituksena on ohjelmistojen toiminnallisuuden varmistaminen. Tietohallinto ei tee koodikatselmuksia tai puutu muuten ohjelmistokoodin sisältöön. Haittaavana tekijänä on, ettei testiympäristöistä ole dokumentaatiota.

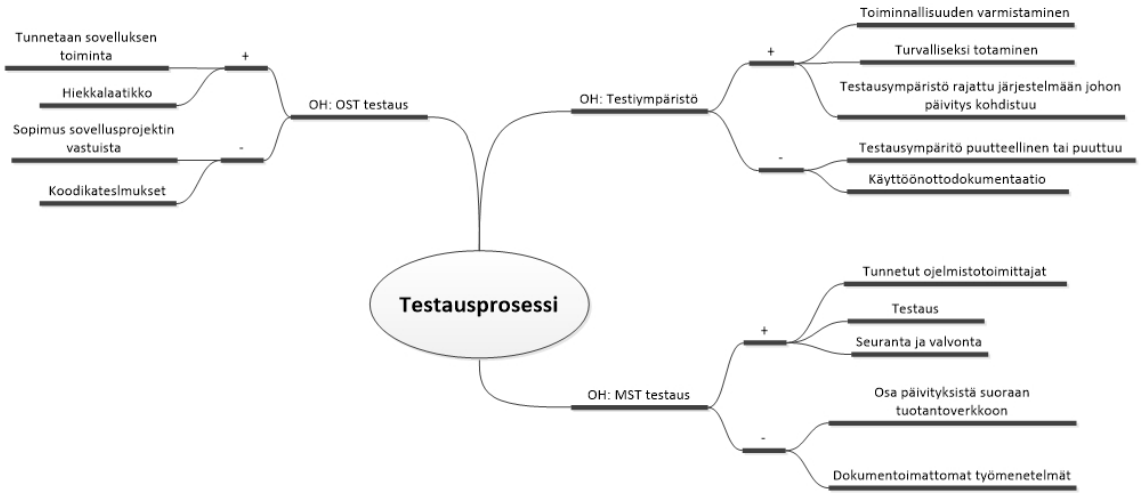
Oman sovellustuotannon testauksen etuna on, että sovellusten toiminnallisuus on tiedossa ja niiden testaus voidaan suorittaa hiekkalaatikkoympäristössä. Haittaavana tekijänä on, ettei organisaatioilla ole resursseja tehdä koodikatselmuksia ja yleensä sovellusprojektien vastuista ei ole kirjallista sopimusta. Muualla tuotettujen sovellusten tietoturvapäivityksiä tai uusia ohjelmistoversioita ei välttämättä testata, koska näiden päivitysten uskotaan parantavan tietoturvaa. Testauksista ei ole mitään dokumentoitua työmenetelmää.

Organisaatioiden tietohallintojen vastuulla on järjestelmäohjelmistojen testaus (ks. Kuvio 19 Tietohallinto ei tee kaikille ohjelmistotoimittajien päivityksille testauksia. Yleinen käytäntö ongelmatilanteiden ilmetessä on palauttaa järjestelmän tila takaisin aikaisempaan palautuspisteeseen, jos asennetut päivitykset aiheuttavat ongelmia.

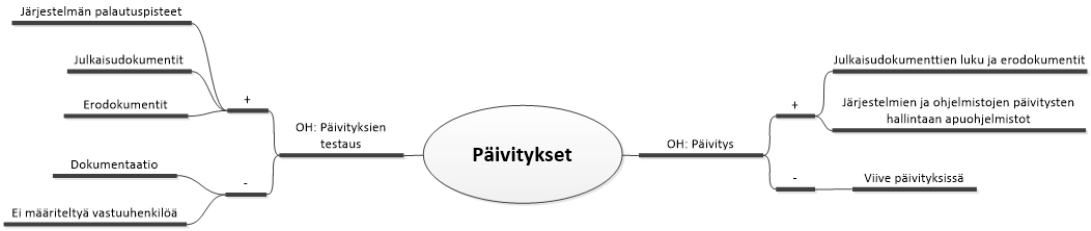


Kuvio 17. Sovelluskehityksen hallinta mikro- ja makrotasojen vuorovaikutussuhteilla

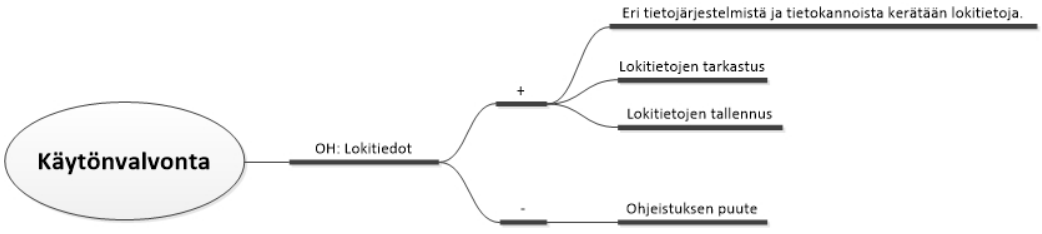
Organisaation tietohallinto vastaa järjestelmien ja ohjelmistojen käytönvalvonnasta (ks. Kuvio 20). Käytönvalvonnan työkaluina käytetään lokitietoja. Nämä tiedostot keräävät automaattisesti tietoja tilasta ja käyttäjistä. Organisaatiot tekevät tarkastuksia käyttöönotettavien järjestelmien ja ohjelmistojen lokitiedoista ja muokkaavat niitä vastaamaan tarpeitaan. Lokitietoja myös tallennetaan, jos on tarvetta todistaa tapahtuneita väärinkäytöksiä. Haittaavana tekijänä on, ettei organisaatioilla ole riittävää ohjeistusta lokitietojen hallintaan.



Kuvio 18. Testausprosessi mikro- ja makrotasojen vuorovaikutussuhteilla



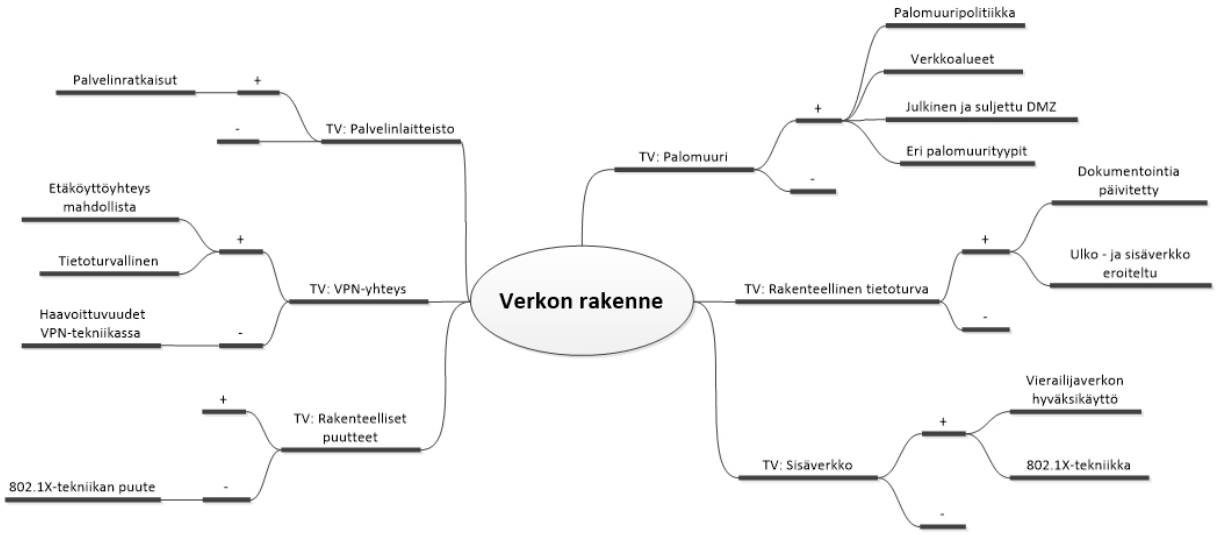
Kuvio 19. Päivitykset mikro- ja makrotasojen vuorovaikutussuhteilla



Kuvio 20. Käytönvalvonta mikro- ja makrotasojen vuorovaikutussuhteilla

Tietoverkkotaso

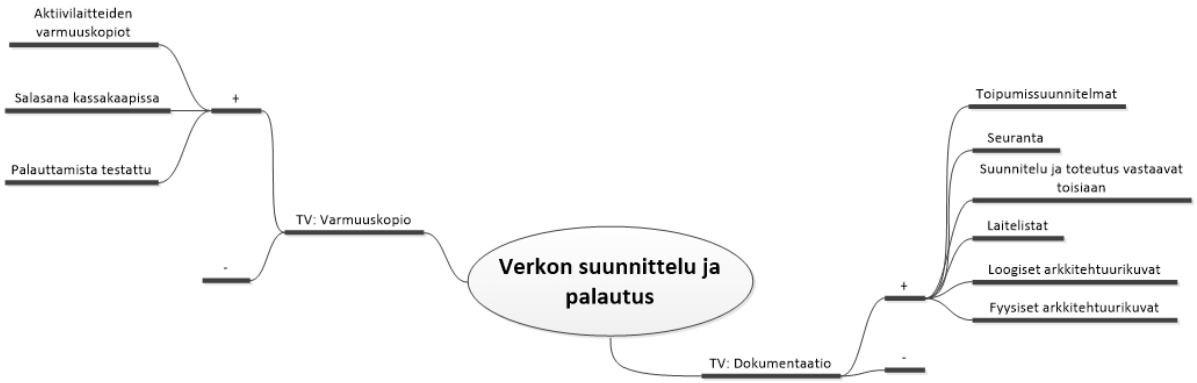
Organisaation johdon on otettava kantaa suunnittelussa tietoverkon rakenteeseen ja niiden tietoturvaan. Verkon rakenne tulisi suunnitella ja toteuttaa siten, että se olisi mahdollisimman selkeä ja helposti hallittavissa (ks. Kuvio 21). Tietoverkko tulisi suunnitella kerrokselliseksi, jotta vähemmän kriittiset ja kriittiset palvelut voitaisiin selvästi erotella toisistaan. Tällä toiminnalla suojataan tärkeitä kriittisiä palveluita verkkoteknisesti, etteivät ulkopuoliset tahot pääsisi niihin helposti käsiksi.



Kuvio 21. Verkonrakenne mikro- ja makrotasojen vuorovaikutussuhteilla

Organisaatioissa tietohallinnon vastuulla on suunnitella tietoverkon suunnittelu ja palautusdokumentaatiot (ks. Kuvio 22), joissa otetaan kantaa käytettävään varmuuskopiointiin ja tietoverkoista luotaviin dokumentteihin. Varmuuskopioinnin laajuuteen vaikuttaa tietoverkon rakenne ja kuinka hyvin se halutaan varmuuskopioitavan. Tietoverkkodokumentaatioiden tulee olla kattavia ja niiden suunnitteludokumentaatioiden ja toteutuneen tietoverkon on vastattava toisiaan.

Ensimmäinen tutkimuskysymykseni tarkasteli, miten tietoturvamallit näkyvät organisaatiossa haastateltavien kertomana. Vastauksena ensimmäiseen tutkimuskysymykseen aineistoanalyysin pohjalta tarkentui, etteivät organisaatiot käytä tietoturvansa hoidon apuna lainkaan tietoturvamallien tarjoamaa lähestymistapaa organisaatio-, ohjelmisto-, tai tietoverkko tasoilla. Tarkastelin aineistoa kaikkien alakatekategorioiden tasolla suhteessa siihen, onko tietoturva-



Kuvio 22. Verkon suunnittelu ja palautus mikro- ja makrotasojen vuorovaikutussuhteilla

malleja käytössä. Mallit keskittyvät ratkaisemaan yhden ongelman ja niiden välillä on monia suhteita toistensa välillä, joten myös yksittäinen käytetty tietoturvamalli tulisi ilmi. Tärkein tietoturvamallien välinen suhde on hienostuneisuus. Tämä tarkoittaa sitä, että yhden tietoturvamallilla toteutettu ratkaisu auttaa muita malleja, jotka ratkaisevat muita mallin lähellä olevia osa-ongelmia alkuperäisestä ongelmasta.

Organisaatiotasolla haastateltavat kuvasivat organisaatiossa tietoturvatason suunnitelmia perustasolla. Ohjelmisto- ja tietoverkkotasolla mallien tulisi esitellä laadukas ja luotettava ratkaisu, joka korjaa tietyn tietoturvaongelman optimaalisesti. Lisäksi mallien tulisi luokitella tietoturvan tiedot jäsenneltynä ja ymmärrettävällä tavalla, sekä niiden tulisi auttaa tallentamaan organisaation tietoturvaosaaminen ja täten auttaa parantamaan organisaation tietoturvaa. Tietoturvamallien tarkoituksen ei ole vain korostaa ratkaisua vaan myös ongelmia ja täten luettelemaan ongelmaan vaikuttavat voimat, sudenkuopat, seuraukset ja ratkaisun.

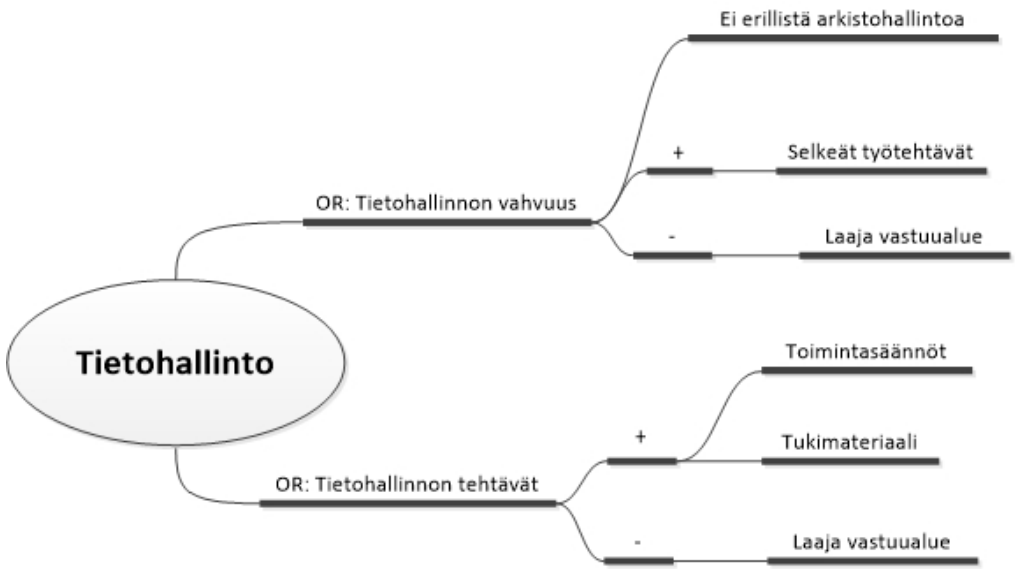
Toinen tutkimuskysymykseni tarkasteli miten organisaatiot huolehtivat tietoturvasta. Vastaan toiseen tutkimuskysymykseen aineistoanalyysin ja paradigma-analyysin keinoin tietoturvan hoidosta haastateltavien kertomana. Tarkoitukseni oli analysoida kaikkien tässä luvussa esiteltyjen luokkien ja niiden alaluokkien tietoturvavelvoitteiden toteutumista ja saada vastaus tutkimuskysymykseen. Näissä kuvioissa vertaan organisaatioiden tietoturvan toteutumisessa ilmeneviä piirteitä lakien, standardien, hyvien käytänteiden ja tietoturvaohjeistusten suosituksiin.

Paradigma-analyysiä käytetään osa-analyysinä ja siinä kuvataan muodostuneiden alaluok-

kien suhdetta pääluokkaan, joten tämä on vain osa keino analysoida tuloksia. (+)-merkki tarkoittaa sitä, että alaluokassa ilmenee tietoturvanhoidon piiteitä, joten se vie kohti pääluokkaa eli tietoturvan hoidossa on otettu kantaa tähän piirteeseen ja (-)-merkki vie alaluokkaa poispäin tutkittavasta luokasta eli tietoturvan hoidossa on vähemmän otettu kantaa tähän piirteeseen. Seuraavaksi läpikäydään organisaatio-, ohjelmisto- ja tietoverkkotason tietoturvaan vaikuttavat osatekijät.

Organisaatiotaso

Tietohallinnon työtehtäviin kuuluu eri tietojärjestelmien sovellutuksien ylläpito ja hoitaminen. Tietohallinnon toimintaan vaikuttavat annettujen työtehtävien määrä sekä tietohallinnon työntekijöiden vahvuus (ks. Kuvio 23). Tietohallinnon vahvuudessa tietoturvaa parantavina ominaisuuksina ovat selkeät työtehtävät ja se, että on määritelty oma arkistovastaava, joka huolehtii arkistohallinnosta. Heikentävän ominaisuutena on laaja vastuualue. Tietohallinnon työtehtävissä tietoturvaa parantavia ominaisuuksia ovat toimintasäännöstöt ja tukimateriaalit ja heikentävänä ominaisuutena laaja vastuualue.



Kuvio 23. Tietohallinto mikro- ja makrotasojen vuorovaikutussuhteilla

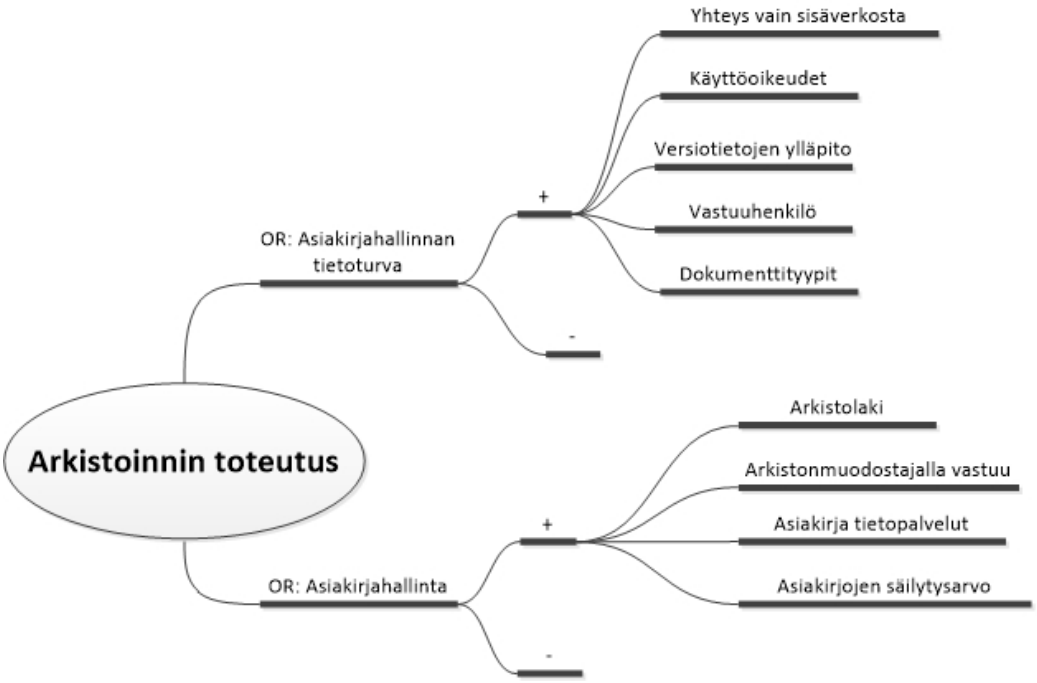
Koulutusorganisaatiot ovat määrittäneet tietoturvatason suunnitelmadokumentit, jolla he hoitavat organisaation tietoturvaa. Suunnitelmat koskevat tietoturvapolitiikka ja -strategia dokumentteja (ks. Kuvio 11). Tietoturvapolitiikassa ja -strategiassa tietoturvaa parantavina omi-

naisuuksina ovat johdon sitoutuminen ja dokumentoinnin olemassa olo ja että ne ohjaavat tietoturvan toteutumista. Muutokset näihin dokumentteihin parantavat tietoturvaa, koska tällöin suoritetaan ulkopuolinen auditointi, jolloin nämä dokumentit käyvät läpi myös ulkoisen katselmuksen jonka seurauksena tietoturvaohjeistuksen laatu parantuu. Heikentävänä ominaisuutena on dokumentaation määrä, koska tämä vie työntekijöiden huomion työtehtävien hoidosta ja heikentää tällöin tietoturvan tasoa. Tietoturvanhallintajärjestelmän parantavia ominaisuuksia ovat johdon parempi sitoutuminen tietoturvaan, joka parantaa rajauksia ja soveltamista tarkentaen vastuita sekä valtuuksia tehdä ratkaisuja. Heikentävänä ominaisuutena on dokumentoinnin määrän lisääntyminen. Heikentävänä ominaisuutena on uusi järjestelmä, joka lisää dokumentoinnin sekavuutta.

Suomessa arkistoinnin toteutukseen ja asiakirjahallintaan vaikuttaa kansallinen arkistolaki, joka määrittää koulutusorganisaatioissa arkistonmuodostajan. Arkistonmuodostajan on määritettävä, miten arkistointi on suunnittelu ja miten vastuut ja hoitokäytännöt järjestetään. Arkistotoimen tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen sekä huolehtia asiakirjoihin liittyvästä tietopalvelusta. Lisäksi arkistotoimi määrittää asiakirjojen säilytysarvon ja hävittää tarpeettoman aineiston (ks. Kuvio 24). Asiakirjahallinnan tietoturvaa parantavia ominaisuuksia ovat laki, joka määrittää vastuut ylläpitää arkistoa. Näissä vastuissa määritellään dokumenttityypit, säilytysajat jne. Asiakirjahallinnan tietoturva parantaa asiakirjojen saatavuutta, käyttöoikeuksia, ylläpitoa. Säilytettäville dokumenteille määritellään dokumenttityypit, jotka määrittävät niiden omaisuusarvon organisaatiolle.

Organisaation johdon on huolehdittava tietojenkäsittelytehtävissä ja etenkin tietoturvallisuuden hallintajärjestelmän asiantuntijatehtävissä toimivien henkilöiden osaamisesta sekä koulutuksesta. Tietohallinnon on myös varmistuttava eri keinoin siitä, että työntekijöillä on vaadittava pätevyys, joka voi syntyä koulutuksen, työkokemuksen tai harjoittelun tuloksena (ks. Kuvio 25). Tällä pätevyydellä on vaikutus myös sen tietoturvan tasoon, joten on tärkeää kyetä määrittämään mitä työtehtäviä voidaan tarjota kokemattomalle työntekijälle.

Turvallisuusosaamisen ylläpidon tehtäviin kuuluu työntekijöiden aikaisemman työkokemuksen tunnistaminen. Uusi kokenut ja pätevöitynyt työntekijä lisää organisaation tietoturvallisuutta, koska hän osaa välttää työtehtävissään tietoturvaa vaarantavia toimia. Toimenkuva ja kouluttautuminen vastaavat tietoturvakäytänteiden vaatimuksia. Tietoturvan laaja-alaisuudesta



Kuvio 24. Arkistoinnin toteutus mikro- ja makrotasojen vuorovaikutussuhteilla

johtuen yksittäinen henkilö ei voi tietää kaikkea, joten kursseille lähetetään soveltuvat henkilöt ja heille pyritään löytämään syvällistä asiantuntijatason koulutusta. Nämä henkilöt sitten opettavat oppimansa tiedon muulle henkilökunnalle suullisesti nk. tiedon valutuksen keinoin.

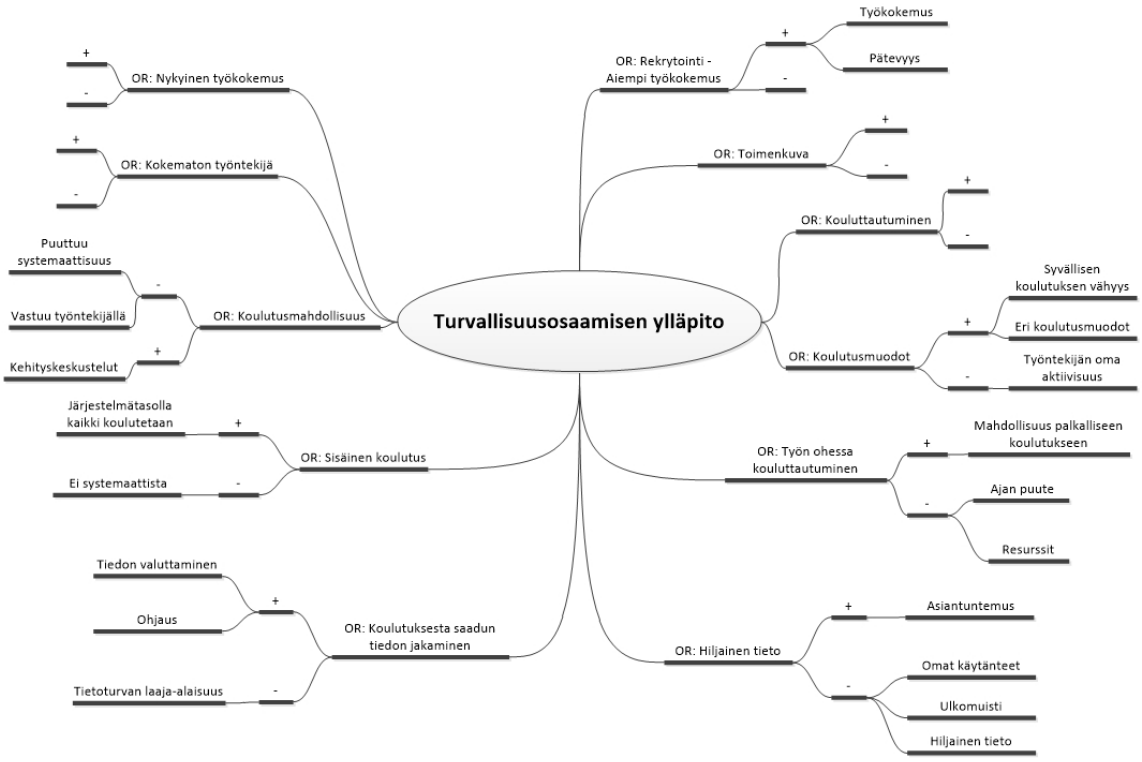
Työntekijät saavat edistää osaamistaan työn ohessa työsääoppimisen tai etäopiskelun keinoin kirjallisuuden, verkkokurssin- tai verkkowebinaarin muodossa, mutta tämä on omatoimista opiskelua. Koulutukseen hakeutumisen esteenä on yleensä resurssien tai ajan puute.

Organisaatioissa on tapana antaa tarvittavat työohjeistukset suullisina nk. "hiljaisena tietona". Nämä ohjeistukset parantavat työntekijän asiantuntijuutta suorittaa työtehtäviä paremmin, mutta opastukset ovat kahdenkeskisiä. Vaarana näissä dokumentoimattomissa ohjeissa on, että ne perustuvat ulkomuistiin, jolloin ne voivat tahattomasti muuttua tai henkilö voi muistaa saamansa neuvoa väärin tai hän ei alun alkaen ole osannut kysyä oikeita kysymyksiä.

Työntekijöillä on koulutusmahdollisuus ja koulutustarvetta käydään läpi kehityskeskusteluissa. Heikentävänä puolena koulutusmahdollisuudessa on, että nämä jäävät kehityskeskusteluissa kartoituksen asteelle ja kouluttautuminen jää työntekijän vastuulle. Haastatel-

tavien työtehtävät ovat asiantuntijatehtävien tasoisia, mutta he eivät välttämättä käy suoritustason koulutuksissa. Tämä voi johtua siitä, että työnkuvan työtehtävät voivat olla liian laaja-alaisesti määriteltyjä. Syntyy tilanne, ettei työntekijä tiedä mitä kaikkea hänen tulisi tietää.

Sisäinen koulutus on yleensä järjestetty suurten järjestelmien käyttöönoton yhteydessä. Organisaatiot saattavat kouluttaa käyttäjiä käyttöönoton yhteydessä, mutta kouluttavatko he uudet työntekijät, jotka tulevat käyttöönoton jälkeen? Onko suuri järjestelmäpäivitys käyttöönotto?



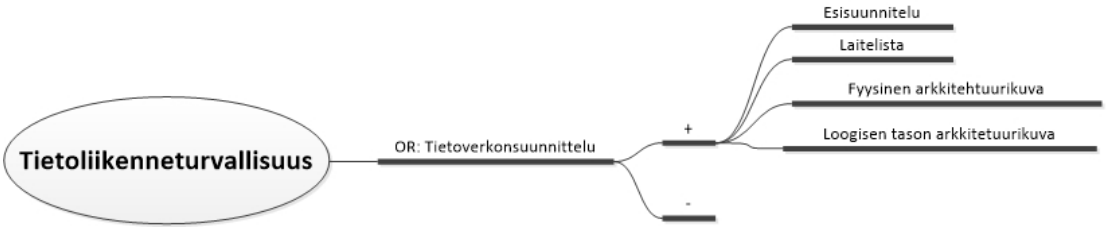
Kuvio 25. Turvallisuusosaamisen ylläpito mikro- ja makrotasojen vuorovaikutussuhteilla

Organisaation tietoturvapoikkeamatilanteiden hallinnan kannalta organisaation tulee kirjata muistiin havaittuja tietoturvapoikkeamia (ks. Kuvio 12).

Tietoturvaongelmien tapahtuma-analyysin poikkeamatilanteita varten organisaatioiden tulisi luoda etukäteissuunnitelmat tai analysoida, kuinka heidän tulisi säilyttää häiriötilanteiden tai poikkeusolojen aikana toimintakykynsä. Analyysissä on määritelty tiedoille vakavuusasteet omaisuuserien tärkeyden mukaan. Poikkeaman rajoittamisella tarkoitetaan toimia niihin tilanteisiin, joissa tahallisen tai tahattoman tapahtuman aiheuttama tilanne on vaarantanut organisaation tietojen tai palveluiden tarkoituksenmukaisen tason. Suhteessa määritellään ensin todellinen uhka omaisuuserille ja onko siihen haavoittuvuutta, jos suhdetta ei ole, niin tällainen uhka ei ole tietoturvaongelma. Tietoturvaongelmien tiedottamisessa organisaatio on ottanut kantaa sisäiseen ja ulkoisen viestinnän keinoihin tietoturvaongelman esiintyessä. (ks. Valtionvarainministeriö 2005, 6) Sisäiseen ja ulkoiseen viestintä on suunniteltu ja keinot tietoturvaongelman lieventämiseen on tunnistettu. Organisaatio on myös luonut toimintaohjeistuksen tietotuvanpoikkeamien varalle. Heikentävänä tekijänä on, ettei haastateltavat kyenneet nimeämään laajamittaista tositoimista käyttöä, vaikka näitä tietoja voitaisiin käyttää hyväksi tunkeutumisenhavainnoinnissa historiatiedoissa. Haastateltavat eivät tuoneet esiin syiden ja oireiden suhdetta.

Organisaation pääsynhallinta pitää sisällään käyttäjätunnusten hallinnan (ks. Kuvio 13). Käyttöoikeudet edellyttävät, että organisaatio myöntää henkilöstölle yksilöllisen tunnuksen. Tämä tunnus luodaan keskitetysti ylläpidossa. Pelkälle yksilölliselle tunnukselle ei luoda ryhmäoikeuksia automaattisesti. Oikeudet myönnetään työtehtävien mukaisesti ja käyttäjäroolit dokumentoidaan. Tämä tunnus voi myös pitää sisällään muitakin tietoja käyttäjästä. Käyttäjätunnustenhallinnan uudistamisella tehostetaan käyttäjäoikeuksien ja parannetaan käyttäjätunnusten hallintaa, koska vanhassa järjestelmässä on puutteita henkilöhistorian hallinnassa.

Organisaatiot ovat ottaneet kantaa esisuunniteltuvaiheessa tietoliikenneturvallisuuteen (ks. kuvio 26). Tässä esisuunnitteluvaiheessa luodaan fyysinen arkkitehtuurikuva, jossa verkon tarvitsemien aktiivilaitteiden sijainnit ja tarvittavat verkko-osoitteet määritellään. Loogisen tason arkkitehtuurikuva puolestaan selventää tietoverkon kaapeloinnit ja tarvittavat verkko-osoitteet ja mahdolliset muut tarvittavat tiedot. Näiden korjaaminen jälkikäteen on usein vaikeaa ja hyvin kallista verrattuna niiden tekemiseen alusta alkaen kunnolla.



Kuvio 26. Tietoliikenneturvallisuus mikro- ja makrotasojen vuorovaikutussuhteilla

Organisaatioiden sisällä kaikki sidosryhmät ovat velvollisia raportoimaan tietoturvauhkista (ks. Kuvio 14). Raportointi tulisi järjestää sähköisesti keskeisten toimintojen ja näitä tukevien järjestelmien vastuuhenkilöille. Eli heidän tulisi puuttua ja tehdä raportti havaitusta uhkasta. Organisaation johdon on laadittava erilaisia raportointikäytäntöjä eri aiheiden ja tilanteiden mukaisesti, sekä valtuutettava jatkuva raportointi keskeisten toimijoiden ja toimintaa tukevien järjestelmien vastuuhenkilöille. Laitevalvonnan ja raportoinnin tulisi tukea tilannekuvan muodostumista siten, että tämän perusteella resurssit voitaisiin kohdentaa tärkeisiin kohteisiin. kuten erityistilanteen (ihmiset, omaisuus), vakavan uhkan (tieto) tai vakavan vahingon ollessa kyseessä (korjaaminen). Virastoaikaan tietohallinto ja ilta-aikaan vahtimestarit tarkkailevat käyttäjiä ja omaisuuden kuntoa.

Ohjelmistotaso

Organisaatiot ovat määritelleet miten ja mitä lokitietoja ne keräävät käytönvalvonnan tarpeisiin (ks. Kuvio 20). Organisaatiot keräävät eri tietojärjestelmistä ja tietokannoista käyttö-, muutos- ja virhelokeja. Ohjelmien keräämät lokit tarkastetaan ja tallennettaan myöhempää tarkastelua varten. Haittaavana tekijänä on oheistuksen puute siitä, kuinka lokeja käsitellään. Haastateltavat eivät kertoneet kenen työtehtäviin kuului kerättyjen lokitietojen asetusten ja niiden keräämien tietojen tietoturva. Toisaalta ei ollut kirjattua suunnitelmaa mitä ja miten lokitiedoissa kerätään.

Organisaatioiden sovelluskehityksen hallinnassa on otettu kantaa omaan ja muualla tuotettuun sovellustuotantoon (ks. Kuvio 17). Käyttöönoton tarkastuksien tarkoituksena on huomioida etukäteen ohjelmistojen soveltuvuus infrastruktuurin tietoturvaratkaisuihin ja -tasoon. Organisaatiot eivät ole dokumentoineet näitä käyttöönoton tarkastuksien etukäteisvaatimuksia ja käyttöönoton tarkastukset olivat summittaisia. Haittana tästä saattaa olla se, että in-

frastruktuuri voi asettaa vaatimuksia uudelle tai päivitettävälle sovellukselle. Voi myös olla, että uusi sovellus asettaa tiukempia tietoturvavaatimuksia olemassa olevalle infrastruktuurille.(ks. Valtionvarainministeriö 2013a, 60-61)

Koulutusorganisaatiosta yliopistolla on omaa sovellustuotantoa. Näissä ohjelmistoissa on riskeinä, jos organisaatio ei vaadi sovellusprojekteille tietoturvatavoitteita ja niiltä tietoturvatietoisia sovelluskehittäjiä tai testaajia. Voiko näiden sovellusten tietoturva tai toiminnalliset vaatimukset olla vaatimustason vastaisia? Ohjelmistoprojektit olisivat koulutusorganisaation sisäisiä, niin tästä huolimatta sovelluskehitystä opettavat koulutusorganisaatiot eivät opeta näissä kunnolla tietoturvan huomioon ottamista. Tämä edesauttaa kriittisten virheiden mahdollisuutta. Omasta sovelluskehityksestä huolimatta usein niissä tukeudutaan muiden sovellustuottajien tuotteisiin (tietokannat, ohjelmistokielet, avoimen lähdekoodin tuotteet), jolloin nämä ohjelmistot ovat vain omia sisältönsä puolesta.

Etuina muualla tuotetuissa sovelluksissa tuotekehitykselle on se, että ne voidaan valita tunnetuilta valmistajilta, jotka tuottavat ohjelmistot tunnetulla tekniikalla. Näihin ohjelmistoihin on yleensä saatavilla automaattisesti päivityksiä, jolloin organisaation ei tarvitse olla tietoturvahaavoittuvuuksien ilmetessä ohjelmoimassa omia päivityspaketteja. Muualla tuotetut sovellutukset ovat räätälöitävissä, koska yleensä ohjelmistotoimittajilla on resursseja tehdä vaadittavia muutoksia ohjelmistoihin. Muualla tuotettujen ohjelmistojen etuina on valvonta, seuranta ja puuttuminen. Haittaavana tekijänä on ulkopuolisista toimijoista riippuvuus.

Muualla tuotetuille sovelluksille on tarjolla ohjelmistotukea. Uusiin ohjelmistoihin voidaan järjestää koko organisaation laajuisia koulutuksia sekä tietohallinnon työntekijöille että käyttäjille. Tietoturvan kannalta organisaatioissa on valtavirtaan kuuluvat ohjelmistot laajalti käytössä, joten ongelmista löytyy yleensä laitetoimittajien keskustelupalstoilta muiden käyttäjien kommentteja ja neuvoja ongelmatilanteisiin. Ohjelmistotoimittajat valmistavat tietoturvaa parantavia skannausohjelmia, joilla organisaatiot voivat varmistua järjestelmien tietoturvasta.

Testausprosessien ylläpidosta vastaa yleensä tietohallinto (ks. Kuvio 18). Organisaatiot ovat luoneet ohjelmistojen testaukseen testausympäristöjä. Näiden testausympäristöjen tarkoituksena on ohjelmistojen toiminnallisuuden varmistaminen ja niiden turvalliseksi toteaminen,

etteivät ne riko tuotantojärjestelmän toiminnallisuutta. Haastattelujen perusteella nämä testiympäristöt ovat puutteellisia tai ne puuttuvat kokonaan ja testiympäristöistä ei löydy dokumentaatioita.

Oman sovellustuotannon ohjelmistojen testauksen etuna on, että sovellutuksen haluttu toiminnallisuus on tiedossa ja niiden testaus tehdään ns. hiekkalaatikkoympäristössä. Tässä ympäristössä ohjelmaa suoritetaan siten, ettei se vaikuta isäntäkoneen muiden ohjelmistojen toimintaan. Toimintoja on rajoitettu siten, ettei ohjelmisto pääse kaikkiin laitteistoresursseihin. Haittaavana tekijänä on, ettei niihin suoriteta koodikatselmuksia ja organisaatio ei tee etukäteissopimuksia sovellusprojektien vastuista.

Ohjelmistojen tai järjestelmien testaukset suoritetaan testausympäristössä tai sitten käytetään kokemusperästä tietoa päivitysten luotettavuudesta. Testausympäristö on vastaamaan heidän kriittisimpään järjestelmään, joten testiympäristö ei välttämättä ole samanlainen kuin tuotantoympäristö. Testausympäristön olosuhteiden tarkoituksena on varmistaa, että ohjelmistot ovat päivitysten jälkeen toiminnallisuudeltaan tarkoitukseen sopivia ja tietoturvallisia.

Muualla tuotettujen sovellusten tietoturvapäivitykset ja uudet ohjelmistoversiot testataan testiympäristössä. Tällöin tarkastelun kohteena on vain, etteivät tietoturvapäivitykset riko mitään tuotantojärjestelmässä. Muita päivityksiä sekä Windowsin sovellustuotteiden tietoturvapäivityksiä ei testata. Testauksesta ei ole mitään dokumentoitua työmenetelmää.

Organisaatioiden tietohallinnot huolehtivat järjestelmäohjelmistojen päivitysten testauksesta (ks. Kuvio 19). Muualla tuotettujen ohjelmistojen toimittajat julkaisevat ennen päivitystä erodokumentit, joissa kerrotaan tulevista päivityksistä ja niiden vaikutuksista järjestelmiin. Dokumentit perustelevat päivityspaketin tarpeen ja miksi päivitystä tarvintaan ja mitä ongelmia se korjaa. Heikentävänä tekijänä on, ettei kaikkia ohjelmistotoimittajien kriittisiä päivityksiä asenneta testauksen jälkeen tai automaattisesti niiden ilmestyttyä. Tämä voi heikentää järjestelmän tietoturvaa.

Päivitysten testausta helpottaa julkaisu- ja erodokumenttien sisältö. Päivitykset voidaan myös ajaa suoraan tuotantojärjestelmään, koska ennen päivittämistä voidaan luoda palautuspiste ja jos ohjelmisto aiheuttaa häiriöitä tuotantojärjestelmän toimintaan, voidaan järjestelmä palauttaa takaisin sitä edeltäneeseen kokoonpanotilaan. Haittaavana tekijänä on, etteivät or-

ganisaatiot ole dokumentoineet päivitysten testausta eivätkä määrittäneet henkilöä suorittamaan näitä testauksia.

Tietoverkkotaso

Organisaation tietoverkon suunnittelu ja palautusdokumentaatio vaikuttaa tietoverkon tietoturvaan (ks. Kuvio 22). Dokumentaation tarkoituksena on määrittää kuinka verkon rakenne toteutetaan. Fyysinen arkkitehtuurikuva määrittää verkon tarvitsemien aktiivilaitteiden sijainnit ja tarvittavat verkko-osoitteet. Loogisen tason arkkitehtuurikuva selvittää tietoverkon kaapeloinnit ja mahdolliset muut tarvittavat tiedot. Laitelista on listaus käytettävistä laitteista. Seurantadokumentaatiossa määritellään kuinka tietoverkon laitteiden toimintaa ja verkkoliikennettä seurataan. Toipumissuunnitelmassa otetaan kantaa, kuinka organisaatiossa on suunniteltu vakavista häiriötilanteista toipuminen. On myös tärkeää, että suunnitteludokumentit noudattavat samaa rakennetta kuin määrittelyvaiheen dokumentit. Verkon laitteiden asetuksista tulisi ottaa varmuuskopio, joka tulisi sijoittaa helposti saataville, jotta organisaatio kykenisi toipumaan häiriötilanteesta mahdollisimman nopeasti. Myös näiden varmuuskopioiden palauttamista tulisi testata ja harjoitella säännöllisin väliajoin.

Verkon rakenne tulisi suunnitella ja toteuttaa siten, että se olisi mahdollisimman selkeä ja helposti hallittavissa (ks. Kuvio 21). Tietoverkon perusrakenne tulisi olla toiminnallisuudeltaan rajattu, siten että sen eri kerrokset (ulko- ja sisäverkko) olisivat palomuurein suojattu ja eroteltu. Verkkoalueiden eri kerroksia tulisi kyetä suojamaan. Erottelulla on pyritty suojaamaan kriittiset sisäiset palvelut ja järjestelmäpalvelut verkkoteknisesti siten, ettei organisaatioiden ulkopuolelta niihin päästä helposti käsiksi.

Organisaatioilla on mahdollisuus valita käyttöyhteyksien hallintaan eri ohjelmistovalmistajien valmistamia VPN-ratkaisuja. Valmistajat käyttävät eroavia protokollia kahden reitittimen välille. VPN-yhteys on toimiva ja tietoturvallinen ratkaisu etäkäyttöyhteyden muodostamiseen yksittäisen koneen ja etäkäyttöpalvelimen välille.

Organisaation tietoverkon hallinnanvalvonnasta vastaa tietohallinto. Hallinnanvalvonnan puolella määritellään, kuinka eri kiinteistöjen tietoverkkoihin päästään käsiksi sekä miten niiden verkkoliikennettä ja laitteiden toimintaa valvotaan (ks. Kuvio 27). Aktiivilaitteet kuuluvat yleensä verkkovalvonnan piirin ja ne raportoivat itse itsestään. Kaupallisilla hallinnanval-

vontaohjelmistoilla kyetään lukemaan kytkimien, tukiasemien ja reitittimien tila ja niiden asetukset (ks. Andreasson ja Koivisto 2013, 72-73).

Kuvio 27. Turvallisuuden hallintajärjestelmä mikro- ja makrotasojen vuorovaikutussuhteilla

Toinen tutkimuskysymys oli miten organisaatiot huolehtivat tietoturvasta. Organisaatiotasolla tietoturvasta huolehtivat tietoturvapäällikkö, tietohallinto ja asiakirjanhallinta. Organisaatiotasolla tietoturvasta on huolehdittu jokaisella sen osa-alueella resurssien ja varojen sallimissa rajoissa.

Organisaatiotasolla tietoturvatasoon vaikuttavat suunnitelmadokumentaatiot, kuten toimintapolitiikka ja -strategia sekä se, että tietoturva- ja tapahtumahallintajärjestelmät on luotu. Organisaatioiden johto on sitoutunut näiden dokumenttien kehittämiseen sekä tietoturvan eteenpäinvientiin. Tutkimusaineistosta näkyy halu parantaa ja kehittää tietoturvaa. Niiden toiminnallista testausta ei suoriteta säännöllisin väliajoin. Organisaatiot huolehtivat heidän fyysisestä omaisuudesta, kuten työntekijöiden tiedoista, kiinteistöitä, laitteista, käyttäjistä ja kalustosta.

Toisaalta tietohallinnon toiminnasta heijastuu jonkinlainen resurssipula toisessa koulutusorganisaatiossa. Tämä heijastuu ylläpitävän henkilöstön esiintuomana etukäteissuunnitelmien sisällöllisten ja toiminnallisten tietojen puutteina, heidän omaan työhön vaikuttavien toiminnallisten tietojen dokumentoinnin puutteena sekä heidän muille käyttäjille tekemien dokumenttien puutteellisena täyttönä, kuten ok-merkintöinä tietokentissä. Asiakirjanhallinnasta huolehditaan lain määräysten mukaisesti, mutta haastatteluaineistosta saaman käsityksen mukaisesti asiakirjanhallinnossa on olemassa dokumenttipohjat, sekä henkilöstön että käyttäjien dokumentaatiolle, mutta niiden täyttäjät eivät ole halukkaita tekemään niistä yhdenmukaisia tai täyttämään niitä lainkaan. Tämä heijastuu dokumenttihakujen epämääräisyytenä.

Puutteet dokumenteissa voivat heikentää organisaation tietoturvatasoa.

Ohjelmistotasolla organisaatio on ottanut kantaa sovellusten tietoturvan hoidossa käytönvalvontaan, sovelluskehityksen hallintaan, testausprosessiin ja päivityksiin. Organisaatioiden tulisi nimetä jokaiselle ohjelmistokehityksen osa-alueelle vastuuhenkilö, jotta niiden toteuttamisesta voitaisiin varmistua.

Lokitiedostojen keräämisen tarkoituksen on käyttää niitä käytönvalvonnassa säädösten ja ohjeiden mukaisesti. Organisaatiot tekevät tarkastuksia siitä, keräävätkö nämä lokit turhia kansallisten lakien vastaisia tietoja. Lokitiedot siis voivat sisältää tietosuojan piiriin kuuluvia tietoja. Haittaavana tekijänä on jos lokikäytänteistä ei ole dokumentoitua suunnitelmaa.

Omien ja muiden sovellusten ohjelmistotuotannon projekteissa tulisi ottaa huomioon ohjelmiston tietoturva. Organisaatioiden tulisi määrittää jokaiselle ohjelmistokehityksen osa-alueelle vastuuhenkilö varmistamaan osa-alueen toteutuminen.

Organisaatioiden testausympäristöjen tarkoituksena on testata ohjelmistoista, rikkovatko ne tuotantojärjestelmän toimintaa. Muu testaaminen jätetään ohjelmistokehittäjille. Heidän vastuullaan on varmistua ohjelmistojen virhetilojen oikeasta käsittelystä ja lokien kattavuudesta. Ohjelmistoprojekteissa luodaan sovelluksen testiympäristöt. Yliopisto luottaa siihen, että omassa ohjelmistotuotannossa suoritetaan nämä toimet. Voi olla, että nämä sovellukset toteuttavat tietoturvasta tietämättömät ohjelmoijat, kuten opiskelijat, joille ei opiskelujen yhteydessä opeteta ohjelmistojen tietoturvaa lainkaan.

Tietohallinto testaa päivityksiä ennen niiden päästämistä tuotantojärjestelmään, mutta kriittiset päivitykset päästetään tuotantojärjestelmään testaamatta. Organisaatioiden päivitysten testaus on suunniteltu siten, että ohjelmistoversiot testataan, mutta pienempiä päivityksiä ei testata, koska tämä säästää resursseja muuhun ylläpitotoimintaan.

Aineistosta ilmenee, että ohjelmistotasolla suurimmat puutteet ovat toiminnallisten ja ohjausdokumenttien puuttuminen. Lisäksi ohjelmistojen tietoturvallisen toiminnan varmistaminen tapahtuu verkkoliikennettä tarkkailemalla ja skannausohjelmistojen avulla.

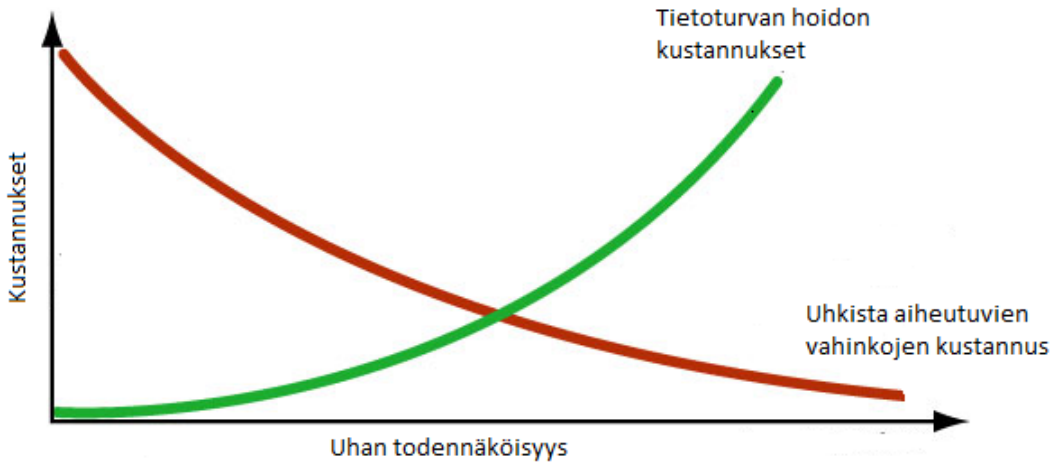
Tietoverkkotasolla organisaatio ovat määritelleet verkon suunnittelu- ja palautusdokumentaatiot, joissa otetaan kantaa varmuuskopiointiin ja tietoverkon dokumentaatioon. Tietoverk-

kotasolla varmuuskopiointi pitää sisällään aktiivilaitteiden varmuuskopioinnin. Tällä varmistetaan pahojen häiriöiden aiheuuttamista ongelmista toipuminen. Varmuuskopioinnin palautuksesta on testattu, että varmuuskopio ei ole korruptoitunut. Pääkäyttäjän salasana on tallennettu kassakaappiin, eikä se ole yhden ihmisen ulkomuistissa. Tietoverkkodokumentaatio on kattavaa ja sisältää esisuunnitteludokumentit, toteutunut tietoverkko ja suunnitelmat vastaavat toisiaan.

Tietoverkon rakenne on yksikertainen ja sen laajentaminen onnistuu vaarantamatta muun tietoverkon tietoturvaa. Tietoturvallisen siitä tekee sen kerroksellisuus ja se, että verkon laitteista vain harva on suorassa kosketuksessa Internetiin. Tämä tarkoittaa sitä, ettei sisäverkon järjestelmien osia tarvitse asettaa korkeimpaan tietoturvallisuusluokkaan. Turvallisuuden hallintajärjestelmän tarkoituksena on tietoverkon aktiivilaitteiden tarkkailu, verkkoliikenteen valvonta ja haavoittuvuuksien automaattinen poisto.

Vastauksena organisaatiot hoitavat organisaatio-, ohjelmisto- ja tietoverkkotasoilla tietoturvaa organisaation johdon hyväksymällä riskitasolla. Tietoturvariskien arviointikriteerit on luotu ja määritelty organisaation johdon hyväksymien periaatteiden mukaisesti ja sitä toteutetaan tietohallinnossa. Arviointikriteereissä määritellään millaisen riskin organisaatio voi ottaa. Tämä tietoinen päätös on tehty asetetun kriteeritön perusteella siten, että organisaatioiden tietoturvan hoito tulisi olla kustannustehokasta. Tietoturvan kustannusten ja uhkista aiheutuvien kustannusten suhde tulisi olla tasapainossa eli näiden kuvaajien leikkauspisteessä (ks. Kuvio 28). Organisaatiot tarkastavat ja kehittävät tietoturvasuunnitelmiaan. Organisaatiot hoitavat tietoturvaa tietoturvan hallinnan viitekehysten kontrollein, mutta toinen organisaatio tehostaa tietoturvan hallintaa Katakri auditoinnilla, jota käytetään tietojärjestelmiensä turvallisuuden arviointiin. Tämä auditointi on tullut ajankohtaiseksi kyberturvallisuuskeskuksen aloittamisen seurauksena. Viranomaiset pyrkivät varmistamaan kohdeorganisaation turvallisuusjärjestelyt, jotta salassa pidettävien tietoja paljastuisi kohdeorganisaatiosta.

Kolmas tutkimuskysymykseni tarkasteli sitä, että löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien käyttöä tai niiden piirteitä. Vastauksena kolmanteen tutkimuskysymykseen aikaisempien tutkimuskysymysten pohjalta tarkentui, ettei organisaation tietoturvan hoidossa esiintynyt tietoturvamallien käyttöä. Myöskään tietoturvamalleille ominainen dialogi haitoista ja hyödyistä ei tullut esiin tutkimusaineistosta.



Kuvio 28. Organisaatioiden tietoturvan oikea taso

Piirteitä esiintyi kummassakin aikaisemmassa tutkimuskysymyksessä, joten vastaus tutkimuskysymykseen on, että koulutusorganisaatioiden tietoturvan hoidosta löytyy tietoturvamallien piirteitä. Tietoturvamallien, kuten myös muiden tietoturvan hyvien käytänteiden sekä tietoturvastandardi lähestymistavan tarkoituksena on ratkaista ilmeneviä tietoturvaongelmia ja täten parantaa organisaatioiden tietoturvaa.

Seuraavassa luvussa tarkastelemme saatujen tutkimustuloksien suhdetta tutkimuskirjallisuuteen ja esitellään hypoteeseja sekä arvioidaan tulosten käytettävyyttä luotettavuutta ja merkityksiä.

6 Diskussio

Tämän työn tarkoituksen ei ollut löytää uutta tietoturvateoriaa, vaan tarkoituksenani oli tutkia löytyykö koulutusorganisaatioiden tietoturvan hoidosta tietoturvamallien piirteitä tai niiden käyttöä. Lisäksi pyrkimyksenäni oli tarkastella miten tietoturvamallit näkyvät tutkittavissa organisaatioissa? ja miten organisaatiot huolehtivat tietoturvasta? Näitä tutkimuskysymyksiä tarkastelin kerätystä aineistosta Grounded Theory menetelmän avulla.

Grounded Theory eli ankkuroitu teoria laadullisen tutkimuksen analyysitekniikkana tuo jäsentyneen vastauksen selvitettäviin tutkimuskysymyksiin (ks. Hirsjärvi, Remes ja Sajavaara 2013, 224). Teorialla tarkoitetaan tietoa, joka on systemaattisesti kerätty ja analysoitu läpi tutkimusprosessin sekä tämä teoria on johdettu kerätystä datasta (ks. Strauss ja Corbin 1998, 12-13). Organisaation tietoturvan laaja-alaisuudesta johtuen lähestymme tätä kysymystä kolmesta eri osa-alueelta, joita olivat organisaatio-, ohjelmisto- ja tietoverkkotaso. Organisaatiotaso oli suurin yksittäinen osa-alue. Työyhteisön kannalta tämä taso on kaiken toiminnallisuuden määrittävä taso. Suunnitellut tietoturvatason suunnitelma-ja ohjeistusdokumentaatiot ohjaavat kaikkia organisaation toimintoja. Ohjelmistotaso on toiminnallinen taso, jolla toteutetaan suunnitteludokumentaatioiden sisällöllisiä määritelmiä järjestelmäsovellusten tietoturvalliseen toteutukseen ja käyttöön. Suurin tekijä tällä tasolla on sovellusten toiminnallisuuden ylläpito ja testaaminen. Tietoverkkotaso on toinen toiminnallinen taso. Tämän tason tärkein tehtävä on turvata tietoverkkojen häiriötön ja luotettava toiminta. Laadullisen analyysin suurin yksittäinen koodi oli tietoverkon rakenne.

Tutkielmassa käytetty tutkimusaineisto on kerätty yksilöhaastatteluin hyväksikäyttäen puolistrukturoitua teemahaastattelua. Haastatteluiden kohdejoukko valittiin hyväksikäyttämällä lumipallo-otantaa (engl. Snowball Sampling), jolloin varmistuttiin siitä, että kohdejoukko oli ammatillisesti ja työtehtävien perusteella oikea kerättävälle tutkimusaineistolle. (ks. Hirsjärvi ja Hurme 2011, 59-60)

Tutkija ei ole omaa työkokemusta organisaation tietoturvanhoidon osa-alueilta. Tietoturvaosaamiseni koostuu korkeakoulutasoisista tietoturvakursseista ja itse opituista keinoista tuottaa ja huolehtia ohjelmistojen ja tietoverkkojen tietoturvasta. Valitsin tämän tutkimusaineen

puhtaasta mielenkiinnosta. Mielestäni tutkimusmenetelmäksi sopi laadullinen tutkimusote, koska aihe-alue ja sen laaja-alaisuus oli tiedossa. Grounded Theory lähestymistavassa Strauss ja Corbin tarkoittavat termillä teoria aineistosta löytynyttä tietoa. Tämän tiedon tulee olla peräisin tutkimusaineistosta, joka on systemaattisesti kerätty ja analysoitu tutkimusprosessin kuluessa. Tämä johdos todennäköisimmin muistuttaa "todellisuutta" kokoamalla yhteen joukon käsitteitä. Tämä käsitejoukko perustuu kokemukseen tai pelkästään ajatukseen, miten asian pitäisi toimia. (ks. Strauss ja Corbin 1998, 12-13)

6.1 Organisaatioiden tietoturvamallit tietoturvanhoidon välineenä

Tietoturvamallien käyttöä organisaation tietoturvanhoidon välineenä on aikaisemmin tutkittu paljon. Tutkijat ja eri yhteisöt ovat luoneet ja ylläpitävät luvussa 3.7 esitellyillä luokittelujärjestelmillä luvussa 3.6 esiteltyjä mallikokoelmaluetteloita. Tietoturvamallien tarkoituksena on organisaatioiden tietoturvan hoitovälineenä antaa luvussa 3.3 määrittelemän mukaan kolme tärkeää etua. Lisäksi niiden tulisi luoda sidosryhmien välille yhteisen tietoturvaa käsittelevän sanaston. (ks. Yskout ym. 2008, 1)

Aineistoanalyysistä saadun tuloksen mukaan koulutusorganisaatioiden tietoturvanhoidon apuna ei ilmene organisaatio-, ohjelmisto- tai tietoverkkotasoilla tietoturvamallien käyttöä. Syinä tietoturvamalli lähestymistavan hyödyntämättömyyteen saattaa olla vaihtoehtoisten lähestymistapojen helpompi käytettävyys. Lähestymistapoina voidaan mainita pelkkien luvuissa esiteltyjen tietoturvan hallintaan luotujen viitekehysten 2.5 tai tietoturvastandardien 2.6 käyttö. Tietoturvamallein käyttämättömyyteen saattaa vaikuttaa myös luvussa 3.1 esitelty tietoturvamallien määritelmä, joka on epämääräinen. Tietoturvamallikokoelmissa esiintyy huomattavaa päällekkäisyys sekä luvussa 3.7 esiteltyjen luokittelujärjestelmätapojen erilaiset lähestymistavat saattavat olla haittaava tekijä.

Aineistoanalyysissä saadut tulokset ovat linjassa aikaisempien tutkimusten tulosten kanssa. Tietoturvamallien käyttöä tietoturvanhoidon välineinä saattaa rajoittaa myös kahdessa aikaisemmissa tutkimuksissa esiin tulleet seikat. Ensimmäisessä suoritetussa tutkimuksissa tulkittiin vuosien 1996-2006 välisenä aikana julkaistuja kirjallisuudesta löydettyjä tietoturvamalleja. Tutkimuksessa otannassa olleista 220 tietoturvamallista vain 55 % voitiin luokitella

tietoturvamalleiksi, 35 % oli ohjeita ja periaatteita sekä 10 % kuvasi prosessien toimintoja. (ks. Heyman ym. 2007).

Toisessa tutkimuksessa analysoitiin kirjallisuudesta löytyviä 38 eri tietoturvamalliluettelon tietoturvamalleja. Otannassa mukana olleista 218 tietoturvamallista luokiteltiin 50 % tietoturvamalleiksi, 20 % ohjeiksi tai toiminnoiksi, 20 % algoritmeiksi, protokolliksi tai tekniikoiksi ja loput 10 % eivät sisältäneet riittävää ratkaisua tai olivat soveltamisalan ulkopuolisia malleja. (ks. Yskout ym. 2008)

6.2 Organisaatioiden tietoturvan hoito

Organisaatioiden tietoturvan hoitoa on tutkittu valtavasti. Tämän tutkimuksen tuloksena on syntynyt luvussa 2.6 esiteltyjä kansainvälisiä standardeja ja luvussa 2.5 esiteltyjä kansainvälisiä ja kansallisia tietoturvan hoidon viitekehyksiä. Organisaatioiden tietoturvan hoito jaettiin tutkielman rajauksen (ks. Kuvio 6) mukaisesti organisaatio-, ohjelmisto- ja tietoverkkotasoihin.

Organisaatiotasolla aiempien tietoturvatutkimusten tuloksia mukaillen tulokset viittaavat siihen, että koulutusorganisaatiot hoitavat organisaatiotason tietoturvaa kaikilla luvussa 2.7.1 määrittelemillä osa-alueilla.Organisaatiotasoon vaikuttavat osa-alueet ovat luvussa 2.4 määritellyt käytettävyys, eheys, saatavuus, luottamuksellisuus, kiistämättömyys, pääsynvalvonta ja autenttisuus. Organisaatiotaso kytkeytyy organisaation tietoturvaan, joka tiedettiin jo analyysin alussa.

Tietohallinto tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.1 esittämää linjaa, jonka mukaan johto tai sen nimeämä tietoturvapäällikkö vastaa tietohallinnon vahvuudesta ja toimenkuvista.

Tietoturvataso tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvuissa 2.7.1, 2.5 ja 2.6 esittämiä linjoja. Toimintapolitiikka ja -strategia dokumentit kuuluvat tietoturvapolitiikkaan. Toinen koulutusorganisaatioista oli päivittämässä tietoturvatasoaan Katakri-standardin mukaiseksi, koska heidän yhteistyökumppaneiden kanssa käsittelemien tietojen suojaluokkataso vaatii yhteistyökumppaneilta tietoturvan auditointia. Tietoturvajärjestelmä

ja tapahtumanhallintajärjestelmä liittyvät luvussa 2.6.1 esitellyn standardin tapaan parantaa johdon sitoutumista tietoturvaan.

Arkistoinnin toteutus tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.7.1 esittämiä linjojen mukaisesti. Asiakirjahallinta ja asiakirjahallinnan tietoturvaa toteutetaan arkistolaitoksen määräysten mukaisesti(ks. Valtionvarainministeriö 2006).

Turvallisuusosaamisen ylläpito tuli esille tuloksissa ja se aikaisempien tutkimusten luvussa 2.7.1 esittelemää linjaa. Organisaation tulee varmistua, että henkilöstö on työtehtäviin soveltuvaa ja työtehtävät ovat selkeästi rajattuja. Koulutusmuodot noudattavat (ks. Valtionvarainmisteriö 2013a) esittelemiä linjoja. Luvuissa tietoturvan hallinnan viitekehykset 2.5 ja ISO/IEC 27000-standardissa 2.6.1 otetaan kantaa henkilöstön sitouttamiseen siitä lähtökohdasta, että henkilöstö sitoutuu koulutukseen omista lähtökohdistaan (ks. Hakala, Vainio ja Vuorinen 2006, 114). Hiljainen tieto käsittää organisaation työntekijöiden suulliset työohjeistukset. Nämä ohjeistukset parantavat työntekijän tietotaitoa suorittaa työtehtäviä paremmin, mutta ne voivat tahattomasti muuttua tai ne voidaan muistaa väärin. Sisäiset koulutukset pitävät sisällään suurten järjestelmien käyttöönottokoulutusta.

Tietoturvapoikkeamatilanteiden hallinta tuli esille tuloksissa aikaisempien tutkimusten (ks. Valtionvarainministeriö 2005, 6), ottaa kantaa tietoturvapoikkeamatilanteiden tapahtuma-analyysiin. Organisaation tietoturvapoikkeamiin reagointi pohjautuu tapahtuma-analyysin. Tietoturvapoikkeaman tiedottamisella on keskeinen tehtävä, jolla voidaan estää lisävahinkojen syntyminen (ks. Valtionvarainministeriö 2005, 6). Organisaatiot ovat määrittää viestintä- ja tiedotusvastuut näitä tilanteita varten, mutta näitä toimintoja ei ole vielä laajamittaisesti testattu tositoimissa.

Pääsynhallinta tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.6.1 esittelemää linjaa. Pääsynhallinta pitää sisällään käyttäjätunnusten hallinnan. Käyttäjätunnusten hallinnan tarkastuksilla, voidaan korjata puutteita henkilöhistorian hallinnassa.

Tietoliikenneturvallisuus tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.7.3 esittelemiä linjoja. Luokassa otetaan kantaa tietoverkon esisuunnittelussa luotaviin dokumentteihin.

Tietoturvan toteutuminen tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.7.1 esittelemiä ratkaisuja. Laitteiden valvonnasta vastaavat tietohallinto ja vahtimestarit. Organisaation sisällä sidosryhmät ovat velvollisia raportoimaan tietoturvauhkista.

Ohjelmistotasolla aiempien tietoturvatutkimusten tuloksia mukaillen tulokset viittaavat siihen, että koulutusorganisaatiot hoitavat organisaatiotason tietoturvaa kaikilla luvussa 2.7.2 määrittelemillä osa-alueilla. Ohjelmistotasoon vaikuttavia tietoturvan osa-alueita ovat luvussa 2.4 määritellyt käytettävyys, luottamuksellisuus ja eheys. Ohjelmistotaso kytkeytyy organisaation tietoturvaan, joka tiedettiin jo analyysin alussa.

Käytönvalvonta tuli esille tuloksista ja se noudattaa aikaisempien tutkimusten luvussa 2.7.1 esittelemiä linjoja. Käytönvalvontaan käsittävät lokitiedot tallentuvat automaattisesti ja ne sisältävät tietoja järjestelmien virhetilanteista ja tapahtumista. Aineistoanalyysin tuloksena ilmeni, etteivät organisaatiot ole ohjeistaneet tarkasti, kenen työtehtäviin kuuluu ohjelmistojen lokitietojen asetusten ja niiden sisältöjen tietojen tarkastus.

Sovelluskehityksen hallinta tuli esille tuloksista ja se aikaisempien tutkimusten luvussa 2.7.2 ja (ks. Valtionvarainmisteriö 2013a) esittämiä ratkaisuja. Sovelluskehityksen eli ohjelmistokehityksen tarkoituksen on vaikuttaa ohjelmistojen tietoturvaan. Organisaatioiden sovelluskehitys kattaa oman ja muualla tuotetun ohjelmistotuotannon. Omasta sovellustuotannosta huolimatta usein niissä tukeudutaan muiden sovellustuottajien tuotteisiin kuten tietokantoihin, ohjelmistokieliin, avoimen lähdekoodin tuotteisiin, jolloin nämä ohjelmistot ovat vain omia sisältönsä puolesta. Etuina muualla tuotetuissa sovelluksissa tuotekehitykselle on se, että ne voidaan valita tunnetuilta valmistajilta, jotka tuottavat ohjelmistot tunnetulla tekniikalla. Tuotteisiin on yleensä saatavilla automaattisia päivityksiä, jolloin organisaatioiden ei tarvitse palkata sovellusohjelmoijia.

Testausprosessi tuli esille tuloksista ja noudattaa aikaisemman tutkimuksen (Valtionvarainmisteriö 2013a) esittämiä ratkaisuja. Ohjelmistojen testaukseen organisaatiot ovat rakentaneet testausympäristöjä. Näiden tarkoituksena on ohjelmistojen toiminnallisuuden varmistaminen ja niiden turvalliseksi toteaminen. Oman sovellustuotannon etuna on, että sovelluksen haluttu toiminnallisuus on tiedossa. Muualla tuotetuista kaupallisista sovelluksista tietoturvapäivityksiä eli muutokset ajetaan suoraan tuotantoverkkoon.

Päivitykset tulivat esille tuloksista ja se noudattaa aikaisempien tutkimusten luvussa 2.7.2 ja (ks Hakala, Vainio ja Vuorinen 2006, 164-165) esittämiä ratkaisuja. Päivitysten asentamista ja testaamista helpottavat ennen päivitystä julkaisevat erodokumentit, joissa kerrotaan tulevien päivityksistä. Dokumentit perustelevat päivityspaketin tarpeen ja miksi päivitystä tarvintaan ja mitä ongelmia se korjaa.

Tietoverkkotasolla aiempien tietoturvatutkimusten tuloksia mukaillen tulokset viittaavat siihen, että koulutusorganisaatiot hoitavat organisaatiotason tietoturvaa kaikilla luvussa 2.7.3 määrittelemillä osa-alueilla. Tietoverkkotasoon vaikuttavia tietoturvan osa-alueita ovat luvussa 2.4 määritellyt käytettävyys, luottamuksellisuus ja eheys. Tietoverkkotaso kytkeytyy organisaation tietoturvaan, joka tiedettiin jo analyysin alussa.

Verkon suunnittelu ja palautus tuli esille tuloksista ja se noudattaa tutkimuksen luvuissa 2.7.3 ja 2.7.1 esittämien linjojen mukaisesti.

Verkonrakenne tuli esille tuloksista ja se noudattaa tutkimuksen liitteen A esittämiä linjojen mukaisesti.

Turvallisuuden hallintajärjestelmät tuli esille tuloksista ja se noudattaa (ks. Andreasson ja Koivisto 2013) esittämiä ratkaisuja. Kaupallisilla hallinnanvalvontaohjelmistoilla kyetään lukemaan kytkimien, tukiasemien ja reitittimien tila ja niiden asetukset.

Aineistoanalyysin tuloksena ilmenee, että koulutusorganisaatiot toteuttava organisaatiotason tietoturvasuunnitteesta pääasiallisesti luvussa 2.5 esiteltyjen tietoturvan hallinnan viitekehysten mukaisesti. Organisaatioiden tietoturvasuunnitteesta ilmenee vahvasti myös luvussa 2.6.1 esitellyn 27000-standardisarjan määrittelemä tietoturvan hallintajärjestelmän ISMS ja sen prosessimainen suunnittele-toteuta-arvio-toimi PDCA-malli toteutustapa.

Aineistoanalyysin tuloksena ilmenee, että organisaatiot toteuttavat ohjelmistotason tietoturvaa pääasiallisesti luvun 2.5 esiteltyjen tietoturvan hallinnan viitekehyksen mukaisesti. Organisaatiot ovat tehneet harkitun päätöksen luopua oman ohjelmatuotannon mallista. Tietoverkkotaso vastaa parhaiten tietoturvan viitekehysten mukaisia suosituksia.

Aineistoanalyysistä saadut tulokset ovat linjassa aikaisempien tutkimuksen linjoilla, että organisaatioiden tietoturvassa löytyy parannettavaa. Esimerkkinä Advanced Cyper Security

(ACSC) on seurannut julkisesti raportoituja haavoittuvuuksia 2001-2005 välisenä aikana ja tulokset osoittavat, että haavoittuvuuksien määrä on noussut tarkkailuvälin aikana 55 %. Näistä vain 25 % johtui käyttöjärjestelmäohjelmistojen rakenteesta ja 75 % haavoittuvuuksista aiheutui väärästä ohjelmistojen soveltamisesta. Haavoittuvuuksien määrä viittaa enemmän riittämättömään turvallisten ohjelmistotekniikoiden hyväksymiseen. (ks. Yskout ym. 2006)

Hewlet-Packardin 2011 teettämää tutkimuksessa selvitettiin organisaatioiden käyttöoikeuksien hallintaa. Tutkimukseen otokseen osallistuneista organisaatiosta 68 %:ssa sisäisistä tietoturvahyökkäyksistä johtui työntekijöistä, joiden työtehtävät olivat muuttuneet tai heille oli annettu tavallista laajemmat käyttö-oikeudet. Ponemon Instituten tuottamassa The Insecurity of Priviledged Users - tutkimuksessa, jossa otantana oli 5500 eri maista olevaa IT- ja tietoturvajohtajaa kävi ilmi, että 52 %:lla vastanneilla oli rajoittamaton pääsy heidän työnkuvan edellyttämättömiin luottamuksellisiin tietoihin ja näistä 60 % raportoi tutkineensa heille kulumattomia luottamuksellisia tietoja silkasta uteliaisuudesta. (ks. Andreasson ja Koivisto 2013, 107)

6.3 Tietoturvamallien käyttö ja piirteet organisaatioiden tietoturvan hoidossa

Tietoturvamallit ovat olleet erittäin suosittu tutkimuskohde 15 viimeisen vuoden aikana. Tutkijat ja eri yhteisöt ovat luoneet ja ylläpitävät luvussa 3.6 esiteltyjä mallikokoelmaluetteloita, joita on luotu luvussa3.7 esitellyillä eri luokittelujärjestelmillä. Organisaatio-, ohjelmisto- ja tietoverkkotaso kytkeytyy organisaation tietoturvan hoitoon, joka tiedettiin jo analyysin alussa. Analyysin tuloksena tarkentui aikaisemmassa luvussa 6.1, että koulutusorganisaatiot eivät käytä tietoturvamalleja tietoturvan hoidon välineenä. Tietoturvamallien piirteitä esiintyy organisaatioiden tietoturvan hoidossa, koska ne ovat vaihtoehtoinen tapa hallita organisaation tietoturvaa. Muita vaihtoehtoisia tapoja on esiteltyjen luvuissa tietoturvan hallintaan luotujen viitekehysten 2.5 tai tietoturvastandardien 2.6.

Organisaatiotasolla tietoturvamallit eivät ota tarkkaa kantaa tietoturvatason, arkistoinnin toteutuksen, tietoturvallisuuspoikkeamatilanteiden hallintaan sekä tietohallinnon, koska näistä

osaa ovat valitun tietoturvallisuuslähestymistavan, kansallisten lakien tai säädöksien määräämiä asioita. Malliajattelussa oletetaan, että organisaatioiden johto on toteuttanut tietoturvasuunnitteludokumentaatiot ennen tietoturvamallien mahdollista käyttöönottoa tai ne toteutetaan tietoturvamallien käyttöönoton yhteydessä.

Turvallisuusosaamisen ylläpito tuli esille tuloksissa ja se aikaisempien tutkimusten luvussa 2.7.1 ja C esittelemää linjaa.

Tietoliikenneturvallisuus tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.7.3 ja C esittelemää linjaa.

Pääsynhallinta tuli esille tuloksissa ja se noudattaa aikaisempien tutkimusten luvussa 2.6.1ja C esittelemää linjaa.

Tietoturvaohjeistus ja yleisohjeistus tulivat esille tuloksissa. Ne eivät vastaa aikaisempien tutkimusten luvuissa 3.1, 3.3 ja 3.5 esiteltyä tietoturvamalli lähestymistavan dokumentaatioita. Niiden sisällöstä ilmenee kuitenkin tietoturvan hoidon piirteitä.

Ohjelmistotasolla aiempien tietoturvatutkimusten tuloksia mukaillen tulokset viittaavat siihen, että koulutusorganisaatiot hoitavat organisaatiotason tietoturvaa kaikilla luvussa 2.7.2 määrittelemillä osa-alueilla.

Käytönvalvonta tuli esille tuloksista ja se noudattaa aikaisempien tutkimusten luvussa 2.7.1 esittelemiä linjoja.

Sovelluskehityksen hallinta tuli esille tuloksista ja se aikaisempien tutkimusten luvussa 2.7.2, (ks. Valtionvarainmisteriö 2013a) ja D esittämiä ratkaisuja.

Testausprosessi tuli esille tuloksista ja noudattaa aikaisemman tutkimisen (Valtionvarainmisteriö 2013a) ja D esittämiä ratkaisuja.

Päivitykset tulivat esille tuloksista ja se noudattaa aikaisempien tutkimusten luvussa 2.7.2, (ks Hakala, Vainio ja Vuorinen 2006, 164-165) ja D esittämiä ratkaisuja.

Tietoverkkotasolla aiempien tietoturvatutkimusten tuloksia mukaillen tulokset viittaavat siihen, että koulutusorganisaatiot hoitavat organisaatiotason tietoturvaa kaikilla luvussa 2.7.3

määritelemillä osa-alueilla.

Verkon suunnittelu ja palautus tuli esille tuloksista ja se noudattaa tutkimuksen luvuissa 2.7.3, 2.7.1 ja E esittämillä ratkaisuilla.

Verkonrakenne tuli esille tuloksista ja se noudattaa tutkimuksen liitteen A ja E esittämiä ratkaisuja.

Turvallisuuden hallintajärjestelmät tuli esille tuloksista ja se noudattaa (ks. Andreasson ja Koivisto 2013) ja E esittämiä ratkaisuja.

Aineistoanalyysissä saadut tulokset ovat linjassa tietoturvamallien käyttöä ohjelmistojen suunnitteluun tehdyn tutkimuksen tuloksia. Tutkimus kartoitti tietoturvamallien käyttöä ohjelmistojen suunnitteluun ja se toteutettiin KU Leuven yliopiston ohjelmistoarkkitehtuuri kurssin yhteydessä. Kohdejoukkona oli maisteritason opiskelijoita, jotka muodostivat 32 kahden hengen tiimiä. Tutkimuksessa suoritettiin kuusi tehtävää, joista sattumanvaraisesti puolet tapahtui ilman tietoturvamalleja. Tuloksena tässä tutkimuksessa oli, ettei tutkimuksessa pystytty osoittamaan tietoturvamallien käytön parantavan ohjelmistojen tietoturvaa tai ohjelmistosuunnittelijoiden tuottavuutta. Luvussa **??** esitellyn tietoturvamallien tarkoitus ei täyty nykyisillä tietoturvamalleilla. Tämä johtuu tutkimuksen päätelmien mukaan mahdollisesti siitä, että mallien dokumentaation laatu ei ole optimaalinen. Välittämättä käytetyistä keinoista ryhmät päätyivät samantyyliseen ratkaisuun. (ks. Yskout, Scandariato ja Joosen 2015)

6.4 Tutkimuksen luotettavuus ja validiteetti

Tutkielman tutkimusaineisto on kerätty yksilöhaastatteluin hyväksikäyttäen puolistrukturoitua teemahaastattelua. Teemahaastattelun luotettavuutta voidaan tarkastella tutkimusprosessin eri vaiheista. Luotettavuuteen vaikuttavia seikkoja ovat käsite-ja sisältövalidius, haastateltavien valinta, haastateltavista johtuvat virheet, siirtämistarkkuus, muuttujien muodostus vaihe ja tekemämme johtopäätökset. Teemahaastattelun reliaabelisuutta ei voida tarkastella, koska haastattelutilanteet ovat ainutkertaisia ja se, että saman henkilön haastatteleminen toistamiseen muuttaisi tutkimusaineistoa keinotekoisemmaksi. (ks. Hirsjärvi ja Hurme 2011, 128-130)

Tutkielman aiheen valinnan yhteydessä oli selvää, että tutkimushaastattelut kohdennettiin vain korkeakouluorganisaatioihin, koska tiesimme, että näihin oli ylipäätään mahdollista päästä tekemään tietoturva-aiheista tutkimusta. Tutkimuksen haastateltavien kohdejoukko valittiin heidän ammatillisten sekä työtehtävien perusteella lumipallo-otanta menetelmää hyväksikäyttäen. Otannassa hyväksikäytetään haastateltavien avainhenkilöiden ammattitaitoa ja tietämystä siitä, ketkä henkilöt kuuluvat oikeaan kohdejoukkoon kerättävälle tutkimusaineistolle (ks. Hirsjärvi ja Hurme 2011, 58-60). Tutkimuksen otantametelmästä huolimatta kerätyissä tutkimusaineistoissa ilmeni pienen harhan mahdollisuus. Tämä harha johtuu kohdejoukon ammatillisesta työtehtävien vastuualueen rajauksista. Harha ilmenee vastuualueen ulkopuolisien tietoturvan hoitoon liittyvien käytänteiden sen hetkisenä parhaana tietämyksenä.

Tutkielman haastatteluissa käytetyn kysymysrungon teema-alueluettelon kysymykset olivat pääasiassa teoriataustasta heränneitä käsitteellisiä kysymyksiä, jotka muodostuivat teoreettisten pääkäsitteiden ympärille. Kysymysten asetteluun vaikutti myös organisaation tietoturvan tarkasteleminen organisaatio-, ohjelmisto- ja tietoturvatasojen mukaisti. Organisaation tietoturva olisi muuten ollut liian laaja-alainen. Käsitevalidiutta heikensi mielestäni se, että käytin haastatteluissa pelkästään teoriatausta löytyneitä termejä niiden määritellyissä muodoissa, kun taas haastateltaville oli muodostunut organisaation sisäinen käsitteistö, joka ei aivan täydellisesti vastannut kirja käsitteitä.

Haastattelun sisältövalidiutta heikensi se, ettei haastattelurunkoon valittuja alustavia kysymyksiä testattu esihaastatteluilla. Tästä huolimatta en muokannut haastatteluiden kuluessa alustavia kysymyksiä, vaan haastatteluista saamani kokemuksen perusteella, varauduin seuraavissa haastatteluissa esittämään useampia tarkentavia lisäkysymyksiä. Näillä toimenpiteillä mielestäni saavutin aineistoteorian sisältövalidiuden.

Haastatteluissa kerätyn teoria-aineistoon vaikuttavista virheistä voidaan mainita haastattelijasta ja haastateltavista johtuvia virheitä. Haastattelijasta johtuvina virheinä voidaan mainita haastattelijan kokemattomuus haastatteluihin, mutta luonnollisin vaihtoehto haastattelun toteuttajaksi oli tutkielman tekijä. Ensimmäisiä haastatteluja tehdessä havaitsin virheitä kysymystekniikassa, tämä johtui siitä, että pysyin liian tiukasti teemaluettelon alueella. Tein tämän huomion kuunnellessani nauhoituksia ensimmäisen haastattelun jälkeen. Haastattelu-

tilanteessa muistiinpanoja tehdessä tein huomion, että liiallinen muistiinpanoihin ja tarkentavien kysymyksiin keskittyminen, haittasi haastateltavien seuraamista ja toisinpäin useita tärkeitä tarkentavia kysymyksiä jäi kysymättä, koska niitä ei ollut kirjoittanut niitä muistiin paperille. Tästä tilanteesta johtuen tutkimusaineistosta saattoi hävitä tärkeää tietoa. Tämä saattaa vaikuttaa aineiston laadulliseen sisältöön.

Tutkielman aihe-alueen arkaluontoisuudesta johtuen haastateltavat peittelivät tietämystään ilmeistä, eleistä ja sanoista päätellen. Esimerkkinä tällaisista sanallisista tilanteista oli jatkokysymyksiin vastaamatta jättäminen tai keskustelun siirtäminen toisaalle. Haastattelutilanteissa tehdyt muistiinpanot ns. kehon kielelliset viestit eli ei-kielellisistä viesteistä voidaan mainita haastattelijoiden jäykkyys haastatteluiden alussa. Tämä johtui ilmeisesti pöydällä olleen tallentimen esillä olosta. Haastatteluiden edetessä haastateltavat jäykkä istuma-asento vaihtui rennompaan asentoon. Haastattelutilanteessa useampi henkilö kuitenkin teki lisäliikkeitä, kuten tarkkaili kelloa tai napsutteli mustekynää haastattelutilanteessa.

Aineiston siirtämistarkkuus taattiin käyttämällä haastatteluiden tallennusvälineistönä digitaalista tallenninta, josta aineiston litteroitiin tarkasti haastattelunauhoitteiden mukaisesti. Poikkeuksena täydelliseen litterointiin oli, ettei täytesanoja ja taukoja otettu huomioon. Tähän päätökseen vaikutti se, ettei kysymysrunkoa lähetetty etukäteen haastatteluun osallistuneille.

Grounded Theoryn analyysivaiheen muuttujien muodostusta eli käsite- ja sisältövalidiutta paransi se, että suoritimme käsitteiden ja luokkien laadullista analyysia katselmointien yhteydessä tutkielman ohjaajien kanssa. Ankkuroitu teorialla tarkoitetaan tietoa, joka on systemaattisesti kerätty ja analysoitu läpi tutkimusprosessin sekä tämä teoria on johdettu kerätystä datasta (ks. Strauss ja Corbin 1998, 12-13).

6.5 Pohdinta ja jatkotutkimus

Tänä päivänä koulutusorganisaatiot ajetaan entistä tiukemmille taloudellisesti ja henkilöstö menoissa pyritään säästämään kaikilla sen osa-alueilla. Koulutusorganisaatiot ovat tehneet tietoturvan hoidolliset strategiset päätökset aikaisemmin ja tarkastavat tietoturvallisuuteen vaikuttavia päätöksiä keskipitkällä tai pitkällä aikavälillä (ks. Hakala, Vainio ja Vuorinen

2006, 7).

Tarkasteltaessa vaatimuksia, jos koulutusorganisaatioiden päättäisivät soveltaa tätä lähestymistapaa.Lähestymistavassa oletetaan, että organisaatiossa olisi laadittuna turvallisuussuunnitelmat ja politiikkadokumentit tai heidän tulisi suunnitella käyttöönottovaiheessa ne uudelleen. Organisaatioiden tietoturvan hoidon avuksi suunnitellut tietoturvamallit vaatisivat käyttöönottovaiheessa paljon henkilöresursseja, koska henkilöstön tulisi läpikäydä kaikki käytettävät tietoturvamallit. Valittaessa haluttuja malleja, tulee huomioida niiden käyttäytyminen, rajoitukset ja niihin liittyvät turvallisuutta koskevat periaatteet. Periaatteisiin vaikuttaa se, millä luokitusjärjestelmälähestymistavalla halutut tietoturvamalli on luotu, jos valmiita malleja halutaan soveltaa eri luokittelujärjestelmistä. Organisaatiot voivat myös muokata malleja ja täten paremmin mallintamaan niitä omaan järjestelmäarkkitehtuuriin.

Tietoturvamallien käytöstä saatavina hyötyinä voitaisiin mainita. Asiantuntijat voisivat tunnistaa, nimetä ja keskustella tietoturvaongelmista ja ratkaista niitä jäsennellysti. Niiden tarkoituksena olisi dokumentoida organisaatioiden järjestelmäasiantuntijoiden ja ylläpitäjien hiljainen tieto dokumentaatioon, jolloin ne loisivat organisaation sisälle yhtenäisen sanaston.

Organisaatioissa tietoturvan hoidon vaatimukset tulevat haasteellisimmiksi ja vaatiman aina vain enemmän huomiota järjestelmän ylläpitäjiltä. Tähän vaikuttaa tietotekniikan monimuotoisuus, joka näkyy nykypäivän järjestelmistä uusina eri viestinnän ominaisuuksina. Tämä kehitys vaatii melkoisesti lisää asiantuntemusta ei-toiminnalliselta tietoturvavaatimukselta.

Organisaation tietoturvan hoidon tason on määriteltävä ottaen huomioon organisaatioiden toimintaympäristöt. Toimintaympäristöön vaikuttavia ulkoisia tekijöinä ovat kansalliset ja kansainväliset lait sekä viranomaismääräykset. Sisäisinä tekijöinä voidaan mainita organisaation toimintapolitiikassa määrittelemät säännöt.

Tietoturvan hoitamiseksi organisaation tulee tunnista sen kriittiset varat, joita se haluaa suojella. Tällaisten aineellisia tai fyysisiä varoja voi olla tietovarat tai taloudelliset tiedot. Näiden joutuminen asianosattomien hallintaan aiheuttaisi sellaisia kustannuksia, että ne tekisivät vahinkoa organisaatiolle. Yleensä tällaisia varoja ovat lakien nojalla suojeltaviksi määritettyjä tietoja kuten tiedonhallinnan ja henkilötietojen aiheuttamat tietosuojariskit tai muita organisaatiolle strategisesti tärkeitä tietoja. Organisaation tulee tunnistaa näihin varoihin kohdistu-

via hyökkäys mahdollisuuksista aiheutuvia uhkia. Todellisten uhkien tunnistamisen jälkeen, niihin pitää löytää järjestelmistä haavoittuvuus, jos tällaista uhkaa ei tunnisteta. Tällöin uhka ei ole tietoturvaongelma ja tällaisiin uhkiin varautuminen tekee tietoturvan hoidosta tehotonta ja kallista.

Tietoturvan hoidossa ilmenevinä tietoturvamallin piirteitä ilmenee kaikkialla organisaation määrittelemissä uhka haavoittuvuuspareissa, joita organisaatio yrittää suojata tietoturvan keinoin. Tietoturvan hoitoa voidaan tehostaa käyttämällä siinä apuna tietoturvamalleja. Mallien tarkoituksena auttaa ratkaisemaan tietoturva ongelma, esittämällä kysymyksiä tietoturvan tarpeellisuudesta ja millaisia tietoturvaominaisuuksia on lisättävä, jotta suojattavat varat olisivat turvassa.

Jatkotutkimuksen aiheita voisi olla laadullisen tai määrällisen tutkimuksen keinoin selvittää, kuinka korkeakouluorganisaatioiden tietohallinnon ja tiedekuntien/tieteenalojen tietoturvatasojen yhtenäisyys, eli vastaavatko nämä organisaation tietoturvasuunnitelmissa määriteltyä tasoa. Toisena jatkotutkimus aiheena voisi tarkastella tietoturva-aiheesta tietohallinnon, tiedekuntien ja tieteenalojen tietoturvakäsitykset. Kolmantena jatkotutkimusaiheena voisi tarkastella tiedekuntien välisten ohjelmistoprojektien tietoturvan hallinta.

Lähteet

Alexander, C. 1979. *The timeless way of building.* Nide 1. New York: Oxford University Press.

Alexander, C. 2002. *Book two: The Process of Creating Life.* Nide 10. Berkeley, CA: Center for Environmental Structure.

Alexander, C., S. Ishikawa ja M. Silverstein. 1977. *A pattern language: towns, buildings, construction.* Nide 2. Oxford University Press, USA.

Alvi, A.K., ja M Zulkernine. 2011. "A Natural Classification Scheme for Software Security Patterns". *Dependable, Autonomic and Secure Computing, IEEE International Symposium on* (Los Alamitos, CA, USA): 113–120.

Alvi, Aleem Khalid, ja Mohammad Zulkernine. 2011. "A natural classification scheme for software security patterns". Teoksessa *Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on,* 113–120. IEEE.

Andreasson, A., ja J. Koivisto. 2013. *Tietoturvaa toteuttamassa.* Helsinki: Tietosanoma.

Bandara, A., H. Shinpei, J. Jurjens, H. Kaiya, A. Kubo, R. Laney, H. Mouratidis, A. Nhlabatsi, B. Nuseibeh, Y. Tahara ym. 2010. "Security patterns: Comparing modeling approaches".

Bell, D.E., ja L.J. LaPadula. 1973. *Secure computer systems: Mathematical foundations.* Tekninen raportti. DTIC Document.

Berners-Lee, T. 1989. "Information management: A proposal". Viitattu 20. tammikuuta 2013. `http://www.w3.org/History/1989/proposal.html`.

Blakley, B., C. Health ja Members of The Open Group Security Forum. 2004. "Technical Guide G031". Viitattu 13. huhtikuuta 2013. `https://www2.opengroup.org/ogsys/catalog/G031`.

Blakley, B., ja C. Heath. 2004. "Introduction to Security Design Patterns: Security Design Patterns".

Brand, S. L. 1985. *DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria (Orange Book).* Viitattu 15. kesäkuuta 2015. `http://csrc.nist.gov/publications/history/dod85.pdf`.

Brewer, D.F.C., ja M.J. Nash. 1989. *The Chinese wall security policy,* 206–214.

A Comparison of Commercial and Military Computer Security Policies. 1987.

Coad, P., ja E. Yourdon. 1991. *Object-oriented design.* Nide 92. Yourdon Press.

Communities–Commission, European, ym. 1991. *ITSEC: Information Technology Security Evaluation Criteria (Provisional Harmonised Criteria, Version 1.2, 28 June 1991).*

Crowley, E. 2003. "Information system security curricula development". Teoksessa *Proceedings of the 4th conference on Information technology curriculum,* 249–255. ACM.

Dougherty, C., K. Sayre, Seacord R., D. Svoboda ja K. Togashi. 2009. *Secure Design Patterns.* Tekninen raportti CMU/SEI-2009-TR-010. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University. Viitattu 20. kesäkuuta 2013. `http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9115`.

Edwards, J., ja R. Bramante. 2009. *Networking Self-Teaching Guide.* Wiley.

Fernandez, E. B., ja R. Pan. 2001. "A pattern language for security models".

Fernandez-Buglioni, E. 2013. *Security patterns in practice: designing secure architectures using software patterns.* John Wiley & Sons.

Gamma, E., R. Helm, R. Johnson ja J. Vlissider. 1995. "Design patterns: elements of reusable object-oriented software". *Reading: Addison Wesley Publishing Company.*

Glaser, B., ja A. Strauss. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research.* Aldine Publishing Company, Hawthorne, NY.

Gollman, D. 2009. *Computer Security.* John Wiley & Sons.

Goodyear, M. 1999. *Enterprise System Architectures: Building Client Server and Web Based Systems.* CRC.

Hafiz, M., P. Adamczyk ja R.E. Johnson. 2007. “Organizing security patterns”. *Software, IEEE* 24 (4): 52–60.

Hafiz, M., ja R.E. Johnson. 2006. “Security patterns and their classification schemes”. *University of Illinois at Urbana-Champaign Department of Computer Science, Tech. Rep.*

Hakala, M., M. Vainio ja O. Vuorinen. 2006. *Tietoturvallisuuden käsikirja.* Docendo.

Hasheminejad, S.M.H., ja S. Jalili. 2009. “Selecting Proper Security Patterns Using Text Classification”. Teoksessa *Computational Intelligence and Software Engineering, 2009. CiSE 2009. International Conference on,* 1–5. IEEE.

Hazif, M., P. Adamczyk ja R. Johnson. 2007. “Organizing Security Patterns Software”. Viitattu 20. huhtikuuta 2013. doi:10.1109/MS.2007.114. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=4267603&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4267603.

Heath, H., ja S. Cowley. 2004. “Developing a grounded theory approach: a comparison of Glaser and Strauss”. Viitattu 29. maaliskuuta 2015. http://www.sciencedirect.com/science/article/pii/S0020748903001135.

Heyman, T., K. Yskout, R. Scandariato ja W. Joosen. 2007. “An Analysis of the Security Patterns Landscape”. Teoksessa *Proceedings of the Third International Workshop on Software Engineering for Secure Systems,* 3. IEEE Computer Society. doi:10.1109/SESS.2007.4.

Hilliard, Rich. 2000. “Ieee-std-1471-2000 recommended practice for architectural description of software-intensive systems”. *IEEE, http://standards.ieee.org* 12:16–20. Viitattu 20. elokuuta 2013. http://scholar.google.fi/scholar?hl=fi&q=IEEE+1471%E2%80%932000&btnG=.

Hirsjärvi, S., ja H. Hurme. 1991. *Teemahaastattelu.* 5. painos. Helsinki: Yliopistopaino.

———. 2011. *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Helsinki: Gaudeamus.

Hirsjärvi, S., P. Remes ja P. Sajavaara. 2013. *Tutki ja kirjoita.* 18. painos. Porvoo: Tammi.

ISO. 2008b. “ISO/IEC 15408–3:2008. Information Tecnology Security Techniques. Evaluation Criteria for IT Security. Part 3: Security Assurance Components.” Viitattu 4. syyskuuta 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413.

———. 2009. “ISO/IEC 15408–1:2009. Information Tecnology Security Techniques. Evaluation Criteria for IT Security. Part 3: Security Assurance Components.” Viitattu 4. syyskuuta 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50341.

Juvonen, A. 2011. “Poikkeuksien havaitseminen WWW-palvelinlokidatasta. Pro gradu-tutkielma”. Viitattu 15. syyskuuta 2013. https://jyx.jyu.fi/dspace/handle/123456789/38455.

Kettula, E. 1999. *Tietoverkkojen tietoturva. 2., uudistettu painos.* Edita.

Kienzle, D., M. Elder, D. Tyree ja J. Edwards-Hewitt. 2002. *Security patterns template and tutorial.* Viitattu 20. kesäkuuta 2013. doi:10.1.1.131.2464. http://www.scrypt.net/~celer/securitypatterns/template%20and%20tutorial.pdf.

Kienzle, D.M., ja M.C. Elder. 2002. “Security patterns for web application development”. *University of Virginia technical report.*

Kienzle, D.M., M.C. Elder, D. Tyree ja J. Edwards-Hewitt. 2002. “Security patterns repository version 1.0”. *DARPA, Washington DC.*

Kodituwakku S., R., P. Bertok ja L. Zhao. 2001. “Aplrac: A pattern language for designing and implementing role-based access control”.

Kumar, A., ja E.B. Fernandez. 2012. “Security Patterns for Intrusion Detection Systems”. Viitattu 15. huhtikuuta 2016. http://www.laccei.org/Security%20Patterns%20for%20Intrusion%20Detection%20Systems.pdf.

Laaksonen, M., T. Nevasalo ja K. Tomula. 2006. *Yrityksen tietoturvakäsikirja: ohjeistus, toteutus ja lainsäädäntö.* Edita.

Lamminmäki, T. 2008. “Tietoturvamallien hyödyntäminen sovelluskehityksessä. Pro gradu-tutkielma”. Viitattu 15. heinäkuuta 2016. https://jyx.jyu.fi/dspace/bitstream/handle/123456789/18415/URN_NBN_fi_jyu-200804241390.pdf?sequence=1.

Laverdière, M.A., A. Mourad, A. Hanna ja M. Debbabi. 2006. “Security design patterns: Survey and evaluation”. Teoksessa *Electrical and Computer Engineering, 2006. CCECE'06. Canadian Conference on,* 1605–1608. IEEE.

Leeuw, K.M.M. de, ja J. Bergstra. 2007. *The history of information security: A comprehensive handbook.* Elsevier Science.

Mowbray, T.J., W.J. Brown ja H.W. McCornnick III. 1998. *AntiPatterns: Refactoring Software, Architectures, and Projects in Crisis.* John Wiley & Sons, Hoboken, NJ.

Newstaff, Inc. 2013. “Information Security Services”. 12. helmikuuta. http://www.newstaff.com/criteria/tcsec/index.html.

Oikeusministeriö. 1999. “Henkilötietolaki 523/1999: Valtion säädöstietopankki. Ajantasainen lainsäädäntö”. Viitattu 5. maaliskuuta 2015. http://www.finlex.fi/fi/laki/alkup/1999/19990523.

Ruohonen, M. 2002. *Tietoturva.* Docendo.

Scandariato, R., K. Yskout, T. Heyman ja W. Joosen. 2008. “Architecting software with security patterns”. *CW Reports.*

Schumacher, M. 2003. *Security engineering with patterns: origins, theoretical models, and new applications.* Nide 2754. Springer.

Schumacher, M., E. Fernandez-Buglioni, D. Hybertson, F. Buschmann ja P. Sommerlad. 2006. *Security Patterns: Integrating security and systems engineering.* Nide 7. Wiley.

Schumacher, Markus, ja Utz Roedig. 2001. “Security Engineering with Patterns”. Viitattu 22. tammikuuta 2013. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.58.6519.

Sciences, National Academy of. 1991. “Computer at Risk: Safe Computing In the Information Age: System Security Study Committee. Computer Science and Telecommunication Board. Comissinon on Physical Science, Mathematics, and Applications”. Viitattu 20. tammikuuta 2013. http://www.nap.edu/openbook.php?record_id=1581.

SecurityArchitecture), OSA (Open. 2013. *Library Overview.* Viitattu 10. helmikuuta. http://www.opensecurityarchitecture.org/cms/library.

Seppänen, O. 2012. *Tietoturvallisuuden kehittäminen yrityksessä.* Laurea-ammattikorkeakoulu.

SFS, Suomen Standardisointiliitto. 2006. “Kumottu 07.01.2015 ISO/IEC 17799:fi: Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje”. Viitattu 20. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID9/1/667.html.stx.

Shoch, J.F., ja J.A. Hupp. 1982. “The “worm” programs—early experience with a distributed computation”. *Communications of the ACM* 25 (3): 172–180.

Shostack, A. 2008. “Experiences threat modeling at microsoft”. Teoksessa *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK.*

Smith, H., B. 2012. *Empirically Developing a Security Test Pattern Catalog using a Grounded Theory Approach.* North Carolina State University.

Standards, National Institute of, Technology (NIST) ja National Security Agency (NSA). 1992. “Federal Criteria for Information Technology security - Draft Version 1.0”.

Strauss, A., ja J. Corbin. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques.* Sage Publications, Inc.

———. 1998. *Basics of Qualitative Research: Techniques abd Procedures for Developing Grounded Theory.* 2. painos. Sage Publications, Inc.

Suomen Standardisoimisliitto, SFS. 2008a. “Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008)”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/108846.html.stx.

Suomen Standardisoimisliitto, SFS. 2008c. “ISO/IEC 15408–2:2008. Information Techology. Seurity Techniques. Evaluation Criteria for IT security. Part 2:Security Functional Components.” Viitattu 4. syyskuuta 2013. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414.

———. 2009a. “ISO/IEC 27000:2009. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto. ISO/IEC 27000:2009. Information technology. Security techniques. Information security management systems. Overview and vocabulary”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/139961.html.stx.

———. 2009b. “Informatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita: Information technology. Security techniques. Information security management system implementation guidance”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/157873.html.stx.

———. 2010. “Informatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita: Information technology. Security techniques. Information security management system implementation guidance”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/170408.html.stx.

———. 2011a. “Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta: Information technology. Security techniques. Information security risk management”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/228613.html.stx.

———. 2011b. “Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmä auditointiohjeet: Information technology. Security techniques. Guidelines for information security management systems auditing”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/228608.html.stx.

———. 2013. “Informaatioteknologia, Turvallisuus, Tietoturvallisuuden hallintakeinojen menettelyohjeet: Information technology. Security techniques. Code of practice for information security controls”. Viitattu 26. kesäkuuta 2016. https://sales.sfs.fi/fi/index/tuotteet/SFS/ISO/ID2/2/270200.html.stx.

Trowbridge, D., W. Cunningham, M. Evans, L. Brader ja P. Slater. 2004. “Describing the enterprise architectural space”. *MSDN, June*.

Valtionvarainministeriö. 2005. “VAHTI 3/2005 Tietoturvapoikkeamatilanteiden hallinta”. Viitattu 20. tammikuuta 2015. https://www.vahtiohje.fi/c/document_library/get_file?uuid=7c31a8bf-2aca-47be-b918-334bd5db9675&groupId=10128.

———. 2006. “Asiakirjahallinnan tietoturvallisuutta koskeva ohje 5/2006”. Viitattu 25. tammikuuta 2016. https://www.vahtiohje.fi/c/document_library/get_file?uuid=4f7868bb-8f96-46f6-8b90-666928b4f32a&groupId=10128&groupId=10229.

———. 2007. “Tietoturvallisuuden tuloksia: Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 2/2007”. Viitattu 28. elokuuta 2013. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/name.jsp.

———. 2008a. “Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta. VAHTI 1/2008”. Viitattu 15. syyskuuta 2013. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf.

———. 2008b. “Valtionhallinnon tietoturvasanasto, VAHTI 8/2008”. Viitattu 6. heinäkuuta 2016. https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto.

Valtionvarainmisteriö. 2008b. “VAHTI 8/2008 Valtionhallinnon tietoturvasanasto: Määritelmät V, VAHTI”. Viitattu 20. tammikuuta 2016. https://www.vahtiohje.fi/web/guest/maaritelmat-v.

———. 2013a. “VAHTI 1/2013 Sovelluskehityksen tietoturvaohje”. Viitattu 20. tammikuuta 2016. https://www.vahtiohje.fi/web/guest/vahti-1/2013-sovelluskehityksen-tietoturvaohje.

Valtionvarainministeriö. 2013b. “Voimassa olevat tietoturvaohjeet ja-määritykset”. Viitattu 15. syyskuuta 2013. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp.

Whitman, M.E., ja H.J. Mattord. 2011. *Principles of information security.* 4. painos. Cengage Learning.

Willis, H. 1970. “Ware. Security controls for computer systems (U): report of defense science board task force on computer security”. *The RAND Corporation, Santa Monica, CA (Feb. 1970).* http://csrc.nist.gov/publications/history/ware70.pdf.

Yoder, J., ja J. Barcalow. 1998. “Architectural patterns for enabling application security”. *Urbana* 51:61801.

Yoder, Joseph, ja Jeffrey Barcalow. 1998. “Architectural patterns for enabling application security”. Viitattu 16. lokakuuta 2014. http://www.idi.ntnu.no/emner/tdt4237/2007/yoder.pdf.

Yskout, K., T. Heyman, R. Scandariato ja W. Joosen. 2006. “A System of Security Patterns”. *Catholic University of Leuven, Belgium, Dept. of Computer Science, Technical Report CW-469.*

———. 2008. “Security patterns: 10 years later”. *CW Reports.*

Yskout, Koen, Riccardo Scandariato ja Wouter Joosen. 2015. “Do security patterns really help designers?” Teoksessa *Proceedings of the 37th International Conference on Software Engineering-Volume 1,* 292–302. IEEE Press.

Zachman, J.A. 1987. “A framework for information systems architecture”. *IBM systems journal* 26 (3): 276–292.

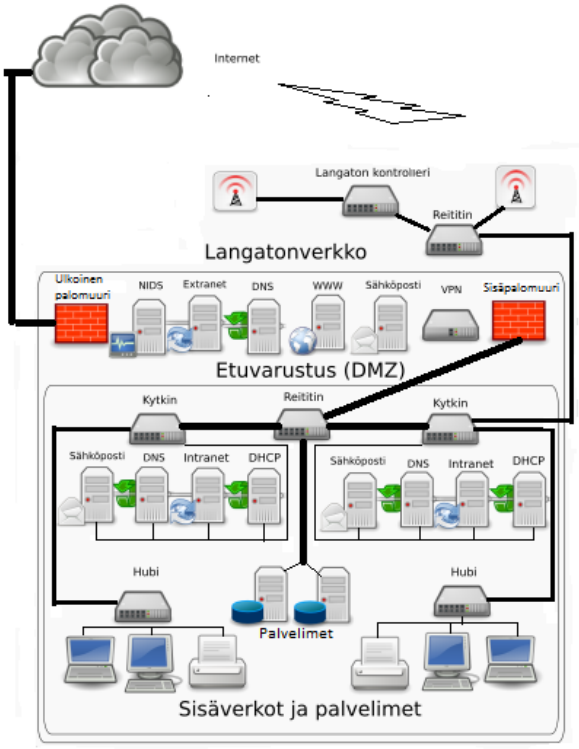
Liitteet

A Organisaation tietoverkon komponenttikuvaukset

Tietoverkon suojaaminen

Organisaation tietoverkko (ks. Kuvio29) tulisi eristään Internetistä liitteen A palomuurilla. Tämän lisäksi sisäverkko tulisi jakaa turvallisuusdokumentaation määrittelemien turvallisuusvaatimusten mukaisesti eri verkkoalueisiin siten, että eri turvallisuusvaatimusten toiminnoille ja laitteille olisi omat verkkoalueet ja näiden välistä liikennettä rajoitettaisiin liitteessä A esitellyillä kytkimillä tai liitteen A palomuureilla. (ks. Hakala, Vainio ja Vuorinen 2006, 185–186)

Organisaation sisäverkon verkkoalueet voidaan jakaa etuvarustukseen reitittimien sekä kytkinten avulla tarvittavan moneen erilliseen sisäverkkoon. Sisäverkossa tietokoneet voidaan kytkeä HUBien avulla kytkimille, jotka mahdollistavat myös usean VLAN (engl. Virtual Local Area Network) Virtuaaliverkon määrityksen esimerkiksi opiskelijoille, henkilökunnalle ja vierailijoille. Luvussa A esitellyn DHCP-palvelimen tarkoituksena on mahdollistaa HUBien ja palvelimien määrän lisäämisen, koska niiden avulla laitteistolle voi tehdä TCP/IP-asetukset siten, että työasemille ei anneta IP-osoitetta verkkoasetuksissa, vaan työasemat pyytävät IP-osoitteen ja aliverkonpeitteen palvelimelta. Etuvarustukseen (engl. Bastion network), jota kutsutaan myös DMZ (Demilitarized Zone) E.1 sijoitetaan pakettisuodattimena toimivan reitittimen segmentteihin kaikki organisaation Internetiin liittyvät palvelut, joiden tietoturvataso sallii, että niitä vastaan voidaan hyökätä ja niiden toimimattomudesta ei ole suoranaista vaikutusta organisaation toimintaan. Tällaisia palveluja ovat WWW, Luvussa A esitelty DNS, luvussa A määritelty Extranet ja sähköpostipalvelin. DNS palvelimen tarkoituksena etuvarustuksessa on vain huolehtia etuvarustukseen kuuluvien laitteiden DNS-nimistä. (ks. Hakala, Vainio ja Vuorinen 2006, 184–186)



Kuvio 29. Organisaation tietoverkon kuvaus

Reititin

Reititin (engl. Router) ohjaa sille tulevat viestit eteenpäin, niiden kohdeosoitteiden perusteella. Viestien suunta määräytyy reititystaulukon tietojen perusteella. Reitittimet jataan kahteen ryhmään, joita ovat staattiset sekä dynaamiset reitittimiin, niiden reititystaulukon määrittelyn perusteella. Staattisissa reitittimissä reititystaulukko on ennalta määriteltyjä, kun taas dynaamisissa reitittimissä reititystaulukkoa muutetaan muilta reitittimiltä reititysprotokollien avulla saatujen tietojen perusteella. (ks. Ruohonen 2002, 58)

Staattisessa reitittimessä vastaanotettua viestiä verrataan reititystaulukossa esiintyviin verkkotunnuksiin. Tunnusten ollessa samat viesti lähetetään eteenpäin reititystaulukon tietojen mukaisesti, kun taas tunnistamattomat verkkotunnukset reititin lähettää eteenpäin oletusreitittimen tiedoilla. Oletusreitittimen oletusreitti voi ohjata viestin lähiverkosta esimerkiksi Internetiin. (ks. Ruohonen 2002, 59)

Dynaamisessa reitityksessä reititintaulukoon on alussa merkitty tiedot vain reitittimeen kyt-

ketyistä verkoista. Tämän jälkeen reititin lähettää oman reititintaulukon tiedon suoraan siihen kytketyille reitittimille, jotka puolestaan vastaavat sille lähettämällä vastauksena takaisin niiden reititintaulukon tiedot. Verkon muuttuessa reitittimet päivittävät verkon tilan ja täten jokainen reititin muuttaa automaattisesti reititystaulukkoaan. Tämän takia reitittimet pystyvät lähettämään viestit aina kustannustehokkaasti eteenpäin. (ks. Ruohonen 2002, 60)

Kytkin

Organisaatioiden Extranet tietoverkkoihin on nykyään kytkimiä saatavilla pienistä työryhmistä aina järeisiin ydinverkkokytkimiin. Kytkimet ovat periaatteessa yksikertaisia Plug and Play laitteita, joihin ei välttämättä tarvitse tehdä määrityksiä, mutta ne pitävät sisällään myös hallintaominaisuuksia. Määrityksen muuttamiseen organisaatio tarvitsee hallintaohjelmiston sekä ylläpitohenkilöstöä, jotta ne saadaan toimimaan halutulla tavalla. (ks. Hakala, Vainio ja Vuorinen 2006, 227)

Yleisimpiä kytkintekniikoita ovat puskurilla varustetut (engl. Cross Bar Switch), jaetulla muistilla (engl. Shared Memory Switch) ja suurnopeus väylällä varustetut (engl. High Speed Bus Switch) kytkimet. Vanhimmat ja edullisimmat kytkimet ovat toteutettu porttikohtaisella puskuroinnilla, jolloin liikennöivien pakettien kehys tallennettaan ennen sen lähettämistä vastaanottajan porttiin. Jaetun muistin kytkimet ovat yleensä asynkronisia kytkimiä, joilla voidaan välittää eri nopeuksista Ethernet-segmenttien välistä liikennettä. Nämä kytkimet sallivat myös jonotuksen(engl. Queuing) optimoinnin, joka voidaan määrittää kahdella eri tavalla. Vaihtoehdot ovat (engl. Cut Through) jossa bitit lähetettään ilman jonokäsittelyä ja (engl. Store and Foreward), jossa liikenne lähetetään halutun suuruisina kehyksinä. Suurinopeusväylässä kytkentäväylät käsittelevät siirrettävät kehykset nopeammin kuin laitteet kykenevät niitä tuottamaan. (ks. Hakala, Vainio ja Vuorinen 2006, 227)

Palomuuri

Palomuurin (engl. Firewall) tarkoituksen on eristää organisaation tietoverkko Internetistä sekä erotella suunnitellusti sisäverkon osia toisistaan siten, että ei-haluttujen pakettien pääsy näiden verkkojen välillä estetään. Palomuurin avulla voidaan myös kontrolloida mitä lii-

kennettä sallitaan eri verkon osien ja laitteiden välillä. Nykyisin on myös suositeltua, että yksittäiset työasematkin suojataan palomuurilla, jos työasemaa käytetään organisaation sisäverkon lisäksi ulkopuolisissa verkoissa. Palomuuria valittaessa on otettava huomioon mihin tarkoitukseen sitä halutaan käyttää, koska on olemassa useita erilaisia palomuurimalleja, kuten pakettisuodatin palomuureja, tilallisia palomuureja ja Proxy-pohjaisia palomuureja. (ks. Andreasson ja Koivisto 2013, 71) Organisaation tietoturvapolitiikan osana luodaan palomuuripolitiikka. Tässä dokumentissa määritelmän palomuurien vastuut (ks. Seppänen 2012, 27).

Pakettisuodatinpalomuurit (engl. Packet Filter Firewall) tarkoituksena on estää sellaisten pakettien läpipääsy, jotka ovat sen suodatussääntölistan vastaisia (engl. ACL, Access Control List). Suodatus tapahtuu saapuvasta ja lähtevästä verkkoliikenteestä ja toimii siten, että pakettien otsikkotietoja verrataan suodatussääntölistassa määriteltyihin säännöstöihin ja niiden käsittelyssä käytetyt vaihtoehdot ovat hyväksy (engl. Allow or Accept), kiellä (engl. Deny) ja hylkää (engl. Drop). Tarkoituksena on estää pakettien mahdollisesti sisältämien viruksia ja sovelluskohtaisia hyökkäyksiä päädy järjestelmiin. (ks. Ruohonen 2002, 65-66)

Tilallisia palomuureja (engl. Statefull Firewall), joiden tarkoituksena on suodattaa saapuvaa ja lähtevää pakettiliikennettä, perustuen sen kauttakulkevien yhteyksien tilanteisiin, josta palomuurin on kyettävä määrittääkseen pakettien hyväksyntä tai hylkäys, eli onko tulevat paketit vastauksia tietokoneiden lähettämiin paketteihin tai lähetetäänkö ne suojatun verkon tietokoneiden avaamilla yhteyksillä. Tilallista palomuuria käytettäessä ulkopuoliset tietokoneet eivät kykene aukaisemaan yhteyttä suojatussa verkossa olevaan tietokoneeseen. (ks. Ruohonen 2002, 70)

Proxy-pohjaisia palomuureja (engl. Proxy-based firewall), joiden tarkoituksena on suodattaa saapuvaa ja lähtevää verkkoliikennettä. Verkkoliikenteelle voidaan suorittaa tarvittaessa virustarkastuksia. Tällä palomuurityypillä voidaan estää ei-toivottujen WWW-sivustojen latautuminen, WWW-sivuilla olevat ei toivottujen sovellusten toiminta sekä FTP-protokollan komentoja. (ks. Ruohonen 2002, 71-72)

DNS

DNS (engl. Domain Name System) järjestelmä on kehitetty auttamaan tietokoneen käyttäjän muuttamalla Internetiin kytkettyjen tietokoneiden IP-osoitteet ihmiselle helpommin muistettaviin DNS-verkkotunnuksiin. DNSn tehtävänä on selvittää käyttäjän selaimen osoiterivillе kirjoittaman verkkotunnusta vastaava palvelun IP-osoite, koska DNS-palvelimet tunnistavat kaikki tietokoneet niiden IP-osoitteiden avulla. DNS-palvelimelta saadaan vastauksen verkkotunnusta vastaavan IP- osoitteen takana olevan palvelut tai jos verkkotunnus ei ole saatavilla niin pelkkä virheilmoitus. (ks. Ruohonen 2002, 38–39) Sisäverkon DNS-palvelin määritetään orjapalvelimeksi ja se huolehtii vain sisäverkon laitteiden kyselyjen suorittamisen ja ohjaa sisäverkon ulkopuolelle suuntautuvat kyselyt etuvarustuksessa olevalle julkiselle DNS-palvelimelle. (ks. Hakala, Vainio ja Vuorinen 2006, 186)

DHCP-palvelin

DHCP-palvelimen (engl. Dynamic Host Configuration Protocol) tarkoituksen on hallita samassa verkossa olevien työasemien IP-osoitteiden jakamista. Jakaminen tapahtuu palvelimelle määritellystä osoiteavaruudesta sitten, että jokaisella työasemalla on käytössään yksilöllinen IP-osoite sekä sen käyttöikä, oletusreitittimien ja DNS-palvelimien IP-osoitteet. Kun käyttöiästä on kulunut 87,5 % työasema tekee palvelimelle pyynnön uudesta IP-osoitteesta. Hyötynä palvelimen käytöstä on se, ettei verkon mahdollisissa muutostöissä tarvitse jokaisessa tietokoneessa määrittää muutosta erikseen vaan, muutokset voidaan tehdä keskitetysti yhdestä paikasta. (ks. Ruohonen 2002, 24–25)

NIDS ja IDS

Tunkeutumisen havaitsemisjärjestelmä (Network Intrusion Detection System, NIDS) tai IDS (Intrusion Detection System) ja tunkeutumisen estämisjärjestelmät IPS (Intrusion Prevention System) on tarkoitettu lähiverkon ja sen laitteiden valvontaan. Valvonnallinen toiminnallisuus perustuu verkkoliikenteen ja järjestelmien normaalin toiminnan määrittämiseen sekä määritelmästä poikkeavien toimintojen aiheuttamien hälytysten tunnistamiseen. (ks. Andreasson ja Koivisto 2013, 190)

IDS-järjestelmiä on kehitetty kymmeniä vuosia ja niitä tutkitaan edelleen ahkerasti, koska nykyään tietoturvaa ei voida varmistaa pelkästään palomuurein ja muin tietoturvaratkaisuin. Järjestelmät jakautuvat isäntäkonetta tutkiviin (engl. host-based), jossa järjestelmä toimii yhden koneen sisällä ja verkkoa tutkiviin (engl. network based) järjestelmiin, jossa järjestelmä tutkii tietoverkon liikennettä. (ks. Juvonen 2011)

IDS voidaan jakaa niiden hälytykseen reagoinnin mukaisesti passiivisesti tai aktiivisesti toimiviin järjestelmiin. Passiivisissa järjestelmien havaitsemat poikkeamat aiheuttaa vain hälytyksen. Hälytykset kirjataan ylös järjestelmän lokiin. Useimmat käytettävät järjestelmän ovat tällaisia, koska ne eivät tällöin haitta verkon toimintaa. Aktiiviset eli IPS-järjestelmät pyrkivät loki kirjauksen lisäksi pysäyttämään havaitun poikkeaman aiheuttaman vahingot. IPS–järjestelmä kykenee toiminaan:

- Linkkikerroksella, jolloin sen avulla voidaan sulkea tiettyjä järjestelmän portteja.
- Verkkokerroksella, jolloin reitittimien ja palomuurin sääntöjä voidaan muuttaa ja täten estää verkkoliikenne ei-toivotuista IP-osoitteesta
- Siirtokerroksella, voidaan katkaista haitallisten pakettien vastaanotto
- Sovelluskerroksella, voidaan muokata järjestelmälle haitallista dataa.

Tunkeutumisen havaitsemisjärjestelmä käytön tärkeimpinä etuina pidetään sitä, että niiden avulla voidaan havaita ja mahdollisti estää järjestelmiin tulevia vielä tuntemattomia nollapäivityshyökkäyksiä (engl. Zero Day Attack). (ks. Juvonen 2011)

VPN

Organisaatio voi hyödyntää Internet-yhteyksiä eri toimipisteiden yhdysverkkona tai sallia etäyhteydenotot organisaation verkon ulkopuolelta. Etäyhteyden voi muodostaa niin sanotun suojatun tunnelin avulla eli VPN-yhteyden (Virtual Private Network) avulla, jolloin sisäisen liikenteen pääseminen julkiseen verkkoon on estetty. VPN-yhteydessä verkkoliikenne on suojattu salakirjoituksella. Toimipisteiden välinen verkkoliikenne muodostetaan organisaation reitittimien välille, jolloin reitittimet salakirjoittavat ja purkavat niiden välillä liikennöivät IP-paketit. Etäkäyttäjän ja organisaation välillä yhteys muodostetaan yksittäisen tietokoneen ja etäkäyttöpalvelimen välille. (ks. Hakala, Vainio ja Vuorinen 2006, 284–285) VPN

on yleisnimi verkkoliikenteen suojaukseen käytettävistä tekniikoista. Yleisimpinä suojaustekniikoita, joita käytetään VPN-yhteyksien kanssa, ovat luvussa esitellyt A SSL-salaus tai A IPSEC-pohjainen salaus (engl. Internet Protocol Security). (ks. Andreasson ja Koivisto 2013, 74)

SSL-salaus

SSL-salausprotokolla (engl. Secure Socket Layer) on luotu turvallisen tiedonsiirron aikaansaamiseksi. Salaus luodaan kahden koneen välille ja se toteutetaan 129-bittisellä salaustekniikalla. Protokollan tarkoituksena on turvata yhteyden luvun 2.4) luottamuksellisuus ja eheys sekä todentaa käyttäjät. SSL-varmenteen voi ostaa kansainvälisiltä sertifikaateista vastaavilta yrityksiltä. SSL-salausta voidaan käyttää HTTP (www-selaus), SMTP (sähköposti), NNTP (uutisryhmä) ja FTP (tiedostojen siirto) protokollille, jolloin nämä protokollat korvautuvat siten, että HTTP muuttuu HTTPSksi, SMPT muuttuu SSMPTksi, FTP muuttuu FTPS-protokollaksi. (ks. Hakala, Vainio ja Vuorinen 2006, 390)

SLL-salausprotokolla voidaan jakaa kättely (engl. Handshake) ja rekisteröintikerros (engl. Record Layer) protokolliin. Kättelyprotokollassa työasema lähettää palvelimelle tiedon sen hallitsemista salakirjoitusmenetelmistä. Palvelin valitsee käytettävän salausprotokollan ja lähettää työasemalle tiedon valitsemastaan salakirjoitusmenetelmästä. Tämän jälkeen työasema ja palvelin vaihtavat istuntoavaimen salakirjoitusmenetelmää hyväksikäyttäen. Tämän jälkeen työaseman ja palvelimen välillä lähetetyt viestit ovat salattuja. Rekisteröintikerros protokollassa palvelimen ja työaseman välillä lähetettävien viestien salakirjoituksessa käytetään salaisen avaimen menetelmää, jonka eheys varmistetaan tiivistefunktiolla. (ks. Hakala, Vainio ja Vuorinen 2006, 391)

IPSec

IPSec (Ip Security) salausprotokollan tarkoituksena on suojata luodussa yhteyskäytävässä lähetettyjä viestejä luvussa 2.4 esiteltyjen eheyden ja luottamuksellisuuden mukaisesti sekä todentaa käyttäjän. Salausprotokollaa voidaan käyttää kahden osapuolen välisen yhteyden salaamiseen kuljetusmoodissa. Useamman osapuolen kautta viestit voidaan kuljettaa turval-

lisesti tunnelimoodissa. (ks. Hakala, Vainio ja Vuorinen 2006, 393)

IPSec:n turvallisuuskäytänteissä (engl. Security Policy) määritellään kaikille protokollaa käyttäville laitteille turvallisuuskäytänne tietokannassa, mitä sääntöjä niiden tulee käyttää lähteville ja tuleville viesteille (engl. SPD, Security Policy Dastabase). Säännöstö käsittelee viestit valitsimien (engl. Selectors) mukaan siten, että lähtevät tai tulevat paketit hylätään, hyväksytään tai hyväksytään käsiteltäviksi salausprotokollalla. (ks. Hakala, Vainio ja Vuorinen 2006, 394)

Protokollassa välitettyjen viestien eheys varmistetaan käyttämällä tarkistussumman (engl. IVC, Integrity Check Value) tiivistettä. Tarkastussumman luomisessa käytetään hyväksi tiedettyjen viestin IP-protokollan hyötykuorman ja otsikkotietojen sisältöä. IPSec-protokolla mahdollistaa myös tapahtumien valvonnan, koska tätä tekniikkaa käytettäessä tapahtumat voidaan kirjata loki-tiedostoihin. (ks. Hakala, Vainio ja Vuorinen 2006, 395)

Intranet

Intranet on sisäverkko ja se on IP-pohjainen tietoverkko, joka toimii samalla periaatteella kun Internet. Ainoana erotuksena niiden välillä on, että Internet on kaikille avoin verkko, kun taas Intranetiin voi kirjautua sisään vain luvan saaneet käyttäjät. Organisaatioiden LAN-verkko on hyvä esimerkki tällaisesta verkosta. Intranetiä on mahdollisuus käyttää organisaation sisältä tai kirjautua siihen etäyhteyttä hyväksikäyttäen. Tällöin on mahdollisuutta käyttää organisaation sisäisen Intranetin sovelluksia Internetin välityksellä. Intranetistä käytetään nimitystä Extranet, kun organisaation sisäverkko avataan ulkopuolisille käyttäjille täysin tai osittain. Tällöin valtuutetut käyttäjät kuten asiakkaat, toimittajat, myyjä ja jne. saavat kirjautumismahdollisuuden organisaation Intranetiin. (ks. Edwards ja Bramante 2009, 7)

Intranetin eli sisäverkon riskinä pidetään haittaohjelmia, laiterikkoja, ohjelmistovirheitä sekä ulkopuolisen käyttäjän kytkeytymistä omalla kannettavalla tietokoneella vapaana olevaan tai irtikytketyn laitteen verkkoliitännän kautta sisäverkkoon. Tämä mahdollisuus voidaan poistaa ottamalla käyttöön IEEE (Institute of Electrical and Electronics Engineers) 802.1X porttiperustainen autentikointi (engl. Port Pased Authentication) standardin käytöllä. 802.1X-standardia käytetään lähi- ja langattomissa verkoissa estämään luvattomien laitteiden kyt-

keytyminen lähiverkkoon liitäntäpisteiden kautta. Tunnistaminen voidaan suorittaa Windows palvelimissa sisäänrakennetun 802.1X tuen kautta tai RADIUS-palvelinta hyväksikäyttämällä. (ks. Andreasson ja Koivisto 2013, 75–76)

RADIUS-palvelin

RADIUS-palvelin (engl. Remote Authentication Dial In User Service) tarkoituksena on tarjota keskitetty käyttäjäntunnistus tietoverkon verkkolaitteiden välille. Käyttäjän kirjautuessa palveluun RADIUS-palvelin vertaa syötetietoja, sen tietokannassa oleviin käyttäjätunnus ja salasanapariin. RADIUS-palvelimen heikkoutena on se, että asiakkaan ja palvelimen välillä tieto siirtyy suojaamattomassa tilassa, joten tätä palvelua suositellaan käytettäväksi sisäisessä tietoverkossa, jossa palveluntarjoaja voi taata verkon turvallisuuden. (ks. Edwards ja Bramante 2009, 584)

Langattomat verkot

Langattomien verkkojen toteutustekniikka perustuu radioverkkotekniikkaan, jossa erilaiset langattoman verkon laitteet voidaan yhdistää toisiinsa ilman kytkentäkaapelia. Langaton verkko voidaan liittää osaksi organisaation langallista tietoverkkoa kytkemällä langaton tukiasema verkkolaitteiden kytkennän mahdollistavaan reitittimeen. Langattomien verkkojen yleisimmät ongelmat esiintyvät luvussa 2.4) määriteltyjen käytettävyyden ja luottamuksellisuuden osa-alueilla. Luottamuksellisuuden kannalta verkot ovat erittäin alttiita tietoturvaloukkauksille. Käytettävyyteen vaikuttavia tekijöitä ovat rakennuksessa olevien kiinteiden esineiden kuten seinien aiheuttamat signaalien heijastumiset ja läpäisemättömyys, sekä muiden rakenteiden aiheuttamat signaalien taittumiset. Näiden takia verkon rakentaminen siten, että sen käytettävyyteen vaikuttavien katvealueiden poistaminen on erittäen haastavaa. Lisäksi käytettävyyttä haittaavia tekijöitä ovat lähiympäristön muut laitteet, kuten mikroaaltouunit ja eri radiotaajuuksilla toimivat laitteet. (ks. Hakala, Vainio ja Vuorinen 2006, 293–294)

B Tietoturvamallien luokittelujärjestelmät

B.1 Zachmanin kehys

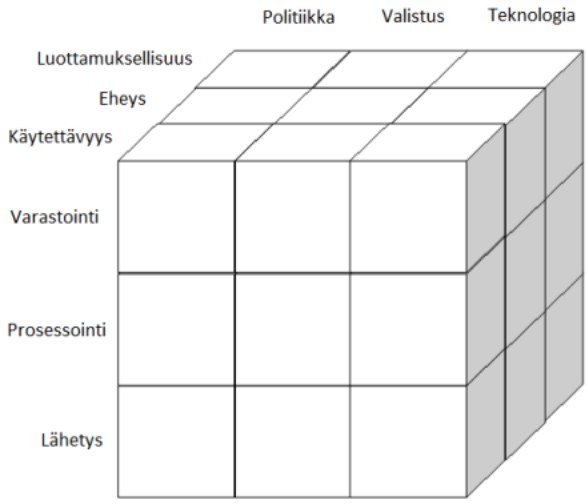
Zachmanin kehys (engl. Zachman framework) esiteltiin 1987. Luokittelumalli luotiin alun perin määrittelemään tietojärjestelmille kuvaileva kehys, jossa tietojärjestelmän kasvaneen koon ja monimutkaistumisen takia oli tärkeää ottaa käyttöön järjestelmien osien ja rajapintojen valvomiseen kehys. Kehys perustuu kaksiulotteiseen taulukkoon, jossa kuvataan riveillä tietomallien osia ja sarakkeilla arkkitehtuurisia näkemyksiä. Arkkitehtuuri on jaettu kolmeen keskeiseen osa-alueeseen, jotka ovat omistaja, suunnittelija ja ohjelmoija. Taulukossa on viisi riviä ja kuusi saraketta. Riveillä esitellään toimijat ja sarakkeilla eri toiminnot, joita ovat data (mitä?), toiminta (miten?), verkko (missä?), ihmiset (kuka?), aika (kun?) motivaatio (miksi?). (ks. Zachman 1987, 276–292) Tietoturvamallien luokitteluun tätä kehystä muutettiin lisäämällä siihen sarake, jossa käsitellään turvallisuuden näkymää (ks. Taulukko 16). Näkymässä käsitellään kaikki tietoturvamallin tasot, jotta se käsittäisi kaikki kehyksen toiminnot organisaation soveltamisalalla. Kehyksen alkuperäinen tarkoitus on käsitellä ensisijaisesti erilaisia funktionaalisia toimintoja, mutta tietoturvallisuuden ollessa ei toiminnallinen funktionaalinen ominaisuus, niin ontologiselta kannalta lisäämällä turvallisuuden näkymä tämän taulukkomuotoiseen kehykseen käyttö on ongelmallista. (ks. Hafiz ja Johnson 2006, 7-8)

	Mitä?	**Miten?**	**Missä?**	**Kuka?**	**Kun?**	**Miksi?**	**Tietoturvan näkymä**
Organisaatio malli:							
Järjestelmän malli:							
Teknologian malli:							
Yksityiskohtainen edustusto:							
Toimiva järjestelmä:							

Taulukko 16. Zachmanin kehyksen kaksiulotteinen taulukko

B.2 McCumberin kuutio

McCumberin kuutio-luokittelumallin (engl. McCuber Cube) on luonut John McCumber 1991. Luokittelumalli perustuu osittain, Commitree on National Security System (CSNN) antamiin suosituksiin. Malli tarjoaa graafisen esityksen tietoturvallisuuden arkkitehtoniseen lähestymistapaan. Malli on kolmiulotteinen 3 x 3 x 3 kuutio, jossa on 27 solua, jotka edustavat tietoturva-alueita, joihin on puututtava. Näin nykyaikainen tietojärjestelmä kyetään turvaamaan (ks. Kuvio 30), jossa on kolme ensisijaista luokkaa eli politiikka, teknologia ja valistus eli inhimilliset tekijät. Toinen akseli käsittää tietoturvallisuuden luottamuksellisuuden, eheyden ja käytettävyyden näkökulman. Kolmas akseli pitää sisällään varastoinnin, siirron ja prosessoinnin tilat. Mallin teknologian, eheyden ja varastoinnin leikkauspisteiden välillä vaaditaan ohjausta ja suojaustoimenpiteitä, joissa käsitellään tarvetta käyttää tekniikoita suojaamaan tietojen koskemattomuutta niiden säilytyksen aikana. Yksi tällainen ohjaustoimenpide voisi olla, kun järjestelmä havaitsee tunkeutumisen. Ohjaustoimenpiteen tulisi suojata tiedon eheys ja varoittaa tietoturvavastaavia mahdollisista kriittisistä tiedon muuttamisista. (ks. Crowley 2003, 1-29), (ks. Whitman ja Mattord 2011, 15–16)



Kuvio 30. Graafinen kolmiulotteinen lähestymistapa tietoturvallisuuden arkkituuriin

B.3 CIA-malli

CIA-mallissa (engl. CIA-model) kuvaillaan ITCEC (European Communities, 1991) määrittelemän kolmen tietoturvan luokituksen mukaisen luvussa 3.7 määritellyn luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Tämä luokitus perustuu näiden kolmen luokituksen hyväksikäyttöön, jolloin voidaan tiedon ylimäärän sekä käsittelyvirheiden poistolla parantaa käytettävän tiedon eheyttä ja täten parantaa järjestelmän ohjelmistojen ja tietojärjestelmien turvallisuutta. Etuna tästä luokittelusta on se, että tietoturvamallien luokittelussa voidaan hyväksi käyttää tietoturvan standarditermistöä. Ongelmalliseksi tämän luokituksen tekee se, ettei näitä kolmea tietoturvan luokitusta voida erillistää toisistaan ja useimmat tällä luokituksella luodut tietoturvamallit kuuluisivat määrittämättömälle harmaalle alueelle, jos niiden osuutta tutkittaisiin yksityiskohtaisesti. (ks. Hafiz ja Johnson 2006, 16) Lisäksi CIA-mallia hyväksikäyttäen on luotu useita tietoturvamalleja, jotka kattavat enemmän kuin yhden tietoturvan luokituksen näkökulman ja kolme sellaista mallia, jotka kattavat koko määritysalueen. (ks. Hafiz, Adamczyk ja Johnson 2007, 54)

B.4 Rakenteellinen ja menettelymalli

Rakenteellinen ja menettelymalli (engl. Structural and Pucedural Model) rakenteen tarkoituksena ei ollut olla virallinen tietoturvamallien luokitusmalli. Tutkijat eivät väitä sen olevan täydellinen, mutta tutkijat pitivät tärkeänä, että heidän kehittämänsä mallit seurasivat jotain perusrakennetta. Luokittelumallilla tietoturvamallit jaetaan kahteen rakenteelliseen ja menettelymalli päätyyppiin. Rakenteelliset mallit pitävät sisällään suunnittelumalleja, jotka sisältävät rakenteellisia ja dynaamisen vuorovaikutuksen. Näitä malleja käytetään lopputuotteen toteutuksessa. Menettelymalleja käytettiin parantamaan ohjelmistojen turvallisuuskriittisiä prosesseja ja ne vaikuttavat usein myös organisaationalisiin tai hallinnollisiin kehityshankkeisiin. (ks. D. Kienzle ym. 2002, 6–7) Tätä luokittelumallia hyväksikäyttäen on luotu yksittäinen tietoturvamalliarkisto (ks. D.M. Kienzle ym. 2002, 6–7).

B.5 Suojatun ja saatavilla olevan järjestelmän mallit

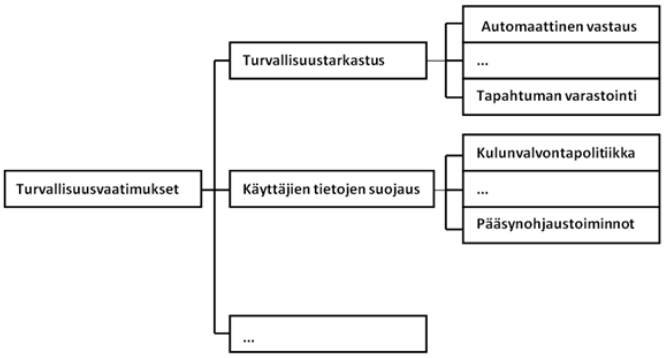
Suojatun ja saatavilla olevan järjestelmän mallien (engl. The Available and The Protected System model) tarkoituksena on parantaa järjestelmän ohjelmistojen suunnittelua ja tietoturvaa. Luokittelumallissa käytetään genetiiviseen sekvenssiin (engl. Genetive Sequences) perustuvaa algoritmia. Sekvenssimallin on kehittänyt Christopher Alexander ja se on esitelty 2002 ilmestyneessä kirjassa Book 2: The Process of Creating Life (ks. C Alexander 2002). Algoritmi on resepti luoda malli, jossa sekvenssi kertoo järjestyksen, miten tietoturvamallia haetaan tietoturvamalliluettelosta. Mallien haku tapahtuu aloittamalla korkeantason tietoturvamalleista, joissa määritellään sovellettavia toimenpiteitä. Toiseksi valinnan jälkeen tietoturvamallista ei luovuta, kolmanneksi tehdään tunnettuja valintoja ja lopuksi kukin vaihe käsittää valinnan, jossa tietoturvamallia sovelletaan, jos askel on todennäköinen. (ks. Blakley, Health ja The Open Group Security Forum 2004, 13-15)

Tavoitteena on saada entistä joustavampi lähestymistapa tietoturva- ja arkkitehtuurimalleille. Lähestymistapa koostuu pääsekvenssistä sekä kaksiosaisesta alasekvenssistä, joilla tietoturvamallit voidaan jakaa suojattuihin ja saatavilla oleviin järjestelmämalleihin. Saatavilla olevat järjestelmämallit sisältävät rakennesuunnittelumalleja, joilla kyetään rakentamaan järjestelmiä, jotka tarjoavat käyttäjille ennustettavissa olevan keskeytymättömän käyttöoikeuspalvelun ja resurssit. Suojatunjärjestelmän mallit sisältävät malleja jotka helpottavat suojaamaan järjestelmän arvokaita resursseja luvattomalta käytöltä, muuttamiselta ja luovuttamiselta. Pääsekvenssin vaiheita ovat, valitaan tietoturvamallit, jotka täyttävät organisaation järjestelmän toiminnalliset tavoitteet. Toiseksi käytetään saatavilla olevan järjestelmän järjestystä (engl. Apply the Protected System Sequence). (ks. Blakley, Health ja The Open Group Security Forum 2004, 13-15)

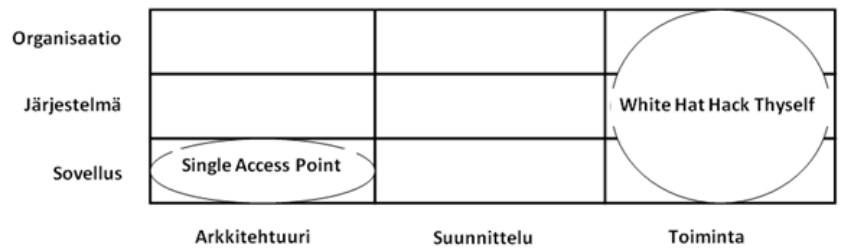
Hyötyinä luokittelujärjestelmän käytöstä on, että sillä kyetään luokittelemaan tietoturvamallit ohjelmistoarkkitehtuurin mukaisesti. Haittapuolia luokittelujärjestelmässä on, että siinä esitetään liian laaja osiointotapa ja tämän takia käyttäjien on hankala hallita tätä luokitustapaa. (ks. Hafiz ja Johnson 2006, 6)

B.6 Moniulotteinen lähestymistapa

Moniulotteisessa lähestymistavassa käytetään hyväksi ohjelmistosuunnittelun tarkoitus ja soveltamisalan mukaista luokitusta, joka on esitelty Desing Patterns: Elements of Reusabele Object-Oriented Software (ks. Gamma ym. 1995) teoksessa. Tietoturvamallit luokitellaan näiden määriteltyjen eri lähestymistapojen mukaisesti. Moniulotteisella tavalla voidaan yhdistää arkkitehtuuri, suunnittelu ja toiminta elinkaaren mukaisesti ja organisaatio, järjestelmä ja sovellukset kerroksellisuuden mukaisesti luokiteltuun lähestymistapaan. Tällöin lähes kaikki organisaatiossa käytettävät tietoturvamallit voitaisiin luokitella järjestelemällä ne kahteen kategoriaan. Lähestymistavassa tietoturvamalleja voitaisiin helposti laajentaa aina tarpeen mukaan. Luokittelemalla tietoturvamallit elinkaaren mukaisesti, voidaan jakaa vasemmalta alkaen arkkitehtuuri, suunnittelu ja toiminnallisuuden tasoille (ks. Kuvio 31). Käyttämällä kerroksellisuutta hyväksi, voidaan tietoturvamallien käyttöä havainnollistaa helposti (ks. Kuvio 32) (ks. Schumacher 2003, 16–17)



Kuvio 31. Moniulotteisen lähestymistavan mukainen elinkaariluokittelu



Kuvio 32. Moniulotteisen lähestymistavan mukainen kerroksellinen luokittelu

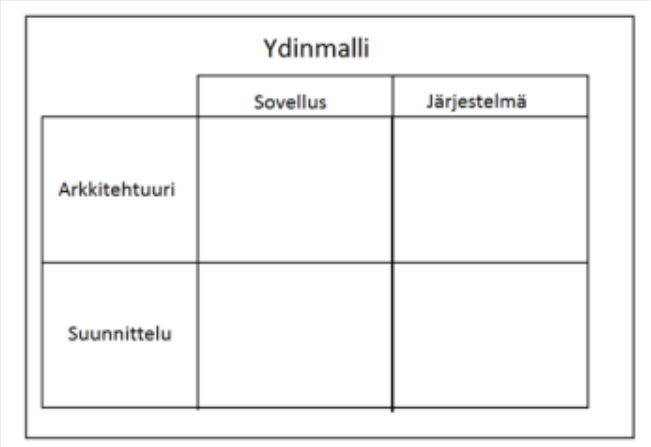
B.7 Soveltuvuuteen perustuva luokitus

Soveltuvuuteen perustuva luokitus (engl. Classification Based on Applicability) esiteltiin 2004. Luokituksessa tietoturvamallit jaetaan kahteen pääryhmään, perustuen suljettuihin ja käytettävissä oleviin järjestelmiin. Suljetut järjestelmät luokitus suojelee järjestelmän arvokkaita resursseja luvattomalta käytöltä, luovuttamiselta ja muuttamiselta. Käytettävissä olevien luokituksen järjestelmämallit muodostavat vakaan halutun ja keskeytymättömän palveluiden ja resurssien käytön. Hyötynä luokittelusta on, että se luokittelee tietoturvamallit ohjelmistoarkkitehtuurin mukaisesti. Haittapuolena luokittelusta on, että se on liian laaja, joten käyttäjien on hankala hallita tätä luokitustapaa. (ks. Hafiz ja Johnson 2006, 6)

B.8 Tietoturvamallien kartoitus ydin ja ei ydin malleihin

Tietoturvamallien kartoitus ydin ja ei ydin malleihin (engl. Security Patterns Inventory Core and Non-Core Patterns) luokittelussa ydinmalleja voidaan käyttää arkkitehtuurin ja suunnittelun yhteydessä ja niiden tarkoituksena on lisätä suunnittelun turvallisuutta. Ei-ydinmalleja ovat sellaiset mallit, jotka ovat liian korkealla abstraktion tasolla, ettei niitä voi liittää suunnittelun apuvälineeksi tai ne ovat täytäntöönpanotasolla, kuten salaus (engl. Encryption), Kerberos tai hajautetun verkon tiedostojärjestelmä (engl. Andrew File System (AFS)). (ks. Yskout ym. 2006, 9), (ks. Joseph Yoder ja Jeffrey Barcalow 1998, 3)

Ydinmallit voidaan jakaa järjestelmä tai ohjelmistosovelluksissa vaikuttaviin tietoturvamalleihin. Mallit jakautuvat myös soveltuvuutensa mukaisesti arkkitehtuuri tai suunnitteluvaiheisiin. Malli on sovellusarkkitehtuurinen, jos se käytöllä on koko järjestelmän laajuiset vaikutukset, kun taas sovellussuunnittelumallin käytöllä on paikallinen vaikutus (ks. Kuvio 33). (ks. Yskout ym. 2006, 10)



Kuvio 33. Graafinen kolmiulotteinen lähestymistapa tietoturvallisuuden arkkituuriin

B.9 STRIDE

STRIDE luokittelumallin toiminnallisuus perustuu yksiulotteiseen taulukkoon, jossa uhkat luokitellaan ainutlaatuisiin elementtiryhmiin. Mallin nimitys saadaan sen elementtiryhmien alkukirjainten mukaisesti, joita ovat:

- Huijaus (engl. Spoofing)
- Peukalointi (engl. Tampering)
- Kieltäminen (engl. Repudiation)
- Palvelujen estäminen (engl. Denial of Service)
- Etuoikeuksien nosto (engl. Elevation of Privilege)

Luokitusmallia käytetään uhkien mallinnukseen ja mallinnus tapahtuu 1999 kehitetyllä turvallisen kehityksen elinkaari (engl. Security Development Lifecycle) mallinnustapamenetelmää hyväksikäyttäen. Mallin alkuperäisenä tarkoituksena on ollut ohjelmistoarkkitehtuurin uhkien ryhmittely. Ryhmittely tapahtuu siten, että arkkitehtuurissa ilmeneviä uhkia verrataan jokaista edellä mainittua elementtiä vasten. (ks. Shostack 2008, 4-5)

Tietoturvamalleja luokitellessa STRIDE:ssä ilmenee samat ongelmat, kun muissakin taulukkomuotoisissa luokitteluissa, joten sekään ei kykene ratkaisemaan kysymystä, miten luokitella sellaiset tietoturvamallit jotka eivät mahdu sen yksittäiseen luokituksen sisälle. Tämän takia luokittelumalliin on lisätty ylimääräinen kenttä kaikki (engl. All), johon kerätään kaikki

useamman elementtiryhmän alueella vaikuttavat tietoturvamallit. Tällä muutoksella luokittelumalli käsittelee kaikkia tietoturvamalleja tasavertaisesti. (ks. Hazif, Adamczyk ja Johnson 2007, 58)

B.10 Taulukkomuotoinen luokittelujärjestelmä malleille

Taulukkomuotoinen luokittelujärjestelmä tietoturvamalleille (engl. Tabular Classification Scheme for Patterns) tämän luokitusjärjestelmän esitysasu perustuu luvussa 3.7 ja liitteessä B.1 esiteltyyn Zahmanin kehykseen, IEEE 1471–2000 standardiin (ks. Hilliard 2000), Andersen Consulting Enterprise Information Architecture (ks. Goodyear 1999) ja testilähtöiseen kehityksen (engl. Test-driven Development), tämä luokittelujärjestelmä esiteltiin 2004. Järjestelmän tarkoituksena on auttaa tietoturva-mallikirjoittajia järjestämään olemassa olevia malleja ja tunnistamaan järjestelmästä dokumentoimattomia alueita. Sarakkeet tässä taulukossa jaetaan tarkoitukseen (Why?), dataan (What?), toimintoon (How?), ajoitukseen (When?), verkostoon (Where?), ihmiseen (Who?) ja pistelaskutaulukkoon (Scorecard), mutta niiden järjestys voi olla mielivaltainen. Käyttämällä taulukon tapaa järjestää organisaation vaativia järjestelmiä voidaan luoda arkkitehtuuritasojen tärkeistä päätöksistä malleja ja käytäntöjä (ks. Taulukko 17). Luokittelujärjestelmän taulukon rivit jaetaan kokonaisarkkitehtuurin viiteen laajaan organisaation kattavaan näkökulmaan (ks. Trowbridge ym. 2004), näitä päänäkökulmia ovat:

Päänäkökulma	**Työnkuva**	**Toiminto**	**Esimerkki tietoturvamallista**
Liiketoiminta arkkitehtuuri (engl. Business architecture)	toimitusjohtaja (engl. Chief Executive Officer (CEO))	Funktio	Turvallisuuden tarpeiden tunnistaminen (engl. Security Needs Identification). Luo yhteyden yrityksen omaisuuden ja turvallisuustarpeiden välille
Integraatio arkkitehtuuri (engl. Integration architecture)	Yritysarkkitehti	Funktio	Kertakirjautuminen (engl. Single Sign On). Sallii käyttäjän käyttää useita palveluja kirjauduttuaan verkkoympäristöön.

... jatkuu seuraavalla sivulla

Päänäkökulma	Työnkuva	Toiminto	Esimerkki tietoturvamallista
Sovellus arkkitehtuuri (engl. Application architecture)	Arkkitehtuuri	Data	Virheiden havaitseminen ja korjaaminen (engl. Error Detection and Correction). Ylimäärään lisätty tietoja virheiden havaitsemisesta ja korjauksesta.
		Funktio	Yksi pääsypiste (engl. Single Access Point). Sallii vain yhden merkintä jokaiselle prosessille.
	Suunnittelu	Tietoverkko	Tilallinen palomuuri (engl. Stateful Firewall). Suodatetaan liikennettä perustuen tilan tietoon.
		Data	Salattu varastointi (engl. Encrypted Storage). Palvelimen tila on suojattu salauksella.
		Funktio	Palvelimen hiekkalaatikko (engl.Server Sandbox). Palvelimet toimivat siten, että vähiten etuoikeuksia omaavan asiakkaiden toimintaa rajoittamalla.
	Kehitys	Funktio	Turvattu tietorakenne (engl. Safe Data Structure). Muistipuskurit sisältävät tietoa joka on tarkastettava ennen ajoa.
		Testi	Valkohatut hakkaavat itseään (engl. White Hats hack Thyself). Testataan järjestelmän turvallisuutta hyökkäämällä siihen itse.

... jatkuu seuraavalla sivulla

Päänäkökulma	Työnkuva	Toiminto	Esimerkki tietoturvamallista
Toiminnan arkkitehtuuri (engl. Opreational architecture)	Arkkitehti	Funktio	Alhaalla roikkuva hedelmä (engl. Low Hanging Fruit). Hankitan nopeita ratkaisuja, kun yritetään suunnitella järjestelmä uudelleen, joka kerta kuin haavoittuvuus löytyy.

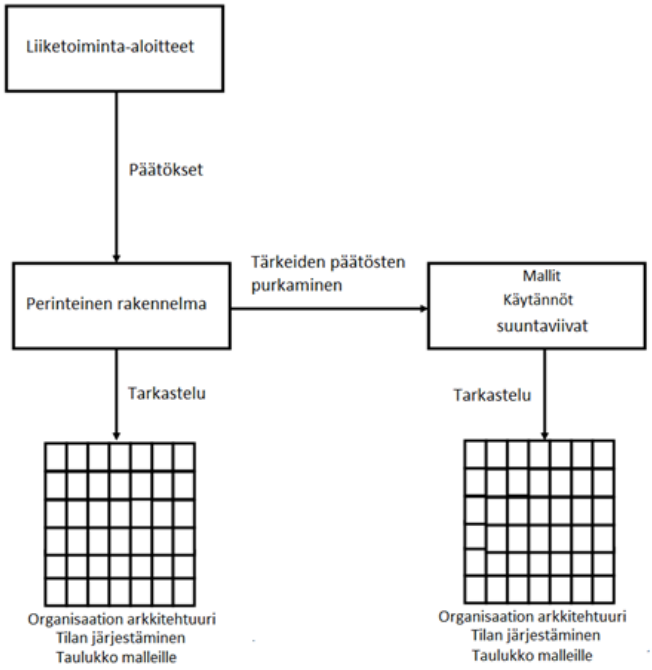
Taulukko 17: Tietoturvamallien luokittelu Microsoftin taulukkomuotoisella luokittelujärjestelmällä

Organisaation tietoturvamallien luokittelu taulukkomuotoisella luokittelujärjestelmällä auttaa suurien tietoturvamallikokoelmien hahmottamista. (ks. Hafiz ja Johnson 2006, 11) Luokittelujärjestelmän käyttö auttaa käyttäjiä ymmärtämään organisaation kokonaisarkkitehtuuria ja täten he kykenevät tarkastelemaan taulukon solujen avulla järjestelmässä esiintyviä ongelmakohtia ja löytämään ratkaisuja niihin. (ks. Kuvio 34) on esitelty perinteisen arkkitehtuurimallin ja mallilähestymisarkkitehtuurin ero. (ks. Trowbridge ym. 2004, 10)

Luokittelujärjestelmän huonona puolena mainitaan, että useita tietoturvamalleja ei voida määrittää yhteen soluun, vaan se ulottuu koko sarakkeen kaikkiin riveihin. Esimerkkinä tästä on testisarakkeessa olevat mallit, jota ei voida tarkastella yhdetä näkökulmasta. (ks. Hafiz ja Johnson 2006, 9)

B.11 Six-Sigma luokittelulähestymistapa tietoturvamalleille käyttäen toivottavia ja ei toivottavia ominaisuuksia

Six-Sigma luokittelulähestymistapa tietoturvamalleille käyttäen toivottavia ja ei toivottavia ominaisuuksia (engl. Six-Sigma Approach for the Classification of Security Patterns Using the Desirable and Undesirable Properties) tarkoituksena on ehdottaa toivottavia ominaisuuksia, joilla etsitään tietoturva- ja suunnittelumalliluetteloista puutteita (ks. Laverdière ym.



Kuvio 34. Perinteisen arkkitehtuurimallin ja malliarkkitehtuurin ero

2006, 1607). Toivotut ja ei-toivotut ominaisuudet ovat:

- Ei toivotut ominaisuudet
  - Alimääritellyt mallit. Malleja jotka ovat toteutettu epätäydellisesti tai ne eivät sisällä tarpeellisia ominaisuuksia. Tällaiset mallit aiheuttavat järjestelmissä täytäntöönpano ongelmia
  - Harvinaiset mallit. Kuvaavat harvinaista toimintaa, jotta sitä voitaisiin käyttää yleisesti eri tilanteissa.
- Toivotut ominaisuudet
  - Oikea abstraktiotaso. Tietoturvamallia voidaan käyttää eri yhteyksissä ilman uudelleenmäärittelyä
  - Täydellisyys. Tietoturvamalli on valmis ja se on oikein määritelty
  - Helppokäyttöisyys. Mallin tulisi soveltua mahdollisimman vähin vaikutuksin sitä hyödyntäviin ohjelmiin
  - Uudelleenkäytettävyys. Mallin tulisi olla helposti sovellettava ja käytettävä ei yhteyksissä ja sen tulisi olla helppokäyttöinen muiden mallien kanssa

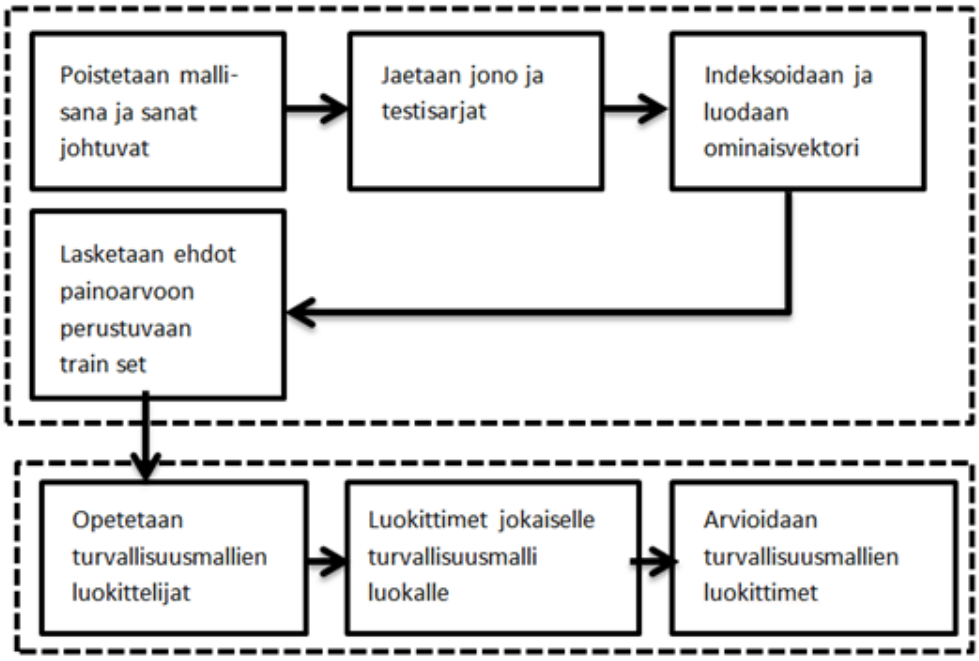
- Alustariippumattomuus. Tietoturvamalli on määritelty ilman tiettyä ohjelmistokieltä tai käyttöjärjestelmää
- Malliriippumattomuus. Malli on riippumaton ja sitä voidaan käyttää itsenäisellä tavalla
- Kuvauksen täydellisyys. Mallin rakenne on sellainen, että siinä on vaaditut tiedot.

B.12 Oikean tietoturvamallin valitseminen käyttäen tekstiluokitusta

Oikean tietoturvamallin valitseminen käyttäen tekstiluokitusta (engl. Selecting Proper Security Pattern Using Text Classification) on halvempi ja yksinkertaisempi luokittelujärjestelmä, kuin muut lähestymistavat. Etuina on sen riippumattomuus tietoturvamallien kuvauksista ja se perustuu oppimisentekniikkaan, joka parantaa tarkkuutta ja automatisoi tietoturvamallien valinnan sekä menetelmä kykenee tunnistamaan samankaltaisuuksia tietoturvamalleista. Automaattiseen tunnistukseen on ehdotettu ontologista ja muodollista lähestymistapaa. Oikean mallin valitseminen käyttäen tekstiluokitusta tietoturvamallipohjat erotellaan vektorimuotoon siten, että jokaisen mallipohjan sana edustaa yhtä paikkaa vektorissa. On useita tapoja määritellä sanan painoarvo, jotta se toteuttaisi jonkun seuraavista Booleaan muodoista, jotka ovat termien taajuus (engl. Term Frequency (TF)), Term Frequency Inverted Document Frequency (TF-IDF)), Time-Frequency Correlation (TFC) ja entopia painotuksista (engl. Entopy Weighting). (ks. Hasheminejad ja Jalili 2009, 1-5), (ks. A. K. Alvi ja Mohammad Zulkernine 2011, 113–114)

On olemassa useita koneoppimisen tekniikoita, joihin voidaan soveltaa tekstinluokittamista esimerkiksi K-nearest Neighbour Classifiers (KNN), Decision Trees (C4.5), Bayesian Classifiers (Naive Bayse) ja Support Vector Machines (SVM). Luokittelun toiminnallisuuden ensimmäisenä vaiheena on poistaa ”malli” sana. Sanan poistetaan ja tällöin ”malli” sana johtuu (engl. Stemming). Seuraavaksi jokainen turvallisuusmalliluokan opetussarja (engl. Train Set) luodaan. Opetussarjan luonti perustuu etiketin luotiin, tämä tarkoittaa että jokaiseen mallipohjaan on merkitty joko +1 tai -1. Toiseksi valitaan jokaisesta luokasta opetussarjaan liittyvät mallipohjat ja niihin liittymättömät mallipohjat, nämä mallipohjat erotellaan, jonka jälkeen valitaan mallipohjista 70 % satunnaisesti. Loput mallipohjat otetaan testisarjaan (engl. Test Set). Kolmanneksi indeksoidaan ominaisuusvektori, tähän käytetään vektoriava-

ruudenmallia ja muodostetaan vektori. Tämän jälkeen luodaan luokittelijan ominaisvektori. Vektorissa kuvataan kaikki mallipohjissa toistumattomat termit ja näin muodostetaan kokoelmavektorit, jotka liittyvät opetussarjan mallipohjaan. Neljännessä vaiheessa käytetään valittua painotusmenetelmää, joilla painoarvot lasketaan. Viidennessä vaiheessa luokittelijat ovat oppineet ja voimme käyttää kaikkia koneoppimisen vaiheita tässä vaiheessa. Viimeisenä vaiheena opetetut luokittelijat arvioidaan perustuen arviointi-malliin (ks. Kuvio 35). Mallissa on suositeltavaa käyttää arviointimallina Evaluation Metrics Fucion Formula (EMFF), joka on paras oppimisentekniikka. (ks. Hasheminejad ja Jalili 2009, 1-5)



Kuvio 35. Perinteisen arkkitehtuurimallin ja malliarkkitehtuurin ero

C Organisaatiotason tietoturvamallit

C.1 Tietoturvan tarpeiden tunnistaminen organisaation varoille

Tietoturvan tarpeiden tunnistaminen organisaation varoille (engl. Security Needs Identification for Enterprise Assets) on juuritietoturvamalli kaikille organisaation tietoturvanäkökohdille. Malli auttaa ratkaisemaan kysymyksen tietoturvan tarpeellisuudesta ja mitä tietoturvan ominaisuuksia olisi lisättävä, jotta organisaation omaisuus olisi turvassa. Turvallisuusominaisuuden seikkoja ovat luottamuksellisuus, saatavuus, eheys ja vastuullisuus.

Esimerkki

Organisaatio avaa uuden sivukonttorin ja heillä on kokemusta helmien käsittelystä ja niiden varastaminen on todella suuri riski ja haluaa suojella niitä varkauksilta. Organisaatio pitää myös hallussaan tietoa heidän kokoelmista, työntekijöiden tiedoista, joita tulisi suojella luvattomalta muuttamiselta sekä poistamiselta. Joissakin tapauksissa tietoja pidetään luottamuksellisina. Miten organisaatio määrittää omaisuuden, joita heidän tulisi suojella ja minkä tyyppistä suojausta ne tarvitsevat.

Tausta

Organisaatio pitää tietoturvaa merkittävän ei-toiminnallisena vaatimuksena. Keskeiset liiketoiminnalliset tekijät ja organisaation varojen arvo ymmärretään.

Ongelma

Organisaatio joka pitää turvallisuutta erittäin tärkeänä, on suunniteltava turvallisuus huomioiden, kaikki asiat laadittujen liiketoimintasuunnitelmien mukaisesti. Organisaatiossa tulisi olla laadittuna turvallisuussuunnitelmat ja politiikkadokumentit tai heidän tulisi suunnitella ne uudelleen. Sama koskee kaikkia tietoteknisiä järjestelmiä, jotka ovat merkittäviä organisaation omaisuuseriä. Organisaatio voi joutua hyväksymään olemassa olevat tietojärjestelmät tai luoda ne uudelleen toisella arkkitehtuurilla. Määrittääkseen sopivan valinnan ja toteutuksen tulisi olla tietoturvalleen, joten heidän olisi määriteltävä tietoturvan tarpeensa.

Ongelman ratkaiseminen on vahvasti sidoksissa organisaation toimintaympäristöön, jolloin siihen voi kohdistua seuraavanlaisia voimia, joita ovat:

- Organisaation tulee noudattaa kansallisia sekä kansainvälisiä lakeja ja määräyksiä
- Toimiakseen organisaatio tarvitsee käsitellä sellaisia arkaluontoisia tietoja, jotka nauttivat luottamuksellisuuden suojaa
- Organisaation on noudattava sen määrittämää sisäistä politiikka, joissakin suojauskäytännöissä
- Organisaatio tarvitsee sisällyttää riittävä suojan toimintakriittisille liiketoiminnallisille varoille
- Organisaation on varmistuttava, että turvallisuushenkilöstöllä on pienin mahdollinen vaikutus yrityksen tehokkuuteen ja se ei suojaa enempää kuin on välttämätöntä
- Sen on tiedettävä milloin suunnittelemattomat tapahtumat ilmenevät
- Sen on kyettävä toipumaan ei-toivotuista tapahtumista
- Kaikki kustannukset on voitava minimoida

Ratkaisu

Systemaattisesti ja selkeästi tunnistetut liiketoiminnallisuuden tyypit, jotka tarvitsevat suojelua on määritelty ja tunnistettu. Toiminta antaa tiedon, minkä tyyppistä suojelua ne tarvitsevat. Tämä määrityksen tyypillisesti tekevät organisaation arkkitehti tai strateginen suunnittelija. Määritykset yleensä pitävät sisällään viisi eri vaihetta, jotka ovat:

1. Organisaation on tunnistettava liiketoiminnan omaisuuserät, joita ovat:
    (a) Tiedot tai tietovarat, kuten henkilöstö ja/tai taloudelliset tiedot
    (b) Fyysinen omaisuus, kuten henkilöstö ja kiinteistöt
2. Tunnistaa liiketoiminnan tekijät, jotka vaikuttavat organisaation ulkoisiin ja sisäisiin turvallisuuden tarpeisiin, joita ovat:
    (a) Kansainväliset ja kansalliset lait ja asetukset
    (b) Organisaation kumppanuussuhteet
    (c) Organisaation missio, päämäärät ja tavoitteet
    (d) Organisaation halu vahvista taloudellista terveyttään
    (e) Liiketoiminta prosessit
3. Selvitettävä mitkä varat liittyvät liiketoiminnan tekijöihin

(a) Työntekijöiden tietoihin sovellettavat yksityisyydestä määrittävät lait
(b) Eri toimipaikoissa olevat aineelliset varat
(c) Taloudelliset tiedot, jotka jaetaan yrityskumppanien kanssa

4. Tunnista turvallisuuden tarpeet, joita ovat:

   (a) Luottamuksellisuus. Suojautuminen tahalliselta tai luvattomalta luovuttamiselta.
   (b) Eheys. Suojautuminen tahattomalta tai tahalliselta muutokselta.
   (c) Saatavuus. Tehdä liiketoiminta varat saataville luvalliselle käytölle.
   (d) Vastuullisuus. Kaikkiin sen toimiin vastuullisuuden asettaminen.

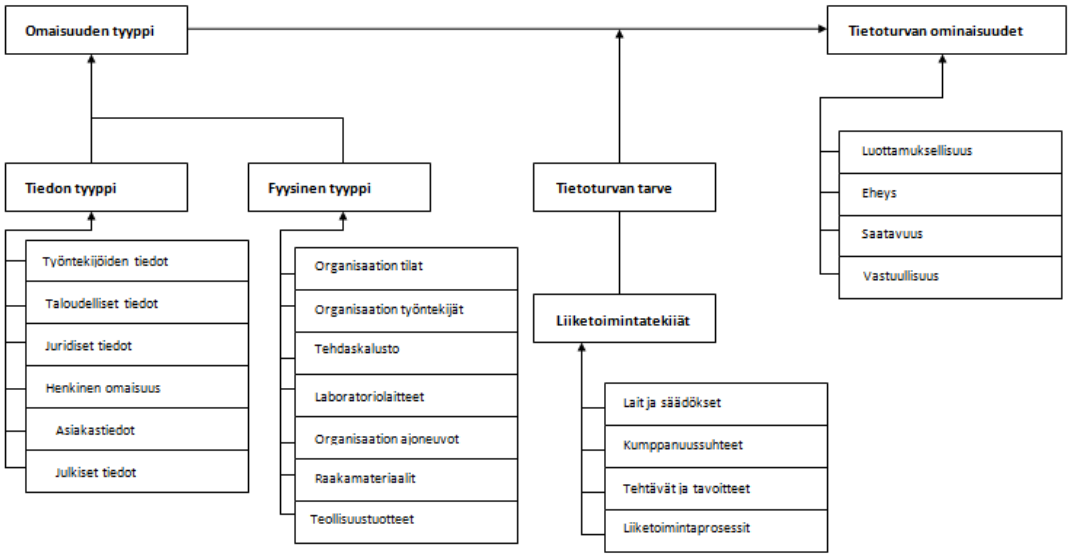
   Luottamuksellisuus, eheys ja saatavuus ovat keskeisiä turvallisuus ominaisuuksia kirjallisuudessa. Vastuullisuus on myös tärkeää, mutta se ilmenee eri tilanteissa. Luottamuksellisuus, eheys ja saatavuus ovat omaisuutta suojelevia ominaisuuksia, mutta vastuullisuus ei tätä ole. Määritellessä turvallisuusominaisuuksia organisaation omaisuudelle, on tärkeää tunnistaa, kuka on vastuussa turvallisuuteen liittyvissä toiminnoista ja tällöin vastuullisuus tulee mukaan kuvioon.
5. Perustuen liiketoiminnan tekijöihin, kukin voi määritellä jokaisen olemassa olevan omaisuuserän tyypin ja minkälaista tietoturvaa tarvitaan. Tietoturvan suunnittelun tulee olla tasapainossa vaadittujen resurssien määritysten kanssa. Lisätietoja yleisimpiin tietoturvan ominaisuuksiin määritellessä tietoturvan tarpeita on annettu täytäntöönpano osiossa. Näitä annettuja vaiheita voidaan soveltaa lineaarisesti, mutta on myös muita mahdollisia vaihtoehtoja. Näitä tapauksia käsitellään dynamiikka jaksossa.

Rakenne

Käyttämällä UML-luokkakaaviota, yleisien suhteiden väliset ominaisuudet, toiminnalliset tekijät ja tietoturvan ominaisuudet on esitelty (ks. Kuvio 36). Tietoturvan tarve on omaisuudentyyppien ja tietoturvan ominaisuuksien välinen yhdiste. Kukin omaisuuden tyyppi tarvitsee yhden tai useamman tietoturvan ominaisuuden.

Dynamiikka

Sallittujen sekvenssien suorittamiseksi ratkaisun vaiheet on esitelty (ks. Kuvio 37) Omaisuuden ja liiketoiminnan tekijöiden tunnistaminen ovat pääosin itsenäistä toimintoja ja näin



Kuvio 36. Tietoturvan tarpeiden ratkaisun rakennekaavio

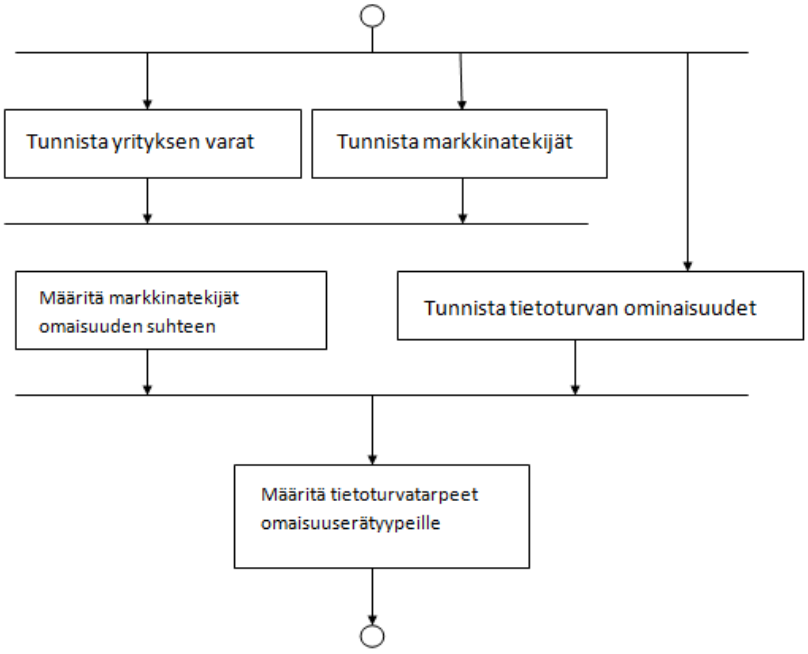
ne voidaan suorittaa rinnakkain. Molemmat toiminnot on tehtävä ennen ominaisuuserien ja liiketoiminnan tekijöiden suhteiden määrittämistä. On olemassa kolme eri rinnakkain suoritettavaa vaihetta tietoturvan ominaisuuksille.

Ominaisuuksien määrittely voi olla myös triviaalia, kunhan organisaation suunnittelijat tunnistavat luottamuksellisuuden, eheyden, saatavuuden ja vastuullisuuden. Organisaatiot saattavat haluta keskittyä osaan näistä tiloista ja lisätään muita siihen liittyviä ominaisuuksia kuten yksityisyyden, turvallisuuden tai luotettavuuden. Jokaisessa tapauksessa on kuitenkin määriteltävä ominaisuus ja suhteet ennen viimeistä vaihetta turvallisuuden tarpeiden määrittämistä.

Täytäntöönpano

Liiketoiminnalliset tekijät pyrkivät luomaan ristiriitaisia voimia tietoturvakysymyksiin. Näitä voimia ovat lait ja asetukset sekä tiettyjen omaisuuserien arkaluonteisuus ja halu pitää organisaatio tietoturvallisena. Toisaalta kustannusten asettama rajallisuus, kun halutaan pitää talous terveenä. Avoimuudella on myös rajoittava vaikutus tietoturvaan.

Tietoturva tarvitsee investointeja, jotta elintärkeisiin omaisuuseriä voidaan suojella, mutta suurempi riski voidaan hyväksyä ei-tärkeille omaisuuserille. Kriittiset varat ovat tyypillises-



Kuvio 37. Tietoturvan tarpeiden ratkaisu sekvenssikaaviona

ti niitä, joiden aiheuttamat kustannukset tekisi huomattavaa vahinkoa yritykselle. Tällaisia ovat varat, joiden suojelu on lakien, strategisten suunnitelmien, kilpailuetuun liittyvien varojen, korvaamattomien kohteiden, joiden menetykseen liittyy merkittäviä kustannusvaikutuksia. Ei-kriittiset varat ovat selliaisa, joiden aiheuttamat haitat ovat organisaatiolle vähäiset tai niitä ei esiinny lainkaan. Näitä ovat helposti vaihdettavat kohteet tai tiedot, joiden paljastumisesta on vähäiset tai mitättömät vaikutukset.

Välttämättömät kriittisten hyödykkeiden tyypit voivat vaihdella vaadetyypeittään. Luottamuksellisuutta ja eheyttä sovelletaan tyypillisesti tietoihin. Vastuullisuutta ja saatavuutta sovelletaan fyysisiin ominaisuuksiin. Saatavuus koskee palveluita ja tietoja. Vastuullisuus sisältää toimia, joita otetaan omaisuuteen. Luottamuksellisuus on ristiriidassa jossain määrin saatavuuden kanssa. Enemmän käytettävät omaisuuserät ovat vähemmän luottamuksellisia.

Jossain tapauksissa omaisuuserät tai tyypit voivat vaatia tyyppistä tietoturvan suojausta. Esimerkiksi ohjelmisto voi vaatia:

- Luottamuksellisuutta, silloin kun se on yksinoikeudella valmistettu
- Eheyttä, joten sitä tulee suojata luvattomilta muutoksilta

- Saatavuutta, kun sen on oltava saatavilla valtuutetuille käyttäjille
- Vastuullisuutta, kun tehdyt muutokset ovat tiedossa

Organisaatioiden tarvitsee tunnistaa tyypilliset varat, jotka tarvitsevat suojausta. Tarvittavan tietoturvan tarpeet varojen suojelemiseksi on esitelty (ks. Taulukko 18)ja fyysisen omaisuuden suojaamista on esitelty (ks. Taulukko 19). Taulukoissa esitellään esimerkkejä organisaation näkökulmasta, mutta niitä ei pidä tulkita siten, että ne käsitelevät kaikkia omaisuuserätyyppejä. Luettaessa edellä mainittuja taulukoita on tärkeää ymmärtää, että tiedot syntyvät kaikista organisaation näkökulmista ja nämä tiedot poikkeavat taulukoissa esitellyistä tiedoista.

Eturyhmät	**Suojelun tarve**	**Liiketoiminta tekijät**	**Keskustelu**
Henkilöstötiedon (lukuun ottamatta henkilöstökuluja)	Luottamuksellisuus, eheys, saatavuus ja vastuullisuus	Lait yksityisyydestä ja kilpailukysymykset	Laki yksityisyydestä edellyttää, että henkilöstön yksityisiä tietoja käsitellään luottamuksellisesti. Organisaation henkilökunta tarvitsee varmuutta siitä, että vain henkilöstöhallinnon henkilökunta voi muokata näitä tietoja. Tietojen on oltava käytettävissä henkilöstöhallinnon henkilöstölle ja tietojen on tuettava organisaation palkanlaskentaa.

... jatkuu seuraavalla sivulla

Eturyhmät	Suojelun tarve	Liiketoiminta tekijät	Keskustelu
Taloudelliset tiedot	Luottamuksellisuus, eheys ja vastuullisuus	Raportointivaatimukset verottajalle, kilpailukysymykset ja organisaation toimiala	Taloudelliset lait ja organisaation on hyväksyttävä viranomaisten määräykset ja säädökset, joita sen tulee seurata. Lait ja määräykset edellyttävät organisaation suojaamaan tietonsa luvattomalta muutokselta ja kuinka vastuullisen organisaation tulee toimia. Näiden tietojen tulee olla suojattuina.
Juridiset tiedot (sopimukset ja oikeudenkäynnit)	Luottamuksellisuus, eheys ja vastuullisuus	Lait ja kilpailukysymykset	Organisaation täytyy sisällyttää sopimusoikeudellinen luottamuksellisuus sopimuksiinsa. Sopimusten saatavuus tulee rajoittaa vain tietoja tarvitsevien saataville.
Henkinen omaisuus (tiedot ja prosessit)	Luottamuksellisuus, eheys ja saatavuus	Osittain riippuu organisaation toimialasta sekä kilpailukysymyksistä	Joidenkin henkisten tietojen tulee olla julkisia. Arkaluonteisiin tietoihin tulee pääsyä rajoittaa, mutta toisaalta liiketoimintaprosesseja sisältävien teknisten tietojen tulee olla organisaation sisäisessä käytössä.

... jatkuu seuraavalla sivulla

Eturyhmät	Suojelun tarve	Liiketoiminta tekijät	Keskustelu
Asiakkaiden ja liikelumppanien tiedot	Luottamuksellisuus, eheys ja vastuullisuus	Kilpailukyky ja palvelu kysymykset	Yksityistä tietoa, jonka saattaminen kilpailijoiden tietoon, voi aiheuttaa kilpailuedun menetyksiä. Näihin tietoihin luvaton pääsy tulisi estää ja niiden saatavuus tulisi rajata.
Julkinen tieto	Eheys ja saatavuus	Palvelukysymykset	Tiedon luvaton luovuttaminen voi johtaa toiminnan tai maineen menetykseen.

Taulukko 18: Yleiset tiedon omaisuusluokat ja suojaukset

Eturyhmät	Suojelun tarve	Liiketoiminta tekijät	Keskustelu
Rakennukset	Eheys ja saatavuus	Kriittinen liiketoiminnan prosessi	Organisaation tulee suojata rakennukset, tarjoten työympäristö, jossa luvattomat muutokset ja tuhot on estetty. Tällöin taataan rakennusten saatavuutta.
Työntekijät	Saatavuus ja vastuullisuus	Kriittiseen liiketoimintaan vaikuttava henkilöstö ja prosessit	Organisaation tarvitsee tarjota ympäristö, jotka ovat turvallisia ja saatavilla henkilöstölleen. Ympäristö saattaa vaikuttaa myös työntekijöiden vastuullisuuteen.

... jatkuu seuraavalla sivulla

Eturyhmät	Suojelun tarve	Liiketoiminta tekijät	Keskustelu
Raakamateriaalit ja valmistetut tuotteet	Eheys ja saatavuus	Tarve minimoida aiheutuvia kustannuksia	Raaka-aineiden on oltava saatavilla käyttöä varten, kuten liiketoimintaprosessit edellyttävät. Organisaation on voitava valuuttaa asiakkaat, että en tuotteet ovat saatavilla. Raaka-aineiden varkaus, vahinko tai hävittäminen voi aiheuttaa raaka-ainepulan ja valmistusvirheet tekevät niistä käyttökelvottomia.

Taulukko 19: Yleiset fyysiset omaisuusluokat ja suojaukset

Esimerkkiratkaisu

Esimerkki ratkaisee tunnistetun ongelman, joka on kuvattu aikaisemmin. Organisaatio tunnistaa omaisuuserien tyypit ja liiketoiminnan tekijät, joita ovat:

1. Tietorekisteri tyypit
    (a) Henkilöstötiedot
    (b) Rahoitus/vakuutustiedot ja kumppaneiden taloudelliset tiedot
    (c) Sopimustiedot ja liiketoiminta suunnitelmat
    (d) Tutkimus ja niihin liittyvät tiedot
    (e) Mainokset ja muut julkaistavat tiedot
    (f) Keräämien tietokantojen tiedot
2. Fyysiset omaisuuserät

(a) Rakennukset

(b) Henkilöstö

(c) Kuljetusvälineet

3. Ulkoiset liiketoimien tekijät

(a) Vakuutuksien rajoitteet

(b) Kansainväliset lait ja sopimukset laina materiaalien suhteen

(c) Tietosuojalaki

(d) Tavoitteet ja strategiat

(e) Vaatimukset ja rajoitteet organisaatiota kohtaan

4. Sisäiset liiketoiminnan tekijät

(a) Tuotetiedot, sijaintitiedot ja arvo

(b) Hankintasuunnitelmat

(c) Immateriaalioikeudet selvityksistä, tutkimuksista, tilastoista ja papereista.

(d) Rakennussuunnitelmat

Organisaation suunnittelija luovat ensin listan kaikista edellä mainituista tiedoista. Tämän jälkeen ne esitellään ja muokataan tuottamaan omaisuuden suojelusta listan, joka on esitelty (ks. Taulukko 20).

Eturyhmät	**Tietoturvan ominaisuudet**	**Liiketoimintatekijät**
Organisaation työntekijöiden tiedot	Luottamuksellisuus, eheys, saatavuus ja vastuullisuus	Yksityisyyden lait ja organisaatio työntekijä suhteet
organisaation taloudelliset ja vakuutustiedot, sekä kumppanien taloudelliset tiedot	luottamuksellisuus, eheys ja perus kirjanpito	Sopimusvelvoitteet ja lait taloudellisesta raportointivelvoitteista

... jatkuu seuraavalla sivulla

Eturyhmät	Tietoturvan ominaisuudet	Liiketoimintatekijät
organisaation sopimustieto ja liiketoiminta suunnitelmat	Luottamuksellisuus, eheys ja kirjanpito	Suojata hankinta ja kuljetus suunnitelmat, vakuutuksien rajoitteet ja suojata aikatalutustiedot
Organisaation tutkimus ja liittyvät tiedot	luottamuksellisuus	Immateriaalioikeudet, vuokravaatimukset ja yrityksen maine
Organisaation mainokset ja muut julkiset tiedot	eheys	maine ja vuokra vaatimukset
Organisaation rakennukset	saatavuus	Valutusten rajoitteet
Organisaation henkilökunta	Saatavuus	Lait ja julkinen maine

Taulukko 20: Perusta tietoturva omisaisuuksille

Tunnetut käyttötavat

Organisaation varojen ja niiden tietoturvan tunnistaminen on parhaita käytäntöjä, mutta nämä yleensä tehdään epävirallisina tai osan riskianalyysiä. Tietoturvateknisellä tasolla tämä prosessi määritellään kuuluvaksi riskin arviointiin. Yhteisinä elementtejä ovat

1. Tietoturvaa käsitellään eri organisaation soveltamisalaan
2. Tietoturvatarpeiden yhteen soveltamista käsitellään ulkopuolisten vaatimusten, kuten lakien, säädösten ja standardien mukaan.
3. Prosessin vaikutuksia arvioidaan, kun määritellään ja kuvataan yrityksen omaisuutta huomioiden luottamuksellisuus, eheys, käytettävyys, vastuullisuus, aitous ja luotettavuus.

Eräs organisaatio on määritellyt lähestymistavan yhdistäen parhaita käytäntöjä tietohallinnon alaisuuteen. Tämä kehys perustuu tietoturvan lähestymistapaan, joka on esitelty luvun 2.5.4 tietoturvallisuuden hallintaa koskevan viitekehyksen mukaisesti. Tämän viitekehyksen ohjausobjekteja ovat:

1. Organisaation varojen ja resurssien suhde tietoturvan hallintaan
2. Varojen luokitus ja valvonta, jotta ne voidaan tunnistaa ja suojata
3. Tietoturvapolitiikka
4. Organisaation tulee noudattaa rikos- ja siviilioikeudellisia vaatimuksia. Lakisääteisten asetusten tai sopimusten tuomien velvollisuuksien ja muiden turvallisuusvaatimusten noudattaminen

Näiden vaatimusten vastaavuutta tunnistamaan omaisuutta ja liiketoiminnan tekijöitä ei käsitellä tässä tietoturvamallissa.

Seuraukset

Organisaation varojen tunnistamisella (engl. Enterprise Assets) on seuraavat edut:

1. Helpottaa tasapainottamaan päätöksiä organisaation tietoturvan tarpeista, tunnistamalla kilpailevat voimat ja liiketoiminnan tekijät. Kompromissina nämä tekijät aiheuttavat selvän eron kriittisten ja ei-kriittisten omaisuuserien välille. Todennäköisenä tuloksena on tietoturva ominaisuuksien lisääntynyt soveltamisen tarve. Suojauksen tarve on nimenomaisesti kohdennettu kriittiseen omaisuuteen.
2. Tämä mallin muita hyödyllisiä sovelluskohteita on liiketoiminnan suojelun jäljitettävyys merkityksellisiin liiketoiminnan tekijöihin ja tämä on saatavilla ylimääräiseen käyttöön. Tämä tieto on hyödyllistä kun perustellaan sen tietoturvatarpeiden kehityksen hyödyillä. Sitä voidaan käyttää yksityiskohtaisempia tietoturvavaatimuksia edellyttävään organisaation tietoturvapalveluihin (engl. Enterprise Security Services).

Organisaation varojen tunnistamisella (engl. Enterprise Assets) on seuraavia haittoja:

1. Tätä mallia sovellettaessa, se tulee maksamaan. Se edellyttää ihmisresursseihin investointia, koska se tarvitsee yrityksen omaisuuserien ja liiketoiminnan tekijöiden tuntemusta. Tämän mallin hyötynä kuitenkin sataa olla kustannussäästöt, jotka mahdol-

lisesti ylittävät nämä kustannukset. Tämä tehtävä on annettava sellaiselle ihmiselle, jolla on erittäin hyvät tiedot organisaation varoista ja liiketoiminnan tekijöistä. Saadut tulokset on pidettävä tarkasti paikkaansa, koska paikkaansa pitämättömistä tiedoista ei ole hyötyä.

2. On myös mahdollista, että organisaatio tuottaa hyviä tuloksia tällä mallilla, mutta voi olla ettei se kykene hyödyntämään tämän mallin tuloksia täysin. Molemmissa tapauksissa tämän mallin soveltamisesta voi ylittää hyödyt.

Katso myös

Tämä mallin soveltamisen jälkeen seuraavana askeleena on tyypillisesti soveltaa joukkoa riskinarviointimalleja, jotka entisestään tarkentavat tietoturvan tarpeita. Omaisuuserille tarvitaan riskinarviointia niiden tarkemman tyypin määrittämiseksi näihin turvallisuusvaatimuksiin. Riskimallien joukko auttaa omaisuuden arvostuksen, uhkien ja haavoittuvuuksien arviointiin ja riskien määrittämiseen. Mallit auttavat päätöksissä, kuinka paljon suojaa tarvitaan yrityksen kuhunkin omaisuuserään.

Tietoturvan tarpeiden tunnistus organisaation omaisuuserille (engl. Security Needs Identification for Enterprise Assets) on keskittynyt hieman riskinarviointimalleihin sisältäen ulkoiset ja sisäiset näkökohdat. Riskinarvioinnin seuraava askel on arvioida yrityksen tietoturvaratkaisujen lähestymistapoja, jotka täyttävät yhdistetyn tietoturvan tarpeet ja vaatimukset tässä mallissa ja riskinarvioinnissa.

C.2 Varojen arvostus

Varojen arvostus (engl. Asset Valuation) auttaa määrittämään organisaation tärkeitä paikkoja omaisuuserille joita se omistaa ja hallinnoi. Katoaminen tai vaarantuminen tällaisissa omaisuuserissä voi aiheuttaa kovia kustannuksia, kuten sakkoja tai maksuja sekä pehmeämpiä kustannuksia, kuten markkinaosuuden menetyksiä ja kuluttajien luottamuksen laskua.

Tunnetaan myös nimellä

Vaikutusten arviointi (engl. Impact Assessment) ja Liiketoiminnan vaikutuksen analyysi (engl. Business Impact Analysis)

Esimerkki

Organisaatio on aloittanut riskinarvioinnit ja tunnistaa seuraavat tietovarannot omaisuuseriksi:

1. Työntekijöiden tiedot
2. Rahoitus ja vakuutustiedot sekä kumppanien taloudelliset tiedot
3. Sopimustiedot ja liiketoiminnan suunnittelun
4. Tutkimuksen ja siihen liittyvät tiedot
5. Mainokset ja muut julkaistavat tiedot

Fyysisiä omaisuuseriä ovat

1. Rakennus
2. Henkilökunta
3. Kuljetusvälineet

Tausta

Organisaatio on määritellyt ne omaisuuserät, jotka ovat sisällytettävä yleiseen riskien hallintaprosessiin ja nyt on varmistettava niiden omaisuuserien arvo.

Ongelma

Kyky määritellä näiden omaisuuserien arvo, on kaikkein keskeisintä riskinarvioinnissa. Haavoittuvuuksilta ja uhkatekijöistä, jotka kohdistuvat ja altistavat hyödykkeet osana omaisuuserän arvosta. Ilman tällaista määritelmää yritys ei kykene kunnolla arvioimaan riskiä sen omaisuuteen. Miten organisaation omaisuuserien arvo määritellään yleisesti, sen on ratkaistava seuraavat voimat:

1. Sen on kehitettävä standardisoitu tapa arvioida ja kuvata omaisuuserien arvo.
2. Sen tulee tarjota yhdenmukaisia tuloksia siitä huolimatta, vaikka subjektiivisuus vaikuttaa tähän prosessiin.
3. Sen on kyettävä arvioimaan mahdollisimman paljon pehmeitä kustannuksia, jotka voivat johtua omaisuuserän katoamisesta tai vaarantumisesta.
4. Se ei ehkä pysty täysin arvioimaan tietoturvan tappioiden vaikutuksia, joissa ei ole

aiemin ilmennyt vahinkoja.

5. Kun arvioidaan kovia kustannuksia, yritys voi joutua tuhlaamaan aikaa lisäkuluihin tai pahimmillaan pienempään hyödykkeen suhteellista arvoa.

Ratkaisu

Systemaattisesti määritelty omaisuuserien kokonaisuusarvo on yksilöity soveltamisalan riskinarviointiin. Tämä prosessi tarkoittaa seuraavan neljän vaiheen suorittamista, joita ovat:

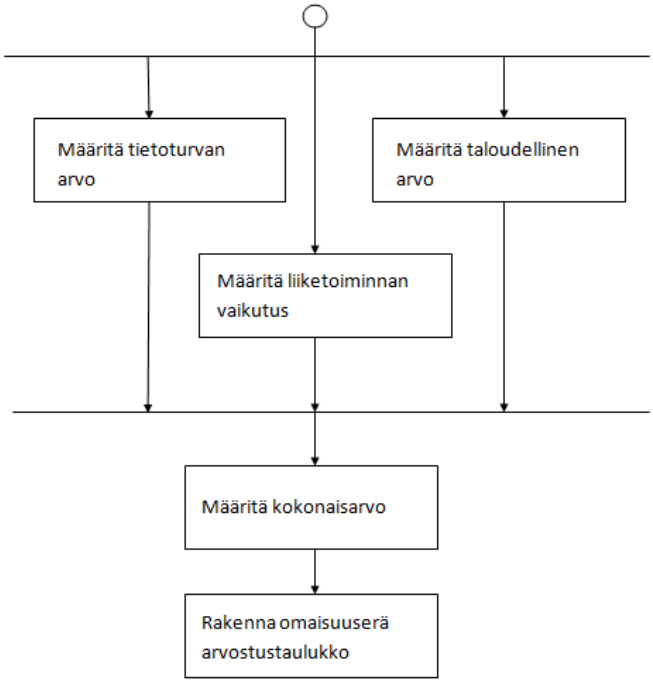
1. Selvitä turvallisuuden arvo. Omaisuuserän perusteella tärkein asema takaa omaisuuserän tietoturvan ominaisuuksia, joita ovat luottamuksellisuus, eheys, saatavuus ja vastuullisuus
2. Määritä taloudellinen arvo. Yrityksen omaisuuden perusteella mahdollisten korjauskustannukset tai vaihtokustannukset ylläpitää ja käyttää omaisuutta.
3. Selvitä vaikutus liiketoiminataan. Määrittää omaisuuserien arvo kompromissin vaikutus omaisuuserän, joita voi olla yrityksen prosesseihin.
4. Määritä kokonaisarvio ja tarkenna omaisuuden arvotaulukko. Yhdistä tulokset, joita ovat tietoturva, rahoitus, liiketoiminnan arvostus ja määritä kokonaisarvo organisaation asema voimavaroihin. Anna nämä tulokset osaksi omaisuuden arvo taulukkoa.

Dynamiikka

Sallitun sekvenssin suorittamiseksi hyödykkeiden arvostusprosessiin on esitetty (ks Kuvio 38). Kolme ensimmäistä tekijää on määrittää tietoturvan arvo, liiketoiminnan vaikutus ja taloudellinen arvo, voidaan arvioida missä tahansa järjestyksessä. Saadut tulokset kerätään ja syötetään omiasuuden arvostustaulukkoon.

Täytäntöönpano

Jokaisessa osassa luodaan arviointiasteikko, jossa määritellään alue, sitten sisällytetään kuvaus. Esimerkiksi tietoturvan ja taloudellinen arvo sekä liiketoiminnan vaikutus. Johdonmukaisuuden säilyttämiseksi uhkien arvioinnista (engl. Threat Assessment) ja haavoittuvuuksien arvioinnista (engl. Vulnerability Assessment) määritellään kuusi arvoa. Arvot voivat muuttua organisaation mieltymysten mukaan, vaikka ne olisivat edelleen koko riskinarviota vastaavia, jotka ovat:



Kuvio 38. Sekvenssin hyödykkeen arvonmääritysprosessin rajoitteet

1. Selvitä tietoturvan arvo hyödykkeelle ja otetaan huomioon seuraavat seikat:

   (a) Kysyntä on usein tietoturvan ominaisuuksien yksittäinen omaisuuserä. Hyödyke, joka vaatii kaikkia neljää ominaisuutta, olisi merkittävä suuremmalla arvolla, kuin hyödykettä jolla on yksi arvo.

   (b) Seuraus laaja-alaisuudesta johtuvasta kompromissista omaisuuserän tietoturva ominaisuudesta. Esimerkiksi seuraus luvattomasta muuttamisesta maksutapahtumassa voi olla paljon ankarampi kuin muutos tutkimus tai tuotekehitys dokumentissa. Molemmat vaativat eheyden toteutumista

   (c) Terveyden tai turvallisuuden aiheuttama vahinko fyysiseen omaisuuteen, esimerkiksi tikkaat, sillat, vartiat tai kattava omaisuus kuten evakonti, tulipalon eristäminen ja ensiapuohjeet.

   Tietoturvavaatimukset ovat normaalisti sisällytetty omaisuuserien omistajille. Muuten tietoturvan tarpeisiin voidaan soveltaa tietoturvan tarpeiden tunnistusta organisaation omaisuuteen (engl. Security Needs Identification For Enterprise Assets).

   Tietoturva omaisuuserien luokittelu on esitetty (ks. Taulukko 21).

2. Määritä omaisuuserien taloudelliset arvot, pohtimalla seuraavia asioita:

   (a) Kustannukset, jotka koituvat vahinkotapahtuman vaihdosta tai korjauksesta
   (b) Lainsäädäntö- tai seuraamukset kuten sakot tai maksut, jotka aiheutuvat tietoturvaloukkauksesta
   (c) Kauppa-arvo mikä vastaa omaisuuserän arvoa
   (d) Tehokkaan työajan menetys tai työ jonka haitta on aiheuttanut

   Vaihto tai korjauskustannukset, joita on tullut osoitetaan hankintaosastolle, joka puolestaan hankkii ne, joko jälleenmyyjiltä tai suoraan tavarantoimittajalta. Sääntelysakot ja rangaistukset ovat yleisesti julkisia ja helposti saatavilla sakkoja valvovilta viranomaisilta. Kovat kustannukset omaisuuseriin, jotka palvelevat terveyden ja turvallisuuden tarkoituksia sisältäen sairaala- ja vakuutusmaksut, samoin kuin uudelleenjärjestelykustannukset tulipalon ja tulvan koittaessa.

   Liiketoiminnallinen laatu saadaan asettamalla ne omaisuuseriin, jotka on esitelty (ks. Taulukko 22)
3. Selvitä vaikutukset liiketoimintaan, pohtimalla seuraavia asioita

   (a) Asiakkaan menetys tai sijoittajien luottamus ovat tuloksia omaisuuserien suojaustason kompromisseista
   (b) Kilpailuedun menetys tietoturva ominaisuuksien vaarantumisesta
   (c) Vaikutus kumppanuussuhteisiin tai muihin sopimusehtoihin
   (d) Vaihtoehtoisten palveluiden puute, jos vaihtoehtoinen palvelu on olemassa jolla voidaan täyttää asiakkaan tarpeet, jos päätyotteen toimituksessa ilmenee puute
   (e) Häiriöiden laajuus yrityspalveluille, joilla on riippuvuus omaisuuseriin
   (f) Prosenttiosuus asiakaskuntaan joihin katkos tai palveluiden heikkeneminen vaikuttaa

   Onnettomuudesta palautumista ja liiketoiminnan jatkuvuutta koskevat suunnitelmat monissa organisaatioissa voidaan lajitella omaisuuserien arvon. Tämä voi tarjota alkupisteen suhteelliselle liiketoiminnan määritelmälle, kun arvioidaan yrityksen voimavaroja. Liiketoiminnan vaikutus on luonteeltaan subjektiivista ja vaikeampaa arvioida, kuin kovat kustannukset. Varsin usein ei ehkä voida täysin ennustamaan asiakkaiden

luottamuksen tai kilpailuaseman menetystä.

Liiketoiminnan arvon ennustaminen omaisuuseriin on esitelty (ks. Taulukko 23)

4. Määritä kokonaisarvo, jonka organisaation omaisuuserien asemaan on tietoturva-, rahoitus- ja liiketoiminnalliset vaikutukset. Määrittäessäsi tämän arvon saat (ks. Taulukko 24) kokonaisarvon. Ei ole suoraa muutoskeinoa kolmesta korkeimmasta arvosta, eli jos omaisuuserällä on erittäin korkea tietoturva-arvo, mutta alhainen taloudellinen arvo täten sen kokonaisarvo pitäisi olla vielä riittävän korkea.

Luokitus	**Laatu**	**Kuvaus**
6	Äärimmäinen	Hyödyke vaatii äärimmäistä luottamuksellisuutta, eheyttä ja saatavuutta. Kompromissi näiden turvallisuusominaisuuksiin altistuessa olisi valtavat tietojen luottamuksellisuudelle ja vaarantaisi yleisen turvallisuuden
5	Erittäin korkea	Hyödyke edellyttää erittäin korkeaa luottamuksellisuutta, eheyttä, saatavuutta ja vastuullisuutta. Kompromissi yhden tai useamman mäistä ominaisuuksista paljastaisi luottamuksellisia tietoja ja mahdollisesti vaarantaisi täten yleisen turvallisuuden
4	Korkea	Hyödyke vaatii suurta luottamuksellisuutta, eheyttä, saatavuutta ja vastuullisuutta. Kompromissi näissä ominaisuuksissa altistaisi arkaluontoiset tiedät ja täten rikkoisi lainsäädäntöä
3	Keskitaso	Omaisuuserällä on kohtalaiset vaatimukset tietoturvan valvotaan. Kompromissi tietoturvaominaisuuksissa rikkoisi yrityspolitiikkaa ja lainsäädäntöä

... jatkuu seuraavalla sivulla

Luokitus	Laatu	Kuvaus
2	Matala	Omaisuuserällä on alhainen vaatimus tietoturvallisuudelle. Kompromissi altistaisi vai ei-kriittiset tiedot
1	Merkityksetön	Tieto on julkisesti saatavilla tai sillä ei ole tietoturva-arvoa yritykselle

Taulukko 21: Tietoturva vaatimusten luokitus

Luokitus	Laatu	Kuvaus
6	Äärimmäinen	Hyödykkeellä on äärimmäinen rahallinen arvo yritykselle. Menetys tai vaurio omaisuuserässä veisi yrityksen todennäköisesti konkurssiin
5	Erittäin korkea	Omaisuuserällä on merkittävä rahallinen arvo. Menetys tai vahinko aiheuttaisi merkittävät taloudelliset vaikutukset yritykselle
4	Korkea	Omaisuuserällä on merkittävä rahallinen arvo. Korjaus tai vaihto vaatisi huomattavia varoja
3	Keskitaso	Hyödykkeellä on kohtalainen taloudellinen arvo. Menetyksen tai vaurion toteutuminen edellyttäisi taloudellista uudelleen tarkoitusta
2	Matala	Hyödykkeellä on alhainen taloudellinen arvo organisaatiolle
1	Merkityksetön	Hyödykkeellä ei ole rahallista arvoa

Taulukko 22: Taloudellisen arvon luokitus

Luokitus	Laatu	Kuvaus
6	Äärimmäinen	Organisaatio ei voi toimia ilman tätä omaisuuserää. Kompromissi tai menetys johtaisi välittömään konkurssiin
5	Erittäin korkea	Tämä omaisuuserä on merkittävä palvelu. Menetys voisi johtaa organisaation palveluiden tai tuotteiden uudelleen järjestämiseen
4	Korkea	Omaisuuserä tulee monia organisaation palveluja. Palvelun menetyksellä olisi suuria vaikutuksia jopa palveluiden alasajoon
3	Keskitaso	Omaisuuserä tukee kohtuullisen monia asiakkaita tai se on suuri tarjottava palvelu. Menetys johtaisi tärkeiden palveluiden alasajoon
2	Matala	Omaisuuserän tuella on liitännäisvaikutus palveluihin. Menetyksellä olisi vähäinen vaikutus yrityksen palveluille
1	Merkityksetön	Omaisuuserän menetyksellä ei olisi vaikutusta liiketoimintaan

Taulukko 23: Liiketoiminnan vaikutuksen luokitus

Luokitus	Laatu	Kuvaus
6	Äärimmäinen	Organisaatio on asettanut korkeimman mahdollisen arvon tälle omaisuudelle. Kompromissi johtaisi ihmisen kuolemaan ja tämän vaikutuksena olisi välitön ja täydellinen menetys tai konkurssi
5	Erittäin korkea	Omaisuuserä edustaa tai tukee yrityksen kriittisiä toimintoja. Menetys tai vahinko johtaa vakaviin vaikutuksiin taloudellisissa, turvallisuudessa tai terveydessä
4	Korkea	Omaisuuserällä on korkea arvo, koska sillä on tietoturvavaatimuksia tai vaikutuksia asiakaslähtöisyyteen. Menetys johtaisi huomattavaan haittaan asiakaspalvelussa tai maineelle
3	Keskitaso	Omaisuuserällä on kohtalainen arvo. Sillä on joitakin tietoturvaan liittyviä tarpeita ja taloudellista arvoa. Kompromissi ei estäisi yrityksen toimintaa
2	Matala	Omaisuuserällä on vähäinen taloudellinen arvo. Kompromissilla olisi pieni vaikutus liiketoimintaan
1	Merkityksetön	Omaisuuserällä on merkityksetön vaikutus organisaatiolle. Hyödyke voidaan helposti korjata tai vaihtaa. Sillä ei ole tietoturvavaatimuksia.

Taulukko 24: Kaiken omaisuuden arvo-asteikko

Esimerkki ratkaisu

Tietoturvamallin varojen arvostamisen (engl. Assets Valuation) jälkeen organisaatio voi määrittää heidän tiedon ja fyysisen omaisuuden arvon. Nämä tiedot on esitelty taulukoissa (ks. Taulukko 25 ja 26)

Omaisuuserä	Tietoturva-arvo	Arvo	Vaikutus	Yhteensä
Organisaation henkilöstötiedot	5	3	5	5
Organisaation taloudellinen / vakuutusarvon sekä liikekumppanien taloudelliset tiedot	4	3	4	4
Sopimuksien tiedot ja liiketoiminnan suunnittelu	4	3	4	4
Tutkimus ja siihen liittyvät tiedot	2	2	3	2
Mainokset ja muut julkiset tiedot	1	2	2	2
Kokoelmatietokannan tiedot	3	3	4	4

Taulukko 25: Tieto omaisuuserien arvosta

Omaisuuserä	Tietoturva-arvo	Arvo	Vaikutus	Yhteensä
Rakennukset	5	5	6	6
Henkilöstö	6	5	6	6
Kokoelmat ja näyttelyt	5	6	5	6
Kuljetusvälineet	3	2	2	3

Taulukko 26: Fyysisten omaisuuserien arvot

Vaihtoehdot

Organisaatio voi valita eri mittakaavoja tai vaatia enemmän täydelliseltä laadulliselta kuvaukselta. Tämä on hyväksyttävissä. Tärkein näkökohta on, että asteikon on oltava käytössä kaikille omaisuuserille. Seuraavanlaisia laadullisia arvioija voidaan käyttää:

1. Suuri: Äsimmäinen herkkyys, jossa on tieto on tarkoitettu tietyille henkilöille. Näiden tietojen katoamisesta tai vaarantumisesta voi aiheutua vakavia taloudellisia, oikeudel-

lisia tai maineen menetyksiä
2. Keskisuuri: Käyttö ainoastaan tiettyjen valtuutettujen ryhmille laillisen liiketoiminnan suorittamiseen. Näiden tietojen katoamisesta tai vaarantumisesta voi aiheutua merkittäviä kielteisiä taloudellisia vaikutuksia
3. Alhainen: Käyttö organisaation sisäisiin tarkoituksiin. Näiden tietojen katoamisella tai vaarantumisella voi olla kielteinen ja vähäinen taloudellinen vaikutus

Tunnetut käyttötavat

Omaisuuserien arvostus on keskeinen laajalti hyväksytty tapa riskienarvioinnissa, joita esiintyy standardeissa ja hyvissä käytänteissä. Näiden painotukset eroavat vain niiden lähestymistavan, tarkoituksen ja yleistavoitteiden osalta.

Seuraukset

Tämän tietoturvamallin käytöstä on seuraavat edut:

1. Yritys saa täyden ja realistisen kuvan omaisuuseristä, jotka ovat sen kriittistä liiketoimintaa
2. Omaisuuserien arvostus dokumentteja voidaan kehittää tai päivittää vahingoista toipumisen tai liiketoiminnan jatkuvuussuunnitelmien yhteydessä
3. Laadullinen arvo voi olla helpommin saatavissa kuin kovat kustannukset, joita vaaditaan määrällistä omaisuuserien arvioinnin yhteydessä. Tämä nopeuttaa riskinarviointia.

Tämän tietoturvamallin käytöstä on seuraavat haitat:

1. Organisaatio voi joutua muuttamaan toimintatapoja, jos se katsoo ettei omaisuuserän arvo ja siihen harkittu muutos enää kannata

C.3 Uhkan arviointi

Uhkien todennäköisyys tai mahdollisuus organisaation määrittämille omaisuuserille tai esineille, joita tulisi suojella vaarallisilta tapahtumilta. Uhkien arviointi tunnistaa nämä uhkat ja määrittää niiden todennäköisyyden tai niiden esiintymistaajuuden.

Esimerkki

Organisaatio on aloittanut riskinarvioinnin ja tunnistaa seuraavat uhat, joita ovat:

Tiedon omaisuuserätyypit

- Työntekijöiden tiedot
- Rahoitus/vakuutus tiedot ja liiketoiminnan suunnitelmat
- Sopimustietojen ja liiketoiminta suunnitelmat
- Mainokset ja muut julkiset tiedot
- Tietokantojen tiedot

Fyysisen omaisuuden tyypit

- Rakennukset
- Henkilöstö
- Kuljetusvälineet

Organisaatiossa on myös havaittu päätietoturvan tarpeet näille omaisuuserille, käyttämällä tietoturvamallia tietoturvantarpeen tunnistaminen organisaation omaisuuserille (engl. Security Needs Identification for Enterprise Assets) ja kuinka niitä täytyy määritellä näille omaisuuserille.

Tausta

Organisaatio on määritellyt omaisuuserät, jotka ovat sisällytetty riskin hyödykkeiksi ja tunnistavat mitkä tapahtumat voivat aiheuttaa haittaa näille omaisuuserille.

Ongelma

Organisaation omaisuuserät kohtaavat hyökkäyksiä ja vaarantavia tapahtumia kaikista suunnista. Ilman näiden tapahtumien tehokasta tunnistamista organisaatio ei voi koskaan tunnistaa näitä tapahtumia ja määrittää niille todennäköisyyttä niiden esiintymiselle. Organisaation on tunnistettava seuraavat vaikuttavat voimat, joita ovat:

- Tunnistettava ne uhat, jotka potentiaalisesti aiheuttavat vahinkoa
- Organisaation yhtiömuodon vaikutus mahdollisten uhkien lähteille

- Organisaatio haluaa kehittää normi tavan tunnistaa uhkat ja arvioida niiden todennäköisyyden, jotka ovat tasapainossa uhkien arvioinnin kanssa
- Ratkaisujen tulee ottaa huomioon kaikki omaisuuserät haavoittuvuuksien riskinarvioinnissa poislukien tietojärjestelmät

Ratkaisu

Systemaattinen ja selkeä tapa tunnistaa ja arvioida organisaatioon kohdistuvia uhkia ja määrittää niiden suojelun tarve on antaa organisaation arkkitehdin tai suunnittelijan määrittää ne. Määritys sisältää seuraavat vaiheet, joita ovat:

- Uhkien tunnistus. Tunnistetaan todennäköiset uhkat omaisuuserille, jotka määritellään riskinarvioinnissa. Jäljittää näihin omaisuuserille kohdistuvien uhkien toiminta ja seuraukset
- Rakentaa uhkataulukko. Rakennetaan uhkataulukko, jossa ryhmitellään uhkat hyödykeryhmittäin ja tämän jälkeen tunnistetaan uhkan lähde
- Luodaan todennäköisyysasteikko. Luokitellaan tapahtumataajuus tai todennäköisyys tapahtumien esiintymisestä. Asteikko edustaa todennäköisyyttä annettuun luonnolliseen tai vahinkotapatumaan tai hyökkäysyrityksille
- Luokitellaan uhkat. Arvioidaan jokaisen uhkan todennäköisyyden asteikko ja päivitetään uhkataulukko vastaamaan tätä määritelmän numero arvoa.

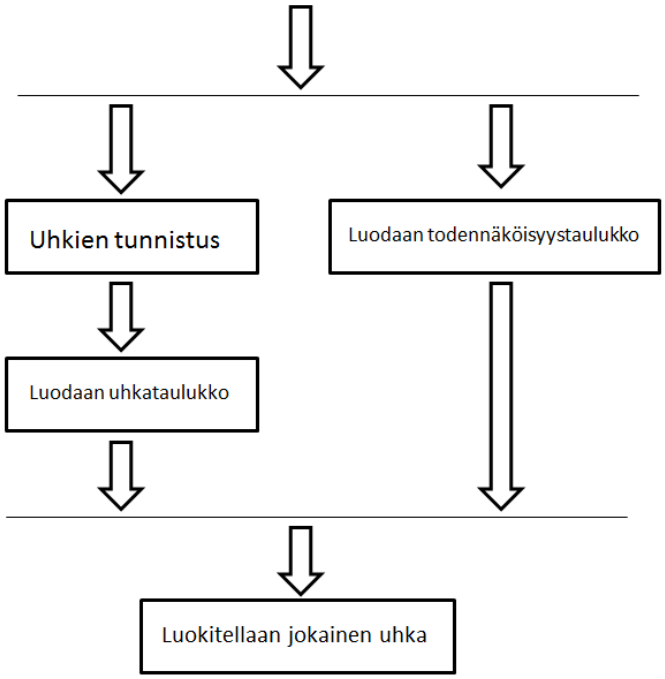
Dynamiikka

Tunnistettavat uhkat omaisuuserille määritellään riskiarvioinnin ja rakennetulla uhkataulukolla. Uhkien todennäköisyysasteikko voidaan kehittää rinnakkain. Lopuksi käytetään uhkien vakavuutta arvioimaan jokainen uhka ja päivitetään uhka taulukossa. Sallittu sekvenssi on esitelty (ks. Kuvio 39).

Täytäntöönpano

Uhkien tunnistamisen prosessi on kuvattu alla:

1. Tunnista uhkat
    - Uhkien lähde käynnistää hyökkäyksen tai aiheuttaa tapahtumia



Kuvio 39. Uhkien arvointisekvenssin rajoitteet

- Uhkan toimita on menetelmä joka aiheuttaa näitä uhkia, kuten haittaohjelmat, huolimattomuus tai veden aiheuttamat oikosulut
- Uhkan seuraus on tietoturvaloukkaus joka johtuu onnistuneesta tunkeutumisen aiheuttamasta vahingosta.

Yleisesti uhkan lähde tai toiminta kootaan yhteen ja ryhmitellään yleisesti uhka ja sisällytetään yksinkertaisesti uhka. Määritellessä uhkia on ainoasataan tarpeellista keskittyä niihin uhkiin, jotka on määritelty riskinarvioinnissa. Vastaavasti, kun järjestelmän rakennetta on muokattu, kuten uusia laitteita on asennettu tai uusia viestintäpolkuja on luotu, niin tällöin uhkamaisema myöskin muuttuu. Suuntaviivat näiden uhkien määrittelemiseksi on seuraavat:

- Erityisen ympäristön uhkat voidaan nopeasti poistaa tietyssä maantieteellisessä tai geologisessa tilanteessa.
- Uhkat, joiden esiintyminen omaisuuserien käyttöajan puitteessa voidaan poistaa. Omaisuuserien käyttöikä voi olla sellainen, että ne voidaan korvata uudella materiaalilla tarvittaessa helposti.

- Uhkat voivat kohdistua vain haavoittuvuuksiin. Jos järjestelmä ei ole alttiina haavoittuvuudelle, niin tällöin ei myöskään ole mitään uhkaa. Esimerkiksi tietoverkon rakenne on määritelty käyttävän Linux koneita, niin tällöin ei Windows IIS web-palvelimen haavoittuvuudesta ole mitään uhkaa.
- Muutokset tietohallinnossa tai muissa yrityksen järjestelmissä muuttaa uhkamaisemaa. Esimerkiksi hyökkäykset, joita ei ollut ennen muutosta ovat mahdollisia, kuten etäyhteyden salliminen organisaatiossa.

Uhkan lähteet voivat olla täten luonnollisia tai ihmisten aiheuttamia. Luonnollisten uhkien lähteenä on ympäristö, kuten tuuli, lumi tai myrskyt. Ihmisen aiheuttamia uhkia voidaan nimetä tarkoitusperäisiin iskuihin tai vahingossa tehtyihin virheisiin.

Uhkan toimet ovat todellisia tapahtumia jotka hyödyntävät löytyviä järjestelmäheikkouksia. Nämä tapahtumat voidaan jakaa luonnollisiin, tahallisiin ja vahingossa tehtyihin heikkouksiin. Luonnollisia uhkia ovat sähköviat, tulvat, tulipalot ja jne. Tahallisia uhkia ovat ulkoiset tai sisäiset hyökkäykset, joiden tarkoitus on uhat suojattavia omaisuuseriä. Vahingossa aiheutettuja uhkia ovat kompastumiset, huolimaton käsittely, tietämättään asennetut virukset jne.

2. Uhkapöydän rakentaminen Ryhmittele omaisuuserät ryhmittäin, jotta siitä tulee hyödyllinen, tällöin lopullinen riski jokaiselle omaisuuserälle voidaan määritellä. Lisäksi uhkien luokittelu takaa, ettei unohdeta tosiasiaa, että samaa uhka toimintaa voi esiintyä eri lähteissä. Samalla uhkalla voi olla eri esiintymistiheys. Esimerkiksi varkauksia voi esiintyä ammattirikollisen tai työntekijän aiheuttamina.

   Uhkan seuraus on sisällytetty kuhunkin toimintaan ja se antaa tuen selvittää mahdollisia tapahtumia. On mahdollista, että uhkataulukon päivitetään haavoittuvuuksien arvioinnin jälkeen, koska uhkien ja haavoittuvuuksien suhde on läheinen. Haavoittuvuuksien tunnistaminen voi johtaa uuden uhkan löytymiseen.
3. Todennäköisyysasteikon luonti Tarkan määrittämisen vaikeudesta huolimatta laadullisia arvoja voidaan käyttää ja numero arvoja voidaan korreloida. Todennäköisyystasoja voidaan esittää (ks. Taulukko 27).

   Huomioitavaa taulukossa on, ettei se pelkästään esittää yhtä tapaa luokitella tapahtu-

mia. Muitakin uhkan arviointi tapoja on olemassa, jotka määrittävät toisenlaisen laajuuden, mutta ne ovat yhtä päteviä tähän tarkoitukseen. Tärkeintä on, että organisaatio käyttää kokoajan samaa luokitusta.

4. Jokainen uhka määritellään

   Jokaisella uhkalla on tietty todennäköisyys tai esiintymistiheys ja jotkut esiintyvät muita useammin, perustuen erityisiin tekijöihin. Huomioitavaa on että tämä ei ole onnistuneiden haavoittuvuuksien esiintymistiheys.

   Uhkien esiintymistiheyden arvioinnin tai ennustamisen harkinta on tarpeellista monissa asioissa. Tekijöitä jotka vaikuttavat luonnollisten uhkien todennäköisyyteen ovat:

   - Etäisyys vaaraa aiheuttavista tehtaista, kuten öljy tai kemiantehtaat.
   - Äärimmäisten sääilmiöiden esiintymistiheys
   - Rakenteelliset toimintaedellytykset, kuten tulipalon esisammuttimet, tukahduttamisjärjestelmät ja muut hätätilanne järjestelmät

   Tekijöitä, jotka vaikuttavat tarkoituksellisten uhkien todennäköisyydelle ovat:

   - Haavoittuvuus on yleisessä tiedossa. Mitä pidempi aika haavoittuvuuden havaitsemisesta, sitä mahdollisempaa on, että hyökkääjät hyödyntävät tätä haavoittuvuutta.
   - Olipa sitten tai ei saatavilla olevaa haavoittuvuutta. Graafinen käyttöliittymä käytöllä on suurempi mahdollisuus sisältää haavoittuvuus, kun komentokehote rajapinnalla.
   - Hyökkäysyritysten suuri määrä lisää todennäköisyyttä, että jokin näistä onnistuu
   - Mahdollisen palkkion tarjoaminen hyökkääjille. Haasteet ja rahalliset palkkiot lisäävät mahdollisuuksia hyökkäyksille riippuen organisaation liiketoiminnasta.
   - Omaisuuserien arvo vaikuttaa enemmän tai vähemmän huomiota organisaatiota kohtaan. Hyökkääjät yleensä kohdistavat hyökkäyksiä sellaisia järjestelmiä kohtaan, josta saa suurta sisällöllistä arvoa.
   - Organisaation järjestelmän haavoittuvuus, joka realisoituu sen haavoittamisen vaikeustasoon. Sellaisen omaisuuserän saaminen haltuun, joka on vahvasti suojeltu vähentää yritysten määrää.

- Julkinen näkyvyys ja liiketoiminnan ilmapiiri. Nämä asiat voivat määräytyä organisaation hyvästä tai huonosta suosiosta voi lisätä hyökkäyksiä.
- Työntekijöiden moraali. Alhaisen moraalin omaavat työntekijät voivat aiheuttaa tahallista tai kostonhimoista toimintaa ja täten lisätä onnettomuuksien tai uhkien mahdollisuutta.
- Menneet syytökset, jotka ovat johtuneet haavoittuvuuksilta johtuneista syytöksistä. Tällöin hyökkääjät pyrkivät helpompaan ja vähemmän riskialttiisiin kohteisiin.

Tekijät, jotka vaikuttavat vahingossa tehtyjen uhkien todennäköisyyteen ovat:

- Osaavan henkilöstön saatavuus, jolloin organisaatio joutuu palkkaamaan epäpätevää henkilöstöä huolehtimaan kriittisistä järjestelmistä. Tämä lisää altistumista virheiden aiheuttamille uhkille.
- Tietoturvaa parantavat hallinnolliset toimenpiteet, kuten käyttäjien koulutus. Nämä toimet lisäävät tietoisuutta eri toimintaperiaatteista ja menettelyjen omaksumisen. Saaduilla toimilla ja taidolla käyttäjät voivat estää sosiaalisia taitoja vaativia hyökkäyksiä tai tulevat tietoisemmiksi tietoturva vaatimuksista.
- Järjestelmämuutosten esiintymistaajuus mukaan lukien korjaukset, päivitykset ja muut muutokset. Mitä enemmän muutoksia tehdään, sitä enemmän on mahdollisuuksia virheiden ilmenemiselle.

Todennäköisesti luotettavimman menetelmän tulevaisuuden määrittämiseen tarvitaan historiallista tietoa. Luonnollisia tapahtumia kirjataan koulutus- ja valtiollisten organisaatioiden toimiesta heidän tutkimukselle. Kaupallisia ja valtiollisia viittauksia tietoturvahyökkäyksiltä on olemassa. Asiaankuuluvia tietoja voidaan myös kerätä organisaation omiin järjestelmiin, joitakin käyttökelpoisia lähteitä ovat:

- Historialliset almanakat luonnonkatastrofeista
- Tietoturva uutiskirjeet ja Web-sivustot. Esimerkkinä CERT, Symantec ja SANS
- Nykyiset ja arkistoidut tunkeutumisenesto tiedot, häiriötilanteiden ja hakujärjestelmien lokitiedostot
- Aikaisemmat arkistoidut uhkan arviointi tiedostot, jos ne niitä on käytettävissä.

Ne voivat sisältää yllättävän tärkeitä tietoja

Luokitus	Todennäköisyys	Kuvaus
6	Äärimmäinen	Uhkaa esiintyy jatkuvasti
5	Erittäin korkea	Toimintaa esiintyy usein
4	Korkea	Uhkaa esiintyy säännöllisesti
3	Keskitaso	Uhkaa esiintyy harvoin
2	Matala	Uhkan toimintaa esiintyy harvoin
1	Merkityksetön	Uhkan esiintyminen on erittäin epätodennäköinen

Taulukko 27: Todennäköisyyden esiintyminen

Esimerkki ratkaisu

Organisaation varojen tunnistamista (engl. Enterprise Assets) alkaen organisaatiossa on tunnistettu tiedollisia ja fyysisiä omaisuuseriä. Tiedon omaisuuserien tyypit ovat:

- Työntekijöiden tiedot
- Rahoitus/vakuutustiedot ja kumppanien taloudelliset tiedot
- Sopimusten ja liiketoiminnan suunnittelun tiedot
- Tutkimus ja niihin liittyvät tiedot
- Mainokset ja muut julkiset tiedot

Fyysiset omaisuuserät ovat:

- Rakennukset
- Henkilöstö
- Kuljetusvälineet

Uhkien arvioinnin (engl. Threat Assessment) jälkeen organisaatiossa on tunnistettu luettelo uhkista tiedollisille ja fyysisille omaisuusrille.

Tunnetut käyttötavat

Uhkien arviointi on määritelty usein standardeissa, jossa esiintyy määritelmä prosesseja, jotka keskittyvät tunnistamaan uhkia ja määrittämään niiden todennäköisyyttä. Asteikot on määritelty korkean, keskitason ja matalan uhkien todennäköisyydelle. Asteikko sisältää nykyiset tarkastukset ja niiden kyvyn neutralisoida uhkat.

NIST (National Institute of Standards and Technology) kuvaa myös koko riskinhallinta prosessin. Prosessissaan se erottelee asteikossaan uhkat ja todennäköisyydet niiden toteutumisen kahdella erillisellä prosessilla.

Microsoft kuvaa uhkat ja vastatoimien mallit joka tarjoaa vaihtoehtoisia menetelmiä tunnistaa, yksilöidä ja arvioida uhkia uhkamalleilla.

Seuraukset

Tämän mallin käytöstä on seuraavat edut:

- Ratkaisut antavat organisaatiolle käsityksen tekijästä, jotka lisäävät tietoa haitallisten tapahtumien olemassa olosta sekä niiden esiintymistaajuudesta.
- Tunnistaa seuraukset, jos tietty uhka olisi toteutunut.
- Uhkien arviointi on tärkeä osa riskinarvioinninmallissa jotka priorisoivat ja johtavat lopulta tietoturvallisempaan organisaatioon.

Malli sisältää myös seuraavat heikkoudet, joita ovat:

- Tarkkoja historia tietoja ei ole käytettävissä, jolloin organisaatio ei voi hyödyntää uhkien esiintymistaajuus tietoja.
- Kaikkien mahdollisten uhkien kuvailu on liian aikaa vievää. Rajoitteita voidaan asettaa täydellisen uhkamaiseman aikaan saamiselle.

C.4 Haavoittuvuuden arviointi

Haavoittuvuus on heikkous, joka mahdollistaa hyödyntämisen, joka aiheuttaa omaisuuserän tietoturvalle. Organisaation haavoittuvuuksien arvioinnin tunnistaminen auttaa tunnistamaan heikkouden omaisuuserissä ja järjestelmissä, joiden avulla ne tuodaan saataville. Arvioinnin tarkoituksena on tunnistaa niiden vakavuus, jos haavoittuvuutta hyödynnetään.

Tunnetaan myös nimellä

Alttiusanalyysi (engl. Vulnerablility Analysis)

Esimerkki

Organisaatio on aloittanut riskinarvioinnin ja tunnistanut seuraavat mahdolliset omaisuuserät:

Tieto omaisuuserissä

- Työntekijöiden tiedot
- Rahoitus ja vakuutustiedot
- Sopimuksien ja liiketoiminnan suunnittelutiedot
- Tutkimukset ja niihin liittyvät tiedot
- Tietokantojen tiedot

Fyysisissä omaisuuserissä

- Rakennukset
- Henkilöstö
- Kuljetusvälineet

Organisaatio on myös yksilöinyt mahdollisia uhkia omaisuuserille ja ne täytyy nyt määritellä haavoittuvuuksilla, jotka voivat vaarantaa nämä tarpeet.

Tausta

Organisaatio on määritellyt omaisuuserät, jotka sisällytetään riskin arviointiin ja on havainnut mahdollisia uhkia, esimerkiksi soveltaessaan tietoturvamallia uhkan arviointi (engl. Threat Assessment). Sen on nyt tunnistettava haavoittuvuudet, jotka voivat hyödyntää näitä uhkia.

Ongelma

Organisaation omaisuuserät ja kontrollit suojelevat niitä siten, että ne ovat täysin tietoturvallisia tai sitten ne sisältävät useita heikkouksia, joista osaa voidaan myös hyödyntää joka

päivä. Ilman asianmukaista haavoittuvuuksien luettelointia organisaatio ei koskaan voi tunnistaa heikkouksien laajuutta heidän omaisuuseriin.

Miten organisaation tulee ratkaista seuraavat voimat näihin haavoittuvuuksiin? Nämä voimat ovat:

- Organisaatiolla saattaa olla kokemuksia yhdestä työkalusta tai menetelmästä löytää heikkouksia. Se ei kuitenkaan ole tietoinen muista tekniikoista, jotka voivat ratkaista tai paljastaa muita potentiaalisia kriittisiä haavoittuvuuksia.
- Se tarvitsee vain haavoittuvuudet, joiden uhat ovat tiedossa ja siksi organisaation on voitava selvittää, onko tiettyyn haavoittuvuuteen olemassa liittyvää uhkaa.
- Organisaatio haluaisi kehittää yleisen tavan tunnistaa haavoittuvuuksia ja arvioida niiden vakavuutta. Tavan tarkoituksena on taata tapa, joka olisi sopusoinnussa myöhempien haavoittuvuusarviointien kanssa.
- Ratkaisussa olisi otettava huomioon kaikki omaisuuserien riskinarvioinnin piiriin, jotka sisältyvät tietojen ja fyysisten omaisuuseriä. Mieluiten sen pitäisi pystyä käsittelemään haavoittuvuuksia tietojärjestelmissä.

Ratkaisu

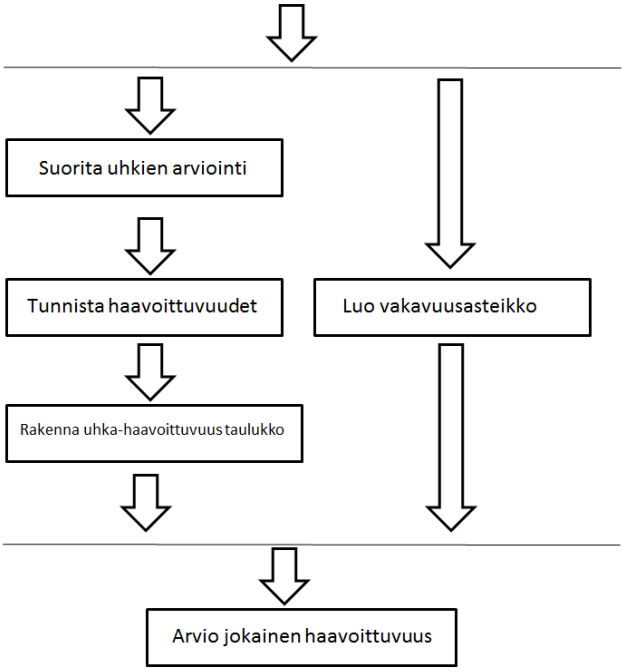
Systemaattinen tunnistaminen ja arviointi todennäköisesti löytää organisaation omaisuuserien haavoittuvuuksia. Tämä prosessi käsittää seuraavat viisi vaihetta:

1. Kerää tietoja uhkista, esimerkiksi tietoturvamallin uhkien arviointi (engl. Threat Assessement) avulla, jolloin mallin tarjoaman uhkataulukossa on saatavissa asianmukaiset tiedot.
- Tunnistaa haavoittuvuudet käyttämällä uhkataulukon tunnistamia haavoittuvuusominaisuuksia ja järjestelmät, joilla suojella niitä riskinarvioinnin laajuudella.
- Rakentaa uhka-haavoittuvuustaulukko, joka luodaan lisäämällä uhkataulukkoon kukin haavoittuvuus.
- Luodaan vakavuusasteikko, jossa on luokitusasteikko haavoittuvuuksien vakavuudelle. Tämän asteikon tarkoituksena on edustaa omaisuuserien määrää, jotka ovat alttiita haavoittuvuuksille. Asteikon tulee sisältää myös mahdolliset vaikutukset miten haavoittuvuutta voidaan hyödyntää.

- Määrittää kukin haavoittuvuus sen vakavuuden mukaan ja päivitä uhka-haavoittuvuustaulukko vastaamaan tätä numeroarvoa.

Dynamiikka

Sallitun sekvenssin suorittamiseksi haavoittuvuuden arviointiprosessi on esitelty (ks. Kuvio 40)



Kuvio 40. Haavoittuvuuden arvointisekvenssin rajoitteet

Ensinnäkin asianmukaiset uhka tiedot kootaan. Toiseksi menetelmiä käytetään tunnistamaan kaikki haavoittuvuudet ja liitetään ne uhkataulukon uhkiin. Luodaan uhka-haavoittuvuustaulukko. Vahvuusasteikko voidaan luoda milloin tahansa. Lopuksi käytämme tätä asteikkoa jokaisen haavoittuvuuden arvioinnissa.

Täytäntöönpano

Prosessi haavoittuvuuksien arvioinnin toteutuksessa on seuraavasti:

1 Kerää uhkatietoa. Näihin tietoihin pitäisi sisällyttää luettelo tapahtumista, jotka voivat aiheuttaa uhkataulukossa
2 Tunnista haavoittuvuuksia käyttämällä joitakin seuraavista menetelmistä tunnistamaan

haavoittuvuuksista hyödyntävistä uhkista uhkataulukossa

2.1 Järjestelmän ominaisuudet

i. Päättyykö ne riippuvien vikojen aiheutumisesta. Harvoin, jos koskaan sovellukset ei ole vuorovaikutuksessa muiden sovellusten tai järjestelmien suorittamien toimintojen kanssa. Vuorovaikutussuhteet voivat olla tietokantataulukoilla jaetut järjestelmäkirjastot, verkkopalvelut, laitteet tai käyttöjärjestelmäresurssit. Sovelluksen käyttäytyminen vikatilanteessa tai niiden riippuvuuksien puuttuminen on hyökkääjien ensisijaisia hyökkäystavoitteita. Esimerkiksi miten sovellus reagoi, kun tietoturva kirjastoa ei voi ladata. Ohittako se kaikki turvallisuus vaatimukset. kirjautumisvirheiden jälkeinen käyttäytyminen, eli jatkuuko vai pysähtyykö kaikki toiminta ja päätyykö toiminta virheilmoitukseen.
ii. Päättyykö ne odottamattomien tietojen syöttöön. Tietojen syötön validoinnin puuttuminen on hyvin yleinen virhe. Se voi olla myös vahingollisinta, koska tulokset tästä voivat vaihdella palvelunestohyökkäyksestä aina järjestelmän pääkäyttäjä tunnusten saamiseen. Puskuriylivuodot ja SQL-injektiot ovat yleisimpiä esimerkkejä tämän luokan hyökkäyksistä.
iii. Päättyykö ne suunnittelusta aiheutuvien haavoittuvuuksien johdosta. Haavoittuvuuksien koon ja monimutkaisuuden kasvaessa, sitä vaikeampi niitä on tunnistaa. Mahdollisuudet hyödyntää suunnittelussa tapahtuvia virheitä kasvaa. Tällaiset suunnitteluvirheet voivat käyttää selväkielisiä protokolien käyttö siellä missä tarvitaan salakirjoituksella suojattuja tietojensiirtoa, kuten päädynhallinta. Suunnitteluvirheinä voidaan mainita myös järjestelmien luvattomat tehtävät ja suunnittelemattomat toiminnallisuudet.
iv. Päättyvätkö ne haavoittuvuuksien täytäntöönpanon johdosta. Tietoturvallinen suunnittelu voi aiheuttaa huomattavaa heikkoutta, jos toteutus on viallinen. Mitä monimutkaisempi järjestelmä on, sitä suuremmat ovat esteet toteuttaa tietoturvallisia järjestelmiä. Mitä suurempi ja monimutkaisempi järjestelmä on sitä enemmän on mahdollisuuksia olemassa oleville toteutusvir-

heille.

Esimerkiksi ohjelmistot, jotka käsittelevät arkaluonteisia tietoja. Tällöin on huolehdittava siitä, että ohjelmistojen ei tule kopioida tietoja väliaikaisesti kiintolevylle tai suojaamattomaan muistiin. Toistuvia hyökkäyksiä täytäntöönpanon heikkouksista ovat verkkohyökkäykset. Tällöin tiedonsiirto on vihamielistä tai vilpillisesti toistuvaa tai viivytettyä. Syöttinä tai vaihtoehtona tällaisessa tapauksissa on, että huijari kalastelee asiakkaita mainostamalla tavaroita erittäin alhaisin hinnoin. Asiakaan innostuttua huijari potentiaaliselle asiakkaalle, ettei mainostettua tavaraa ole saatavilla, mutta hän käynnistää samalla hetkellä (Man in the Middle Attack (MITM)) hyökkäyksen, jossa hyökkääjä voi lukea, lisätä ja muokata osapuolten välisten viestien sisältöä heidän tietämättään.

2.2 Kehityselinkaari

Järjestelmille tai sovelluksille, joita ei ole vielä suunniteltu, pitäisi etsiä haavoittuvuuksia. Tällöin tulisi keskittyä organisaatio tietoturvapolitiikkaan suunniteluilla turvatoimilla, järjestelmän vaatimusmääritelmillä ja myyjien tai kehittäjien tietoturva tuote analyysin. Tässä vaiheessa nämä toteutetut dokumentit ja tiedot tulisivat olla tietoturvallisuuden arvioinnissa käytettävissä.

Järjestelmät, jotka ovat parhaillaan toteuttamisvaiheessa. Niiden haavoittuvuuksien tunnistamisen tulisi laajentaa koskemaan myös tarkempia tietoja, kuten suunniteltujen tietoturva ominaisuuksien kuvailemisen tietoturvasuunnittelu dokumentaatioissa sekä järjestelmäsertifiointi testien tulokset ja arvioinnit. Tällä tietoturvan valvonnan työkalulla voidaan ensin testata sovellukset, ennen niiden tuotantoon siirtämistä. Nämä työkalut sisältävät allekirjoitusperäisiä tarkastuksia, kun tiedossa olevia haavoittuvuuksia testataan.

Tuotannossa olevat järjestelmien haavoittuvuuksien tunnistaminen tulisi perustua järjestelmien tietoturva ominaisuuksien teknisten tai menettelyjen analysointiin suojaamaan järjestelmiä. Järjestelmien suojauksen valvonnan työkalut tai levinneisyystestit tunnistavat heikkouksia tehokkaammin, vaikka ei välttämättä turvallisesti. Niiden toiminta on suoraan testattava tiedettyjen haavoittuvuuksiin, toisin kun teorioida niiden olemassa oloa perustuen dokumentaatioon, politiikkaan tai

vastatoimiin, joilla on tarkoitus estää hyökkäykset. Levinneisyystestit voivat olla monimutkaisia ja edellyttävät monien yksiköiden tietoturva, toimintojen ja sovellusten edelleen kehittämistä. Testi voivat olla tehokkaita, koska niillä testataan järjestelmien heikkouksia sekä niiden vastatoimia.

2.3 Muut

Erikoistuneita teknikoita tietojärjestelmien haavoittuvuuksien paljastamiseksi ovat:

i. Haavoittuvuus skannaukset, joiden toiminnallisuutena on olla automaattisia työkaluja tai menetelmiä tehdä kokeita verkkojen ja sovellusten tai muiden laitteiden haavoittuvuuksien havaitsemiseksi.
ii. Levinneisyystestaus, jonka tarkoituksena on yrittää kiertää, poistaa, muuten kukistaa järjestelmän tietoturvakontrollit käyttäen saatavilla olevia työkaluja tai tekniikoita.
iii. Haavoittuvuusluettelot, jotka sisältävät listan haavoittuvuuksista erityisissä sovelluksissa ja kokoonpanoissa. Esimerkkinä CERT tietokanta, CEV tietokanta ja NIST ICAT.
iv. Avoimen lähdekoodin haavoittuvuustietokanta OSVDB
v. Myyjien tuotteet ja paikkalistat. Kaupalliset myyjät ja avoimen lähdekoodin kehittäjät tarjoavat usein haavoittuvuustietoutta heidän tuotteilleen
vi. Tietoturvan keskusteluryhmät ja postituslistat. Nämä luettelot tarjoavat keskusteluja ja foorumeita haavoittuvuuksille. Esimerkkinä Bugtraq, SANS, Catless

3 Rakenna uhka-haavoittuvuustaulukko

Laajenna uhkataulukkoa haavoittuvuuksilla, luo todellisten haavoittuvuuksien taulukko. Muista, että mitä uhkia on ryhmitelty uhkan lähteiden, kuten luonnollisten, hakkereiden, rikollisten jne. mukaan. Taulukkoon mahtuu myös samojen uhkia useista lähteistä, kuten varkaudesta, jossa työntekijä tai varas esiintyy sen aiheuttajana.

Tämä taulukko valvoo rajoituksia siten, että vain olemassa olevia haavoittuvuuksia ja uhkia tutkitaan. Haavoittuvuuksia havaitaan niihin uhkiin, jotka poistavat haavoittuvuudet tai päivittää uhkataulukon sisältäen uhkan.

Selvittämällä onko haavoittuvuus liittyvä uhka, kysy itseltäsi ja jos on niin, että turval-

lisuusominaisuus kuten luottamuksellisuus, eheys, saatavuus vaarantuu tämän heikkouden seurauksena. Tärkeitä on, että tämä ei ole vastaus, kysymykseen siitä kuka aiheuttaa vaarantumisen tai miten se on tapahtunut, vaan voiko sitä tapahtua.

4 Luo vakavuudenarviointiasteikko

Luo vakavuuden arviointiasteikko ensin määrittelemällä sijoitus, määrittelemällä merkitys ja kuvaus kullekin sijoitukselle, joka on esitelty (ks. Taulukko 28). Luokitus edustaa ominaisuuseriä, jotka ovat alttiita haavoittuvuudelle ja mahdollisille vaikutuksille, jos haavoittuvuutta voidaan hyödyntää. Huomaa, että alue ja kuvaus ovat organisaation harkinnassa. Siinä voidaan muuttaa aluetta, valavuutta aikavälillä ja kuvausta. Tärkein näkökohta on, että taulukko pysyy vakiona koko riskiarvioinnin ja koko organisaationtasolla.

5 Arvioi jokainen haavoittuvuus

Arvioi jokaisen haavoittuvuuden vakavuus alla olevien seikkojen mukaan, jotka ovat:

5.1 Yleiset tekijät.

- Uhkein määrä, joka voidaan toteuttaa tietyn hyväksi käytettävän haavoittuvuuden seurauksena. Lisäksi järjestelmien määrä vaikuttaa haavoittuvuuteen. Jos yksi haavoittuvuus antaa mahdollisuuden monien uhkien toteutukseen ja hyödyntämiseen, silloin vakavuus tulee heijastaa tätä tilannetta.
- Järjestelmien esiintyneisyys vaikuttaa haavoittuvuuteen. Jotkut haavoittuvuudet saattavat vaikuttaa melko harvinaisilta tai harvoin käytetyiltä sovelluksilta tai organisaation resursseilta, kun taas toiset voivat vaikuttaa arjen Internet palveluilta ta fyysisessä infrastruktuurissa.
- Haavoittuvuutta ei ole oletuskokoonpanossa tai asennuksessa.
- Onko olemassa mitään ehtoa, jotka ovat tarpeellisia, ennen kuin haavoittuvuutta voidaan hyödyntää, kuten kompromissia muiden järjestelmien tai tietoturvatoimenpiteinä.
- Onko kyseessä omaisuuserä, joka valvoo tai suojelee muita omaisuuseriä.
- Tarvitseeko hyökkääjän houkutella uhreja vihamielisillä palvelimilla hyödyntääkseen haavoittuvuutta.

5.2 nykyiset tietoturvatarkastukset

Tietoturvatoimet, jotka ovat käytössä merkittävästi vaikuttavat sekä yrityksen haavoit-

tuvuuksien ja vahinkojen vakavuuden alttiuteen.

- Ennaltaehkäisevä valvonta. Nämä tarkastukset käytetään etsimään hyökkäyksiä ja estämään haitallisten tapahtumien pääsemistä määränpäähän. Palomuurit, virus skannerit, koodikatselmukset, salaustekniikat, ovien lukot jne. ovat kaikki ennalta ehkäisevää valvontaa.
- Etsivä valvonta. Etsivää valvontaa käytetään löytämään hyökkäyksiä. Näitä komponentteja käytetään, kun hyökkäys tai tapahtuma on jo päässyt tapahtumaan. Näillä tarkastuksilla pystytään reagoimaan nopeasti vahinkoihin. Teknisinä esimerkkeinä ovat verkko tai palvelin pohjainen tunkeutumisenhavainnointi(IDS), kirjausketju jne. Fyysiseen etsiväpalveluun kuuluu liiketunnistimet. Hallinnollinen valvonta on politiikan sanelema pakollinen työnkierto ja lomat.
- Korjaava valvonta. Valvonnan tarkoituksena on topua menetyksistä tai vahingoista aiheutuneista tapahtumista. Varmuuskopiot, katastrofista elpyminen ja liiketoiminnan jatkumista koskevat asiakirjat ovat esimerkkejä saantokontrolleista

Huomaa, että ehkäisevä valvonta ei sisälly tähän malliin, sillä ne auttavat vähentämään uhkaa tai tapahtuman todennäköisyyttä.

Luokitus	**Todennäköisyys**	**Kuvaus**
6	Äärimmäinen	Haavoittuvuus on triviaalisti hyödynnettävissä ja yleisesti todettu Ihmishenkien menetyksiä ja suuria tuhoja syntyisi järjestelmissä.
5	Erittäin korkea	Haavoittuvuus on helposti hyödynnettävissä ja löytyy järjestelmistä. Joitakin ihmishenkien menetyksiä ja suuria tuhoja ilmenisi järjestelmissä.
4	Korkea	Tämän haavoittuvuuden hyödyntäminen on haaste, mutta se löytyy monista järjestelmistä. Ihmisille aiheutuisi fyysisiä vammoja ja joitakin tuhoja ilmenisi järjestelmissä.

... jatkuu seuraavalla sivulla

Luokitus	Todennäköisyys	Kuvaus
3	Keskitaso	Haavoittuvuutta olisi vaikea hyödyntää ja siihen altistuisivat jotkut järjestelmät. Merkittäviä palveluiden häiriöitä ja kompromisseja omaisuuserien luottamuksellisuudelle, saatavuudelle ja eheydelle aiheutuisi.
2	Matala	Haavoittuvuutta olisi hyvin vaikeaa hyödyntää ilman todellista hyötyä. Lieviä häiriöitä palveluissa lievän omaisuuden vaarantumisen vuoksi.
1	Merkityksetön	Tämä on teoreettinen haavoittuvuus ja olisi vain hyödynnettävissä massiivisessa infrastruktuurissa. Pieniä häiriötekijöitä, eikä turvallisuus ominaisuuksissa tapahtuisi kompromisseja.

Taulukko 28: Haavoittuvuus vakavuusasteikko

Esimerkki ratkaisu

Uhkan arvioinnin (engl. Threat Assessement) jälkeen sisältäen uhkan toiminnan ja haavoittuvuuden arvioiointi (engl. Vulmeravility Assessment) tietoturvamallit organisaatio tunnistaa haavoittuvuudet tiedon ja fyysisistä omaisuuseristä. Taulukot esittävät 29 ja 30) uhkan toiminnallisen taajuuden arviot on otettu molemmista taulukoista uhkan arviointi (engl. Thread Assessment) tietoturvamallista.

Uhkan esiintyneisyys	Haavoittuvuus (Vakavuusaste)
Luonnollinen	
Sähköpiikki tietokonehuoneessa (3)	Ylijännitesuojan puute, UPS-järjestelmä (4)
Sähköisten asiakirjojen menetys (3)	Puutteelliset tai virheelliset tietojen varmuuskopiot (4)
Ammattirikolliset	
Omaisuuserien tietovarkaudet (3)	työntekijöiden herkkyys lahjonnalle (3) Puutteelliset fyysiset tarkastukset asiakirjojen varastoinnissa (lukot) (4)
Työntekijät	
Luvaton pääsy tieto omaisuuseriin (5)	Heikot tietoturvajärjestelyt jotka mahdollistavat luvattoman käytön (3)
Tietojen syöttö virheet (5)	Tiedon valiodinnin puute tiedon syötön yhteydessä (2)
Luottamuksellisten tietojen vuoto (3)	Tietovarojen altistaminen (3)

Taulukko 29: Uhka-haavoittuvuudentaulukko omaisuusrien tiedoille

Uhkan esiintyneisyys	Haavoittuvuus (Vakavuusaste)
Luonnollinen	
Tulipalo (3)	palohälytysjärjestelmän laiminlyönti (6) Palosammutusjärjestelmän käytön epäonnistuminen (5)
Tukevan kalustukden väsymien, rakenteelliset viat (3)	Säännöllisten tarkastuksien puute (4)
Seuranta- ja hälytysjärjestelmien epäonnistuminen (4)	säännöllisten tarkastusten puute (4)

... jatkuu seuraavalla sivulla

Uhkan esiintyneisyys	Haavoittuvuus (Vakavuusaste)
Ammattirikolliset	
Kokoelmien varkaus (2)	Säännöllinen hälytysjärjestelmien testauksen puute (3) Riittämätön fyysisen omaisuuden varastointi ja suojelu (3)
Fyysinen hyökkäys henkilökuntaa vastaan (3)	Perehdytyksessä turvallisuus puutteita (4)
Työntekijät	
Vahingot kokoelmiin (4) Vahingot ajoneuvoihin (4)	Työntekijöiden huolimattomuus (2) Huolimattomuus ajaessa (2) Puutteet säännöllisessä huoltotarkastuksissa (4) Riittämättömät henkilöstön tausta tarkastukset (4)
Varkaudet (2)	puute säännöllisten hälytysjärjestelmien testauksessa (3) Riittämätön fyysisen omaisuuden varastointi ja suojelu (3) Alttius työntekijöiden lahjontaan (4)
Väärät seuranta ja hälytysjärjestelmät (4)	Puute säännöllisissä hälytysjärjestelmätesteissä (3)
Vartiointi	
Vahingot omaisuudelle (3)	Huolimattomuus vartioinnin katselmoinnissa (2)

Taulukko 30: Uhka-haavoittuvuudetulukko fyysisille tiedoille

Vaihtoehdot

SANS ja CERT ovat kaksi tunnettua tietoturvakeskusta. Ne tarjoavat haavoittuvuusluetteloita ja tietokantoja yleisistä haavoittuvuuksista. CERT käyttää puhtaasti määrällistä asteikkoa 0-180 haavoittuvuuksien vakavuuksille. Kun taas SANS käyttää seuraavanlaisia laadullista järjestelmää, jossa esiintyy:

- *Kriittisen haavoittuvuudet* ovat sellaisia, jossa lähes kaikki mahdollinen on hyökkääjän puolella. Nämä haavoittuvuudet vaikuttavat yleensä oletusasetuksissa ja ovat erittäin laajalti käytössä ohjelmistoissa. Pääkäyttäjän salasanan haavoittaminen palvelin tai infrastruktuurin laitteissa ja hyödynnyksen tarvittavat tiedot ovat laajalti hyökkääjien tiedossa.
- *Korkeat haavoittuvuudet* ovat yleensä sellaisia, joilla on potentiaalista tulla kriittisiä, mutta on yksi tai muutama lieventävä tekijä, jotka tekevät hyväksikäytöstä vähemmän houkuttelevan.
- *Kohtalaiset haavoittuvuudet* ovat sellaisia, jossa on mahdollinen riski sen hyödyntämiselle. Tällöin hyökkääjä oleskelee samassa lähiverkossa kun uhri.
- *Alhaiset haavoittuvuudet* ovat sellaisia, jotka eivät vaikuta ylläpitämiseen tai hyödyntäminen ei houkuttele hyökkääjiä. Usein nämä edellyttävät kehittämään erikoistuneita hyökkäysskenaarioita ja johtavat vain rajoittuneeseen vahinkoon.

NIST käyttää seuraavia määritelmiä haavoittuvuuksien vakavuuksille, joita ovat:

- *Suuri* haavoittuvuus (1) voi johtaa erittäin kallisiin aineellisiin tai resurssien menetyksiin ja voi merkittävästi loukata, vahingoittaa tai estää organisaation mainetta, etua tai voi johtaa ihmisen kuolemaan tai vakavaan vammaan.
- *Keskisuuri* haavoittuvuus (1) voi johtaa kallisiin aineellisiin tai resurssien menetyksiin. Saattaa rikkoa, vahingoittaa tai estää organisaation mainetta ja etua tai aiheuttaa henkilövahinkoja.
- *Alhainen* haavoittuvuus voi johtaa joidenkin aineellisten tai resurssien menetyksiin. Saattaa vaikuttaa organisaation maineeseen ja etuihin.

Tunnetut käyttötavat

Haavoittuvuuden arviointi on keskeisin osa kaikkia yleisesti hyväksyttyjä riskiarvioita, mukaan luettuna NIST ja ISO13335-3. Vaikka, ne eroavat hieman niiden lähestymistavan, tavoitteiden ja yleisten tavoitteiden johdonmukaisuudesta.

Seuraukset

Tämä mallin käytöstä on seuraavat edut:

- Organisaatio hankkii kaikista haavoittuvuuksista luettelon, jotka voivat vaikuttaa heidän järjestelmiin. Osa haavoittuvuuksilta saattaa olla aikaisemmin tuntemattomia.
- Organisaatio voi pisteyttää haavoittuvuuksia niiden vaikeusasteen mukaisesti ja niiden mahdollisia vaikutuksia.
- Organisaatio pystyy tunnistamaan mitkä haavoittuvuudet voidaan jättää pois joissa ei ole mukana uhkaa.

Tämä malli sisältää seuraavia epäluotettavuuksia:

- Perusteellisten haavoittuvuuksien skannaus edellyttää monien osastojen koordinointia ja voi olla vaikeaa aloittaa, jos nämä yksiköt eivät tee yhteistyötä.
- Tätä mallia ei voi käyttää paikkaamaan tai poistamaan haavoittuvuuksia. Tietoturvamallien haavoittuvuuden arviointi (engl. Vulnerability Assessment) pitäisi palauttaa riskin määritys (engl. Risk Determination) mallin, jossa lopullinen riski voidaan määrittää ja asianmukainen valvonta voidaan ottaa täytäntöönpanoon.

C.5 Riskien määrittäminen

Riskien määrittäminen (engl. Risl Determination) on viimeinen vaihe riskien arviointiprosessissa ja se sisältää tulokset omaisuusarvojen arvioimisesta, uhkien arvioinnista ja haavoittuvuuksien arvioinnista. Käyttämällä näiden mallien sisällön organisaatio voi arvioida ja priorisoida riskien vaikutuksen sen omaisuuseriin.

Tunnetaan myös nimellä

Riskien arviointi (engl. Risk Evaluation)

Esimerkki Organisaatio on tunnistanut seuraavien omaisuuserien riskit osana sen riskinarviointia:

- Työntekijöiden tiedot
- Rahoitus /vakuutustiedot ja liiketoiminnan suunnittelu
- Sopimukselliset tiedot ja liiketoiminnan suunnittelu
- Tietokantojen tiedot

Fyysiset omaisuuserät osana sen riskinarviointia:

- Rakennukset
- Henkilöstö
- Kuljetusvälineet

Organisaation tulee myös suorittaa kolme tärkeää askelta riskien arvioinnin määrittelyssä omaisuuserien arvostus (engl. Assets Valuation), uhkien arviointi (engl. Threat Assessment) ja haavoittuvuuden arviointi (engl. Vulnerability Assessment): Näiden tietoturvamallien tuottamien tieiojen mukaan arvioidaan kokonaisriski ja tulokset.

Tausta

Organisaatio on määritellyt omaisuuserät sisältäen riskienarvioinnin ja arvioinut sen tärkeät omaisuuserät omaisuuden arvostustaulukossa, uhkien ja haavoittuvuuden arvioinnit. Tämän jälkeen luonut näistä kerätyistä tiedoista uhka-haavoittuvuustaulukon.

Ongelma

Organisaation on saanut määriteltyä omaisuuserän arvioinnin, uhkan ja haavoittuvuuksien arvioinnit. Tämän jälkeen niihin on vaikuttavien riskien suuruus määritettävä. Ilman viralista määritelmää, joilla riski määritellään ja miten voidaan olla varmoja, että näihin tehtävät investoinnit eivät ole liian suuret tai matalat.

Omaisuuseriin vaikuttavien riskien arvioinnissa on otettava huomioon seuraavat voimat:

- Riskien arvioinnin tulokset on ymmärrettävä johtoryhmässä ja heidän tulee käsitellä organisaation riskejä tehokkaasti.

- Riskien määrittämiseen liittyy suoranainen substanssi, uhkan todennäköisyys ja haavoittuvuuden vakavuus.
- Riskienarvioinnin suorittaminen edellyttää resursseja, kuten aikaa, ihmisiä ja tulosten seurantaan sitoutumista.
- Määrälliset riskimittarit edellyttävät suurempaa tarkkuutta ja ovat siksi parempia laadullisia indikaattoreita. Määrällisten tulosten tulee kuitenkin perustua mittauksiin, koska väärä tarkkuus riskitasossa voi olla harhaanjohtavaa.

Ratkaisu

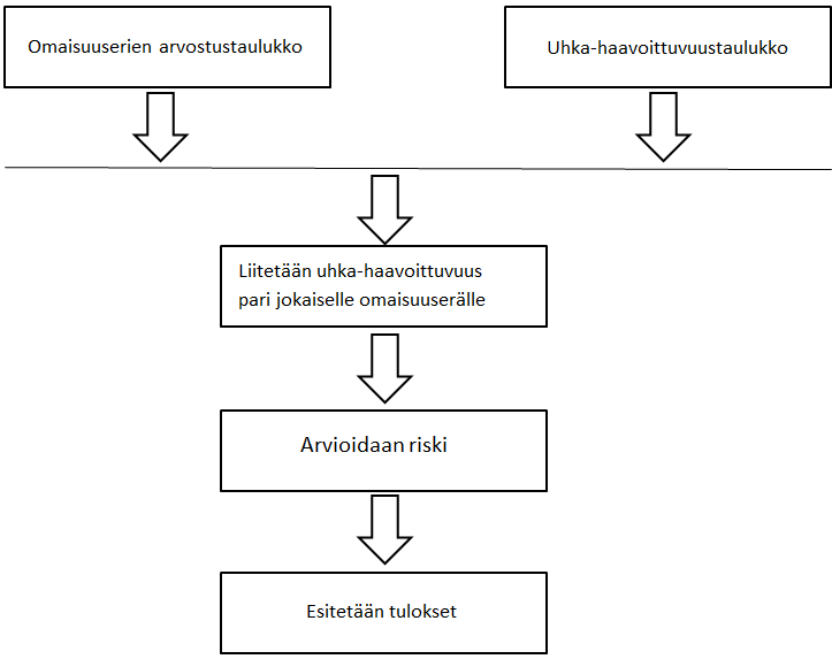
Systemaattisesti määritelty riski esitellään organisaation omaisuuserille. Prosessi sisältää seuraavat neljä askelta:

1. Kerätään tiedot omaisuuserien, uhkien ja haavoittuvuuksien arviointiin tietoturvamalleista. Nämä ovat aiemmat vaiheet tulee olla arvioitu, koska nyt näitä sovelletaan seuraavasti:
   (a) Omaisuuserien arvostustaulukko. Tässä taulukossa on yrityksen omaisuuserien kokonaisarvo.
   (b) Uhka-haavoittuvuustaulukko. Taulukossa luetellaan uhkia ja niihin liittyvät haavoittuvuudet. Jokainen uhka sisältää todennäköisyysluokituksen ja jokainen haavoittuvuus sisältää vakavuusluokituksen.
2. Liitetään uhkat ja haavoittuvuudet omaisuuserä pareiksi. Käyttämällä uhka- haavoittuvuustaulukko, jossa tunnistetaan kaikki uhka-haavoittuvuus parit, jotka aiheuttavat välitöntä vaaraa jokaiselle omaisuuserälle.
3. Arvioidaan riski käyttäen numeraalisia arvoja omaisuuserien arvioinnin, uhkan todennäköisyyteen ja haavoittuvuuksien vakavuuteen. Tulos edustaa lopullista riskiä jokaiseen omaisuuserään.
4. Esitetään tulokset, jolloin nämä lajitellaan käyttäen laadullista asteikko esittämään tuloksia.

Dynamiikka

Riskin määrityksen suorittamiseksi esitellään sekvenssi (ks. Kuvio 41), jonka vaiheet ovat:

- Kerätään ensin omaisuuserien ja uhka-haavoittuvuustaulukko ja haavoittuvuuden arviointi.
- Käytä riskiyhtälöä määrittämään riski jokaiselle omaisuuserälle.
- Lopuksi lajitellaan ja esitellään tulokset laskevassa järjestyksessä.



Kuvio 41. Riskin määrittämisen sekvenssi

Täytäntöönpano

Prosessin toteuttamista varten riskin määrittämistä on kuvattu seuraavasti:

1. kerätään tulokset etujen arvostusmallista C.2, uhkien arvostusmallista C.3 ja haavoittuvuuden arviointitekniikat **??** tietoturvamalleista. Käytetään näitä kolmea mallia ja kerätään tiedot omaisuuden arvostus ja uhka-haavoittuvuus taulukoista.
2. Liittää uhka-haavoittuvuusparit varoihin

   Molemmat sekä uhkien arvostus ja haavoittuvuuden arviointitekniikat on ryhmitelty fyysiseen tai tiedon varojen tyyppeihin. Tässä vaiheessa riskien määritysmallia hyväksikäyttäen on harkittava uhka-haavoittuvuustaulukon parien hyötyjä erikseen. Uhka-haavoittuvuus taulukossa ilmenee kaikki uhkat ja niitä vastaavat haavoittuvuudet. Jokainen näistä pareista voivat aiheuttaa vaaraa yhdelle tai useammalle fyysiselle tai tie-

to omaisuuserälle. Tämän takia on tärkeää tunnistaa kaikki uhka-haavoittuvuusparit, jotka voivat vaikuttaa mihin tahansa omaisuuserään. Tämä on erittäin tärkeää, koska jokaiseen erikseen liitetyt uhka-haavoittuvuusparit voisivat johtaa identtisiin merkittömiin tuloksiin. Yksittäinen uhka-haavoittuvuuspari voivat varmasti vaikutta useaan omaisuuserään suoraan.

3. Riskin arviointi. Riippumatta todellisesta yhtälöstä tai menetelmästä, jota käytetään riskin arvioinnissa, on otettava huomioon seuraavat ominaisuudet:

   - Sellaisten haavoittuvuuksien määrä lisääntyy, jotka mahdollistavat pääsyn varoihin ja järjestelmiin, joten riskit kasvavat.
   - Mitä vakavampi haavoittuvuus, niin sitä suurempi riski.
   - Mitä suurempi määrä uhkia jotka hyödyntävät haavoittuvuuksia, sitä suuremmaksi riski kasvaa.
   - Mitä todennäköisempiä uhkat ovat, sitä suurempi on riski.
   - Mitä arvokkaampia on varat, sitä suurempi on riski.
   - Varoihin ei ole riskiä, jos niihin ei ole määriteltyä uhkaa tai haavoittuvuutta.

   Mikä tahansa määrä yhtälöstä löytyy, niin tällöin voidaan laskea riskien arvo, mukaan lukien esitettävät vaihtoehdot ja tunnetut käyttötavat. Tätä mallia varten käytetään seuraavaa yhtälöä.

   Riski(A) = SUM[uhkat * haavoittuvuus](A)* Varojen arvo(A)

   Tästä voidaan lukea riksi varalle 'A' on summan yhdistelmä uhkien todennäköisyydestä kerrottuna haavoittuvuuksien vakavuudella, kerrottuna hyödykkeen arvolla.

4. Esiteltävät tulokset. Tulokset esitetään laskevassa riskin järjestyksessä. Suurimmalla riskillä on suurin lukuarvo. Kaikkien arvojen tulee olla suurempia kuin nolla ja riskien arvot vaihtelevat riskinarvioinnista toiseen. Tarvittaessa nämä arvot voidaan esittää taulukkomuodossa.

   Tulosten esittäminen selkeässä muodossa on hyvin tärkeää, koska johtoryhmän on kyettävä tulkitsemaan näitä tuloksia ja kehittämään suunnitelmia näiden lieventämiseksi. Yleensä johtoryhmä on kiinnostunut riskien arvon suhteesta muihin varoihin, joten todellinen arvo ei ole tärkeää.

Esimerkki ratkaisu

Käyttämällä uhkien arvostus ja uhka-haavoittuvuustaulukkoa riskien määrityksen tulona, organisaatio voi arvioida sen omaisuuteen kohdistuvia riskejä. Näitä riskejä organisaatiot voivat laskea aikaisemmin esitellyllä riskien arvo yhtälöä hyväksikäyttämällä.

Vaihtoehdot

Vaihtoehtoisena laskentakaavan riskin määritykseen on olemassa Riski = Todennäköisyys * Vahingon mahdollisuus, jossa sekä todennäköisyys ja vahingon mahdollisuusmuuttujat ovat numeerisia arvoja 1-10 välillä. Tällöin pienen riskin arvo lähtee numerosta 1 ja suurin riski saa arvon 100. Tällöin matalan riskin arvot ovat 1-33, keskitason riskit saavat arvon 34-66 ja korkeariskiset saavat arvot 67-100. Huomattavaa on, että tämä menetelmä on uhka pohjanen ja sen antaa erityiselle uhkalle riskiarvon varoihin.

Tunnetut käyttötavat

NIST800-30 käyttää 3x3 matriisia, joka koostuu uhkan todennäköisyydestä ja vaikutuksesta. Uhkan todennäköisyydelle on annettu laadulliset arvot, joita ovat korkea 1,0, keskitaso 0,5 ja matala 0,1. Uhkan laadulliset arvot muunnetaan numeroiksi, joita ovat korkea 100, keskitaso 50 ja matala 10. Laskennassa on vaarana, että ne kerrotaan uhkan todennäköisyydellä, joilla ne vaikuttavat tunnistettuihin uhka-haavoittuvuuspareihin. Vaikka tämä menetelmä on yksinkertainen se ei kuitenkaan tarjoa yleistä riskiluokitusta tietyille varalle, vaan riskin yksittäiselle uhka-haavoittuvuusparille.

Seuraukset

Tämä tietoturvamallin käytöstä on seuraavat edut, joita ovat:

1. Organisaatio voi tunnistaa ja käsitellä sen varoihin vaikuttavia riskejä osana riskinhallinta toimenpiteitä.
2. Laadullisia tuloksia on täten helpompi laskea, priorisoida ja tulkita.
3. Tuloksia voidaan arkistoida ja käyttää seurantaan, kun tehdään uusia riskinarviointeja.

Tämä tietoturvamallin käytöllä on seuraavia vastuita, joita ovat:

1. Riskiyhtälöllä ei voida selittää kaikkia suhteita uhkien, haavoittuvuuksien ja varojen arvoihin.
2. Tulokset perustuvat täydellisesti ja subjektiivisesti varojen arvostus, uhkan arviointi ja haavoittuvuuden arviointi tietoturvamalleihin ja sen takia niitä voidaan pitää vain todennettuina tai taattuina.
3. Koska todellisen riskin arvolle on erilaisia laskentatapoja. Tällöin organisaatioilla voi olla vaikeaa tunnistaa yhtälöitä, joka vastaa heidän riskinarvioinnin tarpeisiin.

D Ohjelmistotason tietoturvamallit

D.1 Tietoturvatavoitteiden dokumentointi

Jotta organisaatio voi tehdä johdonmukaisia ja älykkäitä valintoja sen tietoturvan kannalta, heidän on ymmäerettävä koko järjestelmän tavoitteet ja liiketoimintamallin joka on niiden takana. Tietoturvatavoitteiden dokumentoinnin laiminlyönti ja puuttuminen johtaa organisaatiossa epäjohdonmukaiseen politiikkaan ja sopimattomiin mekanismeihin.

Ongelma

On olemassa erilaisia menetelmiä, joita käytetään ohjelmistojen kehittämiseen. Alkuvaiheessa tärkeänä toiminnallisena vaiheena useimmissa kehitysprosesseissa liittyy vaatimuksien kerääminen ja määrittäminen. Toiminnallisten ydin vaatimuksien määrittäminen on yksiselitteisesti tehtävä aikaisessa kehittämisvaiheessa. Ei-toiminnallisten vaatimukset, kuten tietoturva jätetään usein epämääräiseen tilaan tai sitä ei määritellä lainkaan. On olemassa erilaisia ongelmia, joita voi ilmetä tietoturvan tavoitteita ei ole dokumentoitu.

Kehitystiimin dokumentoimatta jättämien vaatimuksien ja määritelmien takia on yksittäisten kehittäjien mahdoton tehdä yhdenmukaisia tietoturvaavapäätöksiä, jotka kattaisivat koko järjestelmän toiminnallisuuden sekä sen elinkaaren ajan. Tietoturvavaatimusten epämääräisyydestä johtuen kehittäjät voivat kohdistaa tietoturva määritykset vääriin uhkiin tai jopa rakentaa ne toimimaan sopimattomia toimenpiteitä vastaan. Näiden toimien seurauksena järjestelmän yleinen tietoturva kärsii, koska sen on niin vahva tai turvallinen kuin sen heikoin lenkki. Liian heikot komponentit vaarantavat järjestelmän turvallisuuden. Liian vahvat komponentit eivät paranna tietoturvallisuutta, koska yleensä hyökkääjät kohdistavat toimenpiteensä heikkoja puolustusmekanismeja vastaan. Vahvat komponentit voivat myös heikentää käytettävän järjestelmän käytettävyyttä ja suorituskykyä.

Pahin mahdollinen seikka olisi se, että kehittäjät eivät ole kiinnostuneet tietoturvan käsitteistä koko kehitysprosessin aikana. On yleisesti tunnettu seikka, että tietoturva tulee ottaa huomioon ja rakentaa heti järjestelmän kehittämisen aloituksesta lähtien. Tietoturvaa on hankala lisätä valmiiseen järjestelmään kustannustehokkaasti tai rakentaa siitä tehokasta, jos sitä ei ole otettu kehityksen aikana huomioon.

Ilman organisaation tietoturvan tavoitteiden ymmärtämistä kehittäjien on mahdotonta rakentaa järjestelmiä oikein. Liiallinen tai vähäinen tietoturva johtaa väkisin vääränlaiseen tietoturvatasoon ja täten järjestelmäkehityksen hintana voi olla ylisuuret kehityskustannukset.

Ratkaisu

Organisaation tulee dokumentoida tietoturvan tavoitteet hankkeiden alkuvaiheessa vaatimusten määrittelyn ja keräämisen osana. Riippumatta minkälaisesta projektista on kyse, sen tietoturva vaatimukset tulisi käsitellä varhaisessa vaiheessa. Vaikka näintä määritelmiä ei usein ole mahdollista dokumentoida alkuvaiheessa, niin niitä pitäisi pyrkiä dokumentoimaan, koska suurimpien tietoturva riskien määrittely on tietoturvan kannalta elintärkeää.

Spiraalimaisessa kehitysmallissa, jossa tarkoituksena on tunnistaa kukin kehitysiteraatio ja huomioida merkittävimmät jäljellä olevat tietoturvariskit. Tässä mallissa tietoturvan tavoitteiden dokumentointi ei johda liian suuren asiakirjaan, vaan niiden tulisi olla tarkoitettu järjestelmäkehittäjät kohderyhmänään. Korkean tason dokumentaation tietoturva vaatimusten tulisi tehdä seuraavasti:

- Tunnistaa käyttäjäluokat ja näiden luokkien suoritusoikeudet
- Määrittää suhteellinen merkitys luottamuksellisuuden, eheyden, saatavuuden ja hallintakustannukset huomioiden toiminnallisuuden tärkeämpänä tekijänä
- Lakisääteiset rajoitukset sen eri tiloille, kuten saatavuudelle, yksityisyydelle ja salaukselle.
- Lisätä riskianalyysi, jossa määritellään minkälaiset tappiot järjestelmän käytöstä on sidettäviä.

Tietoturvan tavoitteiden dokumentoinnin jälkeen ne tulisi jakaa koko kehitystiimin saataville. Kehittäjät eivät saa tehdä paikallisia päätös kompromisseja, joiden vaikutukset heijastaisivat suhteellisiin tavoitteisiin, jos he eivät ymmärrä mitä nämä tavoitteet ovat. On myös tärkeää, ettei vain tietoturva ihmiset ymmärrä näitä tavoitteita. Tällöin varmistutaan, että ristiriidan tietoturvan ja muiden tavoitteiden välillä ratkaistaan kehityksen varhaisessa vaiheessa.

Projektin edetessä tietoturvan tavoitteet ja kaikkien muiden toiminnallisten ja ei-toiminnallisten vaatimuksien yksityiskohdat hiotaan niin yksityiskohtaisesti esiin ja kaikki konfliktit näiden

välillä selvitetään. Tietoturvan tavoitteiden dokumentointi tulisi tarkastaa säännöllisin väliajoin, koska on väistämätöntä että muutoksia tapahtuu.

Kysymykset

Tietoturvan tavoitteiden dokumentoinnissa on ymmärrettävä koko järjestelmän tietoturva. Huomioitavia seikkoja ovat:

- Tietoturvan tavoitteiden kehityksessä on tunnistaa eri luokkien sidosryhmät, kuten loppukäyttäjät ja pääkäyttäät. Jokaisen sidosryhmän tulisi lisätä prosesseihin. Lisäys voi selventää yleisiä tavoitteita ja auttaa löytämään kompromissin tietoturvan ja muiden tavoitteden analyysissä.
- Vältä kiusausta vaatia sopimattomien tietoturvajärjestelyjä. Dokumentin tavoitteena on tukea miksi näitä ala parhaita tietoturva toimia tarvitaan ja miksi ne ovat kustannustehokkaita.
- Sen tulisi kuvat nimenomaan toiminnallisia vaatimuksia ja niihin liittyvät kulut, jotka tietoturva edellyttää.
- Mieti tietoturvapolitiikkaa ja menettelyjä kun määrität tavoitteita. Turvallinen hallintajärjestelmä tili ei ole hyvä, jos määriteltyä politiikkaa ja menettelyjä ei ole otettu täytäntöönpanossa.

Määritellessä tietoturvan saavuttamisen edellytyksiä on ymmärrettävä liiketoiminta kysymykset, mukaan lukien oikeudelliset ja sääntelystä johtuvat kysymykset.

- Käyttäjä data voi sisältää joitakin vastuita ja siihen voi liittyä väärinkäyttöä. Esimerkiksi luottokortit vaativat suojausta. Niihin sisältyy luottokorttiyhtiöiden vaatimuksia ja automatisoitua käyttöä. Yleensä sosiaaliturvatunnusten keräämiseen ja käyttöön liittyy rajoituksia. Web-sivustoille voi olla rajoituksia mitä tietoja saa kerätä alaikäisiltä. Tietoturvan tavoitteet dokumentti tulisi vastata näihin vaatimuksiin.
- Jos organisaatio tarjoaa palveluita web-sivustoilla, näihin voi kohdistua väärinkäyttöä. Tällöin organisaation tulisi ottaa vastuu näiden väärinkäytön estämiseksi. Tiedostojen varastointi voi johtaa laittomien ohjelmistojen tai lapsipornon levitykseen tai kunnianloukkauksista johtuviin korvauksiin. Anonyymeja sähköpostitilejä voidaan käyttää laittomaan toimintaan. Tietoturvan tavoitteet dokumentissa tulisi ottaa kantaa näi-

hin oikeudellisiin ja lainsäädännöllisiin rajoituksiin.

- On ymmärrettävä, että sinut voidaan haastaa oikeuteen kaikesta mihin kirjaudut. Tietoturvan tavoitteissa pitäisi selittää kehittäjälle nämä piilokustannukset, jotka liittyvät muihin tietoihin joihin käyttäjät kirjautuvat.
- Tunnistaa että usein paras puolustus korvausvaatimuksiin on parhaisiin käytäntöihin sitoutuminen. Näitä ovat parhaat käytännöt ja teollisuus standardien käyttö, jotka myös tulisi mainita dokumenteissa.
- On tärkeää, ettei Internet portaali ole kultalautanen. On tärkeää tunnistaa Internet pääsy tekee rajapinnasta haavoittuvan ja kohteen muista heikoista rajapinnoista.

Esimerkki

On huomioitava että on olemassa monia ohjelmistoprosesseja dokumentoida järjestelmävaatimuksia, joista yksi osa on tietoturvan tavoitteet. Niiden käytöstä on joskus vaikea mainita, koska näitä kokemuksia ei ole useinkaan dokumentoitu tietoturvan tavoitteisiin.

Kompromissit

Tietoturvan luokitus	Selite
Vastuullisuus	Tämä malli auttaa varmistamaan että asianmukaisia kompromisseja tehdään vastuullisuuden ja muiden vaatimusten välillä
Saatavuus	Katso vastuullisuus
Luottamuksellisuus	Katso vastuullisuus
Eheys	Katso vastuullisuus
Hallittavuus	Tämä malli parantaa usein hallittavuutta, koska asian mukaiset tietoturvan toimenpiteet lisätään heti järjestelmän kehittämisen alussa. Tällaiset toimet ovat yleensä helpommin hallittavissa, kuin ratkaisut jotka lisätään myöhemmässä vaiheessa
Käytettävyys	Katso vastuullisuus
Suorituskyky	Katso vastuullisuus

... jatkuu seuraavalla sivulla

Eturyhmät	Selite
Kustannukset	Tämän mallin käyttää kasvattaa todennäköisesti kustannuksia lyhyellä aikavälillä, mutte sen pitäisi vähentää sitä pitkällä aikavälillä. Suunniteltaessa järjestelmä tietoturvamallia hyväksikäyttäen kehittäjät voivat olla varmoja, että kustannukset ovat pienemmät, kun tietoturvaongelman jälkeiset kustannukset, joita voi ilmetä myöhemmin.

Taulukko 31: Tietoturvaluokitusten vaikutus tietoturvan määritykseen

Liittyvät mallit

Jaa vastuut tietoturvalle (engl. Share Responsibility for Security) malliin, joka jakaa tietoturvanäkökohdat kehitystiimille. Tietoturvan tavoitteet on dokumentoitu tähän mallin ja niiden on oltava kaikkien tiimin jäsenten tiedossa.

D.2 Turvallisuuden vastuiden jakaminen

Turvallisuuden vastuiden jakaminen (engl. Share Responsibility for Security) tietoturvamalli tekee kaikista kehittäjistä vastuullisen tietoturvallisen sovelluksen tekijöitä. Tietoturva on enemmän kuin salaus, virustorjunta ja palomuuri. Jokainen järjestelmäelementillä voi olla tietoturvanäkökohta jolloin järjestelmäkehittäjien täytyy ymmärtää ja käsitellä tätä huolenaihetta. Mallin käytöllä vältetään vastakkainasettelu tietoturvakavereiden ja muun kehitystiimin välillä.

Tunnetaan myös nimellä

Velvollisuuksien erottamatta jättäminen (engl. Non-Separation of Duty)

Ongelma

Tietoturvasta huolehtiakseen, yleensä projektissa nimetään tähän tehtävään erillinen henkilö tai tiimi, jonka vastuu alueena järjestelmän tietoturva. Yleensä tällaisessa tilanteessa nimetyllä henkilöllä ei ole valtaa toteuttaa mitään todellisia muutoksia. He voivat vain tehdä suosituksia, mutta ne saavat vain yleensä kriittisiä kommentteja osakseen. Eri järjestelmäosien kehittäjät toteuttavat ne itsenäisesti ottamata osaa vaikutuksiin, jotka voivat aiheutua muiden osien välillä. Tällöin usein uhrataan järjestelmän tietoturvan toiminnalliset ja ei-toiminnalliset vaatimukset. Tietoturvasta vastaavien ja muun ryhmän välille voi muodostua tarpeeton epäoikeudenmukainen suhde, kun toiminnallisten ja ei-toiminnallisten vaatimusten tarpeellisuudesta käydään keskustelua. Kehitystiimi saattaa tehdä päätöksiä riippumatta tietoturva seurauksista, koska he eivät vastaa näistä vastuista, toisaalta tietoturva tiimi ei ota huomioon näiden vaatimusten tasapainottamista.

Ratkaisu

Tämä tietoturvamalli jakaa tietoturva vastuut kaikille järjestelmän kehittäjille, jolloin yksittäisen tai tiimin ei pidä olla vastuussa tietoturvasta.

Yksi syy jakaa tietoturvan vastuut on tasapainottaa tietoturva asianmukaisesti muiden toiminnallisten ja ei-toiminnallisten vaatimusten kanssa. Kaikkien kehittäjien täytyy ymmärtää tietoturvan vaikutus heidän tekemän osan muiden tietoturva ja muiden vastuiden välillä.

Toinen syy tietoturvan vastuun jaossa on kannustaa heitä tekemään alusta alkaen turvallisia järjestelmiä, eikä yrittää lisätä tietoturvaa lisäosana järjestelmään jälkikäteen. Tekemällä koko tiimistä tietoturvavastaavia mahdolliset uhkat ja heikkoudet voidaan kartoittaa sen koko elinkaaren ajalta. Tällöin monia ongelmia voidaan ratkaista aikaisemmin kun niitä on helppo tehdä ja korjata.

Tämän tietoturvamallissa tietoturva on tyypillisesti yhtä vahva kuin sen heikoin lenkki. Jos kehittäjistä osa suhtautuu tietoturvaan vakavasti ja toiset eivät on heidän tietoturvaan käytetyt panostukset hukkaan heitettyä. Ilmiselvät haavoittuvuudet vähemmän suojatuissa järjestelmän osissa johtavat usein vaarantumisille. Tämän takia kehittäjien olisi tunnistettava tietoturvan seurantavaikutukset komponentteihin ja täten varmistaa sen asianmukainen ja sa-

mantasoinen taso koko järjestelmässä.

Lopuksi, tämä tietoturvamalli parantaa tietoturva yksinkertaisesti ottamalla enemmän ihmisiä mukaan analyysiin ja ongelmakeskusteluun. Tietoturva paranee usein, jos järjestelmä heikkouksia tarkastelee useampi ihminen. Ihmiset tuovat eri näkökulmia ja tekevät erilaisia oletuksia ja prosessi jakaa vastuu suuremmalle määrälle ihmisiä.

Tämä malli ei suositella korvaamaan tietoturvan sisällöstä vastaavaa asiantuntijaa. On kuitenkin tärkeää, että joillakin jäsenillä on syvällinen ymmärrys tietoturvan uhkista, heikkouksista ja teknologisista ratkaisuista, joilla niitä voidaan käsitellä niitä. Asiantuntijoita tulisi hyödyntää resursseina, jotka voivat auttaa koko kehitystiimiä kun se ratkoo tietoturva ongelmia.

Kysymykset

Kaikissa muissa paitsi rutiini kehitystyössä, joidenkin toiminnallisuuksien kehitys edeltää tietoturvamekanismien sisällyttämistä. On mahdotonta ymmärtää tietoturva seuraukset vasta kun merkittäviä toiminnallisia vaatimuksia on ymmärretty. On kuitenkin tärkeää, että tietoturvan mekanismeja sisällytetään niin paljon kuin mahdollista.

Toistuva prosessi, saattaa olla tarpeen jättää tietoturvan ensimmäisestä iteraatiosta, mutta sen pitäisi ehdottomasti sisällyttää toisen iterointiin. Tietoturva mekanismin poistaminen viimeiseen vaiheeseen asti tuo ongelmia. Yksi hyvin yleinen, erityinen esimerkki tästä on kehittää sovellus ja sitten yrittää ottaa sen palomuurin takana käyttöön vain huomatakseen, että kriittiset palvelut eivät toimi palomuurin takaa.

Järjestelmä kehittäjien olisi tunnustettava ohjelmiston käyttö ja tarjota tarvittavaa koulutusta, mekanismeja ja takeita, jotta operaattorit, pääkäyttäjät ja käyttäjät voivat aktiivisesti ja tehokkaasti osallistua ohjelmiston ylläpitämisessä ja sen tietoturvan kehittämiseen.

Ylläpidon ohjelmoijat ovat toinen ryhmä, joka on katsottava edistää yleistä järjestelmän tietoturvaa. Kehittäjien täytyy pitää huollon ohjelmoijat mielessä, kun he kehittävät tietoturvakriittisten elementtejä. Kehittäjien pitäisi tarjota mielekkäitä kommentteja tietoturvasta.

Esimerkit

Microsoft ilmoitti että organisaatio aloittaa yrityksen laajuisen kampanjan, jossa määritellään tietoturvavastuu kaikille ohjelman. He ovat kouluttaneet kuukauden kaikkia kehittäjiä tietoturvakoulutusohjelmassa. Organisaatio myönsi julkisesti, että aikaisempi lähestymistapa tietoturvaan ei ollut riittävä.

Kompromissit

Tietoturvan luokitus	Selite
Vastuullisuus	Tietoturvamalli parantaa vastuullisuutta, koska sen avulla kehittäjät, suunnittelijat ja muut sidosryhmät ymmärtävät paremmin ja voivat parantaa yleistä sovelluksen tietoturvaa.
Saatavuus	Katso vastuullisuus
Luottamuksellisuus	Katso vastuullisuus
Eheys	Katso vastuullisuus
Hallittavuus	Tietoturvamalli vaikuttaa hallittavuuteen, joko positiivisesti tai negatiivisesti, koska kehittäjät, suunnittelijat ja muut sidosryhmät arvioivat tietoturvan kompromisseja ja hallittavuutta.
Käytettävyys	Katso hallittavuus
Kustannukset	Tietoturvamalli lisää kustannuksia lyhyellä aikavälillä, koska kehittäjien täytyy olla tietoturvakoulutettuja. Tämä kuitenkin vähentää kehitysaikaa ja kustannuksia poistamalla ylimääräiset tietoturva tiimit, jotka eivät ymmärrä liiketoiminnan päätöksentekoprosesseja. Lyhyen aikavälin investoinnit tietoturva koulutukseen ihannetapauksissa vähentävät pitkän aikavälin kustannuksia tuottamalla varmempia järjestelmiä.

Taulukko 32: Tietoturvaluokitusten vaikutus tietoturvan määritykseen

Liittyvät mallit

Tietoturva tavoitteiden dokumentointi (engl. Document Security Goals) liittävä malli, joka vahvistaa tietoturvapolitiikkaa. Tietoturva tavoitteiden dokumentointi on esiaste tämän malliin tai jota tulisi käyttää rinnakkain. Kaikkien järjestelmäkehitykseen olisi ymmärrettävä järjestelmän tietotutuvatavoitteiden dokumentointi.

Punaisen ryhmän suunnittelu (engl. Red Team Design) liittyvä malli, joka kannattaa punaisen joukkueen suunnittelua, koko kehityssyklille. Punaiselle ryhmälle voi olla jaettu vastuut, sillä se edistää paremman tietoturvan ymmärrystä.

E Tietoverkkotason tietoturvamallit

E.1 Etuvarustus (Demilitarized Zone)

Organisaatiot, jotka julkaisevat tietoa Web-tekniikoilla, pitää huolehtia heidän palveluiden helposta saatavuudesta. Nämä palvelut ovat kuitenkin helppo kohde hyökkäyksille Internetistä käsin. Etuvarustuksen tarkoituksena on erotella liiketoiminnan toiminnallisuus ja tieto Web-palvelimista siten, että tietoverkkoon on vaikeampi hyökätä sen kerroksellisuutensa vuoksi ja varmistaa myös, että web-palvelut ovat riittävällä tietoturvalla suojattu.

Esimerkki

Internet järjestelmän pitävät sisällään asiakkaiden profiilitietoja, sekä muita organisaation suojattavia tietoja, joista mitkä tahansa voivat joutua hyökkääjien varastamiksi tai korruptoimiksi. mutta näiden tietojen on oltava organisaatiotasolla saatavilla, mikä tekee näistä haavoittuvaisia.

Organisaatiot voivat käyttää palomuuria hallitakseen pääsyä näihin järjestelmiin Internetistä käsin. Palomuurit tulisivat määrittää siten, että ne sallisivat vain saapuvan liikenteen pääsyn Web-palvelimiin. Palomuurit tulisi määrittää oikein, jotta ne toimisivat oikein. Väärä määrittäminen voi mahdollistaa suoran pääsyn organisaation suojattaviin resursseihin. Palomuurien määrittämistä hankaloittaa se seikka, että mitä käytettävissä olevaa Web-pohjaista järjestelmää, useiden palvelimien tulisi tukea kuormituksen tasausta tai vikasietoisuutta. Näiden järjestelmien ollessa korkea toiminnallisia lisäprotokollat on sallittava palomuurin läpi, jolloin konfiguraatio virheet ovat erittäin todennäköisiä.

Sisältö

Sovelluspalvelinarkkitehtuurin tarkoituksen on mahdollistaa Web-teknologiset sovellukset. Liiketoiminnallisen ja dynaamisen Web-sisällön luominen on sovelluspalvelinten tehtävä. Kaikki niiden staattinen sisältö on säädetty Web-palvelimissa, joiden dynaamiset sisällöt tulisi kulkea suojatun käänteisen välityspalvelimen (engl. Protection Reverse Proxy) kautta, koska sovellukset pitävät sisällään tietoa käyttäjistä ja sisältävät tärkeitä toiminnallisuuksia käyttäjilleen, mutta ovat erittäin alttiita mahdollisille hyökkäyksille.

Ongelma

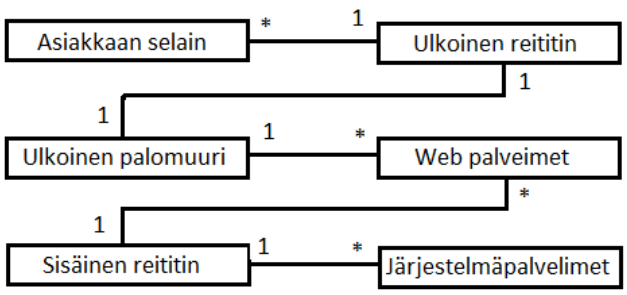
Internet teknologian järjestelmät ja erityisesti julkisen Internetin järjestelmät ovat niiden toimivuuden, resurssien ja tietojen takia säännöllisten hyökkäysten kohteena. Näiden ongelmien ratkaiseminen edellyttää:

1. Tietoturvaratkaisujen kustannukset ovat yleensä korkeat, mutta hyökkäyksistä johtuvien vaurioiden, varkauksien ja näistä johtuvien asiakkaiden menetyskin, voi tulla myös erittäin kalliiksi. Jos hyökkääjien motiivit organisaatiota kohtaan on saavuttaa taloudellista voittoa tai julkisuutta, on tämä riski korkeampi, jolloin mikä tahansa vastatoimi tätä tasoa kohtaan nostaa kustannuksia, joilla estää tunkeutumisia.
2. Jos kaikki hyökkäykset halutaan estää mihin tahansa järjestelmänosaan on tunkeutumisesta tehtävä erittäin vaikeaa. Tämä turvallisuus kuitenkin tekee järjestelmästä niin vaikeita käyttää, että se no ristiriidassa avoimen ja helppokäyttöisen järjestelmän määritelmästä.

.

Ratkaisu

Organisaation tietoverkkoon tarjotaan alue, jota kutsutaan etuvarustukseksi (engl. Demilitarized Zone (DMZ)), joka on erotettu järjestelmän ulkoisille käyttäjille ja sisäisille toiminnoille sekä tiedolle. Tämä alue sisältää eri Web-palvelimia ja muita järjestelmiä, kuten (Exranet, vpn ja sähköposti) ja tällä voidaan rajoittaa ulkoapäin tulevaa verkkoliikennettä tiettyihin fyysisiin palvelimiin ja sisäisiin järjestelmiin. Etuvarustus edellyttää seuraavia seikkoja (ks. Kuvio 42).



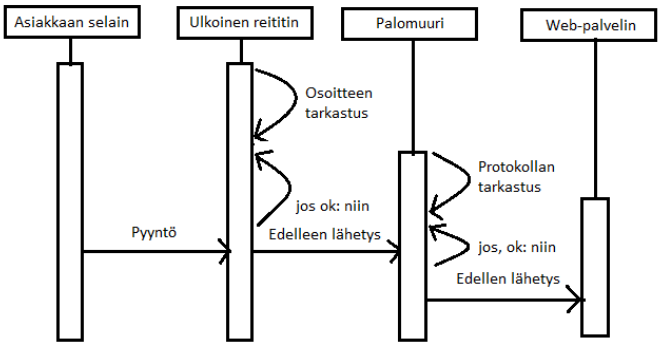
Kuvio 42. Etuvarustuksen (DMZ) rakenne

1. Ulkoinen reitittimen, joka on suodatusreititin (ks. liite A A ja liite C E.2). Reitittimen pääasiallinen tehtävä on varmistaa, että kaikki saapuva liikenne ohjautuu ulkoiselle palomuurille. Toisinsijaisena vastuuna voidaan pitää hyökkääjien tuottaman toiminnan poispitämistä.
2. Ulkoisen palomuurin tehtävänä on vastaanottaa ulkoiselta reitittimeltä saapuvaa liikennettä ja suorittaa tämän tarkempi analyysi. Pyynnön ollessa oikeutettu, se toimitetaan asianmukaisesti eteenpäin Web-palvelimille.
3. Web-palvelimet tarjoavat pääsyn tarjottaviin toiminnallisiin sovelluksiin ja tietoihin. Organisaatiolla voi olla useita palvelimia, joita käytetään kuorman tasaajina. Palvelimet vastaanottavat palomuurilta tulevat palvelupyynnöt ja palvelut joita pyydetään. Pyyntö staattisille resursseille, kuten kiinteille HTML-sivuille tai valokuviin voidaan toimittaa paikallisen levyn välimuistiin. Pyyntö dynaamisiin tietoihin toimitetaan ulkopuolelta tuleviin pyyntöihin suojatun käänteisen välityspalvelimen kautta (engl. Protection Reverse Proxy) kautta. Ei toiminnalliset sovellukset, kuten Servletit tai ASP.NET-sivut tulevat toimimaan Web palvelimilla, jotka ovat alttiita suorille hyökkäyksille. Vaikka Web-palvelimia kuvataan, nämä palvelimet voivat tukea pääsyn tietoihin muita protokollia käyttäen, kuten FTP.
4. Sisäinen reititin, joka on suodatusreitin, jonka pääasiallinen tehtävä on varmista, että sen läpi kulkee vain laillista liikennettä Web-palvelimien läpi sisäiseen verkkoon.
5. Sovelluspalvelimet tarjoavat alustan, jossa sovellukset toimivat. Nämä ovat tyypillisesti Web-komponentteja.

Dynamiikka

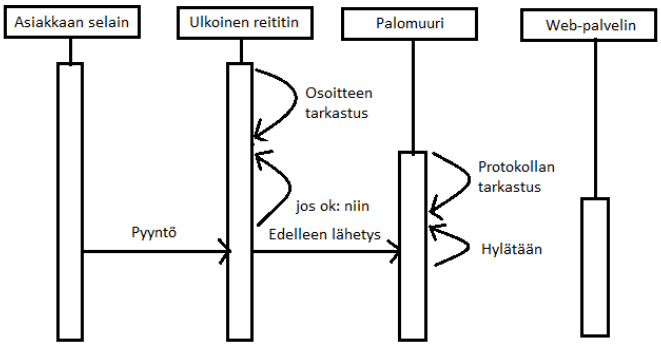
Ensimmäinen skenaario näyttää onnistuneen asiakaspyynnön (ks. Kuvio 45), joka on saapunut tietoverkkoon. Pyynnön on varmistettu ulkoisessa reitittimessä, että se on tarkoitettu palvelimelle. Tämä välitetään palomuurille tarkempaan tarkkailuun. Palomuurin hyväksyttyä protokollan käyttö, pyyntö edelleen ohjautuu asiakkaan pyytämälle palvelimelle.

Toisessa skenaariossa näytetään epäonnistuneen asiakaspyynnön, joka jää palomuuriin. Pyyntö suodatetaan ensin ulkoisessa reitittimessä, jolloin varmistutaan että se on tarkoitettu olemassa olevalle palvelimelle. Pyyntö ohjautuu tämän jälkeen palomuurille tarkkailtavaksi. Tässä vaiheessa palomuuri tunnistaa sen kelpaamattomaksi protokollaksi, joka on ehkä tar-



Kuvio 43. Suodattaan asiakkaan pyyntö etuvarustuksessa (DMZ)

koitettu jonkinlaiseksi protokolla pohjaseksi hyökkäykseksi tai yrittää aiheuttaa pyyntötulvan palvelimelle. Pyyntö hylätään ja tämä toiminta kirjataan ylös (ks. Kuvio 44)



Kuvio 44. Hylätään asiakkaan pyyntö etuvarustukssa (DMZ)

Täytäntöönpano

Pyyntöjen käsittely ja liiketoiminnan toiminnallisuus pitää erottaa suodattimella, niin parasta olisi käyttää verkkokapasiteettia ja sovelluspalvelimia otettaisiin käyttöön järjestelmäpalvelimet, jotka on eroteltu Web-palvelimista. Nämä Sovelluspalvelimet voidaan sijoittaa suojatumpaan sisäverkkoon kun Web-palvelimet. Tästä suojatummasta verkonosasta on mahdollisesti suora pääsy organisaation tietoihin ja palvelut vaativat Web-pohjaisia sovelluksia.

Ulkoisen reitittimen tulisi olla määritelty kieltävän pääsyn mihin tahansa tietoverkko osoitteeseen, jotka eivät ole tiedossa etuvarustuksessa. Lisäksi turvallisuuden lisäämiseksi pyyntöjä muihin kuin kohdeosoitteisiin, jotka eivät vastaa Web-palvelimia pitäisi suoraan hylätä. Ulkoinen reititin voi myös hylätä pyyntöjä perustuen porttinumeroihin eli se voi hylätä kaikki pyynnöt, jotka eivät ole osoitettu porttiin 80. Tällöin ulkoinen reititin tukkii suoria hyökkäyksiä palomuurille ja sisäiselle reitittimelle.

Web-palvelimet rakennetaan toimittamaan staattista Web-sisältöä tai välityspalvelimen kautta pyyntöjä sovelluspalvelimelle. Web-palvelimet olisi lukittava eli ns. kovetettava poistamalla tarpeettomat toiminnot. Tällöin palvelimet estäisivät muita tahattomia pääsyjä palvelimille. Sisäinen reititin rajoittaa verkkoliikenneyhteyksiä etuvarustuksessa olevien Web-palvelinten ja sisäisten palvelinten välillä käyttäen vahvistettua protokollaa. Tämä rajoitus vähentäisi hyökkäyksen riskiä muihin sisäisiin järjestelmiin. Sisäisen reitittimen käyttö vähentää myös ulkoisen reitittimen ylittäneitä hyökkäyksiä. Tämän uhkan vuoksi liikennettä ei pitäisi sallia suoraan ulkoisen ja sisäisen reitittimen välillä.

Reitittimien toiminta ja liikenteen suodatus voidaan ohjata käynnissä olevan palomuurikoneelle. Tämä helpottaa soveltamaan reitittimien sääntöjä johdonmukaisesti ja tilastollisen analyysin keinoin myös havaitsemaan mahdollisia hyökkäyksiä. Tämä kone käsittelisi kehittyneemmän liikenteen suodatusta eri säännöillä joilla voitaisiin havaita monimutkaisempia hyökkäyksiä. Riippuen palomuurin tyypistä verkkoliikennettä voidaan tai ei voida ohjata kulkemaan palomuurin kautta.

Palvelinten alttius ulkomaailmaan vähenee, tämä tarkoitta sitä, että vähemmän eri järjestelmän osat tarvitsevat korkeampaa turvallisuustasoa. Skenaariossa sovelluspalvelimia ei tarvitse kovettaa samalle tasolle kuin Web-palvelimia. Tällöin näille palvelimille ei kohdistuisi vakavaa haavoittuvuutta vaikka hyökkääjät rikkoisivat useita etuvarustuksen turvatekijöitä. Tämän takia DMZ-järjestelmä on hyvä tapa suojata tietoverkko. On kuitenkin muistettava, että järjestelmän suojaaminen etuvarustuksella on vain osa ratkaisua, koska turvallisuuspolitiikan kysymykset sekä teknologia, kuten etuvarustuksen käyttöä on tuettava asianmukaisilla menettelyillä ja prosesseilla. Näin varmistetaan, että järjestelmän turvallisuustaso on edelleen korkealla, jos organisaatio on vielä huolissaan mahdollisista hyökkäyksistä järjestelmään voi järjestelmään asentaa tunkeutumisen havainnointi järjestelmä (engl. Inrtusion

Detection Requirements (NIDS tai IDS)). IDS valvoo tietoverkon liikennettä tai tiettyjä välityspalvelimia etsien epäilyttävää toimintaa. Jos IDS havaitsee epäilyttävää liikennettä verkossa tai palvelimissa, joka ilmentää käynnissä olevaa hyökkäystä se ilmoittaa tästä ylläpitäjille. Tunkeutumisen havainnointi järjestelmää voidaan käyttää etuvarustusta tai sisäverkossa tai molemmissa.

Esimerkki ratkaisu

Organisaatio toteuttaa tyypillisen etuvarustuksen kokoonpanon. Järjestelmä sallisi vain HTTP ja FPT-liikenteen järjestelmiin ja silloinkin tällainen liikenne olisi sallittu ainoastaan web-palvelimille. Tällöin ulkoinen reititin estää kaiken liikenteen, joka yrittää tavoitella sisäistä reititintä. Haitallinen liikenne estetään palomuurilla ja ilmoitetaan järjestelmän pääkäyttäjille avustaen mahdollisten tunkeutujien havaitsemiseksi.

Sisäinen reititin sallii saapuvan liikenteen ainoastaan Web-palvelimille ja jopa rajoittaa sen erityisprotokollia (IIOP) tietylle palvelimelle ja erityisellä porttialueella. Tämä tarkoittaa että tunkeutuja, joka saavuttaa sillanpään ulkovarustuksen sisällä, täytyy myös hyökätä suoraan sisäiselle reitittimelle tai heidän täytyy olla IIOP lukutaitoisia siinä määrin, että he voisivat käyttää sitä päästäkseen johonkin palvelimelle toiselta puolelta sisäistä reititintä.

Palomuuri puhdistaen järjestelmän turvallisuushälytyksiltä ja hallintapäätteeltä antaa pääsyn ulkovarustuksen hallinnalle. Eräs organisaatio valitsi palomuurin ohjelmistoperustaisena ja perinteisen laitteistot käyttöönsä. Palomuuriohjelmisto saa hälytyksiä kahdelta reitittimeltä ja tarjoaa yhtenäisen näkymän DMZ:n turvallisuuden varmistamiseen. Palomuuri ohjaa myös kahden reitittimen konfiguraatiota ja välttää epäjohdonmukaisuuksia kolmen pääkomponentin välillä palomuurijärjestelmässä.

Vaihtoehdot

multi-homed firewall (engl. Multi-homed Firewall). Käytettävien koneiden määrästä riippuen toteuttamiseen osallistuvien etuvarustusten määrä vaihtelee tarvittavan suojelun tasoon. Tämä perustuu ennakoituun riskiin ja rahasummaan joka halutaan käyttää. Yksinkertaisimmassa tapauksessa DMZ voidaan ottaa käyttöön käyttämällä yhtä palomuurikonetta. Tässä koneessa olisi kolme verkkokorttia, jotka olisivat Internet, sisäverkko ja LAN:n joka sisätäisi

vain web-palvelimet ja muut julkiseen verkkoon näkyvät järjestelmän osat. Palomuuri hoitaisi liikennettä näiden kolmen verkkokortin välillä säilyttäen kolme erillistä suojavyöhykettä. Hyötynä tällaisesta "multi-homed isännästä" olisi sellainen kokoonpano, joka vähentäisi kustannuksia ja olisi helppo huoltaa. Tämä järjestelmä luo virheelle yhden pisteen, jossa kyseessä olisi turvallisuus ja käytettävyys. Tämä tarkoittaisi myös sitä, että hyökkääjällä on vain yksi järjestelmä, josta varastaa arkaluonteista tietoa. *suodatinpalomuuri* (engl. Firewall as Filter) Multi-homed palomuurissa verkko osoitteita voidaan käyttää ulkoisen tai sisäisen reitittimen kanssa. Tämä tarkoittaa että kaiken verkkoliikenteen pitää kulkea läpi palomuurista ja riippuen sen suodattimen säännöistä yltääkseen sisäverkkoon tai etuvarustukseen. *Näkymätön palomuuri* (engl. Stealth Firewall) Sen sijaan kun uudelleen sijoitetaan liikennettä etuvarustukseen, niin toimitaan näkymättömässä tilassa ja vain tarkkailla liikennettä mahdollisten tunkeutumisten havaitsemiseksi. Tämä malli tekee palomuurin olemassaolon tunkeutujalle mahdottomaksi havaita.

Tunnettuja käyttötapoja

DMZ:t ovat erittäin yleisiä lähes kaikilla Internet sivustoilla ja neuvoja on saatavilla DMZ-kokoonpanoista lähes kaikilta suurilta verkkolaitteiden ja ohjelmistojen toimittajilta, kuten:

1. Sun SUN
2. Microsoft
3. Cisco

Seuraukset

Seuraavat edut voidaan saavuttaa, kun sovelletaan tätä mallia ovat:

1. Parantunut turvallisuus, koska tällöin on vähemmän järjestelmiä, jotka ovat alttiina hyökkäyksille ja on useita palomuureja, jotka täytyy ohittaa turvallisuuden vaarantamiseksi.
2. Suojauksen taso ja syvyys voidaan vaihtaa vastaamaan ennakoitua riskiä ja näin rajoittaa kustannuksia.
3. Saatu lisäturva on käyttäjälle läpinäkyvää, koska järjestelmän on toimiva ja kehitetty toiminnalliseksi.

4. Vähemmän palvelimia kestämään suoria hyökkäyksiä, kun jos ne olisivat kaikki paljaasti näkyvissä ulkomaailmaan.

Seuraavat mahdolliset vastuut voivat syntyä sovellettaessa tätä mallia ovat:

1. saatavuus saattaa heikentyä, koska palomuurin voi tulla yhden pisteen vika. Tavanomainen menettely olisi siis palomuurivirhe, joka kieltäsi kaiken liikenteen suojattuihin järjestelmiin.
2. Hallittavuus kärsii, koska se on hyvin rajoituksellinen. Nämä rajoittavat pääsyä sisäisiin tietoihin ja voisi olla vaikea saada yhteyttä sisäisiin järjestelmiin.
3. Kustannukset nousevat, koska se sisältää ylimääräisiä elementtejä, joita on hankittava DMZ rakentamiseksi. Näitä ovat paitsi suodatusreitittimet, palomuuri ja palomuurin palvelimet, mutta myös ylimääräiset verkkolaitteet, kuten kytkimet ja kaapelointi kun käytetään ulkovarustusta.
4. Suorituskyky putoaa, koska verkkoliikennettä suodatetaan. Suorituskyky on myös hidastunutta, koska on tarpeen fyysisesti erottaa Web-palvelimet sovelluspalvelimista. Tämä ei välttämättä paranna toiminnallisuutta, mutta se on tehtävä ulkovarustusta käytettäessä ja tämä lisää tietoverkkoon useita ylimääräisiä hyppyjä jokaiseen käyttäjän tapahtumaan.

E.2 Suojaus käänteisellä välityspalvelimella

Asettamalla Web- tai sovelluspalvelin suoraan Internetiin antaa hyökkääjälle suoran pääsyn mihin tahansa haavoittuvuuteen mitä järjestelmäalustalla on (sovelluksia, web-palvelimia, kirjastoja tai käyttöjärjestelmiä jne.). Kuitenkin hyödyllisten Web-palveluja Internetin käyttäjille vaatii pääsyn palvelimillesi. Pakettisuodatinpalomuuri suojelee palvelimia hyökkäyksiltä tietoverkkotasolla. Lisäksi markkinoilla on välityspohjaisia palomuureja (ks. liite A A tällainen palomuuri tai pelkkä välityspalvelin ja niistä suojaus käänteisellä välityspalvelimella (engl. Protection Reverse Proxy) suojaa palvelinten ohjelmistoja sovellustasolla.

Esimerkki

Tarjoat Web-sivuston avulla suuren ohjelmistotoimittajan palvelinohjelmaa. Sinun Web-sivusto käyttää tätä myyjän omaa laajennusta dynaamisen sisällön toteuttamiseen ja olet sijoittanut

paljon Web-sivuston ohjelmistoon. Palvelimesi on suojattu pakettisuodatin palomuurilla (ks. liite A).

Web-palveluiden käytön mahdollisuus pakottaa avaamaan palomuuria antamaan pääsy yleiseen porttiin 80. Internetistä tulevat hyökkäykset, jotka hyödyntävät palvelinohjelmiston haavoittuvuutta ovat usein taakka järjestelmänvalvojalle turvata asennukset. Vaihto toisen valmistajan palvelimeen ei ole mahdollista, koska investoinnit palvelinalustaasi, sen sisältöön ja omiin ohjelmistolaajennuksiin on vienyt rahasi. Lisäksi jokaisen uuden tietoturva ongelman paikkaus, jonka asennat on vaarassa horjuttaa järjestelmän kokoonpanoa, niin että järjestelmä ja sen ohjelmistolaajennukset on varassa lakata toimimasta. Miten voit paeta tätä ratkaisua ja pitää Web-sivustoasi vaarantumatta auki.

Sisältö

Kaikki palvelut joilla on pääsy Internetin kautta toiseen verkkoon, ovat potentiaalisesti vihamielinen verkkoympäristö. Yleensä pääsyprotokolla on HTTP tai HTTPS.

Ongelma

Vaikka asennat yksinkertaisen pakettisuodatinpalomuurin Web-palvelimesi, voi jäädä alttiiksi hyökkäyksille, jotka hyödyntävät sen protokollatoteutuksen heikkouksia. Miten voit suojata Web-palvelin infrastruktuuria sen mahdollisia haavoittuvuuksia hyökkäyksiä vastaan. Ratkaisuna tähän ongelmaan, teidän on ratkaista seuraavat voimat:

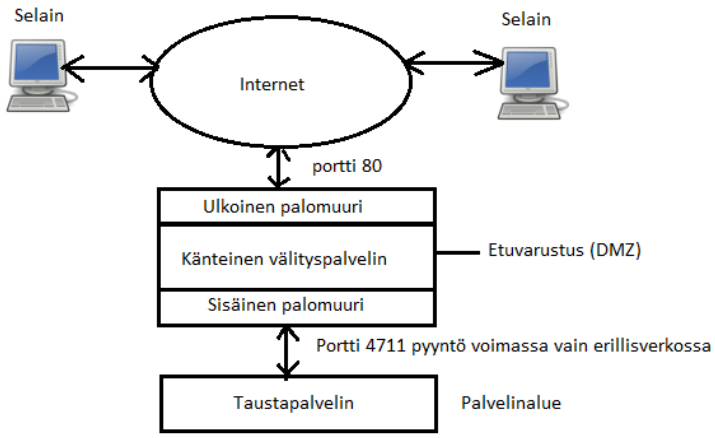
1. Yksinkertainen pakettisuodatinpalomuuri ei riitä suojaamaan web-palvelinta, koska pääsy sen protokollaan eli avoimeen porttiin 80 on annettava avoimeksi Internettiin.
2. Hyökkäysskenaariossa työllistävät usein erityisen pitkät tai erityisiksi muotoillut hakupyyntöparametrit, jotka hyödyntävät puskurin ylivuotoja. Useimmat palomuurit työstävät verkossa pakettitasolla ja eivät voi havaita hyökkäyksiä, jotka käyttävät vaativia pyyntöjä.
3. Kovettamalla web-palvelin voi olla yli kykysi ominaisuuksia, esimerkiksi se tulee mustana laatikkona myyjältä tai se on muuten liian monimutkainen hallita.
4. Asettamalla Web-palvelimen ohjelmisto auttaa välttämään haavoittuvuuksia tunnetussa haavoittuvuuksissa, mutta jokainen ohjelmistopaikkaus on riski, jos järjestelmän

laajennukset lakkaavat toimimasta. Sinun pitää uudelleen ajaa integrointitestit jokaiselle paikkaukselle ja saattaa jopa olla mahdotonta päivittää Web-palvelin ajoissa, koska laajennukset eivät välttämättä ole valmiita.

5. Vaihto toiseen Web-palvelimeen, joiden ohjelmistot ovat eri lähteistä on myös erittäin kallista, riskialtista ja aikaa vievää. Uudessa Web-palvelimessa saattaa olla vähemmän haavoittuvuuksia, mutta se ei ole tuttu. Lisäksi se voi myös edellyttää, että joudut mukauttamaan omia järjestelmälaajennuksia.
6. Et voi tietää haavoittuvuuksia, joita tunnistetaan vasta tulevaisuudessa

Ratkaisu

Vaihda tietoverkkosi topologia käyttämään suojattua käänteistä välityspalvelinta, joka suojaa Web-palvelimesi (ks. Kuvio**??**. Määritä tämä käänteinen välityspalvelin suodattamaan kaikki pyynnöt, jotta vain useimmiten vaarattomat vierailut käyttävät Web-palvelimia. Kaksi pakettisuodatinpalomuuria varmistaa, ettei ulkoinen verkkoliikenne saavuta web-palvelinta. Tuloksena on etuvarustuksen tarjoama tietoverkkotopologia, joka sisältää vain käänteisen välityspalvelinkoneet ja suojatun palvelinvyöhykkeen Web-palvelimillesi.



Kuvio 45. Suojaus käyttäen käänteistä välityspalvelinta

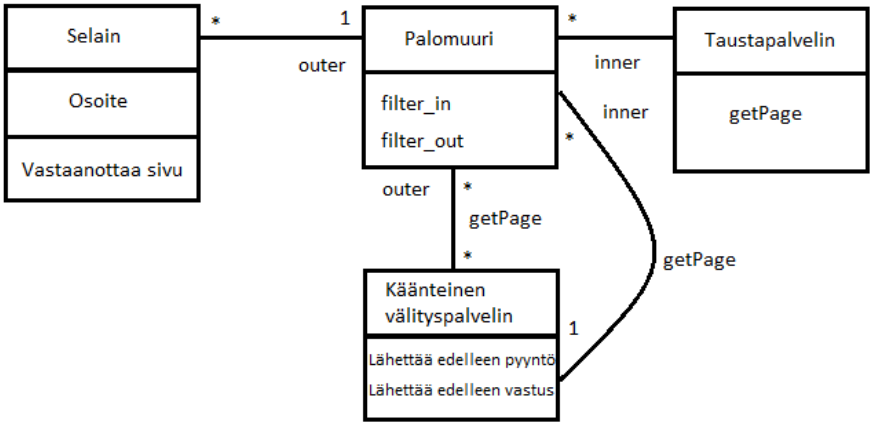
Vaikka tämä ratkaisu käsittää vain Web-palvelimet, se myös koskee muita protokollia, kuten FTP-, IMAP-ja SMTP-protokollia. suojaus käänteisellä Proxy välityspalvelimella voisi esimerkiksi:

- Skannata FTP-palvelimen tiedostoista viruksia

- Rajoittaa ajettavia sisältöjä
- Kieltää lataamasta tiedostoja
- Rajoittaa käytettäviä FTP-komentoja
- Kieltää kolmannen osapuolen yhteyksiä, jotka muuten olisi sallittuja FTP-standardin mukaan

Rakenne

Luokkakaavio suojaus käänteisellä välityspalvelimella on esitetty(ks. Kuvio 46)

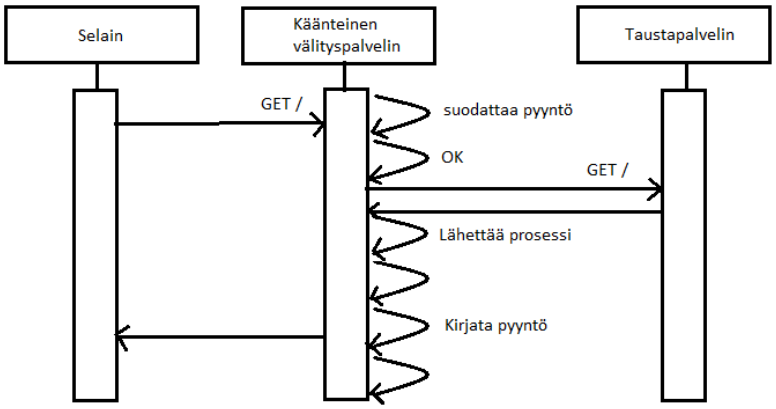


Kuvio 46. Luokkakaavio suojatulle käänteiselle välityspalvelimelle

Dynamiikka

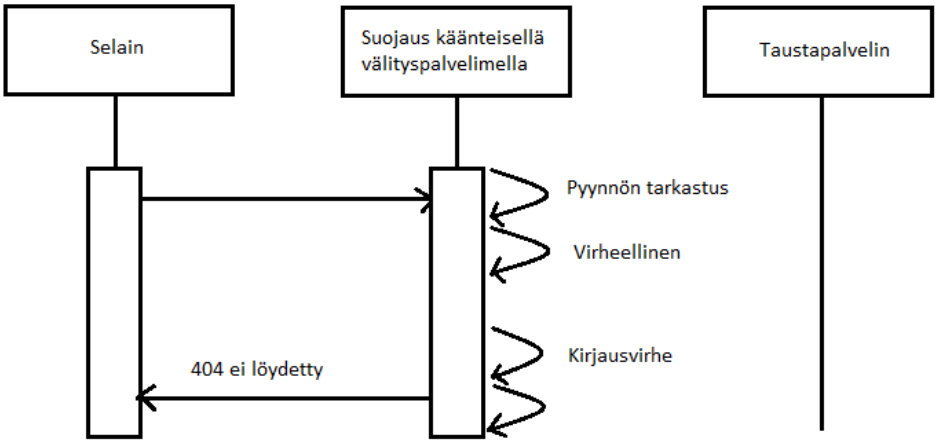
Ensimmäinen tilanne osittaa, miten voimassaoleva pyyntö tarkastetaan ja lähetetään eteenpäin suojatussa käänteisessä välipalvelimessa. Sisemmän ja uloimman palomuurin komponentit oletetaan olevien läpinäkyviä tässä tapauksessa ja näin ollen liikennettä ei ole estetty (ks. Kuvio 47). Jälkikäsittely taustapalvelimessa ja vastaus on valinnainen, mutta sitä voidaan käyttää säätämään esimerkiksi protokollan otsikkokenttää. Pääsyloki kirjoitetaan vasta sen jälkeen kun vastaus on lähetetty. Tämä parantaa järjestelmän reagointikykyä.

Toisessa tilanteessa käänteisen välityspalvelimen estomekanismi suojaa pudottamalla virheellisen ja siten mahdollisen haitallisen pyynnön. Vaikka selain ei saa vastausta, yritys tulee kirjata ylös. Virallisten HTTP (Hypertext Transfer Protocol) tietojen mukaan välityspalvelimen pitäisi palauttaa virhekoodi, joka on tyypillisesti 403-kielletty tai 404-ei löyty-



Kuvio 47. Sallia asiakkaan pyyntö suojatussa käänteisessä välityspalvelimessa

nyt). Riippuu turvallisuuspolitiikasta annatko virhevastauksia ja suljetko yhteyden välipalvelimeen (ks. Kuvio 48).



Kuvio 48. Kieltää asiakkaan pyyntö suojatussa käänteisessä valipalvelimessa

Täytäntöönpano

Tämän mallin toteutuksen käytössä täytyy ottaa huomioon:

1. Suunnittele palomuuri ja tietoverkonasetukset. Vaikka palomuuri päivitetään säännöllisesti, niin on myös hyvä aloittaa muiden komponenttien, jotta palomuurisuunnitelmaan voidaan luottaa. Usein konkreettisia asetuksien tekemiseen täytyy kiinnittää huomiota, vain yhteen protokollaan ja miten näiden muiden protokollien portit palomuu-

riin tulee toteuttaa käänteisessä välityspalvelimessa.

2. Valitse käänteinen välityspalvelin alustaksi. Voit luoda omia käänteisiä välityspalvelimia, esimerkiksi määrittämällä Apache Web-palvelin, jossa on asennettuna mod_-proxy ja mod _ rewrite moduulit. Useat toimittajat tarjoavat ammattimaisia käänteisiä välityspalvelimen ratkaisuja tai sinun pitää toteuttaa oma käänteinen välityspalvelin, jos käytät erityisiä protokollia, jotka eivät ole tuettuna valmiissa ratkaisuissa. Oman käänteisen välityspalvelin asetusten yksityiskohtainen näyttäminen ei kuulu tämän tietoturvamallin piiriin. On kuitenkin olemassa tapauksia, jolloin et voi luottaa palvelun-tarjoajien ratkaisuihin tai et luota omiin taitoihisi rakentaa välityspalvelinta. Kun valitset toimittajaa tai lähdettä sinun välityspalvelimelle pitäisi sinun valita yksinkertainen ja todistettu ratkaisu. Esimerkiksi käyttämällä Apache palvelinta riskeeraat kaikki nämä haavoittuvuudet välityspalvelimen suojaan. Toisaalta Apache web-palvelimet on useassa käytössä, että haavoittuvuudet ja niiltä suojautumiset ovat useiden ihmisten tiedossa.
3. Määritä Web-ja taustapalvelimet. Web-sisältöön pitäisi pystyä luomaan suhteelliset polkunimet ja käyttää sisäisiä nimiä tai IP-osoitteet pitäisi viitata itseensä. Muuten linkit eivät välttämättä toimi, koska tällöin selain ei voi enää käyttää pääsyä koneelle suoraan.
4. Määritä suojattu käänteinen välityspalvelin. Tietoturvan vuoksi sinun täytyy määritellä mitkä pyynnöt olisi päästettävä taustapalvelimiin ja määritellä mitä tapahtuu, jos virheellisiä pyyntöjä ilmaantuu. Esimerkiksi saatat haluta kirjata pyynnöt, jotka ovat estetty välityspalvelimella. On olemassa kaksi lähestymistapaa suodattaa pyyntöjä, jotka ovat mustat listat ja valkoiset listat.

    (a) Mustat listat estävät vain haitalliseksi tiedetyt pyynnöt, mutta päästävät kaikki muut pyynnöt. Mustan listan suodattimia on helpompi ottaa käyttöön, mutta ne ovat riskialttiimpia. Nämä on yleisimmin käytössä korkeamman tason palomuureissa.

    (b) Valkoisen lista suodatin on tiukempi ja vain sallii listalla olevat pyynnöt. Se tarvitsee olla määritelty yksityiskohtaisella tiedolla taustapalvelimilla ja sallitulla URL:llä. Valkoisen lista suodatin tarvitsee olla mukautettu kokoajan taustapalvelimella ja tämä muuttaa palvelimen vastauksia merkittävästi sen URL-

avaruudessa. Kuitenkin se on parempi valinta suojatulle käänteiselle välityspalvelimelle.

Jos taustapalvelimesi tukeutuu uudelleenohjaukseen tai muihin järjestelyihin, jotka käyttävät isäntä osoitetta ja et voi muuttaa sitä. Sinun tulisi määrittää käänteinen välityspalvelin muuttamaan vastaavasti palvelimen lähettämät vastaukset.

5. Käyttä hyväksi kaikkea. Asettamalla palomuurit, tietoverkko, reitittimet ja IP-osoitteet jne. vaatii hyvää suunnittelua. Jos sinulla on järjestelmä valmiina ja toiminnassa, tämä kokonpanon uudelleen määrittäminen tarkoittaa joidenkin palvelujen sammuttamista. Kuitenkin myöhemmät muutokset rakenteeseen on keskitetty käänteiseen välityspalvelimeen ja sisäiseen palomuuriin.

Esimerkki ratkaisu

Näillä soveltamisohjeilla voimme suojella haavoittuvuuksia Web-palvelimissa käyttämällä suojattua käänteistä välityspalvelinta.

Vaihtoehdot

Yhdistymällä käänteinen välityspalvelin ja etuovi (engl. Front Door) voi ja pitäisi yhdistää niiden toiminta. Tämä vaihtoehto antaisi lisää toiminnallisuutta.

Tunnetut käyttötavat

Suojaus käänteisellä välityspalvelimella on suosittua. Jotkut rahoitusmarkkinoiden toimijat pitävät ohjenuorana käyttää käänteistä välityspalvelinta jokaiselle Internetin tarjoamalle protokollalle. Poikkeuksena voidaan sanoa DNS. Tällöin voidaan varmistaa, että heikossa asemassa oleva palvelin ei koskaan pääse suoraan Internetiin. Turvallisuusinfrastruktuurin toimijat pitävät välityspalvelimia osana laajempaa turvallisuusinfrastruktuuria.

Seuraukset

Seuraavat edut saattavat olla hyödynnettävissä tätä mallia käytettäessä, joita ovat:

1. Hyökkääjät eivät voi hyödyntää suoraan taustapalvelimien haavoittuvuuksia. Vaikka taustapalveluilla olisi haavoittuvuuksia, palomuurit estävät niitä Internetin madoilta ja

estävät tulevat pyynnöt taustapalvelimille.

2. Vaikka on tunnettuja haavoittuvuuksia, saatat pystyä pitämään sinun Web-palvelimesi konfiguroinnin vakaana, koska käänteisellä välityspalvelimella on suodatusominaisuuksia voit kieltää Web palvelimien haavoittuvuuksien hyödyntämisen.
3. Helpompi paikkausten hallinta. Vain yksi kone on yhteydessä Internetiin suoraan. Sinun on kuitenkin seurattava mahdollisia haavoittuvuuksia ja onko olemassa paikkaa haavoittuvuuteen, jota voidaan soveltaa. Et kuitenkaan voi sokeasti luottaa käänteisen välityspalvelimen toimintaan. Taustapalvelimien säätämisessä on pidettävä pää mukana, jotta voit välttää haavoittuvuuksien hyväksikäyttöä sallittujen pyyntöjen kanssa.
4. Lisäetuja saadaan yhdistämällä enemmän toiminnallisuutta mukaan, kun käytetään yhdistämistä käänteisellä välityspalvelimella (engl. Integration Reverse Proxy ja etuovella (engl. Front Door).

Vastuut jotka saattavat syntyä sovellettaessa tätä mallia ovat:

1. Mustalla listalla suodatus voi antaa sinulle väärän turvallisuuden tunteen. Kuten ohjelmisto paikalla. Mustat listat voidaan tarkentaa vasta haavoittuvuuden ollessa tiedossa.
2. Valkoisien listojen suodatus voi olla haurasta, kun taustapalvelimelle tehdään muutoksia. Lisäämällä toiminnallisuutta tai uudelleen järjestelemällä taustapalvelimen ja Web-palvelinten rakennetta, voi tämä merkitä lisätyötä kun uudelleen määrität käänteisen välityspalvelimen valkoisen listan suodatusta.
3. Latenssiaika. Käänteinen välityspalvelin lisää latenssiaikaa, ei vain siksi, että se tekee ylimääräistä verkkoliikennettä, mutta myös siksi se lisää suodatus ja validointi pyyntöjä.
4. Jonkin verran läpinäkyvyyttä. Joitakin rajoituksia on asennettu taustapalvelimin. Nämä ovat hyviä käytäntöjä, kuten suhteellinen URL-osoite polut. Kuitenkin taustapalvelimet eivät enää näe viestintää lopunkäyttäjien suoraan tietoverkkotasolla. Protokolla saattaa siis tarjota keinoja tunnistaa alkuperäisen viestinnän loppupisteen, jonka HTTP mahdollistaa.
5. Lisää piste epäonnistumiselle, jos käänteinen välityspalvelin lakkaa toimimasta pääsy web-sivustoille on mahdotonta. Ylimääräiset komponentit, jotka voivat pettää nostavat yleistä riskiä järjestelmä vikaan. Vähentämällä tätä riskiä voit tarjota kuuman tai

kylmän valmiusasennuksen laitteistolle tai ohjelmisto vikatilanne kytkimet.

6. Laitteet, ohjelmistot ja konfiguroinnin yläpuolella suojaus käänteisellä välityspalvelimella vaatii määrittämään ylimääräisen pakettisuodatinpalomuurin, kuten myös ylimääräisen koneen toimimaan käänteisenä välityspalvelimena.

Katso myös

Suojaus käänteisellä välityspalvelimella on erityinen täytäntöönpano yhden palvelupisteen kohtaan (engl. Single Access Point). Yhdistämällä palomuurit ja suojaus käänteisellä välityspalvelimella rakentaa periaatteellisen syväpuolustuksen tietoturvan periaatteita hyväksikäyttäen.

E.3 Etuovi

Etuovea (engl. Front Door) tarvitaan, kun Web-sovellukset ja palvelut usein tarvitsevat käyttäjätunnistusta ja käyttäjäistunnon seurantaa. Sisällyttää useita tällaisia palveluta mahdollistaa yhden kirjautumispisteen istunnon ajaksi. Käänteisen välityspalvelimen tarkoituksena on antaa ihanteellinen paikka toteuttaa todentaminen ja valtuutus toteuttamalla Web sisäänpääsy sinun taustapalvelimille. Valikoiva käänteinen välityspalvelin voi vielä käyttää pääsyn ulkoisille toimijoille tarjoten käyttäjätunnistuksen ja salasana tunnistuksen eli salasanalompakon automaattisesti.

Tunnetaan myös

Pääsynä verkkopalvelimelle (engl. Web Entry Server) ja Verkoon yhdellä kirjautumisella (engl. Web Single Sign On)

Esimerkki

Lisäämällä sovellus, joka vaatii käyttäjätunnistuksen ainoastaan tarkoittaa lisäämällä toinen käyttäjä tietokantaan. Lisäksi organisaatio tunnistaa tämän keinon olevan tarpeellinen tulevaisuudessa, joten halutaan erilaisia sovelluksia yhden kirjautumispisteen palveluun.

Konteksti

Verkkosivusto, joka koostuu useista eri verkkosovellutuksista, jotka vaativat käyttäjäntunnis-

tusta. On olemassa kaksi käänteistä välityspalvelinta, jotka ovat Yhdistäminen (engl. Integration) ja suojaus (engl. Protection). Integroivaa välityspalvelinta tarvitaan, kun useat sovellukset tarvitsevat todentaa käyttäjän verkkopalvelussa (esim. verkkokauppa) ja vain todennetut käyttäjät saavat käyttää tarjottavia alisovelluutuksia. Suojattua välityspalvelinta silloin, kun käyttäjän todentamista tarvitaan vain pääsyyn taustalla olevaan verkkosovelluksen tai molempien yhdistelmään.

Ongelma

Miten annat yhdenkirjautumispisteen usealle verkkosovellukselle tai palvelulle. Ratkaistaksesi tämän ongelman on sinun ratkaistava seuraavat asiat, joita ovat:

1. Haluat yksittäisen käyttäjän tunnistaa itsensä kaikkiin sovelluksiin, vaikka nykyiset verkkosovellukset jo sisältävät oman käyttäjätietokannan.
2. Et halua, että käyttäjiltä vaaditaan erikseen salasanaa jokaiseen sovellutuksen, riippumatta turvallisuuspolitiikasta.
3. Haluat pakottaa käyttäjien tunnistaa itsensä useita kertoja, jotta väärinkäyttävät käyttäjät eivät jää yksin järjestelmään pitkäksi aikaa.
4. Haluat sovelluksesi olla riippumattomia käytettävästä tunnistusmallista. Riippuen turvallisuuspolitiikasta saatat, jopa vaatia erillistä mallia. Esimerkiksi vahvempaa tunnistautumista maksupalveluissa tai heikompaa tunnistautumista esimerkiksi huoltoonpääsysssä.
5. Eri käyttäjillä on erilaiset käyttöoikeudet järjestelmään. Haluat käsitellä näitä käyttäjiä yhdellä ratkaisulla.
6. Haluat integroida uusia sovellutuksia helposti kirjautumismalliin.
7. Haluat käyttää yhtä kirjautumis- ja uloskirjautumiskäytäntöä. Tämä tarkoitta sitä, että käyttäjien pitäisi istuntoa aktiivisena, kun kukaan muu ei käytä taustapalvelimia ilman uudelleenkirjautumista.

Ratkaisu

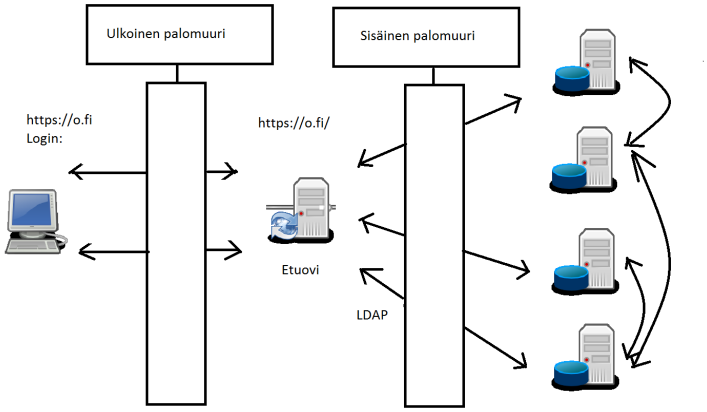
Tukeutua etuoveen ja käyttää palvelimien kanssa integroitua käänteistä välityspalvelinta helpottaa tunnistamaan käyttäjät ja pitämään kirjaa käyttäjien istunnoista. Tämä palvelin tukee käyttäjien henkilöiden tunnistusta ja istunnonpituuden kirjausta kaikilla taustapalveluilla.

Etuovi voi kirjata kaiken toiminnan keskeiseen lokiin. Riippuen ratkaisun luonteesta, jotkut taustapalvelimista saattaa olla avoinna kaikille ja etuovi ainoastaan suojelee taustapalvelimia todentamattomilta käyttäjiltä. Muista kuitenkin, että tämä ratkaisu toimii myös käyttäen suojattua käänteistä välityspalvelinta julkisessa osassa verkkosivuja.

Sinun täyttyy yhdistää käyttäjien henkilöllisyys olemassa olevissa taustasovelluksissa. Säilytä tiedot käyttäjäprofiileissa yhdistämällä käyttäjien identiteetti ja käyttöoikeudet yhteen käyttäjä hakemistoon. Tällä hetkellä LDAP-palvelin on suosittu tähän ratkaisuksi, mutta myös jokin muu ratkaisu voi olla sopiva. Hallintojärjestelmän käyttäjätiedot ja käyttöoikeudet eivät kuulu tähän malliin, mutta se on usein tarpeen. Suurissa ratkaisuissa käytetään järjestelmämyyjien ratkaisuja pääsyoikeuksien hallintaa. Voit käyttää esimerkiksi Windows pohjasessa järjestelmässä Active Directory pääsyoikeuksien hallintaan.

Rakenne

Voit päätyä seuraavanlaiseen rakenteeseen, jos käytät etuovea (engl. Front Door) skenaario on seuraavanlainen. Tavallinen paikka etuovelle on oma palvelinkone etuvarustuksessa (ks. Kuvio 49).



Kuvio 49. Etuoven lisääminen

Dynamiikka

Lisäksi yhdistetyn käänteisen välityspalvelimen kartoitus taustapalvelimille, etuovi lisää uuden käsittelyvaiheen tarkastamalla ensin käyttäjän käyttöoikeudet. Riippuen tämän tarkas-

tuksen tuloksesta pyyntö, joko reititetään halutulle taustapalvelimille tai sitten ei. Kirjautumissivustolla käyttäjä voi todentaa itsensä. Kuten suojaus käänteisellä välityspalvelimella ja etuovi voisivat hiljaa pudottaa luvattomia pyyntöjä ja kirjautumisyrityksiä.

Täytäntöönpano

Etuoven lisäystä toteuttaessa käänteiselle välityspalvelimelle on otettava huomioon annetut mallit, joita ovat:

1. Käyttäjien esitysten ja tietokannan yhtenäistäminen. Tämä on helppoa, jos aloittelet tietoverkon rakennusta tai sinulla on ainoastaan yksi henkilötietokanta olemassa. LDAP-palvelin on suosittu tallennusväline tallentamaan käyttäjätunnuksien salasanoja ja käyttöoikeuksia. Jos haluat integroida olemassa olevat taustapalvelut, mutta et voi muuttaa niintä, ehkä lisäämällä objekti identiteetti ja salasanalompakko hakemistoon, jotta automaattinen identiteetin ja salasanan uusinta, kun käytetään tällaista taustatoimintoa.
2. Määrittele autentikointimeksnismi. Suosittu suojausmekanismi on käyttäjätunnus-salasana, kertakäyttöinen salasana, kertakäyttöinen merkkipohjainen salasana, haaste-vaste symbolit, biometriset tunnisteet, todistukset tai muut näiden yhdistelmät. Ainoasta tällöin etuovessa täytyy ottaa käyttöön käyttäjätunnistus tällöin se on helppo muuttaa tai laajentaa todennusmekanismin mukaan myöhemmin ilman mitään vaikutusta nykyisiin sovelluksiin.
3. Määritä käyttöoikeudet järjestelmään tarvittaessa. Erilaisia lähestymistapoja on olemassa, joilla voidaan hoitaa käyttöoikeudet ja käyttäjien kartoitus sallittuihin palveluihin. Etuoven tarkoituksena on, että karkeatekoinen malli riittää, mutta yksittäiset sovellutukset saattavat tarvita hienojakoisen ohjauksen sisäiseen toiminnallisuuteen. Hienostunut täytäntöönpano antaa täydellisen mallin soveltaa paitsi etuovea, mutta myös kaikkia tarvittuja sovellutuksia. Pääsynhallintamalli (engl. Access Control Models) tarjoaa joitakin oivalluksia näihin kysymyksiin.
4. Suunnittele käyttäjä ja istunnonpituusesitys. Pääsy taustapalveluihin otsikkokentän kautta. Tämä voi olla erikseen nimetty otsikkokenttä tai voit käyttää HTTPn perus autentikoitumismekanismia tunnistaa käyttäjän henkilöllisyys. Jos tämä ei ole yhdenkäyttäjän tunnistusta, niin etuovi voi tarvita kartoittaa käyttäjän käyttäjätunnus yhdelle erityi-

selle taustapalvelulle. Tämä kartoitus on tallennettu käyttäjätietokantaan suunnittelun ensimmäisessä vaiheessa (käyttäjien esitys ja tietokannan yhtenäistäminen). Vaihtoehtoisesti määrittele lisäotsikkokenttä väli ja päätepisteen yhteyteen. Nämä otsikkokentät sitten analysoidaan etuovessa, pitäen istunnon tallessa ja automaattisesti toimitettuna kaikille kiinnostuneille päätepisteille.

Tämä ja seuraavat kolme vaihetta vastaavat suurin piirtein kuvattuja toimintoja turvattu istunto (engl. Security Session) tietoturvamallin täytäntöönpanoa joka on:

1. Suunnitella ja toteuttaa kuinka etuovi pitää kirjaa käyttäjien istunnoista. Jotkin ratkaisut luottavat SSL-selaimen etuovi kommunikaatiossa, käyttäen SSL-istuntotunistetta tähän tarkoitukseen. Istuntoevästeiden käyttö on myös suosittua. Uudelleenkirjoitettaan kaikki URLt lisäävät istuntotunnisteen sisällön taustaratkaisujen vastauksiin, jos evästeet eivät ole käytössä, tuntuu tämä liian suurelta ja liian monimutkaiselta. Evästeiden avulla on mahdollista pystyä pitämään istunnon sisältö vaihteen HTTP ja HTTPS välillä, suorituskyky tai turvallisuus syistä. Etuoven istuntoevästeen tulisi olla salattu ja salausteknisesti allekirjoitettu siten, että oltaisiin varmoja, ettei niitä voida manipuloida. Jos etuoven keksit olisi turvattu tällä tavoin ja ne sisältäisivät myös jotakin niiden aineistolähteestä, etuovi voi jopa hyväksyä tällaisten evästeiden käytön käyttäjätunnisteina vian jälkeen ilman että käyttäjä joutuu todentaman istuntoa uudestaan.
2. Suunnittele ja toteuta etuovi session sisältö. Istuntoeväste voi olla keino tallentaa kaikkien istuntojen sisältö. Kuitenkin, koska evästeen kokorajoitus ja turvallisuuskysymykset voi olla parempi pitää istuntojen palvelinten muistissa. Yksi ratkaisu on pitää istuntolistaa kaikista istuntoyhteyksistä muistissa. Tänä on tehokkain ratkaisu, varsinkin jos käyttäjien käyttöoikeuksien ovat myös välimuistissa, mutta siihen sisältyy riski menettää istunnon tila virhetilanteessa. Toinen vaihtoehto on käyttää pysyvää muistia ja tietokantaa istuntojen yhteydessä. Kuitenkin tänä on yleensä erittäin hidasta, mutta sallii useiden etuovien tapauksessa jakaa istuntojen sisältöä. Kumpikin ratkaisu pitää istunnon sisällön parhaiten riippuu konkreettisista vaatimuksista.
3. Toteuta evästepurkki. Taustapalvelimet käyttävät omia istuntoevästeitä etuovi pystyy säilyttämään istuntoevästeet oman istunnon yhteydessä, eikä siirrä niitä käyttäjän selaimeen. Tämä varmistaa yhden uloskirjautumisen. Jos tätä ei tehdä selain voi lähettää

vanhan sovelluksen istuntoevästeen, kun uusi käyttäjä on kirjautunut etuoveen joka sekoittaa taustapalvelimen.

4. Suunnittele ja toteuta sisäänkirjautuminen ja portaalisivusto. Etuovi voi delegoida käyttäjän tunnistuksen erityiselle taustapalvelimelle tai se voi toteuttaa oman sisäänkirjautumissivuston.

Vaihtoehdot

Kuten suojaus käänteisellä välityspalvelimella voit ottaa kaksi etuovea (engl. Front Door), jotka jakavat taustapalvelimet, yksi Extranetille ja yksi Intranetille (ks. luku Intranet A) käyttäjille.

Tunnettuja käyttötapoja

Peter Sommendalin entinen yritys etuovi-ratkaisu Telekurs Financial Services Ltd:lle toteuttaa suurimman osan täällä annetuista ratkaisusta, lisäksi voi olla että määrittelet suojatun käänteisen välityspalvelimen. Yllä olevan sovelluksen rakenne on C++ koodina saatavana avoimen lähdekoodin ohjelmistona.

Seuraukset

Lisäksi seurauksina tulisi suojus käänteisellä välityspalvelimena ja interaatio käänteisellä välityspalvelimella. Tällä mallilla saatavat edut ovat:

1. Yksi kirjautuminen ja yksi uloskirjaus, koska etuovi seuraa käyttäjän istuntoa ja taustasovellus automaattisesti saa käyttäjätunnisteen etuovelta, sen sijaan kun kysyy sitä uudestaan.
2. Yksi käyttäjäprofiili on mahdollista kaikkiin taustasovelluksiin. Tämä ei välttämättä tapauksissa, esimerkiksi aloitat usean olemassa olevan verkkosovelluksen ja yhdistät ne, mutta etuovi helpottaa mekanismeja, joiden avulla voit toteuttaa ratkaisun, joka käyttää yhtä käyttäjäprofiilia ja yhtä hallintosovellusta.
3. Sovellukset ovat vapautettu kulunvalvonta ja käyttäjätunnistuskäytännöstä. Tämä antaa sinulle mahdollisuuden käyttää verkkosovelluksia nopeasti, kuten helposti integroitava etuovi kulunvalvontaan. Kokemus on osoittanut, että tällainen arkkitehtoninen ohjeistus verkkosovelluksiin voisi olla hyödyllinen, erityisesti intranetissä.

4. Keskitetty kirjautuminen. Sallii käyttäjien seurannan ja raportoinnin. Markkinointi osasto saattaa kuten lokit, jotka pitävät yksityiskohtaisesti kirjaa käyttäjien toiminnasta.

Kuitenkin yhdistely eri mallien vastuut, etuovi suorittaa muutaman lisävastuun, joita ovat:

1. Sovellukset saattavat pakottaa käyttämään omia tietokantoja, tämä nostaa epäjohdonmukaisuuden riskiä. Jos käytät etuovea kahdessa eri tietokannassa, voit lopulta yhdistetään nämä kaksi käyttäjätietokantaa.
2. Keskeiset hallintasovelluksien käyttäjätunnuksia ja käyttöoikeuksia tarvitaan. Ilman kertakirjautumista tämän tarve voi olla olemassa, mutta sitä ei tarvitse tunnistaa. Etuoven käyttöönotto tekee tämän tarpeen näkyväksi. Myös puutteet vastaavanlaisissa organisaation prosesseissa ilmenevät helpommin.
3. Salasanan ikääntymispolitiikassa eri taustasovellukset voivat olla ristiriidassa. Teidän täytyy tuotaa automaattisesti uusia salasanoja, kun ne erääntyvät tai anna käyttäjien huolehtia salasanan muuttamisesta taustasovellusten ja heidän etuovi profiilista.
4. Ristiriitaiset istunnot etuovessa ovat ikääntyneitä ja sovellukset hämmentävät käyttäjiä.

Katso myös

Voit tarkastella etuovea kuin lisäät tarkastuspiste (engl. Check Point) ja turvattu istunto (engl. Security Session) ja integroida ne integoroidun käänteisen välityspalvelimen tai suojata suojatun käänteisen välityspalvelimen taakse ja siten tarjota yhden pisteen (engl. Single Access Point) ja organisaation verkkosovelluksille ja palveluille.

E.4 IDS

Tarkoitus

Monitoroida kaikkea verkon kautta kulkevaa liikennettä ja analysoida sen tunnistaen mahdollisia hyökkäyksiä ja laukaista asianmukaisia vastaksia.

Esimerkki

Organisaation ulkopalomuuri ohjaa liikennettä Internetistä. Kuitenkin olemme edelleen alttiita viruksille ja muille hyökkäyksille, jotka tunkeutuvat läpi palomuurin. Nämä hyökkäykset voivat olla jo tiedossa olevia hyökkäyksiä tai ne voivat olla aivan uusia hyökkäyksiä. Meidän on parannettava vastustuskykyä tällaisiin hyökkäyksiin.

Konteksti

Solmut paikallisen järjestelmän, jotka tarvitsevat kommunikoida toistensa kanssa käyttäen Internetin tai muun ei-turvattua tietoverkkoa.

Ongelma

Hyökkääjät saattavat yrittää tunkeutua järjestelmäämme Internetin kautta ja väärinkäyttää tietojamme luokkien tai muokaten niitä. Meidän täytyy tietää milloin hyökkäys tapahtuu ja ryhtyä tarvittaviin vasta toimenpiteisiin.

Ratkaisu

Tähän ongelmaan vaikuttavat seuraavat voimat:

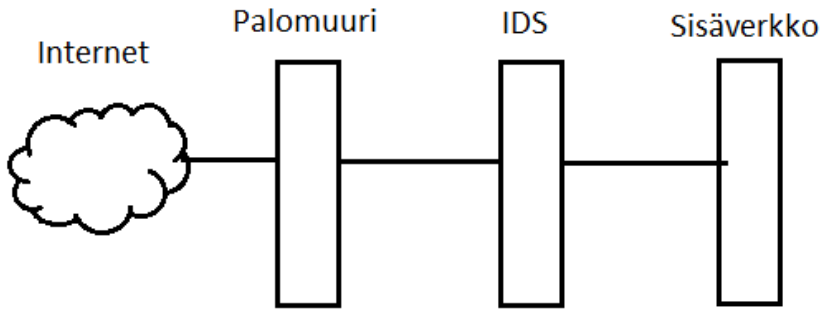
- Viestintä: Järjestelmämme on yleensä turvallisempi, jos käytämme suljettua verkkoa. Kuitenkin nykymaailmassa on parempaa ja realistisempaa käyttää Internetiä tai muuta ei turvallista verkkoa, koska tämä alentaa kustannuksia, mikä saattaa myös olla tietoverkon turvallisuusuhka.
- Reaaliaikainen käyttäytyminen: hyökkäykset tulisi havaita ennen hyökkäyksen vaikutusta ja täten säilyttää tietovarat sekä säästää aikaa ja rahaa. On vaikeaa havaita hyökkäys, kun se on tapahtumassa, mutta tällaisen havaitseminen on välttämättömyys, jotta voimme reagoida ajoissa ja asianmukaisesti.
- Keskeneräinen turvallisuus. Turvatoimet kuten salaus, autentikointi jne. eivät välttämättä suojaa aukottomasti kaikkia järjestelmiä, koska ne eivät välttämättä suojaa mahdollisilta iskuilta.
- Ei epäilyttävät käyttäjät: Järjestelmien suojeleminen palomuurin yli on nopeaa ja helppoa. Kuitenkin pyynnöt, jotka tulevat ei epäilyttävistä osoitteista, jotka on sallittu palomuurissa voivat silti olla haitallisia ja seurattavissa.
- Joustavuus: Kovan koodaajan typpiset hyökkäykset vodaan tehdä helposti, mutta voi

olla vaikeaa ja aikaa vievää sopeutua hyökkäysmalleihin, jotka vaihtuvat jatkuvasti.

Ratkaisu

Jokainen pyyntö käyttää tietoverkkoa analysoidaan tarkistaa, täyttääkö laite hyökkäyksen määritelmän, jos havaitsemme sen hyökkäykseksi suoritetaan hälytys ja ehkä tarvittaviin vastatoimiin ryhdytään.

IDS tyypillisesti sijoitetaan tietoverkkoon täydentämään palomuuria, jos kyseessä etuvarustus, niin se voidaan sijoittaa pelkästään etuvarustukseen tai lisätä omat IDSt etuvarustukseen ja sisäverkkoihin (ks. Kuvio 50). Palomuurin suodattimet suodattavat pyyntöjä palveluihin ja IDS suorittaa lisätarkastuksia epäilyttäville pyyntösekvenssimalleille, jos jotain epäilyttävää havaitaan hälytetään organisaation verkkovastaavat ja jolloin palomuurilla voidaan estää tiukentaa suodatusta siten, että rajoitetaan tai estetään kaikki liikenne.



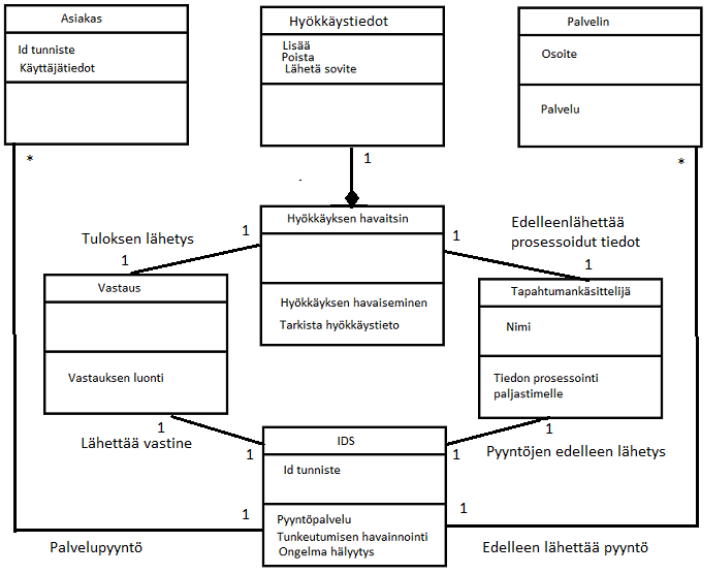
Kuvio 50. IDSn mahdollinen soijoituspaikka täydentämään palomuuria

Rakenne

Internetistä tai Intranetistä saapuva asiakas pyytää joitakin palvelinpyyntöjä. IDS sieppaa pyynnön ja lähettää sen tapahtumakäsittelijälle. Tapahtumankäsittelijä käsittelee tapahtumaa, jotta hyökkäyksen tunnistin voi analysoida tapahtumaa ja toteuttaa joitakin menetelmiä hyökkäystiedon perusteella. Hyökkäyksen ollessa kyseessä vastaus on luotu ja palvelupyyntö ei saavuta palvelinta (ks. Kuvio 51).

Dynamiikka

Kuvaamme tiivistelmän käsitteellisen IDS tietoturvamallin käsitteistä tunnistaa tunkeutumi-

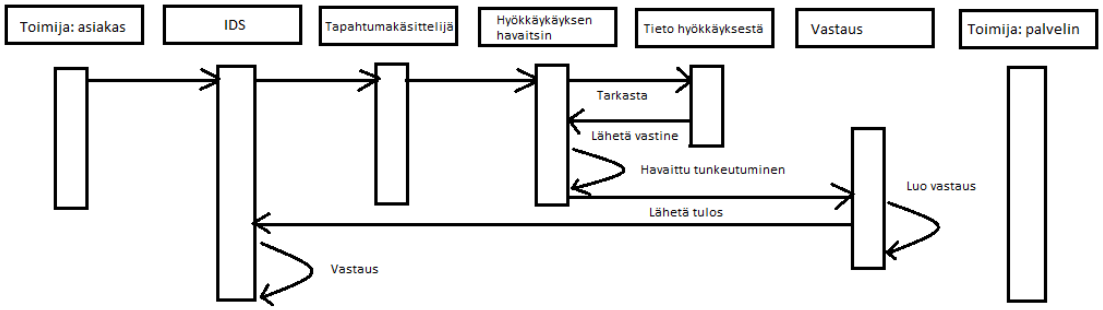


Kuvio 51. Luokkakaavio käsitteelliselle IDS tietoturvamallille

nen (ks. Kuvio 52).

Yhteenveto

Asiakas esittää palvelupyynnön. IDS käsittelee viestin ja tekee tarkastuksen, onko tuleva pyyntö hyökkäys vai ei. Tunnistuksen jälkeen antaa vastauksen. Toimijoina tässä tapauksessa ovat asiakas ja palvelin sekä edellytyksenä on että hyökkäystiedot ovat tiedossa.



Kuvio 52. Sekvenssikaavio kuvitteellisen IDS:n tunkeutumisen havaitseminen

Ensin asiakas tekee palvelupyynnön palvelimelle. IDS lähettää pyynnön tapahtumankäsittelijään. Tapahtumankäsittelijä käsittelee tiedot, jotta hyökkäyksen havaitsin voi tulkita tapah-

tumaa ja yrittää tunnistaa, onko tuleva pyyntö hyökkäys vai ei vertaamalla sitä käytettävissä olevaan hyökkäystieto tietokantaan syntyy eri toimintoja, joita ovat:

1. Pyynnön ollessa oikea, vaste syntyy ja pyyntö lähetetään palvelimelle.
2. Pyynnön ollessa väärä negatiivinen (engl. False Negative) IDS ei ehkä pysty tunnistamaan onko kyseessä hyökkäys.
3. Pyynnön ollessa väärä positiivinen (engl. False Positive) IDS ilmoittaa pyynnön olevat virheellisesti hyökkäys.
4. Pyynnön ollessa hyökkäys vastatoimia luodaan.

Jälkihoitona on, jos hyökkäys havaitaan niin tällöin sopivia ennaltaehkäiseviä toimenpiteitä voidaan soveltaa.

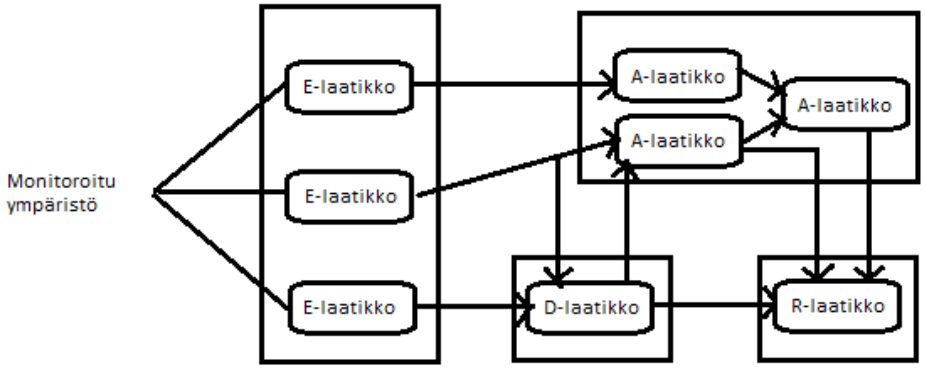
Toteutus

Täytyy luoda tietokanta, jossa on tiedot eri hyökkäyksistä. Voimme tämän jälkeen tarkastuttaa tulevaa liikennettä tätä hyökkäystietokantaa vasten ja päättää onko kyseessä hyökkäys. Konkreettinen eri toimintaversiot mitä tässä tietoturvamallissa käytetään erityyppisten hyökkäyksien havaitsemiseksi ovat.

Yleinen tunkeutumisen havaitsemisen runkorakenne (engl. Common Intrusion Detection Framework, CIDF), jonka on luonut DARPA työryhmä 1998 ja he loivat yhteiset puitteet IDS kenttään. CIDF määritteli yleisen IDS arkkitehtuurin perustuen näkemykseen, jossa on neljä erityyppistä toiminnallista moduulia (ks. Kuvio 53), joita ovat:

1. E-lohko eli tapahtumalaatikko, joka sisältää anturielementin, joilla valvotaan kohdejärjestelmää, mutta tiedon analysointi tapatuu hyväksikäyttämällä muita lohkoja
2. D-lohko eli tietokantalaatikko, ovat lohkoja jonne on tarkoitus tallentaa tietoja myöhempää käsittelyä vaten A ja D laatikoissa
3. A-lohko eli analyysilaatikko on prosessointi moduuli, jossa analysonnit tapahtuvat ja havaitaan mahdolliset hyökkäykset
4. R-lohko eli Vastelaatikko, jonka päätehtävä on tehdä vasteellaan tyhjäksi havaitut tunkeutumiset.

Konkreettinen rakenne



Kuvio 53. Yleinen CIDF arkkitehtuuri IDS järjestelmälle

IDS voi olla käyttäytymisen(sääntöpohjainen) tai poikkeavaan käytökseen perustuvaa. Merkittävimmät erot näiden kahden välillä on niiden käyttö ja tehokkuus. Mallit molemmissa sekä allekirjoituspohjaiset ja käyttäytymiseen perustuva IDS ovat seuraavat:

1. Hybridi mallissa allekirjoitusperustainen ja käyttäytymisperustainen IDS ovat yhdessä käytettävissä. Käyttäytymiseen perustuva IDS havainnoin poikkeamia liikenteestä ja vertaa näitä poikkeamia allekirjoitusperustaisen IDS tietokantoihin.
2. Riippuen resursseista joita valvotaan. IDS järjestelmät ovat jaettu kahteen luokkaan perustuen verkkoasema (engl Host Based) ja tietoverkkopohjaisiin (engl. Network Based) IDS järjestelmiin. Verkkoasema pohjaiset järjestelmät ovat asennettu paikalliin koneisiin ja niiden toiminnan arvioimiseksi ja ne hyödyntävät sisäistä avainpalvelinta. Verkkopohjainen järjestelmä tarkastaa paketit verkkoliikenteestä. Tämä järjestelmä ei kuulu tämän tietoturvamallin sisältöön.

Tunnetut käyttötavat

Käyttää NID on vapaasti saatavilla oleva hybridi tunkeutumisen havaitsemisen paketti, joka voidaan asentaa käytettävään koneeseen. NID monitoroi verkkoliikennettä ja etsii tunkeutumisyrityksen läsnäoloa sekä normaalista poikkeavaa verkkoliikennettä.

Seuraukset

Tätä tietoturvamallia käyttämällä saavutetaan seuraavat edut:

1. Viestintä: Havaitessamme useimmat hyökkäykset, voimme turvallisesti käyttää Inter-

netiä tai muita suojaamattomia tietoverkkoja pääsynä muihin järjestelmiin.

2. Reaaliaikainen käyttäytyminen: Hyökkäykset voidaan havaita niiden tapahtuessa ja tehdä hälytys, jos organisaation käytössä on riittävät ja asianmukaiset tiedot. Tällöin voidaan säästää aikaa ja rahaa elvytystoimissa ja estää väärinkäytökset.
3. Puutteellinen turvallisuus. Voidaan vahvistaa eri turvallisuuskerroksilla, joita ovat salaus ja autentikointi.
4. Ei epäilyttävät käyttäjät: Tuleva pyyntö tulee palomuurissa sallitusta osoitteesta. Nämä pyynnöt tulee säilyttää myöhempää edelleen tarkastusta ja analysointia varten
5. Joustavuus: Tiedot voidaan muokata keskittymään uusiin hyökkäyksiin tai uuden haitallisen toiminnan estämiseksi.

Tällä tietoturvamallilla on olemassa seuraavat haitat:

1. Jotkut hyökkäykset voivat olla niin nopeita, että niitä on vaikeita tunnistaa reaaliajassa.
2. Hyökkäysmallit ovat liian sidoksissa tiettyyn ympäristön käyttöjärjestelmään, laitearkkitehtuuriin jne., joten niitä ei voida soveltaa muihin järjestelmiin. Tarkoittaen, että valmista ilmaisuinformaatioita joudutaan muuttamaan järjestelmäsopivaksi.
3. On olemassa yläpuolista laitteistoa, kun IDS järjestelmää asennetaan.

Liittyvät mallit

Palomuurit voidaan liittää täydentämään IDS toimintaa, koska yleensä palomuureilla kielletään pyyntöjä tuntemattomista osoitteista. Niillä voidaan suojautua luotetuista lähteistä tulevilta hyökkäyksiltä ja voidaan estää osoitteet, joista hyökkäykset ovat peräisin. Tällöin voitaisiin käyttää esimerkiksi strategista mallia (engl. Strategy pattern)

E.5 TSL VPN

Tunnetaan myös nimellä

SSL virtuaalinen yksityinen tietoverkko (engl. SSL Virtual Private Network)

Tarkoitus

TSL Virtual Private Network tietoturvamalli kuvaa suojatun kanavan perustamista kahden

päätepisteen välille, käyttäen salattua tunnelointi menetelmää siirtokerrosten välillä. Autentikointi ja valtuutus tapahtuu tässä tunnelointi menetelmässä kummassakin loppupisteessä.

Esimerkki

Organisaatio tarjoaa Web-pohjaista sähköistä kauppapaikkaa. Tarvitsemme vakuuttaa asiakkaille, että he ovat vuorovaikutuksessa oikean sovelluksen kanssa. Asioidessa sovelluksessa he voivat turvallisesti maksaa ja ostaa tavaroita.

Konteksti

Suuri määrä käyttäjiä monissa Web-sovelluksissa tarvitsevat turvallisempaa tapa kommunikoida toistensa kanssa, käyttää Internetiä tai muissa turvattomissa tietoverkoissa. Useimmiten vuorovaikutus tapahtuu Web-sivustoilla.

Ongelma

Miten voimme luoda turvallisen kanavan kuljetuskerroksen tietoverkon loppukäyttäjille, jotta he kykenisivät vaihtamaan viestejä kiintopisteiden välillä. Ratkaisuna tähän ongelmaan on ratkaistava seuraavat ongelmat:

- Viestit menevät prosessien välillä palvelimien ja reitittimien kautta. Viesti tulee säilyttää tietoturvallisena tämän viestinnän ajan.
- Suorituskyvyn tulisi olla hyvä sekä normaali sekä että huippukuormituksella.

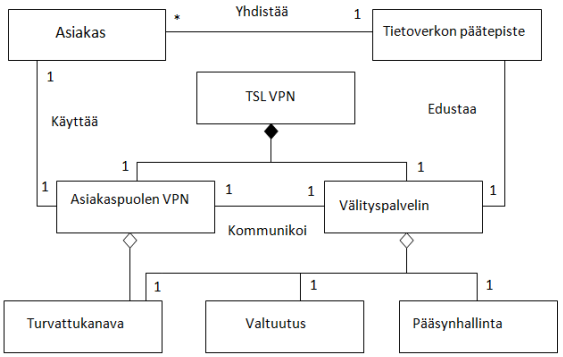
Ratkaisu

Käytä tietoverkossa käänteistä välityspalvelinta, joita kutsutaan yleisesti SSL välityspalvelimiksi etäyhteys käytössä. Etäkäyttäjät tarvitsevat hyödyntääkseen organisaation sovelluksia Internetselainta tärkeän URL-välityspalvelimen kautta ja yhdistyä sen kautta TSL-suojausta käyttävään HTTP-yhteyteen. Tämän jälkeen käyttäjä todentaa itsensä välityspalvelimelle. Todennuksen jälkeen käyttäjä voi käyttää sallittuja sovelluksia, joihin pääsyä välityspalvelin valvoo.

Rakenne

Luokka kaavio TSL VPN mallissa on seuraavanlainen (ks. Kuvio **??**). Kuvassa välitys-

palvelin edustaa päätepistettä ja toimii valtuuttajana, turvattukanavana ja kulunvalvojana eli valtuuttajana.



Kuvio 54. Luokkakaavio TSL VPN:lle

Toteutus

Autentikointialgoritmilla on toteutettu palvelimella, joka autentikoi yhteyden palvelimelta asiakkaalle. Turvallinen kanava muodostetaan yleisen verkon sopivalla salausalgoritmia, jonka avulla käyttäjät voivat turvallisesti kommunikoida palvelimiin. Jotkut TSL VPNs tarjoavat laitteistokiihdyttimiä. Asiakkaan on ladattava ennen yhteydenmuodostamista palvelimeen tarvittava VPN-ohjelmisto.

Esimerkki ratkaisu

SSL välityspalvelimen voi todentaa palvelimen käyttäjälle ja muodostaa turvallisen kanavan, jotta etäkäyttäjät voivat lähettää taloudelliset tiedot salatussa muodossa, yhus suojaavan salakuuntelulta hyökkäykseltä.

Seuraukset

TSL VPN mallin käytöstä on seuraavanlaisia hyötyjä, jotka ovat:

- Jos pääsyyn tarvitaan ainoastaan web-pohjaista sovellusta. Tällöin ratkaisut on erittäin kätevä käyttäjille ja helpompi asentaa ja ylläpitää etäkäyttöratkaisuilla.
- Välityspalvelin voi todentaa käyttäjät, ennen kuin he voivat saada pääsyä sovelluksiin. Toisin, kuin käyttäjät muodostaisivat yhteyden suoraan näytöltä kirjautuessa yksittäiseen sovellukseen.

- Tämä lisää toisen tietoturvallisuus tason sallimalla vain todennetut käyttäjät, jotka voivat nähdä mitä sovelluksia on tarjolla.
- TSL VPNn käyttävät asiakasjärjestelmät ovat yhteysverkkokerroksen yläpuolella, joten ne eivät ole samassa verkkokerroksessa kuin IPsec asiakkaat. Tämä heikentää kykyä hyökätä tai väärinkäyttää järjestelmiä organisaation tietoverkossa.
- Välityspalvelin voi todentaa itsensä käyttäjille.
- Kirjautuminen palveluihin on nyt helpompaa, se on vain yksi toiminnallinen välityspalvelin.

Mallin käytöstä voi olla seuraavat mahdolliset vastuut:

- Ei-web-pohjaisia sovellukset ja sovellus, jotka ovat haastavampia välityspalvelimelle, kuten ne jotka käyttävät useita dynaamisia portteja. Yleensä vaativat ylimääräisiä ohjelmistoja ja palveluita, kuten päätepalvelimia ja erityisiä asiakasohjelmia. Tämä tekee ratkaisusta enemmän resursseja vaativia ja hankalampia käyttää.
- Kompromissi välityspalvelimen kanssa saattaa antaa mahdollisuuden hyökkääjille siepata tietoja ja valtuutuksen moniin eri sovelluksiin yhdellä kertaa.
- TSL (SSL) on monimutkainen protokolla, josta on ollut tietoturvaongelmia joissakin toteutuksissa. Tämä tarkoittaa, että tietoturvan saavutettavuus tätä mallia käyttämällä ei ole niin korkea kuin IPSEC VPN mallilla.

Tunnettuja käyttötapoja

- Citrix tarjoaa SLL VPN-yhteyden etäkäyttäjille suojattuun verkkoon kirjautumiseen ja käyttää sovellutusten käytön organisaation tietoverkossa.
- Sonic Wall hankki Avential ja sen TSL VPN. Tämä tuote sisältää todennuksen ja tietoverkon hallinnan.
- Cyberroamilla on todennuspohjainen TSL VPN.
- Aventall, Cisco, Juniper, Microsoft ja Nokia myös sisältävät TSL VPN-yhteyden.

Katso myös

- Palomuureihin voidaan lisätä jokaiseen päätepisteen tulosuodatus. Niillä voidaan suojautua jonkinlaisiin hyökkäyksiin, jotka ovat peräisin epäluotettavista lähteistä.

- IDS:n voidaan lisätä jokaiseen verkkokerrokseen havaitsemaan hyökkäyksiä reaaliajassa.
- VPN käyttää Turvattukanava (engl. Secure Cannel) tietoturvamallia, joka puolestaan käyttää salakirjoitusta suojellakseen viestejä.
- Valtuutus (engl. Authenticator) tietoturvamallilla voidaan todentaa käyttäjät ja solmut.
- Valtuutus voidaan lisätä jokaiseen Web-sivuston pääsynvalvontaan ilman erityisiä resursointia.
- Itsessään välityspalvelin (engl. Proxy) on tietoturvamalli. Tässä tapauksessa se sieppaa pyyntöjä, jotka menevät päätepisteeseen ja suorittaa vaaditut tarkastukset.