TIETOTURVAN AUDITOINTI

Laura Kokkarinen
Pro gradu -tutkielma
Tietojenkäsittelytiede
Itä-Suomen yliopiston
tietojenkäsittelytieteen laitos
Marraskuu 2012

ITÄ-SUOMEN YLIOPISTO, luonnontieteiden ja metsätieteiden tiedekunta
Tietojenkäsittelytieteen koulutusohjelma

LAURA KOKKARINEN: Tietoturvan auditointi
Pro gradu -tutkielma, 65 s.
Pro gradu -tutkielman ohjaajat: FT Marko Hassinen ja FM Mikko Asikainen
Marraskuu 2012

Avainsanat: Auditointi, tietoturva, tietoturva-auditointi, organisaatio, riskienhallinta

Tämä pro gradu -tutkielma käsittelee tietoturva-auditointia yleisellä tasolla. Tutkielmassa kerrotaan monen eri osa-alueen kautta, mitä tietoturva-auditointi on, mikä on sen merkitys organisaatioille, ja mikä tekee tietoturva-auditoinnista laadukkaan. Tutkielmassa esitellään muun muassa auditoinnin elinkaaren eri vaiheet, auditoinnissa apuna käytettävät työkalut ja menetelmät, käsitellään auditoinnin kohteiden valintaa ja eri kohteiden auditointia, sekä kerrotaan myös itse tietoturvan harjoittamisesta, sisältäen tietoa riskien hallinnasta, tietoturvapolitiikkojen muodostuksesta ja parhaista tietoturvakäytännöistä.

Tutkielma on suurimmaksi osaksi kirjallisuuskatsaus, ja perustuu pääasiassa seuraaviin kolmeen kirjaan: Davis C., Schiller M.: *IT Auditing: Using Controls to Protect Information assets*; Jackson C.: *Network Security Auditing*; Moeller R.: *IT Audit, Control and Security*. Tutkielma sisältää kuitenkin myös empiirisen osuuden, jonka tutkimusmenetelmänä käytettiin haastatteluja.

Empiirinen osuus sisältää haastatteluvastaukset viideltä Suomessa toimivalta, tietoturva-auditointeja suorittavalta organisaatiolta. Haastattelun tuloksena saatiin tietoa organisaatioiden toiminnasta, esimerkkejä siitä, millaisia tietoturva-auditointeja suoritetaan Suomessa, sekä yksityiskohtaista tietoa auditointikäytännöistä. Haastatteluvastauksissa otettiin kantaa myös tietoturva-auditoinnin tulevaisuuden näkymiin. Empiirinen osuus tukee osaltaan kirjallisuuskatsausosiota ja tarjoaa käytännön esimerkkejä tietoturva-auditointeihin liittyen.

Esipuhe

Tämä tutkielma on tehty Itä-Suomen yliopiston tietojenkäsittelytieteen laitokselle keväällä 2012. Tutkielmani ohjaajina toimivat FT Marko Hassinen ja FM Mikko Asikainen, joille haluan osoittaa erityiskiitoksen.

Ohjaajieni lisäksi haluan kiittää kaikkia niitä Suomessa toimivia tietoturva-auditointeja suorittavia organisaatioita, jotka käyttivät paljon aikaa ja vaivaa laatimiini haastattelukysymyksiin vastaamiseen, ja täten mahdollistivat empiirisen osuuden liittämisen tutkielmaan.

Lisäksi haluan kiittää kaikkia lähiomaisiani kannustuksesta opintojeni viime metreillä. Mummoani Anja Korhosta kiitän terveiden paineiden luomisesta. Jo kauan ennen tutkielman valmistumista ”pian” pidettävistä valmistujaisjuhlista koko Kuopiolle kuuluttaminen hoputti minua saamaan tutkielmani valmiiksi. Kiitän myös isääni Veijo Kokkarista, joka osoitti tukensa omalla tavallaan tokaisemalla säännöllisesti "et sitten jätä niitä opintoja kesken", vaikka tuskin hän (toivottavasti) oikeasti epäili asiaa. Myös poikaystäväni Mika Immosen ajoittainen saamattomuus oman gradunsa työstämiseen suhteen oli omiaan motivoimaan minua jollain ehkä hieman sadistisella tavalla.

Haluan myös kiittää nykyistä työpaikkaani atBusiness Oy:ta, joka antoi minulle mahdollisuuden tehdä vajaata työviikkoa, jolloin saatoin varata enemmän aikaa tutkielmani tekoon. Ilman tätä järjestelyä tutkielmani valmistumiseen olisi mennyt huomattavasti pidempään.

Kuopiossa 19.11.2012

_____

Laura Kokkarinen

Käsitteet ja lyhenteet

Auditoinnin kohde	Organisaatio tai tietoturvan osa-alue, jota auditoidaan.
Auditoinnin skooppi	Rajattu alue organisaation tietoturvaa, joka aiotaan auditoida, ja jossa on tarkkaan määritelty auditoitavat kohteet.
Auditointityökalu	Auditointia nopeuttamaan ja helpottamaan kehitetty asia, joka voi esimerkiksi automatisoida osan auditointiprosessia, sopia tarkistuslistaksi tai varmistaa auditoinnin laatua.
Etuus	Termi *etuus* tulee englanninkielen sanasta *asset*, ja tarkoittaa niitä organisaation voimavaroja, jotka ovat tärkeitä sen liiketoiminnalle, ja joiden joutumisesta vääriin käsiin voi olla organisaatiolle huomattavaa haittaa.
Tietoturva-auditointi	Tietoturva-auditointi tarkoittaa kohteen tietoturvan nykytason kattavaa arviointia.
Tietoturvapolitiikka	Tietoturvapolitiikka on kokoelma organisaation laatimia tietoturvaan liittyviä säädöksiä, joita noudattamalla pyritään ehkäisemään organisaatiota koskevien tietoturvariskien toteutuminen.
Tietoturvaprosessi	Tietoturvaprosessi on käytännön toimintatapa, joka panee täytäntöön jonkin tietoturvapolitiikassa mainitun tietoturvasäädöksen.
Tietoturvastandardi	Tietoturvastandardi on kokoelma parhaita toimintatapoja tietoturvan harjoittamiseen liittyen. Standardeja käytetään auditointien viitekehyksinä.
Viitekehys	Viitekehys sisältää kuvauksen siitä, millainen hyvä tietoturvan taso on. Viitekehyksiä käytetään auditoinneissa vertailukohteina, ja niihin verraten voidaan havaita organisaation tietoturvassa olevat puutteet.

Sisällysluettelo

1 JOHDANTO

Tämä pro gradu -tutkielma käsittelee tietoturva-auditointia yleisellä tasolla. Tutkielman tarkoitus ei ole paneutua minkään tietyn tietoturvan osa-alueen auditointiin, vaan antaa hyvä yleiskuva siitä, mitä tietoturva-auditointi on, ja mitä eri huomioon otettavia asioita siihen liittyy. Tutkielmassa käsitellään auditoinnin eri vaiheita, niihin liittyviä haasteita, auditoinnin merkitystä organisaatiolle, ja käydään läpi ne asiat, jotka tekevät tietoturvasta ja sen auditoinnista laadukkaan.

Luvussa 2 kerrotaan lyhyesti tietoturvasta ja sen auditoinnista. Luvussa 3 käsitellään erityyppisiä tietoturva-auditoijia, auditointitiimejä ja heidän työnkuvaansa. Luvussa 4 kerrotaan tietoturvariskien hallinnasta, käyden läpi aihealueeseen liittyvät termit, riskienhallintaprosessi ja riskien eri käsittelytavat. Luvussa 5 käsitellään tietoturva-auditointiprosessin elinkaari kaikkine vaiheineen. Luvussa 6 kerrotaan auditointiskoopeista ja niiden muodostuksesta, käsitellen samalla eri auditointityypit ja -tasot sekä menetelmän auditointikohteiden valintaan. Luvussa 7 puhutaan tietoturvapolitiikoista, niiden merkityksestä ja auditoinnista. Luvussa 8 käsitellään tietoturvan hallintaprosessin auditointia, mikä sisältää henkilöstön, tietoturvaprosessien ja teknologian auditoinnin. Luvussa 9 kerrotaan tietoturvakontrolleista, niiden toteutustavoista, toiminnallisuustyypeistä ja auditoinnista. Luvussa 10 käsitellään tietoturva-auditoinneissa käytetyt työkalut, mukaan lukien testauskehykset, automatisoidut työkalut ja tietoturvastandardit. Luku 11 sisältää tämän tutkielman empiirisen osuuden, jota varten haastateltiin viittä Suomessa toimivaa, tietoturva-auditointeja suorittavaa organisaatiota.

2 TIETOTURVA JA SEN AUDITOINTI LYHYESTI

Tietoturvan harjoittaminen kuuluu tänä päivänä lähes jokaisen organisaation arkipäivään. Tietoturvan kattavuudesta ei kuitenkaan voida olla täysin varmoja ilman sen säännöllistä arviointia. Tässä luvussa kerrotaan lyhyesti tietoturvasta, auditoinnista ja niiden merkityksestä. Luvun tavoitteena on antaa lukijalle pohjatiedot tietoturvasta ja auditoinnista, jonka jälkeen tulevien lukujen sisältämän tiedon omaksuminen on helpompaa.

Luvussa 2.1 kerrotaan lyhyesti tietoturvan harjoittamisesta organisaatioissa, ja mitä seurauksia tietoturvan unohtamisella voi olla. Luvussa 2.2 Kerrotaan puolestaan lyhyesti tietoturva-auditoinnista ja sen merkityksestä organisaatiolle.

2.1 Tietoturvan harjoittaminen

Tietoturvan harjoittaminen tarkoittaa käytännössä organisaation tietojärjestelmien ja liiketoimintaprosessien hallintaa niin, että valtuutetut käyttäjät, joihin kuuluu useimmiten organisaation henkilöstö ja mahdollisesti myös muita sidosryhmiä, pääsevät käsiksi organisaation etuuksiin, mutta valtuuttamattomat eivät. Etuuksilla tarkoitetaan kaikkia organisaation voimavaroja, jotka ovat tärkeitä sen liiketoiminnalle, ja joiden joutumisesta vääriin käsiin voi olla organisaatiolle huomattavaa haittaa. Toimivat liiketoimintaprosessit, turvallisesti säilytetyt tiedot ja hyvä maine ovat esimerkkejä organisaation toiminnalle tärkeistä etuuksista. Valtuuttamattomien henkilöiden mahdollista pääsyä käsiksi organisaation etuuksiin kutsutaan tietoturvauhaksi, ja uhan toteutuminen aiheuttaa useimmiten organisaatiolle tappioita joko suoraan tai esimerkiksi maineen menettämisen ja asiakkaiden vähenemisen kautta.

[Jac10]Organisaatiota uhkaavat tietoturvauhat voidaan karkeasti jaotella seuraaviin kategorioihin: palvelunestohyökkäykset, tietoverkkojen hyväksikäyttö, tietovarkaudet sekä tunkeutumiset ja haltuunotot. Palvelunestohyökkäysten tavoite on estää verkon kautta saatavilla oleviin resursseihin pääsy, millä voi olla suuri vaikutus organisaation päivittäiseen toimintaan. Tietoverkkojen ja niitä hyödyntävien sovellusten tietoturva-aukkoja hyväksikäyttämällä ulkopuolinen käyttäjä voi puolestaan murtautua suljettuun

verkkoon ja kuunnella sen kautta käytävää tietoliikennettä. Tietovarkaudet taas ovat vakava uhka organisaation toiminnan ja imagon kannalta, koska organisaatio usein säilöö paljon arkaluontoista organisaatiota ja heidän asiakkaitaan koskevaa tietoa, jonka joutumisella vääriin käsiin tai vuotamisella julkisuuteen voi olla todella paljon negatiivisia seurauksia. Ja jos ulkopuolinen taho pääsee käsiksi organisaation järjestelmiin, hyökkääjä voi esimerkiksi saastuttaa palvelimia viruksilla tai sabotoida muuten organisaation toimintaa.

2.2 Tietoturva-auditointi

[Jac10]Tietoturva-auditointi on puolueetonta tietoturvan testaamista niin, että saadaan selkeä käsitys siitä, onko organisaation tietoturva riittävä sen etuuksien suojaamiseen, ja mitä tietoturvan osa-alueita pitää vielä mahdollisesti parantaa. Auditoinnin aikana selvitetään organisaation tietoturvariskit ja varmistetaan, että niiltä on suojauduttu asianmukaisesti.

[Jac10]Riittävän tietoturvan arviointi organisaation tilanteeseen nähden on usein hankalaa. Eri teknologioiden avulla voidaan pienentää tietoturvariskejä huomattavasti, mutta ainoastaan silloin, kun niitä käytetään oikein ja oikeissa paikoissa. Tietoturva-auditoijan tehtäviin kuuluu selvittää organisaatiota koskevat tietoturvariskit, niiden toteutumismahdollisuudet ja niiden mahdollisesta toteutumisesta koituvat kustannukset sekä tarkistaa, onko niihin varauduttu tarpeeksi hyvin ottaen huomioon riskien toteutumismahdollisuudet ja niiden toteutumisesta aiheutuvat tappiot. Lisäksi auditoijan täytyy raportoida havaituista puutteista ja esittää puutteille korjausehdotuksia. Ilman järjestelmällistä ja kattavaa arviointia, ei voida koskaan tietää varmaksi, onko organisaation tietoturva toteutettu onnistuneesti.

3 TIETOTURVA-AUDITOIJAT

Tietoturva-auditointien laadukas suorittaminen vaatii paljon ammattitaitoa monilta siihen liittyviltä eri osa-alueilta, mikä tekee auditoijien työstä haasteellisen. Tässä luvussa kerrotaan erilaisista auditoijatyypeistä sekä käsitellään heidän työnkuvaansa. Luvussa 3.1 kerrotaan auditoijista ja heidän työtehtävistään yleisellä tasolla, luvussa 3.2 käsitellään sisäisten- ja ulkoisten auditoijien eroja, ja luvussa 3.3 kerrotaan auditointitiimien rakenteesta.

3.1 Auditoijien työnkuva

[Jac10]Auditoinnin suorittava henkilö on käytännössä puolueeton havainnoija ja arvioija, joka tehtävä on ensisijaisesti tunnistaa, mitata ja raportoida tietoturvariskit ja niihin perustuen määritellä sen hetkinen tietoturvan taso. Auditoija muun muassa haastattelee organisaation henkilöstöä, katselmoi tietoturvan toteutukseen liittyviä dokumentteja ja testaa tietoturvan tekniset osa-alueet. Puolueettomuudella pyritään varmistamaan, että auditointi varmasti suoritetaan oikeellisesti ja oikeudenmukaisesti.

[DaS11]Auditoijilta odotetaan hyvää teknistä osaamista ja kykyä nähdä metsä puilta, jotta he keskittyvät olennaiseen, eivätkä takerru pienimpiin teknisiin yksityiskohtiin. Analyyttiset taidot ovat myös tärkeitä, koska auditoijan tulee pystyä analysoimaan keräämäänsä tietoturvasta kertovaa dataa, ja päättelemään, mitä se todellisuudessa merkitsee organisaation tietoturvan kannalta. Koska auditoija on paljon tekemisissä kohdeorganisaation henkilöstön kanssa läpi auditoinnin koko elinkaaren, hyvät kommunikaatiotaidot ovat tärkeitä niin jokapäiväisessä kanssakäymisessä kuin auditoijan ja asiakkaan välisen luottamuksen muodostamisessa. Myös uusien asioiden nopea oppiminen on auditoijan työssä tärkeää, koska teknologiat ja auditointitekniikat kehittyvät jatkuvasti, ja laadukkaan auditoinnin suorituksessa auditoijan päivitetty ammattitaito on suuressa roolissa.

Vaikka auditoija onkin pääasiallisesti puolueeton arvioija, auditointeja suorittavat organisaatiot usein esittävät asiakkailleen myös parhaat tavat korjata havaitut puutteet. He voivat joskus olla jopa valmiita suorittamaan vaaditut korjaustyöt.

3.2 Sisäiset ja ulkoiset auditoijat

Hyvä auditoija on ammattitaitoinen, tehokas, puolueeton ja tietää organisaation toiminnasta mahdollisimman paljon. Sisäisten ja ulkoistettujen auditoijien ero on siinä, että molemmat auditoijatyypit ovat parempia tietyillä osa-alueilla kuin toinen.

[DaS11][Tie04]Ulkoistetut auditoijat tekevät auditointeja jatkuvasti monille erilaisille organisaatioille, he ovat saaneet kattavan koulutuksen ammattiinsa, voivat todistaa pätevyytensä sertifikaattien avulla sekä jatkuvasti päivittävät osaamistaan tietoturvaan ja auditointiin liittyen. [Laa10]Näistä edellä mainituista syistä he useimmiten ovat ammattitaitoisempia ja tehokkaampia kuin organisaation omat sisäiset auditoijat, joilla auditointi saattaa pahimmassa tapauksessa olla vain sivutehtävä heidän pääasiallisten työtehtäviensä ohella. [Tie04]Kannattaa kuitenkin muistaa, että ulkoisten auditoijien suorittamien auditointien laadussa voi myös olla huomattavia eroja.

[Laa10]Jos tietoturva-auditointi on vain jonkun henkilöstön jäsenen sivutehtävä, sisäisen auditoijan motivaatio voi olla heikko suorittamaan päätoimisten työtehtäviensä ulkopuolisia tehtäviä, ja hän voi vedota kiireisiinsä päästäkseen vetäytymään pois auditoijan roolista. Auditoija saattaa suorittaa tietoturva-auditointeja vain kerran tai pari vuodessa, jolloin hänen ammattitaitonsa ei pääse kehittymään ja tietämys tietoturva-auditoinneista pääsee vanhenemaan. Päätoimisten työtehtäviensä ohessa auditoijalla ei välttämättä ole tarpeeksi aikaa valmistautua auditoinnin suoritukseen dokumentaatioon ja auditoinnin kohteisiin perehtymällä. Lisäksi auditoinnin suorittaminen ja siitä raportointi saattaa jäädä pinnalliseksi kiireen keskellä ja motivaation puuttuessa.

Sisäinen auditoija voi kuitenkin myös olla hyvin koulutettu ja ammattitaitoinen, pelkästään auditointeja suorittava työntekijä, joten edellä mainittu ”kauhu-skenaario” ei aina pidä paikkaansa sisäisten auditoijien kohdalla. Sisäisillä auditoijilla on myös useimmiten paljon parempi tietämys organisaation toiminnasta, millä on useimmiten todella positiivinen vaikutus auditoinnin laatuun. Sisäisten auditoijien avulla tietoturva-auditoinnit saadaan myös yhdistettyä paremmin osaksi organisaation jatkuvaa liiketoimintaa.

Ulkoistetut auditoijat ovat nimensä mukaan organisaation ulkopuolisia henkilöitä, joilla ei ole mitään merkittäviä suhteita organisaatioon, ja täten puolueettomana tahona

toimiminen ei ole heille ongelma. [DaS11]Sisäisille auditoijille puolueettomana tahona toimiminen voi kuitenkin olla joskus todella hankalaa ja ahdistavaa, koska sama organisaatio, joille heidän pitää antaa palautetta mahdollisesti huonosti toteutetusta tietoturvasta, maksaa myös heidän palkkansa. Lisäksi auditoijat todennäköisesti muodostavat vahvoja ystävyyssuhteita muiden organisaation työntekijöiden kanssa, ja heitä saatetaan myös pyytää konsultoimaan erilaisiin tietoturvaratkaisuihin liittyen; nämä asiat saattavat vaikuttaa heidän puolueettomuuteensa.

[DaS11]Vaikka puolueettomana pysytteleminen onkin sisäisille auditoijille haastavaa, heidän ei tulisi sulkea itseään pois muun organisaation päivittäisestä toiminnasta, vaan tarjota tietoturvakonsultaatiota aktiivisesti, kun sitä tarvitaan. Tietoturvakontrollien toteutus oikein niiden elinkaaren alkuvaiheessa on paljon kustannustehokkaampaa organisaation kannalta, kuin jo toteutettujen kontrollien korjaaminen vasta auditoinnin jälkeen. Kun auditoija on ollut mukana suunnittelemassa jonkin tietoturvakontrollin käyttöönottoa, hänellä on myös enemmän tietoa siitä, miten se tulisi auditoida. Auditoijan ei kuitenkaan kannata toteuttaa mitään antamistaan suosituksista, joita hän aikoo myöhemmin auditoida, koska auditoija ottaisi silloin todennäköisimmin puolueellisen kannan eikä välttämättä tulisi testanneeksi kaikkia tarpeellisia asioita. Auditoijan tehtävä on palautteen antaminen tietoturvakontrolleihin liittyen, ei niiden toteuttaminen.

3.3 Auditointitiimit

Tässä tutkielmassa auditoijiin viitataan pääsääntöisesti yksikössä, mutta todellisuudessa tietoturvaa voi olla auditoimassa useampi henkilö. Auditointitiimeissä on se hyvä puoli, että sen suorittamaan auditointiin voidaan sisällyttää paljon enemmän ammattitaitoa kuin mitä yksi henkilö pystyy tarjoamaan, koska tiimi voi koostua hyvinkin erilaisista auditoijista. Auditointitiimi voi koostua muun muassa tietoturva-auditoinnin ammattilaisista, IT-ammattilaisista, henkilöistä, joilla on auditointikokemusta, mutta jotka eivät suorita auditointeja ammatikseen, sekä harjoittelijoista.

Tietoturva-auditoinnin ammattilaisia käsiteltiin jo edellisessä luvussa ulkoistettujen auditoijien yhteydessä. [DaS11]Auditointeja ammatikseen tekevät henkilöt ovat tärkeä osa auditointitiimiä. He tuntevat auditointiprosessin ja ymmärtävät testauksen ja

tietoturvan vahvistamisen merkityksen. He tietävät paljon IT:stä teoriassa, mutta heiltä usein puuttuu käytännön kokemus tietojärjestelmiin liittyvistä päivittäisistä operaatioista. Tästä syystä auditointitiimiin kannattaa ottaa myös hieman syvällisemmän IT-tietouden omaavia henkilöitä.

[DaS11]IT-ammattilaiset tietävät paljon eri teknologioista, mutta heillä ei ole varsinaista auditointikokemusta. He voivat kuitenkin olla tärkeä osa auditointitiimiä, koska he pystyvät tarjoamaan paljon syvällistä tietoa käsiteltäviin teknologioihin liittyen, mikä puolestaan vaikuttaa positiivisesti auditoinnin laatuun. Parhaassa tapauksessa IT-ammattilainen on kohdeorganisaation työntekijä, jolloin hän voi myös kertoa, miten organisaation prosessit toimivat. Kannattaa kuitenkin muistaa, että jotain tiettyä kohdetta auditoimaan ei kannata ottaa sellaista IT-ammattilaista, joka on aikaisemmin ollut sitä kehittämässä.

Henkilöt, jotka eivät ole tietoturva-auditoinnin ammattilaisia, mutta joilla on kokemusta sisäisistä tai ulkoisista auditoinneista, voivat myös olla osa auditointitiimiä. Vaikka nämä auditoijat eivät ole ammattilaisia, he tuntevat auditointiprosessin hyvin ja voivat merkittävästi edistää auditoinnin suoritusta. Auditoijan kokemuksella on todella suuri painoarvo auditoinnin suorituksessa ja pelkkä teorian tunteminen ei riitä. Huonoimmassa tapauksessa tällainen auditoija havainnoi auditoitavia kohteita pinnallisesti ja keskittyy tavallisimpiin ongelmiin tai pyrkii eliminoimaan kaikki riskit täysin sen sijaan, että harkitsisi muita järkevämpiä riskienkäsittelytapoja. Riskienkäsittelytavoista kerrotaan enemmän luvussa 4.3.

[DaS11]Auditointitiimiin voidaan ottaa mukaan myös harjoittelijoita esimerkiksi oppilaitoksista, joissa heille on opetettu auditoinnin perusteet, ja joissa opiskelijat tulevat jatkuvasti tekemisiin uusien teknologioiden kanssa. Heidän lukumääränsä ei saisi olla kuitenkaan kovin suuri suhteessa tiimin kokoon, koska heillä ei vielä ole syvällistä tietämystä auditoinnista ja tästä syystä tarvitsevat paljon ohjausta. Harjoittelijat ovat usein kuitenkin innokkaita ja energisiä, ja voivat tarjota paljon tietoa kaikkein uusimmista ja suosituimmista teknologioista.

4 TIETOTURVARISKIEN HALLINTA

Riskienhallinta on todella olennainen osa tietoturvan toteutusta ja sen auditointia. Ennen kuin voidaan sanoa onko organisaation tietoturva kattava vai ei, täytyy tietää mitkä ovat organisaatiota koskevat tietoturvariskit ja miten näitä riskejä voidaan pienentää mahdollisimman kustannustehokkaasti. Vasta kun nämä asiat ovat selvillä voidaan arvioida, kattaako organisaation tietoturva sille asetetut tavoitteet ja suojeleeko se todella organisaation etuuksia niitä koskevilta riskeiltä.

Koska riskienhallinta on niin tärkeässä asemassa tietoturvan harjoittamisessa ja sen auditoinnissa, aihe käsitellään tässä tutkielmassa ennen varsinaisen auditoinnin elinkaaren käsittelyä. Luvussa 4.1 kerrotaan, mitä tarkoittavat organisaation etuudet, tietoturvauhat, haavoittuvuudet ja tappiot riskienhallinnan näkökulmasta. Luvussa 4.2 kerrotaan riskienhallintaprosessista, ja luvussa 4.3. kerrotaan, mitä eri tapoja on käsitellä havaitut tietoturvariskit.

4.1 Etuudet, uhat, haavoittuvuudet ja tappiot

[Jac10]Organisaatiolla on monia vaihtoehtoja riskienhallintaan, joista osa perustuu matematiikkaan ja osa asiantuntijan kokemukseen ja mielipiteeseen. Kaikille näille tavoille on kuitenkin yhteistä etuuksien, uhkien, haavoittuvuuksien ja uhan toteutumisesta aiheutuvien kustannusten huomioonottaminen.

[Jac10]Etuuksilla tarkoitetaan asioita, jotka ovat tärkeitä organisaation liiketoiminnalle, ja joita tietoturvan harjoittamisen on tarkoitus suojella tietoturvauhilta. Esimerkkejä etuuksista ovat muun muassa tietokannat, liiketoimintaprosessit ja tietoverkkoihin pääsy. Etuuksien merkityksen arviointi on osa riskien kartoitusta, ja tätä merkitystä usein mitataan asettamalla etuuksille jokin rahallinen arvo. Rahallisen arvon asetus voi olla joillekin asioille – kuten esimerkiksi vaihtoehtoiskustannuksille tai organisaation maineelle – kuitenkin vaikeaa, mikä tekee etuuksien tärkeyden arvioinnista haasteellista.

[Jac10]Tietoturvauhka on tapahtuma, jonka seuraukset ovat organisaation kannalta negatiiviset ja usein johtavat rahallisiin tappioihin. Uhkia arvioidaan useimmiten niiden toteutumismahdollisuuksien perusteella.

[Jac10]Haavoittuvuus on johonkin asiaan liittyvä heikkous, joka mahdollistaa uhan toteutumisen. Vaikka sovellus- ja laitteistohaavoittuvuuksia havaintaankin lähes joka päivä, suurin osa haavoittuvuuksista edelleen johtuu järjestelmien vääränlaisesta konfiguraatiosta.

[Jac10]Tietoturvauhan toteutumisen aiheuttamat kustannukset tarkoittavat organisaation konkreettisia tappioita, kun jokin etuus on joutunut tietoturvahyökkäyksen kohteeksi. Etuuksien merkityksen arvioinnilla on suora yhteys tähän, mutta liiketoimintaprosessien ja eri asioiden välillä olevien yhteyksien takia todellisten tappioiden määrä voi olla paljon etuuksien arvioitua arvoa suurempi. Usein voidaan unohtaa muun muassa menetetyn datan tai työajan todellinen arvo.

4.2 Riskienhallintaprosessi

[Jac10]Kuten aikaisemmin mainittiin, riskienhallintaa voi harjoittaa monella eri tavalla. NIST 800-30 on määritellyt riskienhallintaprosessin, joka jakautuu seuraavaan yhdeksään askeleeseen: järjestelmän kartoitus, uhkien tunnistaminen, haavoittuvuuksien tunnistaminen, kontrollien analysointi, uhkien toteutumisen todennäköisyyden selvitys, uhkien toteutumisen seurausten analysointi, riskien selvitys, tietoturvakontrollien suosittelu, ja tulosten dokumentointi.

[Jac10]Riskien analysointiin on myös monia eri tapoja, joista suurin osa jakautuu joko määrällisiin tai laadullisiin lähestymistapoihin. Määrälliset lähestymistavat käyttävät matemaattista kaavaa riskin todennäköisyyden ja rahallisen arvon rinnastamiseksi.

[Jac10]Kaavat itsessään eivät ole vaativia, mutta niissä käytettävän datan muodostaminen voi olla haastavaa. Kaavoja varten on kuitenkin jo olemassa dataa, jota voidaan käyttää. Muun muassa CSI:n (Computer Security Institute) ja FBI:n (Federal Bureau of Investigation) suorittaman vuosittain tapahtuvan tietoturvaa ja tietoturvarikoksia koskevan tutkimuksen raporttia voi käyttää datan lähteenä. Jokainen

organisaatio on kuitenkin erilainen, joten dataa tulee aina myös pohtia kohdeorganisaation kannalta, eikä ottaa suoraan jostain muusta lähteestä.

[Jac10]Laadullinen riskianalyysi jättää numerot taka-alalle ja keskittyy niiden etuuksien löytämiseen, jotka ovat kaikkein riskialteimpia. Chris Jacksonin mukaan helpoin tapa uhkien tunnistamiseen on käyttää CIA:ta, joka koostuu kolmesta asiasta, jota organisaatio haluaa pääasiallisesti suojella: luottamuksellisuudesta (Confidentiality), yhtenäisyydestä (Integrity) ja saatavuudesta (Availability). CIA:n avulla voidaan selvittää näitä kolmea aluetta koskevat uhat. Kun uhat on selvitetty, täytyy ne luokitella niiden toteutumismahdollisuuksien ja kannattavuuden mukaan. Esimerkiksi riskit, jotka liittyvät luottokorttitietoihin, kannattaa luokitella tärkeimpiin käsiteltäviin riskeihin.

4.3 Riskien käsittelytavat

[Jac10]Vaikka riskejä ei voikaan välttää kokonaan, riskien hallinnalla voidaan pienentää niitä huomattavasti. Auditoijan täytyy varmistaa, että organisaation harjoittama tietoturva todellakin suojelee sen etuuksia niitä koskevilta tietoturvauhilta mahdollisimman hyvin. Auditoijan tulisi mielellään myös varmistaa, että tietoturva on toteutettu mahdollisimman kustannustehokkaasti.

[Jac10]Kun organisaation etuuksia koskevat tietoturvariskit on tunnistettu ja analysoitu, täytyy selvittää, miten riskejä kannattaa käsitellä. Riskejä voidaan pienentää todella paljon esimerkiksi erilaisten teknologioiden avulla, mutta tämä on kannattavaa ainoastaan silloin, kun tiedetään missä tilanteessa tällaisista turvakontrolleista on eniten hyötyä. Tarvittavan tietoturvan määrän arviointi riskinhallinnassa on myös tärkeää tästä samasta syystä. Riskeiltä ei koskaan voida suojautua kokonaan, eikä sen tavoitteleminen ole myöskään kannattavaa. Riskien käsittelyyn on olemassa muitakin vaihtoehtoja kuin niiden pienentäminen, jotka voivat tietyissä tilanteissa osoittautua paremmiksi vaihtoehdoiksi.

[Jac10]Riskin hyväksyminen on yksi vaihtoehtoinen riskienkäsittelytapa. Tämä voi olla kannattavaa, jos riskin toteutumisen todennäköisyys on olematon. Organisaation ei myöskään kannata investoida rahaa sellaisen riskin pienentämiseen, jonka toteutumisella on pienemmät kustannukset kuin tarvittavien tietoturvakontrollien

käyttöönotolla. Tähän käsittelytapaan liittyvä riski on se, että organisaatio ei osaa arvioida uhan toteutumisen todellisia kustannuksia.

[Jac10]Riskin välttäminen on toinen vaihtoehtoinen käsittelytapa. Organisaatio voi katsoa parhaaksi olla suorittamatta liiketoimintaansa tavalla, joka asettaisi sen alttiiksi jollekin tietylle riskille.

[Jac10]Riskin siirto tai jakaminen on myös yksi vaihtoehto. Jakaminen voi tapahtua esimerkiksi etuuksia vakuuttamalla, ja siirtäminen jonkin palvelun ulkoistamisella, jolloin kolmas osapuoli on vastuussa palvelun tietoturvasta. Tämä käsittelytapa ei kuitenkaan suojaa organisaatiota esimerkiksi maineen menettämiseltä niissä tapauksissa, kun heidän vakuuttamansa etuus tai ulkoistettu palvelu joutuu tietoturvahyökkäyksen kohteeksi.

5 TIETOTURVA-AUDITOINTIPROSESSIN ELINKAARI

Tietoturva-auditointiprosessi koostuu useasta, tietyssä järjestyksessä tapahtuvasta vaiheesta. Eri henkilöt ovat keksineet näille vaiheille monia eri nimiä, ja vaiheiden väliset rajat on vedetty hieman eri tavoin, mutta yksittäisten vaiheiden nimistä ja tarkasta sisällöstä huolimatta tietoturva-auditointiprosessi sisältää aina samat asiat, jotka tapahtuvat aina samassa järjestyksessä.

Tässä tutkielmassa tietoturva-auditointiprosessin elinkaari on jaettu seuraaviin vaiheisiin: auditoinnin suunnitteluun, kenttätutkimukseen, tutkimusdatan analysointiin, korjausehdotusten laatimiseen, auditoinnin tuloksista raportointiin ja jälkitoimiin. Luvussa 5.1 kerrotaan auditoinnin suunnittelusta eli siitä, mitä asioita tulee ottaa selville ja päättää ennen varsinaisen auditoinnin suoritusta. Luvussa 5.2 kerrotaan kenttätutkimuksesta ja siitä, mitä eri tapoja auditoinnissa tarvittavan tiedon keräykseen on. Luvussa 5.3 käydään läpi kerätyn tiedon analysointiin liittyvät asiat. Luvussa 5.4 puhutaan parhaasta tavasta laatia tietoturvapuutteiden korjausehdotelma. Luvussa 5.5 käydään läpi raportointivaiheen sisältö, ja luvussa 5.6 kerrotaan lyhyesti, mitä tarkoittavat auditoinnin jälkitoimet.

5.1 Auditoinnin suunnittelu

[DaS11]Ennen varsinaisen auditoinnin suoritusta täytyy kartoittaa, mitä kohteita kannattaa tai tulee auditoida. [Jac10][DaS11]Suunnitteluvaihe on ensimmäinen ja kaikkein tärkein auditoinnin vaihe, koska varsinaisen auditoinnin suoritus perustuu siihen. [Jac10]Vaiheen aikana päätetään auditoinnin strategia perustuen sen tarkoitukseen. Auditoinnin tarkoitus voi olla esimerkiksi varmistaa, vastaako organisaation tietoturva jotakin standardia tai ohjeistusta, jota sen tulisi noudattaa. [Jac10][DaS11]Suunnitteluvaiheen tarkoitus on kartoittaa auditoinnin tavoitteet, skooppi, auditoitavat kohteet, aikataulu ja tarvittavat resurssit.

[DaS11]Suunnittelua varten auditoijan täytyy aina tutkia tarkasti organisaation toimintaa, ottaa selvää auditointiprosessiin vaikuttavista seikoista, ja pohtia eri vaihtoehtoja, koska jokainen auditointi on erilainen. [Jac10]Tietoa voidaan kerätä

organisaation rakenteesta, prosesseista ja tiedonkulusta. Lisäksi voidaan selvittää ketä kannattaa haastatella, mitä osastoja tulee katselmoida, mitkä tulevat olemaan auditoinnin aikana käytettävät menetelmät, työkalut ja resurssit, sekä mikä viitekehys sopii parhaiten auditoinnin tarkoitukseen.

[DaS11]Tutkimus voi tapahtua organisaation toimintaa havainnoimalla, henkilöstöä haastattelemalla, dokumentteja – kuten esimerkiksi tietoturvapolitiikkoja – katselmoimalla, ja yleisesti organisaation liiketoiminta-alueeseen tutustumalla. Lisäksi suunnittelussa voidaan käyttää hyväksi standardeja tarkistuslistoja, jotka saattavat huomattavasti helpottaa tarkastettavien asioiden päättämistä. Tarkistuslistoja ei kuitenkaan kannata noudattaa sellaisinaan, vaan ne tulee aina sovittaa auditoitavan organisaation auditointitarpeisiin sopiviksi.

[DaS11] Asiakkaan pyyntöjä ei tulisi myöskään jättää huomiotta. Asiakkaalla on usein hyvä käsitys niistä organisaation etuuksista, joiden suojaamiseen käytetyn tietoturvan tason tarkastaminen on tärkeää. Lisäksi kun asiakkaalta kysytään mielipidettä auditoitavista kohteista, asiakas kokee omaavansa tärkeän roolin auditoinnissa, millä on positiivinen vaikutus muun muassa auditoinnin tuloksia läpikäytäessä, jolloin asiakas todennäköisesti suhtautuu myönteisemmin negatiivisiinkin tuloksiin.

Asiakkaan mielipiteen ei saa antaa kuitenkaan vaikuttaa liikaa auditoinnin suuntaan: auditoijan tulee luottaa ensisijaisesti omaan ammattitaitoonsa ja tietää, milloin asiakkaan huoli jonkin asian tietoturvasta on aiheellinen, ja milloin pyyntö puolestaan kannattaa jättää huomiotta. Auditoinnin skoopin määrittelystä kerrotaan enemmän luvussa 6.

[DaS11]Kun auditoinnin tavoitteet ja skooppi on päätetty, täytyy auditoijan kartoittaa kohdealuetta koskevat tietoturvariskit ja niiden perusteella määritellä varsinaisen auditoinnin yksityiskohtaiset tehtävät. Toimenpiteiden tarkoituksena on saada varmuus siitä, että tietoturvariskit varmasti käsitellään asianmukaisella tavalla. Jos esimerkiksi auditoinnin kohteena on jokin yksittäinen prosessi, auditoijan täytyy miettiä, missä eri kohdissa prosessin tietoturva saattaa mahdollisesti pettää, ja suunnitella näiden kohtien tarkastus. Jos kyseessä on jokin järjestelmä tai teknologia, auditoija voi miettiä niihin liittyviä uhkia ja haavoittuvuuksia, ja tarkistaa niihin liittyvät mahdolliset tietoturvaongelmat.

[DaS11]Auditoinnin aikataulun laatiminen on myös merkittävä osa suunnitteluvaihetta. Aikataulu tulisi sovittaa yhteen kohdeorganisaation aikataulun kanssa, jolloin suunnitelmassa voidaan ottaa huomioon organisaation henkilöstön poissaolot ja organisaation kiireelliset ajanjaksot. Näin auditointi voidaan suorittaa tarvittavien henkilöiden paikalla ollessa ja minimoida organisaation toiminnan hankaloituminen auditoinnin aikana.

[DaS11]Jos auditointi on suunniteltu hyvin, se todennäköisesti myös onnistuu hyvin, kun taas auditoinnin ollessa huonosti suunniteltu, sen laatu tulee todennäköisesti kärsimään auditoinnin elinkaaren myöhemmissä vaiheissa. Auditointisuunnitelma täytyy dokumentoida tarkasti, jotta sitä voidaan helposti seurata ja jokaisen suunnitellun auditointiaskeleen merkitys varmasti ymmärretään. Tietoturva-auditoinnin tarkoitus on aina kohdeorganisaation tietoturvan todellisen tason tutkiminen, eikä auditointisuunnitelman kyselemätön seuraaminen. Auditointiaskelten tarkoituksen ymmärtäminen on tärkeää, jotta auditoinnin aikana auditoija voi tarpeen vaatiessa ehdottaa myös suunnitelmaan kuulumattomien asioiden tarkistusta tietoturvan todellisen tilan selvittämiseksi.

[DaS11]Suunnitteluvaiheen loppupuolella auditoija ja kohdeorganisaatio voivat vielä pitää käynnistyspalaverin, jossa käydään läpi auditointisuunnitelma ja tehdään siihen tarvittaessa muutoksia. Käynnistyspalaverin ja suunnitelman hyväksymisen jälkeen auditoija voi siirtyä kenttätyöskentely- ja dokumentaatiovaiheeseen.

5.2 Kenttätutkimus

[Jac10]Kenttätutkimusvaiheessa kerätään organisaation tietoturvaan liittyvää dataa perustuen suunnitteluvaiheessa laadittuun auditointisuunnitelmaan ja tarkastettavat kohteet kattavaan tarkastuslistaan. [DaS11]Myöhemmin tämä data analysoidaan, jotta voidaan tunnistaa mahdolliset tietoturvariskit ja tarkistaa niiden käsittelytavat. [Jac10]Vaiheen tarkoituksena on myös kerätä todisteita siitä, miten hyvin organisaatio noudattaa valitun viitekehyksen tietoturvasuosituksia.

[Jac10]Tietoa voidaan kerätä esimerkiksi tutkimalla järjestelmien dokumentaatiota, haastattelemalla organisaation johtoa ja työntekijöitä tai suorittamalla kyselyitä

politiikkoihin ja menetelmiin liittyen. Lisäksi voidaan tutkia järjestelmiä ja prosesseja, katselmoida edellisiä auditointikertoja koskevaa dokumentaatiota sekä lokeja ja raportteja, muodostaa tilastoja tiedonsiirtoa koskien sekä tutkia teknisten kontrollien konfiguraatioita. Tiedon keräämiseen voidaan käyttää apuna monia eri työkaluja, jotka keräävät dataa eri kohteista myöhempää analysointia varten, tai jotka suoraan analysoivat tutkimansa kohteen turvallisuuden tasoa perustuen sen eri muuttujiin. [DaS11]Auditoijien tulee kuitenkin aina huolellisesti validoida saamansa tiedot. Tietoturvan auditoinnissa käytetyistä työkaluista ja menetelmistä on kerrottu enemmän luvussa 10.

[DaS11]Vaikka tämä auditoinnin vaihe seuraakin tarkasti auditointisuunnitelmaa, auditoijien tulee kuitenkin olla valmiita auditoimaan myös muita suunnitelmassa käsittelemättömiä asioita, jos auditoinnin aikana huomataan jotain muita vakavia ongelmia. Kuten aikaisemminkin mainittiin, auditoinnin päätehtävä on aina organisaation tietoturvan tason laadukas selvittäminen, eikä suunnitelman kyselemätön seuraaminen. Auditoinnin laadun varmistamiseksi myös dokumentointi on tärkeä osa kenttätutkimusta, ja dokumentaatio voi myöhemmin toimia referenssinä, kun halutaan tarkkaa tietoa auditoinnin suorituksesta.

5.3 Tutkimusdatan analysointi

[Jac10]Kun tieto organisaation tietoturvan sen hetkistä tasoa koskien on kerätty, se täytyy analysoida. Analyysivaiheeseen kuuluu kerätyn tiedon luokittelu, politiikkojen ja menettelytapojen tehokkuuden analysointi, havaittujen tietoturva-puutteiden järjestäminen tärkeys järjestykseen niitä koskevien riskien kriittisyyden mukaan sekä havaintojen vertaaminen käytettyyn viitekehykseen.

[DaS11]Analysointivaiheessa auditoija tutkii tietoturvassa havaitut puutteet tarkoin ja varmistaa, että huolenaihe on varmasti aiheellinen. Puutteen todellisuuden varmistamiseksi on suositeltavaa, että auditoija kertoo mahdollisista puutteista asiakkaalle mahdollisimman pian sen havaitsemisen jälkeen, jotta voidaan varmistaa, että auditoijan keräämä tieto varmasti pitää paikkaansa. Tällä tavoin yhteistyötä tekemällä asiakas myös paljon helpommin hyväksyy auditoinnin negatiiviset tulokset ja ovat valmiimpia korjaamaan puutteet tietoturvassaan.

[Jac10]Analysointivaiheessa auditoijan kokemus ja ammattitaito ovat isossa roolissa, koska niiden avulla auditoija pystyy myös määrittelemään, mitkä löydetyistä tietoturva-aukoista ovat kriittisempiä kuin toiset auditoinnin tarkoituksen kannalta. [DaS11]Puutteiden ja niihin sisältyvien riskien validoinnin lisäksi auditoijan täytyy pohtia, onko riski sen käsittelyn arvoinen. Riskejä, joilla ei ole merkitystä organisaation liiketoiminnan kannalta, on turha raportoida. [Jac10] Jos auditoinnin tarkoitus oli varmistaa, että organisaation tietoturva vastaa jotain standardia tai ohjeistusta, auditoijan tulee myös listata puutteet tietoturvassa kyseessä olevaan viitekehykseen verrattuna.

5.4 Korjausehdotusten laatiminen

[DaS11]Kun tietoturvapuutteet on kartoitettu, auditoija voi myös laatia asiakkaalle ehdotelman, miten organisaatio voi korjata tietoturvapuutteet ja täten parantaa liiketoimintansa tietoturvaa. Ehdotelman laatimiseen on monia eri tapoja, joista parhaat hyödyntävät auditoijan ja kohdeorganisaation tiivistä yhteistyötä.

[DaS11]Korjaavia toimenpiteitä laadittaessa auditoijat voivat yksinkertaisesti ehdottaa toimenpiteitä, jotka asiakkaat joko hyväksyvät tai hylkäävät. Tämä lähestymistapa toimii hyvin, jos auditoija on todella asiantunteva niin tietoturvan kuin organisaation liiketoiminta-alueenkin suhteen, ja siten tietää kokemuksensa perusteella parhaat vaihtoehdot. Asiakasorganisaatiolla on usein kuitenkin auditoijaa parempi tietämys organisaation liiketoiminta-alueesta, jolloin on suositeltavaa, että asiakas on mukana korjausten pohtimisessa. Tällä tavalla asiakas ei myöskään koe itseään ulkopuoliseksi näiden korjaavien toimenpiteiden päättämisessä ja toteutuksessa. Paras tapa korjaavien toimenpiteiden päättämiseksi on siis tiivis yhteistyö auditoijan ja kohdeorganisaation välillä, jotta päätöksentekoon saadaan mukaan auditoijilta tietoturvaan liittyvä ammattitaito ja kohdeorganisaatiolta heidän liiketoimintaansa liittyvä kokemus.

[DaS11]Vaikka korjaavien toimenpiteiden täytäntöönpano on tärkeää kohdeorganisaation tietoturvan kannalta, auditoija ei kuitenkaan voi pakottaa organisaatiota käsittelemään auditoinnin aikana havaittuja puutteita. Auditoijan ensisijainen tehtävä on ainoastaan organisaation tietoturvariskien tunnistaminen ja niistä

raportointi. Auditoijat eivät myöskään usein toteuta itse korjaavia toimenpiteitä, vaikka olisivatkin niistä päättämässä.

5.5 Auditoinnin tuloksista raportointi

[DaS11]Kun korjaavat toimenpiteet havaituille tietoturvapuutteille on määritelty, auditoijan täytyy vielä kirjoittaa auditointiraportti. Raportti täytyy kirjoittaa, jotta auditoija ja kohdeorganisaatio voivat palata auditoinnin tuloksiin myöhemmin, ja jotta kohdeorganisaatio voi tarvittaessa osoittaa eri tahoille, että auditointi on suoritettu raportissa mainituin tuloksin. [Jac10]Laaditun raportin tulee olla yksityiskohtainen ja selkeä, ja siinä tulee selvitä, miksi jokin tietty haavoittuvuus on kriittinen ja mitä sille kannattaa tehdä tietoturvan parantamiseksi. [DaS11] Raporteille on olemassa monia eri formaatteja, mutta ne kaikki kuitenkin kattavat auditoinnin skoopin, auditointiprosessin tiivistettynä sekä listan havaituista puutteista korjausehdotuksineen.

[DaS11]Ennen raportin luovutusta asiakkaalle, se suositellaan läpikäytäväksi palaverissa, jossa auditoija esittelee auditoinnin tulokset organisaation johdolle ja mahdollisesti myös muille tärkeille sidosryhmille. Palaverissa auditoijan on helppo vastata asiakasta askarruttaviin kysymyksiin ja antaa neuvoja organisaation tietoturvaa korjaaviin toimenpiteisiin liittyen. [Jac10]Myös kaikki muu auditointiprosessin aikana luotu dokumentaatio kannattaa antaa organisaatiolle, jotta he voivat arkistoida sen myöhempää käyttöä, kuten tulevia auditointeja varten.

5.6 Jälkitoimet

[Jac10]Auditoinnin jälkitoimet tarkoittaa havaittujen haavoittuvuuksien korjausta ja korjausten auditointia. [DaS11]Auditoinnin elinkaari ei ole täysin päättynyt ennen kuin nämä korjaavat toimenpiteet ja niiden auditointi on suoritettu tai havaittujen puutteiden olemassa olo hyväksytään organisaation johdon toimesta. Jos korjaavat toimenpiteet aiotaan suorittaa, auditoijan kannattaa yhdessä asiakkaan kanssa sopia päivämäärä, johon mennessä korjaavien toimenpiteiden tulee olla käytössä.

[Jac10]Auditoijat eivät usein itse suorita korjaavia toimenpiteitä, jotta heille ei pääse muodostumaan mielipiteitä ja heidän puolueeton asemansa varmasti säilyy.

[DaS11]Auditoijan kannattaa kuitenkin olla säännöllisesti yhteydessä asiakkaaseen, jotta hän voi tarvittaessa konsultoida asiakasta eri toimenpiteiden toteutustavoista, ennen kuin toimenpiteiden käyttöönotto on ehditty suorittaa loppuun.

[DaS11]Kun korjaavat toimenpiteet on pantu täytäntöön, täytyy niiden toimivuus testata. Kaiken auditointi uudelleen ei kuitenkaan ole kovin käytännöllistä. Tästä syystä auditoijan kannattaakin usein vain tarkistaa, että korjaavat toimenpiteet on todella suoritettu, tai pyytää asiakasta kertomaan auditoijalle toimenpiteen toiminnallisuus, ja tätä kautta arvioida sen toimivuutta auditoijan asiantuntemukseen perustuen.

6 AUDITOINNIN SKOOPIN MUODOSTUS

Kohdeorganisaatioita on lukemattomia erilaisia, ja täten myös eri organisaatioiden tietoturva-auditointitarpeet vaihtelevat paljon. Tästä johtuen jokainen auditointi on erilainen ja niiden skooppi yksilöllinen. Tietoturva-auditointeja voidaan jakaa kategorioihin lukemattomalla eri tavalla perustuen niiden skooppiin, eikä yksi jaottelu ole sen parempi kuin toinen.

Tämä luku pyrkii antamaan yleiskuvan tietoturva-auditoinnin mahdollisista skoopeista sekä esimerkin skoopin muodostuksesta. Luvussa 6.1 tietoturva-auditoinnit jaetaan karkeasti eri tyyppeihin ja tasoihin, ja luvussa 6.2 kerrotaan auditoitavien kohteiden päättämisestä auditointiuniversumin avulla.

6.1 Tietoturva-auditointien tyypit ja tasot

[Jac10]Tietoturva-auditoinnit voidaan jakaa tyyppeihin monilla eri tavoilla riippuen auditoinnin tarkoituksesta, rajauksesta ja tarkkuudesta. Tyypit eivät ole kuitenkaan ole toisensa poissulkevia, vaan useaa eri tyyppiä voidaan käyttää auditointiprosessin eri vaiheissa. Chris Jacksonin kirjoittamassa kirjassa ”Network Security Auditing” auditoinnit on jaoteltu tietoturvakatsauksiin, tietoturva-arviointeihin ja tietoturva-auditointeihin.

[Jac10]Tietoturvakatsauksen (*security review*) tavoitteena on huomata kaikkein silmiinpistävimmät ongelmat ja muodostaa niiden avulla lähtökohta auditoinnille. Se on suurpiirteinen tietoturvan tason kartoitus, joka perustuu pääasiallisesti auditoijan kokemukseen ja mielipiteeseen, mutta jossa kuitenkin käytetään apuna monia eri menetelmiä ja työkaluja. Yleisesti käytettyjä menetelmiä ovat penetraatiotestaus, haavoittuvuus-skannaus, riskien kartoitus, arkkitehtuurin katselmointi sekä tietoturvapolitiikan katselmointi ja sen noudatuksen arviointi.

[Jac10]Tietoturva-arvioinnin (*security assessment*) pääpaino on tietoturvassa havaittujen puutteiden analysointi ja niiden oleellisuuden ja kriittisyyden arviointi kohdeorganisaation kannalta. Arviointi perustuu edelleen paljon auditoijan ammattitaitoon, mutta antaa kuitenkin tarkemman kuvan tietoturvan tasosta kuin

tietoturvakatsaus, koska puutteet havainnoidaan ja analysoidaan yksityiskohtaisemmin. Arvioinnin kohteina voivat olla muun muassa havaitut haavoittuvuudet, riskit, arkkitehtuurit ja tietoturvapolitiikka.

[Jac10]Tietoturva-auditointi (*security audit*) käyttää viitekehyksenä auditoijan ammattitaidon lisäksi jotain tietoturvastandardia tai yleisesti hyväksyttyä ohjeistusta ja pitää sisällään niin tietoturvakatsauksen kuin tietoturva-arvioinnin. Sen tuloksena saadaan tietää, miten hyvin organisaation tietoturva vastaa standardin mukaista suositeltua tietoturvan tasoa. Auditoinnin aikana voidaan selvittää muun muassa, miten hyvin henkilöstö noudattaa tietoturvapolitiikkaa, onko tietoturvapolitiikka ja eri prosessit viitekehyksen mukaisia, ja onko organisaatiota koskeviin riskeihin osattu valmistautua kattavasti.

[Jac10]Chris Jacksonin kirjoittamassa kirjassa ”Network Security Auditing” tietoturva-auditointi jaetaan kolmeen eri tasoon: politiikka- (*policy level*), menettelytapa- (*procedure level*) ja kontrollitasoon (*control level*). Auditoinnin skooppi määrittelee, mille tasolle se kuuluu. Tasot eivät kuitenkaan ole toisensa poissulkevia, vaan auditointi voi ulottua useammalle tasolle riippuen sen skoopin laajuudesta.

[Jac10]Politiikkatasolla auditoidaan organisaation tietoturvapolitiikka ja selvitetään, vastaako se organisaation tietoturvaa koskevia vaatimuksia ja tavoitteita. Lisäksi tulee varmistaa, että politiikkaa varmasti noudatetaan. Politiikkaa voi myös verrata standardeihin, joissa on kuvattu parhaat toimintatavat. Tietoturvapolitiikan auditoinnin tarkoitus on siis havaita kaikki politiikkaan ja sen käyttöön liittyvät aukot. Enemmän tietoa tietoturvapolitiikoista on kerrottu luvussa 7.

[Jac10]Menettelytapatasolla varmistetaan, että tietoturvan toteuttavat prosessit on pantu täytäntöön tietoturvapolitiikan mukaisesti ja laadukkaasti. Viitekehyksenä voidaan jälleen käyttää yleisesti parhaiksi koettuja toimintatapoja. Enemmän tietoa menettelytavoista on kerrottu luvussa 8.

[Jac10]Kontrollitasolla auditoidaan tietoturvaprosesseissa käytetyt kontrollit. Auditoijan tehtävä on varmistaa, että kontrolli varmasti tarjoaa tarvittavan suojan riskejä vastaan. Kontrollien arviointi tapahtuu testaamalla niiden toiminnallisuutta, tutkimalla niiden

konfiguraatiota ja katselmoimalla lokeja. Enemmän tietoa kontrolleista on kerrottu luvussa 9.

6.2 Auditoitavien kohteiden päättäminen auditointiuniversumin avulla

[DaS11]Tietoturva-auditointi voi arvioida organisaation koko tietoturvaa tai keskittyä vain joihinkin tiettyihin sen osa-alueisiin. Auditoinnin tulee keskittyä ensisijaisesti sellaisille alueille, jotka ovat riskialttiimpia, ja joiden tietoturvan parantamiseen auditoinnilla on suurin merkitys. Yksi tapa näiden alueiden selvittämiseksi on niin sanotun auditointiuniversumin (*audit universe*) kartoitus. Kartoituksen tarkoituksena on saada parempi käsitys mahdollisista auditointikohteista. Auditointiuniversumin kartoituksen jälkeen sen sisältämät kohteet asetetaan tärkeys järjestykseen. Lopputuloksena auditoijalla on lista kohteista, joiden auditointi voi parantaa organisaation tietoturvaa eniten.

[DaS11]Auditointiuniversumin kartoitukseen ei ole vain yhtä oikeaa tapaa, mutta yksi tehokkaimmista tavoista on ensimmäisenä kartoittaa organisaation keskitetyt IT-toiminnot, joita moni muu toiminto käyttää. Keskitettyjen toimintojen kartoituksessa on se etu, että ne voidaan auditoida erikseen ennen muiden prosessien auditointia, jolloin niitä ei enää myöhemmin tarvitse auditoida osana kaikkia muita prosesseja, mikä nopeuttaa auditoinnin suoritusta.

[DaS11]Keskitettyjä toimintoja ovat hallinnolliset prosessit kuten käyttäjätilien-, muutosten-, ongelmien- ja päivitysten hallinta sekä kaikki muut toiminnot, jotka vaikuttavat koko organisaatioon. Keskitetyt IT-toiminnot vaihtelevat organisaatiokohtaisesti, mistä johtuen auditoijan tulee tutustua organisaatioon näiden toimintojen tunnistamiseksi. Tutustuminen voi tapahtua esimerkiksi haastattelemalla organisaation IT-asiantuntijoita.

[DaS11]Kun keskitetyt toiminnot on kartoitettu, voidaan kartoittaa muut yksittäiset auditoitavat toiminnot. Myös näitä kohteita kartoittaessa organisaation tunteminen on tärkeää, jotta auditoinnin skooppiin osataan sisällyttää kaikkein tärkeimmät asiat.

Lisäksi auditoija voi käyttää auditoitavia prosesseja kartoittaessaan hyväkseen esimerkiksi COBIT-kehystä, joka määrittelee eri IT-prosesseissa tarvittavat kontrollit.

[DaS11]Auditointiuniversumin kartoituksen jälkeen sen sisältämät kohteet tulee laittaa tärkeysjärjestykseen sen mukaan, miten suuri merkitys niiden auditoinnilla uskotaan olevan. Kohteiden tärkeysjärjestykseen laittamiseen ei ole yhtä tiettyä tapaa, mutta on olemassa muutamia asioita, joiden huomioiminen on olennainen osa kohteiden priorisointia. Jos auditoija esimerkiksi tietää, että tietoturvaan liittyviä ongelmia esiintyy jonkin tietyn asian yhteydessä, kohteen tulee mitä todennäköisimmin olla yksi auditoitavista asioista. Jos taas auditoijan kokemuksen mukaan jollain tietyllä alueella on useimmiten puutteita tietoturvassa, voivat nuo asiat olla myös tärkeitä auditoitavia asioita. Myös tietoturva- ja muista IT-asioista vastaavaa organisaation henkilöstöä kannattaa kuunnella, ja jos he ovat huolissaan jonkin alueen tietoturvasta, heidän suosituksensa tulee ottaa huomioon. Auditoijan ei myöskään kannata auditoida sellaisia kohteita, joiden tietoturvaongelmat ovat jo tiedossa. Auditoijan tulee ottaa lisäksi organisaation yksilöllinen toimintatapa huomioon ja miettiä, onko jokin priorisointikriteeri organisaation kannalta olennaisempi kuin muut.

7 TIETOTURVAPOLITIIKAT JA NIIDEN AUDITOINTI

[Jac10]Tietoturvapolitiikat ovat tietoturvan toteutuksen perusta. Ne ovat käytännössä tarkoin laadittuja dokumentteja, joista käy ilmi, miten tietoturvallisuutta tulee harjoittaa ne laatineessa organisaatiossa. Tietoturvapolitiikkoja noudatettaessa voidaan vähentää riskiä, että arkaluontoinen tieto joutuisi vääriin käsiin, ja jos tietovuoto tapahtuu, tiedetään jo etukäteen, miten tilanteessa tulee menetellä.

Vaikka tietoturvapolitiikan laatiminen ei suoraan kasvata organisaation liikevaihtoa, voi sillä silti olla siihen positiivisia vaikutuksia. Kun tietoturvapolitiikka on kunnollinen, se on pantu täytäntöön ja sitä noudatetaan, organisaatio voi sen avulla perustellusti vakuuttaa asiakkailleen, että asiakkaiden tietoja suojellaan organisaatiossa asianmukaisesti ja tarjotut palvelut ovat saatavilla lähes poikkeuksetta, mikä puolestaan voi kasvattaa liikevaihtoa.

[Jac10]Vaikka kunnollisten tietoturvapolitiikkojen määrittely sekä niiden noudatus on tärkeää, yllättävän moni organisaatio ei ole laatinut niitä, tai eivät tiedä, millaiset heidän organisaationsa käyttämät politiikat ovat. Olennainen osa tietoturva-auditointia on kohde organisaation käyttämien tietoturvapolitiikkojen tarkastaminen, ja sen varmistaminen, että ne ovat varmasti kunnollisia, ne on pantu täytäntöön, ja että niitä varmasti myös seurataan.

Tässä luvussa keskitytään tietoturvapolitiikkoihin ja niiden auditointiin. Luvussa 7.1 kerrotaan, mitä tietoturvapolitiikat tarkalleen ovat, mikä on niiden tarkoitus ja, millainen on hyvä tietoturvapolitiikka. Luvussa 7.2 puolestaan keskitytään tietoturvapolitiikkojen auditointiin, ja mitä eri asioita auditoijan tulee ottaa huomioon politiikkoja auditoidessaan.

7.1 Tietoturvapolitiikat

[Jac10]Tietoturvapolitiikka on tarkasti dokumentoitu suunnitelma, jonka mukaan tietoturvallisuus toteutetaan käytännössä, jotta kaikki tietoturvaa koskevat tavoitteet varmasti toteutuvat. Dokumentaatiosta käy siis ilmi, mitä organisaatio tulee tarkalleen tehdä suojellakseen tietojaan ja muita etuuksiaan. Kaikki tietoturvaan liittyvät päätökset

tulee perustaa juuri tähän dokumentaatioon, koska siitä käy ilmi, mitkä asiat ovat sallittuja, vaadittuja tai kiellettyjä organisaation tietoturvan kannalta. Tietoturvapolitiikka määrittelee, miten organisaation tietoturva on toteutettu, miksi jokin turvallisuustoimenpide on olemassa, mitä tietoa suojellaan ja ketä politiikka koskee. Tietoturvapolitiikka on välttämätön asia toimivan tietoturvan toteuttamisessa, ja sen kuvaavan dokumentaation olemassa olo vaaditaan monien lakien ja määräysten toimesta.

[Jac10]Tietoturvapolitiikan tarkoitus on siis kertoa, mitkä ovat organisaation tietoturvavaatimukset, ja määritellä organisaation tavoitteet tietojen ja muiden etuuksien suojeluun liittyen. Politiikan tulee aina perustua kattavaan riskienkartoitukseen, jossa on otettu huomioon organisaation tavoitteet ja juuri kyseistä organisaatiota koskevat uhat. Chris Jacksonin kirjoittaman kirjan ”Network Security Auditing” mukaan tietoturvapolitiikan tulee käsittää vähintään seuraavat asiat: sen tarkoitus, laajuus, yksityiskohtaiset vaatimukset, täytäntöönpano, termien selitykset ja dokumentin versiohistoria.

[Jac10]Tarkoitus-osiossa kerrotaan, miksi politiikka on olemassa, ja siinä voidaan myös esimerkiksi kuvailla, minkälaisia ongelmia pystytään välttämään politiikkaa noudattamalla. Laajuus määrittelee ketä organisaation jäseniä politiikka tarkalleen koskee. Vaatimukset ovat dokumentin suurin osio, ja siinä määritellään yksityiskohtaisesti mitä asioita saa, pitää ja ei pidä tehdä. Täytäntöönpano kattaa muun muassa sen, minkälaisia sanktioita seuraa, jos joku politiikan piiriin kuuluva henkilö tietoisesti jättää politiikan huomioimatta.

[Jac10]Politiikan tulee olla tarkka, kattava ja täytäntöönpanokelpoinen, ja antaa selkeä ohjeistus tietoturvalliseen toimintaan. Politiikan tulee myös kertoa, miksi jokin asia tulee tehdä tietyllä tavalla, jolloin lukija ymmärtää riskialttiin toiminnan seuraukset ja todennäköisemmin seuraa politiikkaa tulevaisuudessa. Tietoturvapolitiikan tulee olla myös tiukka, koska liian löyhät säännökset koetaan usein vain suosituksina. Tietoturvapolitiikka ei ole suositus, jonka mukaan kannattaa toimia, vaan säännöstö, jonka mukaan tulee toimia. Politiikan ei tulisi kuitenkaan olla niin tiukka, että se merkittävästi vaikeuttaa organisaation jokapäiväistä toimintaa.

[Jac10]Tietoturvapolitiikat tulisi säilyttää sellaisessa paikassa, johon organisaation henkilöstön on helppo päästä tarvittaessa tarkistamaan jokin organisaation tietoturvaan liittyvä käytäntö, ja politiikan sijainnista tulisi myös tiedottaa organisaation henkilöstöä. [Jac10]Politiikan käyttö on tärkeää, ja joissain tapauksissa sen pakottaminen voi olla tarpeellista, koska jos yhden henkilön annetaan kiertää se, myös muu henkilöstö voi kokea olevansa oikeutettu samaan, mikä aiheuttaa vakavia ongelmia tietoturvan jokapäiväisen harjoittamisen kannalta. Osa pakottamisesta voidaan tehdä teknisellä tasolla, ja loppujen säännösten noudattamatta jättämisestä voidaan määrätä sanktioita.

[Jac10]On tärkeää pitää tietoturvapolitiikka erillään sen käytännössä toteuttavista toimenpiteistä kertovasta politiikasta ja muista tietoturvastandardeista. Tietoturvan toteutustavat ja tietoturvastandardit voivat muuttua todella usein teknologian kehittyessä, kun taas organisaation tietoturvapolitiikka voi olla hyvinkin staattinen. Ja vaikka tietoturvapolitiikan tuleekin kuvailla asiat tarkasti, sen tulisi kuitenkin jättää sen verran liikkumavaraa, että politiikka pysyy luontevasti yhtenevänä sen toteutuksen kanssa, eikä politiikkaa tarvitse olla muuttamassa pienimpien konfiguraatioasetusten muuttuessa.

7.2 Tietoturvapolitiikkojen auditointi

Tietoturvapolitiikan auditointi on olennainen osa organisaation tietoturvan auditointia. Tietoturvapolitiikan auditointi tapahtuu sen kuvailevaa dokumentaatiota katselmoimalla. Katselmoimalla tietoturvapolitiikkaa auditoija saa hyvän käsityksen organisaation tietoturvasta ja siitä, millainen sen tulisi olla, mikä puolestaan auttaa auditoinnin suunnittelussa ja auditoitavien kohteiden rajauksessa.

[Jac10]Pahimmassa tapauksessa auditoija saattaa heti auditoinnin alussa havaita, että kohdeorganisaatiolla ei ole olemassa sellaista tietoturvapolitiikkaa, joka kattaisi heidän riskialttiit järjestelmänsä. Tässä tapauksessa auditoija ohjeistaa organisaatiota ensimmäisenä luomaan kattavan tietoturvapolitiikan alan standardeja hyväksikäyttäen. Vasta tietoturvapolitiikan auditoinnin jälkeen tietoturva-auditointia kannattaa lähteä viemään eteenpäin.

[Jac10]Jos organisaatiolla on olemassa dokumentoitu tietoturvapolitiikka, auditoijan tehtävänä on varmistaa, että se vastaa organisaation liiketoiminnan asettamiin tietoturvavaatimuksiin, sisältää kaikki tarvittavat asiat organisaation tietoturvan kattavaan ylläpitoon, ja että henkilöstö on tietoinen politiikasta ja noudattaa sitä tietoturvan toteuttaviin toimenpiteisiin liittyen. Haastattelemalla henkilöstöä voidaan selvittää, seurataanko politiikkaa jokapäiväisessä työssä. Jos käy ilmi, että politiikka jätetään pääosin huomiotta, tämä voi kertoa organisaation johdon välinpitämättömyydestä tietoturvapolitiikan täytäntöönpanossa. Säännöllisellä henkilöstölle järjestettävällä tietoturvakoulutuksella voidaan huomattavasti parantaa organisaation yleistä tietoturvatasoa.

[Jac10]Tietoturvapolitiikkaa arvioitaessa auditoijan tulee tarkastella sitä organisaation henkilöstön näkökulmasta, joka lukee politiikan käsittävän dokumentaation ja tulkitsee sen merkityksen. Avainkriteerejä politiikan arviointiin ovat seuraavat kysymykset: Onko politiikka toteutettavissa käytettävät teknologiat ja organisaation tavoitteet huomioon ottaen? Onko politiikka täytäntöönpanokelpoinen jokapäiväisessä työskentelyssä? Onko politiikka helppolukuinen ja yksiselitteinen? Perustuuko politiikka organisaation kartoittamiin tietoturvariskeihin? Ovatko politiikan vaatimat toimenpiteet kustannustehokkaita? Onko politiikka tasapainotettu hyvin tietoturvan ja liiketoimintaprosessien sulavuuden välillä? Saavuttaako politiikka tavoitteensa? Onko politiikka ajan tasalla? Kannattaako organisaation johto nykyistä tietoturvapolitiikkaa? Tiedotetaanko politiikasta henkilöstölle aktiivisesti? Jos jokaiseen näihin kysymykseen voidaan vastata myöntävästi, tietoturvapolitiikka katsotaan kunnolliseksi. Ennen kuin auditoija kuitenkaan pystyy antamaan vastausta näihin kysymyksiin, hänen täytyy tutkia niihin liittyviä asioita tarkasti kaikkien olennaisten puutteiden varalta.

[Jac10]Puutteita kartoittaessaan auditoija voi verrata organisaation tietoturvapolitiikkaa yleisesti käytettyihin politiikkatyyppeihin. Organisaation ei välttämättä tarvitse käyttää kaikkia mahdollisia politiikkatyyppejä, mutta auditoijan täytyy varmistaa, että kaikki tarvitut politiikkatyypit ovat osa organisaation tietoturvapolitiikkaa. Eri politiikkatyyppejä edustavat muun muassa hyväksyttyä käyttöä, vähimmäispääsyä, verkkoon pääsyä, etäkäyttöä, Internetin käyttöä, käyttäjätilien hallintaa, luottamuksellista tietoa, muutoksen hallintaa, palvelinten tietoturvaa, mobiililaitteita, vieraiden pääsyä, fyysistä turvallisuutta, salasanojen käyttöä, haittaohjelmilta

suojautumista, poikkeustilanteiden käsittelyä, auditointia, sovellusten lisensiointia sekä sähköistä valvontaa ja yksityisyyttä koskevat politiikat.

[Jac10]Vaikka tietoturvapolitiikan tuleekin olla tiukka, se ei saisi vaikeuttaa liikaa organisaation jokapäiväisiä liiketoimintaprosesseja. Auditoijan tulee ottaa tämä asia huomioon auditoidessaan organisaation tietoturvapolitiikkaa, ja yrittää löytää tasapaino tietoturvallisuuden ja prosessien tehokkuuden välillä. Liian paljon päivittäistä työskentelyä vaikeuttava tietoturvapolitiikka voi aiheuttaa sen huomiotta jättämistä, kun henkilöstö haluaa kiertää sen säädökset kokiessaan ne liian paljon työskentelyään hankaloittavina.

[Jac10]Edellä mainittujen asioiden lisäksi myös organisaation toiminta-alaa koskevat lait ja säännökset tulee ottaa huomioon politiikkaa arvioitaessa, ja auditoijan onkin suositeltavaa tutustua hieman näihin ennen auditointia. Haastavien lakia koskevien kysymysten esiintyessä kohdeorganisaation tulee kuitenkin kääntyä lakitoimiston puoleen.

Tietoturvapolitiikan tutkimisen jälkeen sitä ei tarvitse luokitella vain joko hyväksi tai huonoksi. [Jac10]NIST on luonut Federal Information Security Assessment Framework -kehyksen, joka sisältää kypsyysmallin tietoturvapolitiikkojen nykytason arviointia varten. Mallissa on kuusi tasoa, jotka on numeroitu nollasta viiteen, ja joista yhdelle organisaation tietoturvapolitiikka voidaan asettaa riippuen sen toteutuksesta ja käyttöönottovaiheesta. Kypsyysmallista voi helposti nähdä, mitä organisaation tulee tehdä seuraavaksi parantaakseen tietoturvapolitiikkaansa.

8 TIETOTURVAN HALLINTAPROSESSIN AUDITOINTI

[Jac10]Tietoturvan hallinta jakautuu kolmeen eri osa-alueeseen: henkilöstöön, prosesseihin ja teknologiaan, joita kaikkia voidaan auditoida. Kaikki toteutuneet tietoturvauhat voidaan useimmiten jäljittää jonkin osa-alueen toiminnan tehottomuuteen, mitä hyökkääjä on päässyt käyttämään hyväkseen. Luvussa 8.1 kerrotaan henkilöstön auditoinnista, luvussa 8.2 kerrotaan prosessien auditoinnista, ja luvussa 8.3 kerrotaan tietoturvan toteuttavan teknologian auditoinnista.

8.1 Henkilöstön auditointi

Vaikka iso osa tietoturvaa toteutetaankin teknisesti, on henkilöstöllä myös iso rooli tietoturvan ylläpidossa. [Jac10]Henkilöstöön kuuluvat kaikki organisaatiossa työskentelevät ihmiset. Henkilöstö on todella tärkeä osa tietoturvan harjoittamista, koska iso osa tietoturvan toteutumisesta organisaation jokapäiväisessä toiminnassa on heidän vastuullaan. Samalla kun tietotekniikan rooli organisaatioiden liiketoiminnassa laajenee, myös tarvittava tietous niiden vaatimista tietoturvatoimenpiteistä kasvaa. Ei riitä, että palkataan yksi tietoturvavastaava hallinnoimaan koko organisaation tietoturvaa, vaan kaikilla organisaation tasoilla tulisi olla tiedossa heidän omat vastuunsa tietoturvan toteuttamisessa. Jos kaikki organisaation jäsenet eivät ole tietoisia käytettävästä tietoturvapolitiikasta, organisaatiota uhkaa väistämättä useampia tietoturvariskejä kuin pitäisi. Riskejä voidaan pienentää järjestämällä tietoturvakoulutusta tai rankaisemalla politiikan noudattamatta jättämisestä. Henkilöstön politiikan käyttöä voidaan joissain tapauksissa kuitenkin myös pakottaa teknisellä tasolla: käyttäjältä saatetaan esimerkiksi vaatia, että hänellä on asennettuna käytetyn anti-virus ohjelman uusin versio, ennen kuin hänen annetaan yhdistyä verkkoon.

[Jac10]Monet eri organisaatiot ovat kehittäneet erilaisia organisaatiorakenteita vastaamaan tietoturvan asettamiin haasteisiin mahdollisimman kattavasti. Vaikka näissä rakenteissa tiimien nimet ja rakenteet eroavat, niiden kaikkien tavoitteena on kuitenkin saavuttaa selkeä raportointirakenne ja jakaa tietoturvavastuuta jokaiselle organisaation tasolle. Chris Jacksonin kirjassa ”Network Security Auditing” organisaatio on jaettu seuraaviin tasoihin, joilla kaikilla on oma tehtävänsä tietoturvan toteutuksessa: hallitus,

turvallisuuden johtoryhmä, johto, tietoturvapäälliköt, tietoturvaohjaajat, tietoturva-analyytikot, tietoturva-arkkitehdit, tietoturvainsinöörit, järjestelmänvalvojat, tietokantajärjestelmävalvojat, loppukäyttäjät.

Hallituksen (*Board of Directors*) tehtäviin kuuluu organisaation sidosryhmien etujen ajaminen ja heidän kannaltaan olennaisen datan suojeluun käytettävien resurssien hyväksyminen. Jotta hallitus voisi suorittaa tehtävänsä kunnolla, heidän tulee tietää organisaatiota ja sen dataa uhkaavat riskit.

Turvallisuuden johtoryhmä (*Security Steering Commettee*) katselmoi auditointituloksia, riskienhallintaa ja järjestelmien suorituskykyä sekä hyväksyvät suurimmat muutokset auditointipolitiikkoihin ja turvallisuusstrategioihin. Johto (*Executive Management*) asettaa organisaatiolle sen tavoitteet, ja tästä syystä sen tulee myös tietää, minkälaiset riskit uhkaavat organisaation luottamuksellisuutta, yhtenäisyyttä ja arkaluontoisen datan saatavuutta.

Tietoturvapäälliköiden (*Chief Information Security Officers*) tehtäviin kuuluu tietoturvastrategian sovittaminen organisaation vaatimuksiin. Tietoturvaohjaajan (*Security Director*) tehtäviin kuuluu tietoturvatoimenpiteiden toteutuksen koordinointi.

Tietoturva-analyytikko (*Security Analyst*) kehittää tietoturvapolitiikat, analysoi riskit ja huomioi uudet organisaatiota koskevat uhat. Lisäksi hänen tehtäviinsä kuuluu liiketoiminnan jatkuvuuden ja ongelmatilanteista palautumisen suunnittelu ennalta arvaamattomien tapahtumien varalta.

Tietoturva-arkkitehti (*Security Architect*) määrittelee ne toiminnot, ohjeistukset ja standardit, joita organisaatio käyttää. Hän avustaa organisaation datan suojeluun käytettävien kontrollien valinnassa ja varmistaa, että ne vastaavat riskiin tarpeeksi hyvin ja organisaation tietoturvapolitiikan mukaisesti. Tietoturvainsinööri (*Security Engineer*) toteuttaa tietoturva-arkkitehdin valitsemat kontrollit ja on vastuussa esimerkiksi palomuurin ja muiden työkalujen ylläpidosta, mikä kattaa päivitykset, testauksen ja muun yleisen tietoturvajärjestelmien ylläpidon.

Järjestelmänvalvoja (*System Administrator*) on vastuussa palvelinten, tulostimien ja päätteiden toiminnan havainnoinnista ja ylläpidosta. Lisäksi järjestelmänvalvojat

lisäävät ja poistavat käyttäjätunnuksia tarpeen mukaan sekä hallinnoivat pääsyä organisaation resursseihin. He voivat myös olla vastuussa organisaatiolaajuisten anti-virus-ohjelmistojen ylläpidosta.

Tietokantajärjestelmävalvojan (*Database Administrator*) vastuita on organisaation tietokantojen suunnittelu ja ylläpito sekä tietoihin käsiksi pääsyn suojaaminen tietokannan yhtenäisyyden säilyttämiseksi. Löyhän tietoturvan harjoittamisella tässä roolissa voi olla vakavat seuraukset.

Loppukäyttäjien (*End User*) roolia tietoturvan harjoittamisessa usein vähätellään. Loppukäyttäjien tulee tietää heidän toimiensa seuraukset tietoturvan kannalta ja heidän tulee pystyä omalta osaltaan suojelemaan organisaation luottamuksellista tietoa. Heidän tulee noudattaa organisaation tietoturvapolitiikkaa ja turvatoimia sekä harjoittaa yleisiä tietoturvatoimenpiteitä käyttäessään tietokoneita, kuten olla avaamatta epäilyttäviä sähköposteja ja niiden liitetiedostoja tai linkkejä, varmistaa, että heidän käyttämänsä virusten- ja vakoiluohjelmien torjuntaohjelmat ovat käytössä, ja päivittää tietokoneella käytössä olevat ohjelmistot ja käyttöjärjestelmät. Kattava loppukäyttäjille suunnattu turvallisuuskampanja voi helpottaa turvallisten tietokoneen käyttötapojen omaksumista.

[Jac10]Organisaation datan turvaamisessa henkilöstöllä on siis monia erilaisia rooleja. Auditoijan tulee tarkkailla mahdollisia osa-alueita, joita voitaisiin vielä parantaa organisaation tietoturvakulttuurin ja eri roolien vastuiden omaksumisen helpottamiseksi. Esimerkiksi henkilöstön hämmentyneisyys ja tietoturvaa koskevan ohjauksen puute ovat usein merkkejä siitä, että johto ei ole täysin sitoutunut organisaation tietoturvan kattavaan toteutukseen. Muita asioita, jotka kielivät heikkotasoisesta tietoturvan harjoittamisesta ovat liiketoiminnan kannalta keskeisten voimavarojen tunnistamattomuus, huono tietoturvaprosessien ja -toimintojen noudattamien, havaittujen tietoturvaongelmien korjaamatta jättäminen, välinpitämättömyys tietoturvaa kohtaan, avainroolien välisten vastuiden jakamattomuus, vaihteleva tietoturvapolitiikan käyttö, huono kommunikaatio eri roolien välillä, epätarkka roolien vastuualueiden kuvaus, ja huono dokumentaatio.

8.2 Tietoturvaprosessien auditointi

[Jac10]Prosessit ovat standardeja menettelytapoja, joiden tarkoitus on turvata organisaation etuudet. Prosesseja tulee päivittää säännöllisesti, niiden täytyy olla johdonmukaisia ja noudattaa niitä koskevia parhaita toimintatapoja. Prosessit ovat yksi tärkeimmistä auditoitavista osa-alueista, koska suurin osa tietoturvahyökkäyksistä, jotka päätyvät suuriin organisaation tappioihin, ovat seuranneet siitä, että jokin prosessin osa ei ole edennyt toivotulla tavalla.

[Jac10]Prosesseja auditoitaessa tulee tarkistaa, että kaikista käytetyistä prosesseista löytyy yleisesti noudatettava menettelytapadokumentaatio. Näiden dokumentoitujen käytäntöjen noudatusta voidaan arvioida henkilöitä haastattelemalla ja heidän työskentelyään tarkkailemalla.

[Jac10]Menettelytavat käsittävä dokumentaatio kuvailee tarkasti, kuinka laadittu tietoturvapolitiikka pannaan täytäntöön. Kun tietoturvapolitiikka keskittyy yleisten tietoturvaa koskevien tarpeiden ja tavoitteiden listaamiseen, menettelytapadokumentaatio kattaa niiden saavuttamiseen tarvittavat teknologiat ja toiminnot. Dokumentti voi sisältää ohjeet esimerkiksi eri järjestelmien kytkemiseksi verkkoon, palomuuriasetusten määrittelyyn tai tärkeän tiedon varmuuskopiointiin. Dokumenttia laadittaessa organisaatio tulee mahdollisesti päivittäneeksi käyttämiään teknologioita ja hyödyntäneeksi parhaaksi koettuja käytäntöjä. Valmiin dokumentin ansiosta organisaatio voi helposti toistaa eri menettelytapoja sekä varmistaa, että niiden mukaisesti toimitaan.

[Jac10]Menettelytavat käsittävän dokumentaation tulee pitää sisällään seuraavat asiat: tarkoitus, laajuus, varoitukset, menettelytavat askeleineen ja dokumentin versiohistoria. Tarkoitus osiolla on aivan sama merkitys kuin tietoturvapolitiikkojenkin kohdalla. Laajuus osiossa käsitellään, ketkä ovat vastuussa eri toimenpiteiden suorittamisesta, missä tilanteissa, ja mitä teknologiaa käyttäen. Varoitukset osiossa käydään läpi turvallisuuteen liittyvät varoitukset, jotka täytyy ottaa huomioon yhtenäisyyden säilyttämiseksi. Menettelytavat ovat dokumentin suurin osuus ja se käsittää tarkasti kuvatut askeleet eri menettelytapoihin liittyvien teknologioiden käyttöönottoon ja konfigurointiin.

[Jac10]Menettelytapadokumenttia lukemalla auditoija voi saada jo etukäteen hyvän käsityksen siitä, miten tarkasti organisaatio noudattaa tietoturvatoimia, ja dokumentti toimii myös hyvänä tarkastuslistana itse auditointia varten. Lisäksi dokumentissa kuvattuja menettelytapoja voidaan arvioida vertaamalla niitä yleisesti hyväksyttyihin ohjeistuksiin ja standardeihin. Tällaisia ovat organisaation omat tietoturvapolitiikat, HIPAA:n, SOX:n, GLBA:n ja PCI:n asettamat ohjeistukset, NIST 800, COBIT, COSO ja ISO 27000 -standardit. Standardeista ja ohjeistuksista on kerrottu enemmän luvussa 10.3.

8.3 Teknologian auditointi

[Jac10]Teknologia osa-alueena edustaa kaikkia niitä laitteita ja sovelluksia, jotka automatisoivat organisaation liiketoimintaa ja toimivat tietoturvakontrolleina. Teknologian ansioista organisaation henkilöstö pystyy suorittamaan usein toistettavat työtehtävänsä nopeammin ja virheettömämmin. Teknologian väärä konfiguraatio tai muuten huono toteutus voivat kuitenkin asettaa organisaation alttiiksi monille tietoturvauhille. Tästä johtuen on tärkeää, että organisaatio käyttää yleisesti parhaiksi koettuja ja tietoturvan kannalta toimivia konfiguraatioratkaisuja.

Teknologiaa auditoitaessa kohteena ovat järjestelmien konfiguraatiot ja haavoittuvuudet. Käytännössä tämä tarkoittaa sitä, että auditoija toteuttaa kontrolloituja väärinkäytösyrityksiä, joiden tarkoituksena on päästä käsiksi organisaation etuuksiin. Testaustapoina voivat toimia esimerkiksi haavoittuvuustestaus ja penetraatiotestaus. Näistä testaustavoista kerrotaan enemmän auditointityökalujen yhteydessä. Tietoturvakontrolleista kerrotaan tarkemmin seuraavassa luvussa.

9 TIETOTURVAKONTROLLIT

[Jac10]Tietoturvakontrollit ovat tietoturvan toteutuksessa käytettyjä komponentteja, jotka ovat käytössä suojellakseen organisaation luottamuksellisuutta, yhtenäisyyttä sekä tiedon ja muiden tärkeiden asioiden saatavuutta. [DaS11]Voidaan siis sanoa, että ne ovat mekanismeja, joiden avulla pyritään varmistamaan organisaation sisäisten prosessien toimivuus. [Jac10]Iso osa auditoinnista kohdistuu juuri näihin kontrolleihin, joiden tehtävä on pienentää organisaatiota uhkaavia tietoturvariskejä. [DaS11][Jac10]Auditoijan tehtävänä on varmistaa, että organisaatiota koskevien riskien minimoimiseksi vaaditut kontrollit ovat käytössä, ja että ne vastaavat tietoturvapolitiikassa niille asetettuja tavoitteita.

Luvussa 9.1 kerrotaan tietoturvakontrollien eri toteutustavoista, ja kuinka ne jakautuvat hallinnollisiin, teknisiin ja fyysisiin kontrolleihin. Luvussa 9.2 puolestaan kerrotaan eri kontrollien toiminnallisuuksista, ja mitä tarkoittavat ehkäisevät, havainnoivat, reagoivat ja elvyttävät kontrollit. Luvussa 9.3 puolestaan kerrotaan tietoturvakontrollien auditoinnista yleisellä tasolla.

9.1 Tietoturvakontrollien toteutustavat

[Jac10]Kontrollit käsitetään useimmiten eri teknologioita käyttävinä komponentteina. Palomuuri on yksi yleisimmistä asioista, joka voi tulla mieleen mietittäessä tietoturvakontrolleja, mutta olemassa on myös toisen tyyppisiä kontrolleja, jotka ovat yhtä tärkeä osa tehokkaan tietoturvan toteutusta. [Jac10][DaS10]Kontrollit voidaan yleisesti jakaa kolmeen eri kategoriaan: hallinnollisiin, teknisiin ja fyysisiin kontrolleihin. Kaikkien näiden osa-alueiden ja niiden myöhemmin kuvailtavien alikategorioiden käyttö tietoturvan toteutuksessa on tärkeää sen onnistumisen kannalta.

[Jac10]Hallinnollisia kontrolleja ovat esimerkiksi organisaation tietoturva-aiheiset politiikat, tietoturvakoulutukset ja tietoturva-auditoinnit. Yleisesti ottaen tämän tyyppiset kontrollit koskevat henkilöstöä ja tietoturvan kannalta epäsopivan käyttäytymisen ehkäisyä.

[Jac10]Teknisten kontrollien tarkoitus on estää tietoturvauhkia teknologisella tasolla. Teknisiin kontrolleihin kuuluvat palomuurit, tunkeutumisenestojärjestelmät (*Intrusion Prevention Systems*), ja muut tekniset mekanismit, joita tarvitaan tietoturvapolitiikan noudattamiseen.

[Jac10]Fyysiset kontrollit voivat olla esimerkiksi lukittuja ovia, avainkorteilla avautuvia lukkoja tai videovalvontaa. Kontrollin tarkoitus on estää fyysisesti tapahtuva luvaton pääsy arkaluontoista tietoa sisältävien laitteiden luokse.

9.2 Tietoturvakontrollien toiminnallisuustyypit

[Jac10]Jokainen näistä kolmesta kategoriasta voidaan jakaa vielä alikategorioihin perustuen kontrollin toiminnan luonteeseen. [Jac10][DaS11]Jaottelu voidaan suorittaa monella eri tavalla, mutta usein kontrollit jaotellaan alikategorioihin seuraavasti: ehkäisevät, havaitsevat, reagoivat ja elvyttävät kontrollit.

[Jac10]Ehkäisevien kontrollien tarkoitus on suojella organisaation tietojen ja muiden etuuksien luottamuksellisuutta, yhtenäisyyttä ja saatavuutta. Niitä voivat olla esimerkiksi palomuuriasetukset. [DaS11]Ehkäisevät kontrollit pyrkivät estämään tietoturvahyökkäysten tapahtumisen. Esimerkiksi käyttäjätunnuksen ja salasanan vaatiminen järjestelmään sisään kirjautuessa ehkäisee ulkopuolisten henkilöiden pääsyä järjestelmään. Ehkäisevien kontrollien käyttöä suositaan eniten, koska niiden ansioista voidaan kokonaan välttää monen tietoturvahyökkäyksen tapahtuminen. Valitettavasti nämä kontrollit eivät kuitenkaan ole aina kaikkein kustannustehokkaimpia, mistä johtuen niiden käyttö ei kaikissa tapauksissa ole viisasta, ja jonkin muun tyyppisen kontrollin käyttö on kyseissä tilanteessa sittenkin parempi vaihtoehto.

[Jac10]Havaitsevien kontrollien tarkoitus on tunnistaa, kun organisaation tietoturva on uhattuna, ja varoittaa siitä. Havaitsevia kontrolleja ovat esimerkiksi videovalvonta tai tunkeutumisenestojärjestelmät. [DaS11]Havaitsevat kontrollit tallentavat hyökkäystä koskevat tiedot, jotta niitä voidaan katselmoida myöhemmin.

[Jac10][DaS11]Reagoivat kontrollit, joita voidaan myös nimittää korjaaviksi kontrolleiksi, nimensä mukaan reagoivat havaitsevien kontrollien tunnistamiin tietoturvauhkiin ja lieventävät mahdollisen tietoturvamurron aiheuttamia haittoja.

Esimerkki korjaavasta kontrollista on tunkeutumisenestojärjestelmä, joka estää pääsyn hyökkäävän IP:lle.

[Jac10]Elvyttävät kontrollit puolestaan vastaavat palveluiden palauttamisesta tietoturvamurron jälkeen. Elvyttäviä kontrolleja ovat muun muassa varajärjestelmät tai -virtalähteet.

9.3 Tietoturvakontrollien auditointi

[Jac10]Tietoturvakontrollien avulla organisaatio voi siis pienentää tietoturvauhkien aiheuttamia riskejä. Tietoturvapolitiikassa on määritelty, mitä kontrolleja organisaatio tarvitsee, ja kyseiset kontrollit puolestaan valitaan perustuen havaittuihin, organisaatiota uhkaaviin riskeihin.

[Jac10]Tietoturvakontrollien auditointi käsittää paljon muutakin kuin palomuurin skannauksen tietoturva-aukkojen varalta tai haitallisten testipakettien lähettämisen verkkoon ja sen seurauksista raportoinnin. Yksinkertaisimmillaan tietoturvakontrollin auditointi arvioi, vastaako kontrollin nykytila organisaation tietoturvapolitiikkaa, parhaita toimintatapoja ja lakia. Kattava tietoturvakontrollien arviointi on siis olennainen osa sen selvittämisessä, noudattaako organisaatio omaa tietoturvapolitiikkaansa, sen perustella laadittuja toimenpiteitä ja yleisiä standardeja, ja täyttääkö se näin sille asetetut tavoitteet tietoturvariskein pienentämisessä.

[Jac10]Tietoturvakontrollien arviointi vaatii, että auditoija tarkastelee järjestelmää hakkerin näkökulmasta ja arvioi, miten eri asioita voitaisiin käyttää väärin luvattoman organisaation etuuksiin käsiksi pääsyn saavuttamiseksi. Turvallisuutta ei voida perustella yksinkertaisesti sanomalla, että jonkin asian ei pitäisi olla väärinkäytettävissä tai sen pitäisi olla suojattu, vaan ainoa tapa selvittää totuus on testata käytetyt tietoturvakontrollit.

10 TIETOTURVA-AUDITOINNIN TYÖKALUT

Tietoturva-auditointiprosessi on paljon aikaa vaativa. Työn täytyy olla tarkkaa ja hyvin suunniteltua, jotta saavutettaisiin siltä tavoiteltu hyöty. Auditointiprosessia helpottamaan ja nopeuttamaan on kehitetty monia ohjeistuksia, tarkastuslistoja ja automatisoituja työkaluja, joita auditoijien pitää ja kannattaa hyödyntää työssään. Luvussa 10.1 kerrotaan testauskehyksistä, luvussa 10.2 automatisoiduista testaustyökaluista, ja luvussa 10.3 tietoturvastandardeista.

10.1 Testauskehykset

[Jac10]Testauskehykset ohjeistavat yksityiskohtaisesti ja prosessimaisesti, miten suorittaa tietoturvan testausta. Kehyksiä on olemassa useita, mutta kaikki ne ovat johdonmukaisia, toistettavissa olevia ja perustuvat parhaisiin toimintatapoihin. Neljä eniten tietoturvan testauksessa käytettyä kehystä ovat Open Source Security Testing Methodology Manual (OSSTMM), Information Systems Security Assessment Framework (ISSAF), NIST 800-115 ja Open Web Application Security Project (OWASP), joilla jokaisella on omat hyvät ja huonot puolensa.

[Jac10]OSSTMM kehitettiin Creative Commons License:n alaisena, jonka tarkoituksena on avustaa tietoturvatestauksen läpikotaisessa ja toistettavassa suorittamisessa. Se jakaa tietoturvatestauksen kuuteen osa-alueeseen: tietojen-, prosessien-, Internet-teknologian-, kommunikaation-, langattomuuden- ja fyysisen turvallisuuden testaukseen. Kehys pyrkii vastaamaan siihen, mitä alueita tulee testata, ja minkälaisia tuloksia testeiltä tulisi odottaa.

[Jac10]ISSAF on yksi suurimmista testauskehyksistä. Jokaisen kontrollin testaukseen liittyy tarkat kuvaukset testityökalujen käytöstä ja odotettavista tuloksista. Kehys on jaettu kahteen dokumenttiin, joista toinen keskittyy tietoturvaan liiketoiminnan kannalta ja toinen tarjoaa kehyksen penetraatiotestausta varten.

[Jac10]NIST 800-115 kehitettiin Yhdysvaltojen hallituksen tietoturvan katselmointia varten, mutta sitä voidaan käyttää myös yksityisellä sektorilla. Kehys sisältää templaatteja, tekniikoita ja työkaluja monien erilaisten järjestelmien ja skenaarioiden

arviointiin. Kehys on jaettu kymmeneen osaan, jotka kaikki tarjoavat kattavaa ohjeistusta aiheeseen liittyen: tietoturvan testauspolitiikat (*Security Testing Policies*), johdon rooli tietoturvan testauksessa (*Management's Role in Security Testing*), testausmetodit (*Testing Methods*), tietoturvan arviointitekniikat (*Security Review Techniques*), järjestelmien tunnistus ja analysointi (*Identification and Analysis of Systems*), skannaus- ja haavoittuvuustestaus (*Scanning and Vulnerability Assessments*), haavoittuvuuksien validointi (*Vulnerability Validation*), tietoturvan testauksen suunnittelu (*Information Security Test Planning*), tietoturvan testauksen suorittaminen (*Security Test Execution*), testien jälkeiset aktiviteetit (*Post-test Activities*).

[Jac10]Huonosti koodatut ja suoritetut web-sovellukset voivat levitä nopeasti ja asettaa suuren osan Internetin käyttäjistä alttiiksi sovellusten haavoittuvuuksia hyväksikäyttäville hyökkäyksille. OWASAP-ohjeistus luotiin web-sovellusten kehittäjiä ja muita tietoturvasta kiinnostuneita varten, jotta tietoturva otettaisiin paremmin huomioon web-sovellusten yhteydessä. OWASAP on nykyään standardi web-sovellusten tietoturvan testauksessa.

[Jac10]OWASAP koostuu kymmenestä osa-alueista, joista jokainen käsittää tiivistelmän niihin liittyvistä ongelmista ja testaukseen käytettävistä työkaluista sekä esimerkkejä odotettavista tuloksista. Osa-alueet ovat tiedon kerääminen (*Information gathering*), konfiguraation hallinta (*Configuration management*), autentikaatiotestaus (*Authentication testing*), session hallinta (*Session management*), valtuutusten testaus (*Authorization testing*), liiketoimintalogiikan testaus (*Business logic testing*), datan validointitestaus (*Data validation testing*), palvelunestotestaus (*Denial of service testing*), web-palveluiden testaus (*Web services testing*) ja Ajax-testaus (*Ajax testing*).

10.2 Automatisoidut testaustyökalut

[Jac10]Auditoijien käyttämien tietoturvan testaustyökalujen määrä kasvaa joka vuosi. Automatisoidut ja muillakin tavoin kehittyneet työkalut ovat suuri apu auditoinnissa, koska niiden avulla säästetään aikaa ja parannetaan haavoittuvuuksien havaitsemista.

[Jac10]Palveluiden kartoitustyökalut (*Service Mapping Tools*), kuten Nmap ja Hping, tunnistavat järjestelmiä, etäpalveluita ja avoimia portteja. Näiden työkalujen avulla voidaan muun muassa testata palomuuriasetuksia tai IP-pakettien antamia vastauksia.

[Jac10]Haavoittuvuuden arviointivälineet (*Vulnerability Assessment Tools*), kuten Nessus ja Red Seal RSM, kartoittavat kohteen tunnettuja haavoittuvuuksia ja generoivat niistä raportin. Haavoittuvuustestauksen tarkoitus on havaita kaikki mahdolliset kohteeseen liittyvät haavoittuvuudet. Haavoittuvuustestauksessa löydetään usein todella suuri määrä mahdollisia haavoittuvuuksia, mutta todellisuudessa kaikki havaitut haavoittuvuudet eivät ole oikeasti väärinkäytettävissä. Auditoijan tehtäväksi jääkin näiden potentiaaliset haavoittuvuuksien asettaminen tärkeysjärjestykseen, ja sen jälkeen niiden todellisen haavoittuvuuden tutkiminen. Haavoittuvuustestausta suorittavia työkaluja käytettäessä täytyy kuitenkin olla varovainen, koska jotkin arviointimekanismeista voivat kaataa jonkin palvelun. Auditoijilla tulee olla suunnitelma näiden palveluiden palauttamista varten, ja testaus tulisi suorittaa vilkkaimpien käyttöaikojen ulkopuolella. Haavoittuvuus-skannereiden lisäksi haavoittuvuuksia voidaan havaita myös tutkimalla konfiguraatioita ja politiikkoja, ja vertaamalla niitä parhaisiin toimintatapoihin.

[Jac10]Pakettien kaappaustyökalut (*Packet Capture Tools*), kuten Tcpdump ja Wireshark, ovat todella hyödyllisiä tietoturvan testauksessa, koska niiden avulla voidaan nähdä tietoliikenteen kuljettamat viestit. Tämä on hyödyllistä esimerkiksi silloin, kun täytyy testata palomuuriasetuksia tai IPS-allekirjoituksia.

[Jac10]Penetraatiotestaustyökalut (*Penetration Testing Tools*), kuten Metasploit ja Core Impact, nopeuttavat huomattavasti tietoturvakontrollien auditointia. Nämä työkalut ovat käytännössä kehyksiä, jotka sisältävät automatisoituja hyökkäyksiä, jotka pyrkivät hyödyntämään kohteen mahdollisia haavoittuvuuksia. Penetraatiotestauksen avulla voidaan arvioida verkkoihin liittyviä kontrolleja, joiden tehtävä on estää tai havaita hyökkäyksiä tai minimoida niiden aiheuttamia ongelmia. Kuten haavoittuvuustestauksessakin, penetraatiotestauksessa yritetään havaita kontrollien haavoittuvuudet, mutta sen lisäksi yritetään vielä ottaa kohdejärjestelmä haltuun. Vaikka järjestelmä on saatu otettua haltuun, ei vielä pystytä suoraan sanomaan, missä vika on, mutta yleensä voidaan kuitenkin helposti rajata, mikä kontrolli ei toiminut.

Penetraatiotestaajat saattavat joskus käyttää yleisesti käytettyjen penetraatiotestaustyökalujen lisäksi myös omia skriptejään ja sovelluksiaan tarkemman testauksen suorittamiseksi.

[Jac10]On myös työkalupaketteja, jotka pystyvät suorittamaan useimpia auditoijien tarvitsemia testejä. Esimerkiksi BackTrack:n avulla voidaan kerätä tietoja, kartoittaa verkot, tunnistaa haavoittuvuudet, analysoida web-sovellukset, analysoida radio-verkot, suorittaa penetraatiotestausta, testata oikeuksien kasvattamista, testata takaporttien kautta pääsyn ylläpitoa, käyttää käänteistekniikkaa (*Reverse Engineering*) haittaohjelmien tunnistukseen, ja testata VoIP-kräkkäystä ja -tallennusta.

10.3 Tietoturvastandardit

[Jac10]Tietoturvastandardit kattavat tietoturvan parhaat käytännöt, joita organisaatioiden tulisi käyttää tietoturvan toteutuksessa, luottamuksellisen tiedon suojauksessa sekä järjestelmien eheyden ja saatavuuden varmistamisessa. Näitä parhaita toimintatapoja on kuitenkin niin monia erilaisia, että kaikkiin asioihin ei ole löydettävissä vain yhtä oikeaa tapaa. Onkin tärkeää, että näistä parhaista toimintatavoista valitaan organisaation tavoitteisiin parhaiten sopivat tavat, ja tästä syystä auditoijan tulee tietää paljon olemassa olevista standardeista, jotta hän voi auttaa organisaatiota valitsemaan vaihtoehtojen välillä ja näin toteuttamaan heidän kannaltaan parhainta mahdollista tietoturvaa. Standardeihin viitaten voidaan luoda kattavat tietoturvapolitiikat ja yleiset menettelytavat, ja niiden avulla voidaan myöhemmin myös selittää ja perustella, miksi jokin asia on sisällytetty organisaation tietoturvapolitiikkaan tai menettelytapoihin. Standardeja noudattamalla organisaatio voi myös saada tietoturvasertifikaatin, joka on virallinen osoitus organisaation tietoturvan kattavuudesta.

[Jac10]Tietoturvan hallintaa koskevat kehykset kertovat, miten tietoturvaa voidaan hallinnoida tehokkaasti. Tietoturvan hallintaa auditoidaan tutkimalla, miten organisaatio hallinnoi niitä prosesseja ja toimintoja, jotka muodostavat organisaation tietoturvaohjelman, ja vertaamalla havaintoja yleisesti hyväksyttyjen tietoturvan hallintaa käsittelevien kehysten kuvaamiin prosesseihin. Auditoijan tulee tietää

käyttääkö organisaatio jotakin kehystä hallintaprosessinsa pohjana, ja jos kyllä, auditoijan tulee tietää mitä kyseinen kehys sisältää.

Aliluvussa 10.3.1 kerrotaan COSO:n laatimasta tietoturvastandardista, aliluvussa 10.3.2 käsitellään COBIT-kehys, aliluvussa 10.3.3 käydään läpi ISO 27000 tietoturvastandardit, aliluvussa 10.3.4 PCI DSS -standardi, aliluvussa 10.3.5 VAHTI-ohjeistukset, aliluvussa 10.3.6 Katakri, ja aliluvussa 10.3.7 Valtionvarainministeriön Tietoturvatasot.

10.3.1 COSO

[Jac10]COSO eli Committee of Sponsoring Organizations of the Treadway Commission perustettiin 1985 parantamaan taloudellisten raporttien oikeellisuutta, ja kehittämään standardia sisäisiä valvontamenetelmiä varten, jotta vilpillistä raportointia voitaisiin välttää. Organisaatio julkaisi vuonna 1994 dokumentin nimeltä ”Internal Controls: Integrated Framework” eli suomeksi käännettynä ”Sisäiset kontrollit: integroitu kehys”, joka määrittelee yleisesti käytetyt termit, määritykset ja arviointitavat organisaation sisäisille kirjanpidon kontrolleille.

[Jac10]Dokumenttia käytetään standardina kirjanpitoa auditoitaessa, ja sen avulla arvioidaan noudattaako organisaatio FCPA:ta ja SOX:n osiota 404. Kehystä käytetään laaja-alaisesti suurissa yrityksissä pääasiallisesti juuri SOX 404 takia. Kehystä on kritisoitu huonoksi pienten yritysten kannalta, mistä johtuen COSO julkaisi vuonna 2006 kehyksen ”Internal Control Over Financial Reporting for Small Public Companies” eli suomeksi käännettynä ”Taloudellisen raportoinnin sisäinen kontrollointi pienissä julkisissa yrityksissä”. Vaikka kehys alun perin kehitettiinkin kirjanpidon prosessien arviointia varten, voi sitä käyttää myös muiden IT-prosessien tietoturvan arviointiin.

[Jac10]COSO:n sisäisistä kontrolleista kertova dokumentaatio käy läpi, mitä kontrollit voivat ja eivät voi tehdä organisaation puolesta. Koko dokumentin ydin on osoittaa yhteys ihmisten, prosessien ja kontrollien välillä, ja yhteys huomioon ottaen käydä läpi, mitkä ovat tehokkaiden kontrollien käyttöönoton periaatteet. Itse kehys koostuu viidestä pääkontrollista, jotka ovat ympäristö (*Control Environment*), riskien arviointi (*Risk*

Assessment), aktiviteetit (*Control Activities*), tieto ja kommunikaatio (*Information and Communication*) ja valvonta (*Monitor*).

[Jac10]Ympäristö määrittelee, kuinka organisaatio rakentaa sisäisen hallinnan ohjelmansa, joka käsittää koko organisaation. Hallintaohjelmaa luotaessa tulee ottaa huomioon eettiset kysymykset, organisaation rakenne sekä henkilöstön roolit ja vastuut. Ympäristö siis koostuu ihmisistä kulttuurista ja organisaation etiikasta.

[Jac10]Riskien kartoitus on tärkeää, koska luonnollisesti ei ole mahdollista suojautua sellaisilta uhilta, joiden olemassaoloa ei tiedetä. Kattavalla riskien arvioinnilla voidaan siis suunnitella käytettävät kontrollit paremmin, ja tällä tavoin avustaa organisaatiota suojautumaan tietoturvauhilta sekä saavuttamaan strategiset tavoitteensa paremmin.

[Jac10]Aktiviteetit -osiossa kuvataan ne kontrollit, joita COSO suosittelee käytettäväksi tietoturvariskien pienentämiseksi. Vaikka kontrollien määrä onkin kattava, kehys ei ota yhtä hyvin kantaa IT-alan ongelmiin kuin kirjanpidon. Se antaa hyvän pääsuunnan toteutettaville aktiviteeteille, mutta ei ota kantaa toteutuksen yksityiskohtiin.

[Jac10]Tieto ja kommunikaatio -osiossa painotetaan sitä, kuinka ihmiset eivät voi hoitaa työtehtäviään kunnolla ilman tarvittavia tietoja, ja ilman tehokkaita ja turvallisia kommunikaatiokanavia organisaatio voi kohdata merkittäviä ongelmatilanteita. Kehyksen tämä osio yhdistää muut neljä osiota.

[Jac10]Valvonta on tärkeää, jotta pysytään selvillä siitä, toimivatko kontrollit tarkoitetulla tavalla. Valvontaa voi esimerkiksi toteuttaa jonkinlainen hälytysjärjestelmä, raportointi, auditointi tai testausmekanismi, joka tarjoaa dataa erilaisten ongelmien korjaamiseksi.

[Jac10]Vaikka nämä viisi osiota ovat IT-alalla tarvitun tietoturvan toteutuksen kannalta täysin relevantteja, itse kontrolleja ei ole käyty läpi yhtä syvällisesti kuin joissain muissa kehyksissä kuten esimerkiksi COBIT:ssa.

10.3.2 COBIT

[Jac10]COBIT eli Control Objects for Information and related Technologies luotiin ISACA:n (Systems Audit and Control Association) ja ITGI:n (IT Governance Institute)

toimesta vastaamaan IT-yhteisön tietoturvatarpeisiin. ITGI on voittoa tavoittelematon organisaatio, joka johtaa COBIT:n kehitystä yliopistoissa ja hallituksissa työskentelevistä asiantuntijoista sekä auditoijista koostuvan komitean kautta. Kehys koostuu ohjeistuksista, jotka käsittelevät kattavan IT-hallinnoinnin, auditoinnin ja palveluntarjonnan toteutusta.

[Jac10]Vaikka edellisessä luvussa mainittiinkin, että COBIT on kattavampi IT-alan kontrollien kannalta kuin COSO, se ei korvaa COSO:a vaan ennemmin tarjoaa lisätietoa COSO:n kehystä käyttäville organisaatioille. COBIT käsittää yksityiskohtaista tietoa COSO:n listaamien asioiden saavuttamisen kannalta tärkeistä kontrolleista, ja kuinka niiden toimivuutta tulee mitata ja auditoida. COBIT ei kuitenkaan käy tarkasti läpi näiden kontrollien käyttöönottoon liittyviä toimia, joten kontrollien käyttöönotosta tietoa täytyy etsiä muualta. Kehys ei esimerkiksi kerro parasta tapaa konfiguroida AES-enkryptausta, mutta se tarjoaa kuitenkin tarvittavat mekanismit sen selvittämiseksi, missä riskitapauksissa enkryptausta tulee käyttää.

[Jac10]Auditiontiin liittyen COBIT tarjoaa hyvin dokumentoidun listan prosesseista ja kontrolleista, joita voidaan arvioida niille asetettujen vaatimusten ja mittareiden avulla. Kehyksen avulla auditoija voi lisäksi helpommin muodostaa tarkastuslistoja niiden organisaatioiden auditointia varten, jotka eivät vielä seuraa COBIT:n ohjeistusta omassa IT-hallinnassaan. COBIT on myös hyvä referenssi auditointiraporttia kirjoitettaessa, koska auditoija voi siihen verraten perustella löydöksiään. Juuri tämän auditoitavuuden takia COBIT:sta on tullut yksi johtavista IT-hallinnan kehyksistä.

10.3.3 ISO 27000 standardit

[Jac10]ISO 27000 standardit ovat kansainvälisesti tunnettuja, yleisesti käytettyjä ja hyväksyttyjä sekä usein mainittuja tietoturvastandardeja. Ne tunnettiin aikaisemmin nimellä ISO 17799 ja ne perustuvat brittiläiseen standardiin 7799. Standardi käsittää laajan skaalan erilaisia tietoturvatarpeita tiedonkäsittelystä fyysiseen suojaukseen ja tietoturvapolitiikkoihin. ISO 27000 kattaa seitsemän eri standardia ja sarjaan on tulossa vielä kymmenen uutta standardia. Näistä yleisimmin käytetyt standardit ovat ISO 27001 ja ISO 27002.

[Int12]ISO 27001:n koko nimi on ISO 27001:2005 Information Technology - Security Techniques - Information Security Management Systems - Requirements. [Jac10]Se kattaa tietoturvanhallintajärjestelmälle asetettavat vaatimukset noudattaen ISO 27002:ssa mainittuja parhaita toimintatapoja. Standardi kuvaa tarvittavat kontrollit ja prosessit, jotka tulee ottaa käyttöön, jos organisaatio haluaa sertifioitua ISO-standardin mukaisesti. Keskeinen asia ISO 27001:ssä on prosessien parantamiseen käytetty Deming-sykli: suunnittele, toteuta, tarkista ja toimi. Sykli on saanut nimensä sen kehittäjän Edwards Demingin mukaan ja sen tarkoitus on osoittaa, että prosessia voidaan parantaa jatkuvasti havainnoimalla sitä, oppimalla virheistä ja jalostamalla sen hyviä puolia entistä paremmiksi.

[Jac10]Syklin suunnitteluvaiheessa tietoturvanhallintaa suunnitellaan organisaation tietoturvapolitiikkojen, prosessien, tavoitteiden ja sitä uhkaavien riskien pohjalta. Toteutusvaiheessa tietoturvanhallinta toteutetaan suunnitelman mukaisesti. Tarkistusvaiheessa tietoturvanhallinta auditoidaan arvioimalla sitä politiikkoihin, tavoitteisiin ja kokemuksiin perustuen. Toimintavaiheessa korjataan havaitut puutteet ja tehdään muut toimet prosessin tehostamiseksi entisestään, jonka jälkeen sykli alkaa alusta.

[Jac10]ISO 27001 tarjoaa siis kattavat ohjeet tietoturvanhallintajärjestelmien käyttöönottoa varten ja tarkistuslistan käyttöönotettavia kontrolleja varten, jos organisaatio haluaa sertifioitua ISO-standardin mukaisesti ja tällä tavoin todistaa osaavansa rakentaa kattavan tietoturvaohjelman sekä tarvittaessa osoittaa vastaavansa joidenkin lakien kuten SOX:n asettamiin vaatimuksiin.

[Int12]ISO 27002:n koko nimi on ISO 27002:2005 Information Technology - Security Techniques - Code of Practice for information security management. [Jac10]Standardi kattaa parhaat toimintatavat järjestelmien tietoturvan toteuttamiseksi, ja käsittelee laajan skaalan aiheita jakaen ne kahteentoista eri osa-alueeseen: johdatus tietoturvanhallintaan, riskien kartoitus ja niihin vastaaminen, tietoturvapolitiikat, tietoturvan organisointi, resurssien hallinnointi, henkilöstöresurssien turvallisuus, fyysinen turvallisuus, kommunikointi ja operaatioiden hallinta, saatavuuden hallinta, tietojärjestelmien hankinta, kehitys ja ylläpito, tietoturvan tapahtumahallinta, liiketoiminnan jatkuvuus, ja

tietoturvan noudattaminen. Näiden lisäksi ISO 27002 esittää tarkat toteutusvaatimukset ISO 27001:stä varten.

10.3.4 PCI DSS

[Moe10]PCI DSS eli Payment Card Industry Data Security Standard kehitettiin vuonna 2007 Payment Card Industry (PCI) -valtuuston toimesta. [Moe10][Jac10]Valtuustoon kuuluu muun muassa American Express, Discover, Master Card, Visa ja JCB. Standardi kattaa tietoturvan vähimmäisvaatimukset luottokorttitietojen turvaamiseksi, ja kaikkien kauppiaiden, jotka haluavat hyväksyä luottokortin maksuvälineenä tai muulla tapaa käsittelevät, tallentavat tai lähettävät luottokorttitietoja eteenpäin, tulee noudattaa PCI DSS standardia. [Moe10]Jos standardia ei noudateta, yritys voi saada siitä sakot ja menettää oikeutensa hyväksyä luottokortteja maksuvälineenä.

[Moe10]Standardin asettamiin tietoturvavaatimuksiin kuuluu niin tietoturvan perusasioita kuin myös hieman kehittyneempiä tietoturvasäännöksiä. Esimerkkejä perusasioista ovat palomuurin käyttö ja tarvittava konfigurointi, muun kuin järjestelmän oletusarvoisen salasanan käyttö, ja anti-virus -ohjelman asennus ja säännöllinen päivitys. Esimerkkejä hieman kehittyneemmistä tietoturvasäännöksistä ovat puolestaan verkon resursseihin ja luottokorttitietoihin pääsyn valvonta, järjestelmien ja prosessien tietoturvan säännöllinen testaus, ja korkean tason tietoturvaperiaatteiden ja -menettelytapojen käyttäminen.

10.3.5 VAHTI-ohjeistukset

[Val12a]Valtionvarainministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnoimaan tietoturvallisuuden yhteistyötä, ohjausta ja kehittämistä. VAHTI:n tehtäviin kuuluu valtionhallinnon tietoturvallisuussäännösten, -ohjeiden, -suositusten ja -tavoitteiden käsittely sekä valtionhallinnon tietoturvatoimenpiteiden ohjaus. Ryhmän päätavoite on valtionhallinnon toimintojen luotettavuuden, jatkuvuuden, laadun, riskienhallinnan ja varautumisen parantaminen tietoturvan kehittämisen kautta.

[Val12b]VAHTI on laatinut monia ohjeistuksia valtionhallinnon tietoturvan parantamiseksi. Esimerkkejä näistä ovat muun muassa ”Johdon tietoturvaopas”,

”Sosiaalisen median tietoturvaohje” ja ”Sisäverkko-ohje”. Ohjeistukset ovat saatavilla PDF-muodossa Valtionvarainministeriön verkkosivuilta.

10.3.6 Katakri

[Suo11]Katakri eli kansallinen turvallisuusauditointikriteeristö julkaistiin vuonna 2009 ja sen toinen versio valmistui vuonna 2011. Se toteutettiin viranomaisten, elinkeinoelämän ja turvallisuusalan toimesta, ja sen sanotaan mahdollistavan vastuuviranomaisten toiminnan läpinäkyvyyden ja yhtäläisyyden sekä elinkeinoelämän kustannustehokkaan turvallisuustoiminnan. Turvallisuusviranomaiset käyttävät Katakria auditoidessaan tietoturvaa ja selvittäessään, vastaako kohteen sen hetkinen tietoturvan taso kansainvälisiä tietoturvallisuusvelvoitteita.

[Suo11]Katakri koostuu neljästä osa-alueesta: hallinnollisesta turvallisuudesta, henkilöstöturvallisuudesta, fyysisestä turvallisuudesta ja tietoturvallisuudesta. Tietoturvallisuusosio kattaa tietoliikenneturvallisuuden, tietojärjestelmäturvallisuuden, tietoaineistoturvallisuuden ja käyttöturvallisuuden. Tietoturvallisuusosio kuvaa vähimmäisvaatimukset luottamuksellisten tietojen turvaamiseksi.

[Suo11]Tietoturvallisuuskriteeristössä on otettu huomioon valtionhallinnon tietoturvallisuusasetus ja sitä täydentävät ohjeistukset. Käytännössä kriteeristö esittää 41 tietoturvaan liittyvää kysymystä, joihin kuhunkin on annettu kolme eri vastausvaihtoehtoa (perustaso, korotettu taso ja korkea taso), joista tulee valita se, mikä kuvaa kohteen tietoturvan tasoa parhaiten. Esimerkkejä kysymyksistä ovat muun muassa ”onko tietoliikenneverkon rakenne turvallinen?”, ”onko hallintayhteydet suojattu asianmukaisesti?”, ”miten suojattavat tiedot säilytetään tietojärjestelmissä?”, ja ”miten on varmistuttu ajettavan koodin turvallisuudesta?”. Katakri on saatavilla kokonaisuudessaan PDF-muodossa Suomen Puolustusministeriön verkkosivuilta.

10.3.7 Tietoturvatasot

[Val08]Valtionvarainministeriön Tietoturvatasot (TTT) -hankkeen tavoitteena on varmistaa valtionhallinnossa käsiteltävien tietojen turvallisuus yhtenäistämällä tietoturvallisuuden hallinnan eri osapuolten välillä. [Tig10]Asetus tietoturvatasoista

annettiin Valtioneuvoston toimesta 1.7.2010 ja hallinnonalojen ja virastojen odotetaan saavuttavan Tietoturvatasojen perustaso vuoden 2013 mennessä.

[Val08]Tietoturvatasoja on määritelty yhteensä viisi: avoin taso, perustaso, korotettu taso, korkea taso ja erityistaso. Näistä kuitenkin vain kolme soveltuu laajaan käyttöön. Avoin taso ei ole valtionhallinnossa käytössä, mutta se on kuvattu tasona, jolta tietoturvaa voidaan aloittaa rakentamaan. Perustaso on valtionhallinnon minimitaso, joka saavutetaan, kun organisaation prosesseilla on yhtenäinen menettelytapa. Korotettu taso saavutetaan, kun organisaation prosessit on dokumentoitu ja henkilöstö koulutettu suorittamaan työtehtävänsä dokumentaation mukaisesti. Korkealla tasolla dokumentoitujen prosessien laatua seurataan, varmistetaan ja parannetaan erilaisten mittareiden avulla. Optimoidulla tasolla käytössä ovat parhaat mahdolliset käytännöt ja mittarit, minkä ansiosta prosesseja pystytään optimoimaan. Optimoidun tason saavuttaminen on valtionhallinnossa tarpeellista vain harvoin.

11 HAASTATTELUT

Tutkielman tekijä halusi tutkielmansa sisältävän kirjallisuuskatsauksen lisäksi myös empiirisen osuuden. Tutkielmaa varten haastateltiin viittä Suomessa toimivaa tietoturva-auditointeja suorittavaa organisaatiota. Haastatteluiden vastaukset kertovat paljon nykypäivänä Suomessa suoritettavista tietoturva-auditoinneista.

Yksittäisiin haastattelukysymyksiin sai vapaasti jättää vastaamatta. Tästä huolimatta ainoastaan yksi organisaatio jätti vain yhden kysymyksen kohdalla vastaamatta. Haastatelluilta organisaatioilta on varmistettu, että heidän antamiaan tietoja saa esitellä tässä tutkielmassa ja heidän niemensä saa mainita. Yksi haastatelluista organisaatioista toivoi, ettei heidän nimeään mainittaisi heidän antamiensa vastausten yhteydessä. Tästä syystä kysymysten yhteydessä ei ole eritelty, mikä haastatelluista organisaatioista antoi minkäkin vastauksen. Vastaukset eivät ole myöskään missään tietyssä järjestyksessä, josta voisi tavalla tai toisella päätellä jonkin tietyn vastauksen antaneen organisaation nimen.

Aliluvussa 11.1 esitellään haastatellut organisaatiot, aliluvussa 11.2 kerrotaan kyseisten organisaatioiden tarjoamista tietoturva-auditointipalveluista, aliluvussa 11.3 käydään läpi, millaiset asiat ovat useimmiten auditoinnin kohteina, aliluvussa 11.4 käsitellään organisaatioiden suorittamien auditointien elinkaarten vaiheet, aliluvussa 11.5 mainitaan käytetyt viitekehykset, aliluvussa 11.6 kerrotaan auditoinneissa hyödynnetyistä auditointimenetelmistä ja -työkaluista, aliluvussa 11.7 käsitellään yleisimmin havaitut puutteet tietoturvassa, aliluvussa 11.8 puhutaan auditoinnin aikana esiintyvistä ongelmista, aliluvussa 11.9 kerrotaan asiakkaiden suhtautumisesta auditointeihin, aliluvussa 11.10 on annettu esimerkkejä auditoinneista veloitettavista hinnoista, ja aliluvussa 11.11 organisaatiot kertovat, miten he uskovat ja toivovat tietoturva-auditointien kehittyvän tulevaisuudessa.

11.1 Haastatellut organisaatiot

Haastattelukysymyksiin vastasi viisi Suomessa toimivaa tietoturva-auditointeija suorittavaa organisaatiota. Heitä pyydettiin omin sanoin kuvailemaan organisaationsa

toimintaa. Toiminnastaan kertoo aliluvussa 12.1.1 Nixu Oy, aliluvussa 12.1.2 XCure Solutions Oy, aliluvussa 12.1.3 Sulava, aliluvussa 12.1.4 KPMG, ja aliluvussa 12.1.5 Poliisi (Pohjois-Savon poliisilaitos).

11.1.1 Nixu Oy

Nixu Oy on Pohjoismaiden suurin tietoturvakonsultointiin erikoistunut asiantuntijayritys. Nixu ohjeistaa, rakentaa, kehittää ja tarkastaa asiakkaidensa tietoturvaa riippumattomana neuvonantajana. Tavoitteena on varmistaa asiakkaiden toiminnan jatkuvuus sekä sähköisten palvelujen toimivuus ennakoimalla ja ehkäisemällä tietoturvaan liittyviä riskejä.

Tietoturvan asiantuntijapalveluihin keskittyneen Nixun palveluksessa on yli 100 kokenutta tietoturvakonsulttia, teknistä asiantuntijaa ja ohjelmistoammattilaista, jotka muodostavat Suomen vahvimman tietoturvan osaamiskeskittymän. Nixun liikevaihto vuonna 2010 oli yli 10 miljoonaa euroa.

Nixun tarjoamat tietoturvan asiantuntijapalvelut ulottuvat kokonaisulkoistuksista yksittäisiin auditointeihin. Nixun asiantuntijat analysoivat riskit, ohjeistavat henkilöstön, rakentavat käyttäjähallinnon prosessit, tarkastavat teknisen turvallisuuden ja kehittävät ohjelmistot turvallisia menetelmiä käyttäen.

Yli 20 vuotta tietoturvan ja verkkoteknologian parissa toiminut Nixu on luotettu neuvonantaja useille suurille yrityksille ja julkisen sektorin toimijoille.

11.1.2 XCure Solutions Oy

Tietoturvapalveluihin erikoistunut asiantuntijayritys. XCure Solutions tuottaa asiakkailleen tietoturvapalveluita niin konsultoinnin kun auditointien muodossa.

XCure Solutions Oy on perustettu vuonna 2006 ja tällä hetkellä yrityksessä on seitsemän työntekijää sekä vaihtuva määrä projektikonsultteja. XCure Solutions Oy:n asiakaskunta koostuu pääasiassa valtionhallinnon eri yksiköistä sekä suuryrityksistä.

11.1.3 Sulava

Sulava on erikoistunut edistämään uudenlaista digiajan työkulttuuria. Työkulttuurin ytimessä ovat pilvipalveluiden ja sosiaalisten teknologioiden tehokas hyödyntäminen.

Sulavan toiminnassa yhdistyvät liiketoiminnan, tietotekniikan ja viestinnän osaaminen. Tietoturvakonsultointi ja auditoinnit ovat osa palvelukokonaisuutta.

11.1.4 KPMG

KPMG on yksi maailman johtavista asiantuntijapalveluja tarjoavista organisaatioista, jonka palveluihin kuuluvat tilintarkastus, vero- ja neuvontapalvelut. KPMG:n ensisijainen tehtävä on tuottaa yhdenmukaisia ja laadukkaita palveluja maailmanlaajuisesti, niin globaaleille kuin paikallisillekin asiakkaille.

KPMG toimii yli 140 000 asiantuntijan voimin 145 maassa ympäri maailmaa. Suomessa KPMG:n palveluksessa on lähes 700 asiantuntijaa 16 paikkakunnalla. Tietoturva-asiantuntijoita on noin 4000.

11.1.5 Poliisi

Pohjois-Savon poliisilaitoksen tietoturvapäällikkö kertoi toiminnastaan seuraavasti: ”Toimin Pohjois-Savon poliisilaitoksen tietoturvapäällikkönä. Toimenkuvaani kuuluu muun muassa tietoturva-auditoinnit. Pohjois-Savon poliisilaitos muodostuu viidestä eri poliisiasemasta (Kuopio, Iisalmi, Varkaus, Suonenjoki ja Juankoski).

Jokaisella poliisiasemalla on omat tietoturvallisuuden yhdyshenkilöt, jotka muodostavat itseni kanssa tietoturvallisuuden työryhmän. Kokoonnumme pari kertaa vuodessa ja työryhmän jäsenet raportoivat minulle muuna aikana tietoturvallisuuteen liittyvistä asioista.”

11.2 Organisaatioiden tarjoamat tietoturva-auditointipalvelut

Haastateltavilta organisaatioilta kysyttiin, minkälaisia tietoturva-auditointipalveluita he tarjoavat, ja mitkä ovat heidän asiakkaidensa yleisimmin käyttämät palvelut. Saadut vastaukset olivat todella erilaisia, ja organisaatioiden tarjoamien palveluiden määrä

riippuu varmasti suurelta osin heidän erikoistumisalastaan ja heillä käytössä olevien resurssien määrästä.

Yksi haastatelluista organisaatioista kertoi keskittyvänsä lähdekoodi-, järjestelmä- sekä alusta-auditointeja. He kertoivat suorittavansa yleisimmin järjestelmäauditointeja.

Toinen organisaatio kertoi, että heidän tietoturvallisuuden nykytilan arviointiin liittyvät palvelut jakautuvat bechmark- ja auditointi-tarkastuksiin. Benchmark-tarkastuksissa tarkastellaan kohdetta yleisiä hyviä käytäntöjä vastaan ja auditoinnissa yhtä tai useampaa tiettyä vaatimuslähdettä vasten. Molempia palveluita he toimittavat yhtä paljon.

Kolmas organisaatio on tehnyt pääasiassa tietoturvallisuuden hallinnollisia auditointeja (ISO 27001, Katakri, tietoturvatasot, Cobit jne.), jatkuvuussuunnitelmien auditointeja, käyttöoikeuksien hallinnan auditointeja sekä ISAE 3402 ja SAS70 varmennuslausuntoauditointeja. He ovat myös tehneet teknisiä auditointeja, kuten käyttöjärjestelmien, tietoverkkojen, tietokantojen, kriittisen infrastruktuurin (SCADA), langattomien toteutusten ja yläkorttien, mobiililaitteiden ja -sovellusten sekä koodin auditointeja. Näiden lisäksi he ovat myös suorittaneet web-sovellustestausta ja muita testauksia, kuten penetraatiotestausta. Organisaatio ei osannut tarkalleen kertoa, mikä näistä palveluista olisi yleisimmin käytetty, mutta he kertoivat penetraatiotestauksen sisältyvän lähes aina erilaisiin testauksiin.

Neljäs organisaatio tarjoaa tietoturvan auditointipalveluita organisaation tietoturvan vaatimusten mukaisuuden auditoinnista, sovellusten lähdekoodin ja tietoliikenneprotokollatoteutusten tarkastukseen. Tyypillisiä heidän suorittamiaan auditointeja ovat vaatimustenmukaisuuden auditointi (esim. PCI DSS ja valtiohallinnon tietoturvatasot), jolloin kohteena yleensä on organisaatio ja sen toimintamallit, ja tietojärjestelmien tietoturvatarkastukset, joissa tarkastusten painopiste tyypillisesti on sovelluksen tietoturvallisuuden auditoinnissa. Yksittäisistä tuotteistetuista auditointipalveluista lukumääräisesti eniten organisaatio tekee web sovellusten -tietoturvatarkastuksia.

Viides organisaatio suorittaa ainoastaan sisäisiä auditointeja, jossa auditoinnin kohteena on heidän itse tuottamiensa palveluiden tietoturva. Haastateltu organisaatio ei

tarkemmin määritellyt suoritettavia tietoturva-auditointeja , mutta kaikkien organisaatioiden tarjoamien palveluiden tietoturvan auditointi vaatii mitä todennäköisimmin monien erityyppisten auditointien suoritusta.

11.3 Tietoturva-auditointien kohteet

Haastateltavilta organisaatioilta kysyttiin, minkä eri kohteiden tietoturvaa he auditoivat. Lisäksi heitä pyydettiin mainitsemaan, mitkä ovat heidän yleisimmin auditoimansa kohteet.

Yksi organisaatio kertoo auditoivansa useimmiten palvelukokonaisuuksia, tietojenkäsittelyprosesseja ja tietojenkäsittelyn ylläpitotoimintoja (esim. palveluhankinnassa toimittajan kyvykkyyden ja tarjouksen-/sopimuksenmukaisuuden arviointi). Toinen organisaation puolestaan kertoo yleisimpien auditoitavien kohteiden olevan rakenteilla olevat tietoliikennejärjestelmät.

Kolmas organisaatio kertoi, että tietoturva-auditointien kohteina voivat olla organisaation vaatimustenmukaisuus, tuotekehitysprosessin tietoturva, valmisohjelmistojen konfiguraation tietoturvallisuus (käyttöjärjestelmät, tietokannat, middleware), sovellusten tietoturvallisuus, sovellusten arkkitehtuuri, sovellusten lähdekoodi, suoritettava ohjelma, sulautetut järjestelmät (kuten esim. päätelaitteet tai tietoliikennelaitteet), teollisuusautomaatiojärjestelmät (SCADA), ja tietoverkon tekninen tietoturvallisuus. Yleisimmin auditoituja kohteita ovat organisaatioiden vaatimustenmukaisuus, sekä tietojärjestelmät ja näihin liittyvät web-sovellukset.

Neljäs organisaatio auditoi julkishallinnon kriittisiä ja suuria järjestelmiä, yritysten keskeisiä tietojärjestelmiä, tilintarkastusasiakkaiden osalta tilinpäätösinformaation oikeellisuuteen vaikuttavia (taloushallinnon) järjestelmiä, uusia tai kehitteillä olevia järjestelmiä sekä yritysten toimintatapoja ja prosesseita. Lisäksi he auditoivat toimittajien (Tieto, Logica, Fujitsu jne.) toimintaa ja asiakkaiden järjestelmiä näillä palveluntarjoajilla.

Viides organisaatio laatii vuosittain auditointisuunnitelman, johon valitaan seuraavan vuoden aikana auditoitavat kohteet. Esimerkkejä auditointisuunnitelmassa mainituista

kohteista ovat muun muassa riskikartoituksen päivittäminen, ja salassa pidettävien tietoaineistojen käsittely ja säilytys.

11.4 Organisaatioiden suorittamien auditointien elinkaaret

Kuten luvussa 5 mainittiin, auditointiprosessi voi jakautua vaiheisiin monella eri tavalla, mutta loppujen lopuksi auditoinnin elinkaaren sisältö on kuitenkin hyvin samanlainen. Haastatelluilta organisaatioilta kysyttiin, minkälainen heidän suorittamansa auditointiprosessin elinkaari on yleensä, miten prosessi etenee, ja kauanko prosessi yleensä kestää. Vastauksista käy selväksi, että hyväksyttyjä vaiheisiin jakamistapoja on monia erilaisia.

Yhden haastatellun organisaation käyttämän auditointiprosessin elinkaaren vaiheet ovat suunnittelu, suunnitelman laatiminen, suunnitelman hyväksyntä, auditoinnin toteutus, raportin luonnostelu, havaintojen käsittely, tulosten läpikäynti asiakkaan kanssa ja raportin viimeistely. Yksittäinen auditointi voi olla muutaman päivän tai yli 100 henkilötyöpäivän projekti. Minkä tahansa yksittäisen järjestelmän hyvä auditointi vie ainakin 15 päivää ja sisältää ainakin testauksen verkosta, alustakomponenttien konfiguraation auditoinnin (käyttöjärjestelmä, tietokanta, sovelluspalvelin), (web)sovellustestauksen ja/tai koodiauditoinnin. Lisäksi se voi vielä sisältää ylläpitoprosessien auditoinnin ja fyysisen tilan auditoinnin.

Haastateltu organisaatio täsmensi vielä, että hyvä auditointi vaatii paljon manuaalista työtä ja osaamista, eikä auditointi hoidu yksinkertaisesti ajamalla automatisoituja työkaluja ja lähettämällä niiden generoimia raportteja asiakkaalle. Lisäksi auditointi kertoo vain sen hetkisen tilanteen, joten on viisasta tehdä seuranta-auditointi säännöllisesti, kuten esimerkiksi puolivuosittain ja muutosten yhteydessä.

Toinen haastatelluista organisaatioista kertoi, kuinka tietojärjestelmiin liittyvät tarkastukset jakautuvat neljään työvaiheeseen: tarkastuksen suunnittelu, tarkastuksen valmistelu, tarkastus, tarkastusten tulosten esittely. Tarkastuksen suunnitteluvaiheessa määritellään kyseessä olevan tarkastuksen rajaukset, työmenetelmät ja -välineet sekä tarkastuksen aikataulun, työmäärän ja lopputulokset. Tarkastussuunnitelma käydään läpi asiakkaan kanssa tarkastuksen kick-off-palaverissa, jossa voidaan vielä tarkentaa

tarkastuksen rajauksia. Itse tarkastus tehdään suunnitelman mukaisesti. Tarkastuksen havainnot luokitellaan kriittisyyden mukaan ja jokaiseen havaintoon kirjataan kriittisyysluokan kuvaus havainnosta ja suositukset korjaaviksi toimenpiteiksi. Tarkastuksen lopputulokset ja johtopäätökset raportoidaan asiakkaalle ja käydään yhdessä läpi tarkastuksen lopetuspalaverissa. Jos kyseessä on vaatimustenmukaisuusauditointi (esim. PCI DSS). Auditoinnin tuloksena asiakas on joko vaatimusten mukainen tai ei ole vaatimusten mukainen. Jos asiakas on vaatimustenmukainen ja palveluun kuuluu sertifiointi, myönnetään tarkastetulle kokonaisuudelle ko. sertifikaatti. Kalenteriajassa auditoinnit aloituspalaverista lopetuspalaveriin kestävät tyypillisesti 4 - 6 viikkoa.

Kolmas organisaatio kuvaili elinkaaren vaiheet seuraavasti: auditoidaan suunnitelman mukainen kohde, analysoidaan auditointi, tehdään korjaus- ja parannusehdotus, varmistetaan ja valvotaan muutokset käytäntöön. Prosessi kestää mahdollisesti muutaman kuukauden.

Neljäs organisaatio kertoi, että tietoturva-auditointiprosessi yleensä alkaa projektin kartoituksella, josta edetään työmääräarvioon. Tämän jälkeen asiakaan päätettyä hankinnasta työ etenee aloituskokoukseen, jossa työn sisältö määritellään tarkemmin yhdessä aikataulun ja muiden työhön vaikuttavien tekijöiden kanssa. Tämän jälkeen suoritetaan itse auditointi jonka tuloksena asiakkaalle tuotetaan loppuraportti joka esitellään loppukokouksessa. Normaalin projektin kesto alusta loppuun on kahdesta kolmeen kuukautta riippuen asiakkaan ja auditoijien muista työkiireistä.

Viidennen organisaation mukaan auditointiprosessi alkaa arviointitavoitteen määrittelyllä ja siitä sopimisella. Vaiheeseen kuuluu myös toimeksianto. Seuraava vaihe on lähdetietojen ja vaatimusten kerääminen. Tiedon keräyksen jälkeen tiedot analysoidaan, ja analysoinnin pohjalta suunnitellaan auditointi ja määritellään sen kriteeristö. Seuraavien kolmen vaiheen aikana suoritetaan varsinainen auditointi. Nämä vaiheet ovat kohteen katselmointi, vastuuhenkilöiden haastattelut sekä ohjeiden ja dokumentaation arviointi. Näitä vaiheita seuraa tulosten analysointi ja niiden vertailu vaatimuksiin. Tulosten analysoinnin jälkeen laaditaan kehitysehdotukset. Tämän jälkeen kehitysehdotukset käsitellään kohteen kanssa. Viimeinen vaihe on auditoinnin raportointi ja raportin esittely. Prosessi kestää kalenteriajassa muutaman viikon.

11.5 Käytetyt viitekehykset

Haastatelluilta organisaatioilta kysyttiin, mitä eri asioita he käyttävät auditoinnin viitekehyksinä. Heitä pyydettiin kertomaa, käyttävätkö he aina jotain tiettyjä standardeja, vai määräytyvätkö käytettävät viitekehykset asiakaskohtaisesti. Asiakaskohtaisilla viitekehyksillä tarkoitetaan organisaation omia tietoturvapolitiikkoja, heidän liiketoimintansa arviointiin soveltuvia standardeja, ja niitä tietoturva-asetuksia, joita organisaatioiden tietoturvan tulee vastata.

Yksi organisaatioista kertoi käyttävänsä auditoinneissaan sekä asiakaskohtaisia viitekehyksiä että valtiohallinnossa valtiohallinnon omia viitekehyksiä (TTT-tasot, Vahti, KATAKRI). Toinen organisaatio kertoi heidän suorittamiensa auditointien perustuvan ISO 27001- ja ISO 17799 -standardeihin sekä Valtionhallinnon yleisiin VAHTI-ohjeisiin.

Kolmas organisaatio kertoi, että viitekehys määräytyy aina asiakaskohtaisesti. Viitekehyksinä voivat toimia esimerkiksi toimialan ja valmistajien yleisohjeet ja tarkastuslistat, standardit, säädökset ja viranomaisten ohjeet, alalla esitellyt uudet poikkeamat ja virhelistat sekä auditoijien omat kokemukset aiemmista auditoinneista.

Neljäs organisaatio kertoi, että viitekehys määräytyy asiakas- ja tapauskohtaisesti, mutta usein he käyttävät asiakkaan omia politiikkoja ja ohjeita, järjestelmien määrittelyjä, sopimuksia, ISO 27001 -standardia, Katakri-kriteeristöä, Tietoturvatasoja, Vahti-ohjeistusta, BS 259999 –standardia, COBIT-kehystä, OWASP-kehystä, teknologioihin liittyviä määrityksiä sekä organisaation omia suosituksia.

Viides organisaatio kertoi käyttävänsä tarkastusten viitekehyksinä alan tunnettuja standardeja tapauskohtaisesti niin, että yleisimmille tarkastuksille he ovat määritelleet käytettävän viitekehyksen. Vaatimustenmukaisuusauditoinneissa he käyttävät luonnollisesti sitä vaatimussettiä, jota tietoturvan tulee vastata, kuten esim. PCI DSS tai Valtiohallinnon Tietoturvatasot. Web-sovellustarkastuksissa tyypillinen vaatimussetti on OWASPin ASVS, sovelluskehitysprosessin tarkastuksissa yleinen vaatimussetti on OpenSAMM. Muita yleisesti käytettyjä viitekehyksiä ovat esimerkiksi CISin tarkastuslistat. Joillekin asiakkaille tarkastuksia tehdään asiakkaan määrittelemien vaatimusten mukaisesti.

11.6 Käytetyt auditointimenetelmät ja -työkalut

Haastatelluilta organisaatioilta kysyttiin, mitä eri auditointimenetelmiä ja -työkaluja he käyttävät auditointeja suorittaessaan. Auditointimenetelmät ja työkalut luonnollisesti riippuvat auditoitavista kohteista, mutta vastauksista kuitenkin pystyy näkemään, mitkä työkaluista ja menetelmistä ovat kaikkein suosituimpia ja käytetyimpiä.

Yksi organisaatioista vastasi käyttävänsä automatisoitua tietoturvaskannauksia sekä haastatteluja. Esimerkkeinä työkaluista he mainitsivat Nessus, Burp Suite ja Acunetix työkalut. Toinen organisaatio kertoi katselmoivansa tarkastettavat kohteet ja haastattelevansa henkilöstöä. Lisäksi he hyödyntävät auditoinnissa käyttämiinsä standardeihin ja ohjeisiin liittyviä tarkastuslistoja.

Kolmas organisaatio kertoi suorittavansa haastatteluita, dokumentaation analysointia ja vertailua, ja kohteiden katselmointia havainnoimalla. Järjestelmien tarkastuksessa he hyödyntävät niiden omia hallintatyökaluja, eivätkä käytä erityisesti mitään järjestelmätarkastuksiin suunniteltuja auditointiohjelmistoja.

Neljäs organisaatio käyttää todella monia työkaluja apuna suorittamissaan auditoinneissa, mutta erityismaininnan sai heidän luomansa penetraatiotestausmenetelmä (penetration testing methodology), joka sisältää kymmeniä työkaluja eri tarkoituksiin. Osa työkaluista on heidän itse kehittämiään, osa ilmaisia ja lisäksi heillä on globaalit sopimukset erilaisten työkalujen toimittajien kanssa. Työkalujen käyttämisen lisäksi he myös katselmoivat dokumentaatioita ja suorittavat haastatteluita.

Viides organisaatio kertoo, että vaatimustenmukaisuuksien auditoinnissa käytetyt työmenetelmät ovat tyypillisesti haastattelut, dokumenttien katselmoinnit ja tekniset tarkastukset. Teknisten tarkastusten työvälineet ja menetelmät puolestaan riippuvat tarkastettavasta kohteesta. Tietojärjestelmien tarkastuksessa tyypillisiä menetelmiä ovat sovelluksen arkkitehtuurin katselmointi, riskianalyysi, uhkatyöpaja, lähdekoodin katselmointi, manuaalinen sovelluksen tietoturvatestaus, haavoittuvuusskannaus, käyttöjärjestelmien, tietokantojen ja middlewaren konfiguraation tarkastus, murtotestaus (penetraatiotestaus) sekä protokollan fuzzaus.

Tietojärjestelmien tarkastuksissa käytettyjä työvälineitä ovat tarkastuslistat, haastattelut, työpajat, porttiskannerit (kuten Nmap), haavoittuvuusskannerit (kuten Nessus ja Acunetix), sovellustestauksessa proxy-työvälineet (kuten Burb), lähdekoodianalysaattorit, fuzzerit, exploit frameworkit (kuten Metasploit ja Canvas) sekä lukuisat custom-ohjelmat eri tyyppisiä kohteita varten.

11.7 Yleisimmin havaitut puutteet tietoturvassa

Haastatelluilta organisaatioilta kysyttiin, mitkä ovat yleisimmin auditoinnin kautta havaitut puutteet asiakkaiden tietoturvassa. Useat vastaajista kokivat kysymykseen vastaamisen haastavaksi, mikä todennäköisesti johtuu siitä, että he eivät omakohtaisesti olleet havainneet joitain tiettyjä puutteita useammin kuin muita. Auditoinnit ja auditoitavat kohteet voivat olla hyvinkin erilaisia, ja luonnollisesti havaitut puutteet myös vaihtelevat paljon eri auditointien välillä.

Yksi organisaatioista kertoo yleisimmin havaittujen puutteiden olevan järjestelmien pohjana olevien käyttöjärjestelmien haavoittuvuudet. Toinen organisaatioista ei osaa eritellä puutteita tarkemmin.

Kolmas organisaatio kertoo puutteiden olevan niin moninaisia, että mitään muutamaa yksittäistä puutetta on vaikea yksilöidä. Tietoturvan osa-alueista sovellusten tietoturvallisuus on kuitenkin sellainen, jossa tyypillisesti on organisaatioissa eniten puutteita.

Neljäs organisaatio erittelee puutteet auditointikohteiden mukaan. Yleisiä puutteita toiminnassa ovat seuraavat asiat: ei tunneta omaan toimintaan kohdistuvia vaatimuksia (esim. yksityisyyden suoja henkilötietoja käsiteltäessä), riskienhallinta ei ole määrämuotoista, eikä perustu asiakkaan johdon vahvistamiin toiminnan tavoitteisiin, ohjaus, valvonta ja raportointi on puutteellista, eikä organisaatiolla ole toipumissuunnitelmia poikkeustilanteiden varalle.

Tekniikassa puolestaan havaitaan usein seuraavia puutteita: tarpeettomia palveluita on päällä ja portteja auki, ei tunneta järjestelmäkokonaisuuden riippuvuuksia ja heikkoja kohtia (esim. single-point-of-failure), salaus- ja tunnistusmekanismit eivät täytä asetettuja vaatimuksia, salassa pidettävää aineistoa käsitellään ilman asianmukaista

suojausta, järjestelmää ei ole testattu käyttöönoton yhteydessä, ja päivityksiä ei tehdä, ei varsinkaan suunnitelmallisesti (testaus jne.).

Viides organisaatio kertoo, että usein henkilöstön jäsenten vastuut ovat epäselvät, eli ei ole sovittu kuka tekee mitä, mikä johtaa siihen, että kukaan ei tee mitään. Lisäksi usein havaittuja puutteita ovat muutoshallinnan ja konfiguraation hallinnan puutteet, huono suunnittelu, jolloin ei tehdä turvallisia järjestelmiä, ja huono ylläpito, mikä voi ilmetä esimerkiksi niin, että jos muistetaan päivittää käyttöjärjestelmä, niin ei kuitenkaan todennäköisesti päivitetä sovelluksia.

11.8 Tietoturva-auditoinnin ongelmat

Organisaatioilta kysyttiin, mitä eri ongelmia ja haasteita auditoinnin elinkaaren aikana ilmenee. Kaikkein yleisimmät ongelmat liittyivät aikatauluihin, niiden yhteensovittamiseen ja ennalta arvaamattomuuteen.

Yksi haastatelluista organisaatioista kertoo, että vaikeinta on saada käyttäjät noudattamaan ohjeita ja saada muutettua asenteet kohdalleen. Toisen organisaation kokemuksen perusteella eri osapuolten aikataulujen yhteensovittaminen on auditoinnissa kaikkein haastavinta.

Kolmas organisaatio kertoo, että tyypilliset ongelmat liittyvät tarkastusten aikataulujen vaikeaan ennakoitavuuteen. Tarkastusten aikataulut siirtyvät helposti, jos esimerkiksi tarkastettava tuote ei olekaan tarkastettavassa kunnossa kun tarkastus pitäisi aloittaa. Myös tekniset järjestelyt tarkastusta varten viivästyttävät tarkastuksen aikataulua usein. Auditointien resursointi on haastavaa tilanteessa, jossa aikataulut viivästyvät jatkuvasti.

Neljännen organisaation mukaan jaetut resurssit, kuten web-hotelleissa olevat sovellukset tai pilvipalvelut on vaikeita testata. Kriittisen infran testaamisessa on todellisten ja jopa fyysisten vahinkojen mahdollisuus. Yleensä auditointikuvioon liittyy myös asiakkaan toimittajia, joilla on asioista omat näkemyksensä ja tarjolla erilaisia NDA- ja muita sopimuksia, jotka oikeasti kuuluisi hoitaa kuntoon auditoijan asiakkaan ja auditoijan asiakkaan toimittajan välillä. Auditoijalla on sopimus oman asiakkaansa kanssa, ei asiakkaan toimittajan.

Viidennen organisaation mielestä haastavinta on se, kun asiakkaalla ei ole olemassa aineistoa, josta selviäisi toiminnan tai järjestelmän vaatimukset, tai asiakkaalla ei ole osoittaa näyttöjä suoritetuista toimenpiteistä. Haastateltavat saattavat myös jättää asioita kertomatta, jos pelkäävät saavansa rangaistuksen havaituista puutteista. Auditoinnin kohde ei myöskään aina ymmärrä auditoinnin tavoitetta tai luonnetta.

11.9 Asiakkaiden suhtautuminen auditointeihin

Haastatelluilta organisaatioilta kysyttiin, miten asiakkaat suhtautuvat auditointeihin ja auditoinnin jälkeisiin tuloksiin. Tietoturva ja sen auditointi on tärkeää asiakasorganisaatioiden liiketoiminnan kannalta, mutta auditoinnin kohteena oleminen sekä tietoturvapuutteista ja tietoturvan parantamiseksi tarvittavista muutoksista kuuleminen tuskin on kenestäkään mukavaa. Auditointeihin suhtautumiseen vaikuttaa kuitenkin merkittävästi se, haluaako kohteena oleva organisaatio itse auditointia heidän tietoturvansa laadun kehittämistä ajatellen, vai onko se jonkin muun tahon vaatima välttämätön paha.

Yksi organisaatioista kertoo heidän asiakkaidensa suhtautuvan auditointeihin vakavasti ja asiallisesti. Toinen organisaatio kuitenkin kertoo, että asiakasorganisaation henkilöstö suhtautuu auditointeihin useimmiten varauksella. Vakiintuneisiin käytäntöihin kajoaminen ja niiden muuttaminen saattavat aiheuttaa närkästymistä. Yleensä auditoinnin palautteeseen reagoidaan kuitenkin positiivisesti ja tarvittaviin toimenpiteisiin ryhdytään välittömästi.

Kolmas organisaatio kertoo, että asiakkaat suhtautuvat positiivisesti, jos ovat itse tilanneet auditoinnin. Jos eivät ole, vaan se on tehty jostain muusta syystä, niin asiakkaiden suhtautuminen vaihtelee. Hyvän auditoinnin tulokset ovat aina kuitenkin hyödyllisiä. Valitettavasti monesti tuloksista aiheutuu toimenpiteitä, joiden kustannuksista asiakas ja heidän toimittajansa - esimerkiksi sovelluksen koodannut firma - eivät ole sopineet mitään, mistä seuraa paljon keskustelua ja sopimista.

Neljännen organisaation mukaan suhtautuminen auditointiin riippuu siitä, millä motiivilla tarkastukset on tilattu. Mikäli kyseessä on vaatimustenmukaisuuden auditointi jostain ulkoisesta vaatimuksesta, on auditointi auditoitavalle pahimmassa tapauksessa

välttämätön paha, joka pitää saada pois päiväjärjestyksestä mahdollisimman pienillä kustannuksilla ja vähäisellä vaivalla, niin että tarvittavat "leimat" saadaan paperiin. Useimmiten kuitenkin auditoinnin tilannut taho on aidosti kiinnostunut siitä mikä on tietoturvallisuuden tila auditoitavassa kohteessa.

Auditoinnin tilaamiseen motiivina voi olla muun muassa ulkoiset vaatimukset (esim. PCI DSS), sisäiset vaatimukset (esim. sisäinen tarkastus tai tuotekehitysprosessissa määritelty osa), tai liiketoiminnan riskienhallinta. Tarkastuksen kohteena oleva organisaatio ei välttämättä ole sama kuin tarkastuksen tilannut (asiakas), joten suhtautumisessa on eroja tässäkin mielessä.

Asiakkaat tyypillisesti suhtautuvat asiaan kuuluvalla vakavuudella tarkastuksen havaintoihin ja asiakkaat yleensä ovat sitoutuneita huolehtimaan siitä, että tarkastuksen havainnot huomioidaan ja niille tehdään suosittelemamme korjaavat toimenpiteet. Usein asiakkaat kokevat auditoinnit myös hyvänä tilaisuutena kasvattaa oman organisaationsa tietoturvatietoisuutta ja -osaamista.

Viidennen organisaation mukaan suurin osa on tyytyväinen löydöksiin, vaikka ne olisivat negatiiviset. Kehitystarpeiden kustannukset voivat kuitenkin huolestuttaa, mikä voi vaikuttaa auditoinnin jälkeiseen riskianalyysiin, mikä ilmenee sen vääristymisellä. Harva asiakas kiistää havaintoja, mutta osa kiistää niiden merkityksen.

11.10 Auditointien hinta

Haastatelluilta organisaatioilta kysyttiin myös, paljonko he veloittavat suorittamistaan auditoinneista. Kysymys on hieman arkaluontoinen ja se, että yksi haastateltava ei halunnut vastata kysymykseen, on täysin ymmärrettävää. Kysymys perustuu täysin tutkielman tekijän omaan uteliaisuuteen, eikä annetuista vastauksista ole tehty tämän tutkielman kannalta mitään olennaisia päätelmiä.

Yksi organisaatio kertoi, että heidän suorittamiensa auditointien päivähinnan olevan 1200-1700 euroa riippuen tarvittavasta asiantuntemuksesta. Toinen organisaatio ilmoitti heidän suorittamansa auditointien maksavan noin 1000 euroa henkilötyöpäivää kohden.

Kolmas organisaatio ei osannut antaa yksiselitteistä vastausta, koska auditointeja on niin monenlaisia. Halvimmat heidän tekemistään auditoinneista ovat maksaneet muutamia tuhansia euroa ja kalleimmat yksittäiset auditoinnit satoja tuhansia euroja. Globaalisti heillä on myös asiakkaita, joiden tietoturva-auditoinneista he ovat veloittaneet yli 20 miljoonaa euroa vuodessa per asiakas. Esimerkiksi erään Brittipankin toimittajien auditointi yhden tietovuodon jälkeen maksoi noin kahdeksan miljoonaa puntaa parissa kuukaudessa.

Neljäs organisaatio kertoi, että he eivät luonnollisesti veloita mitään omalle organisaatiolleen suorittamista sisäisistä auditoinneista.

11.11 Tietoturva-auditoinnin tulevaisuus

Organisaatioilta kysyttiin, uskovatko he tietoturva-auditoinnin kehittyvän tulevaisuudessa, miten, ja miten he toivoisivat sen kehittyvän. Kaikki vastanneet organisaatiot uskovat tietoturva-auditointien kehittyvän, ja ovat kertoneet miten, mistä syystä, ja millaisia vaikutuksia kehityksellä on. Lisäksi organisaatioiden edustajat kertoivat, miten he toivoisivat tietoturva-auditointien kehittyvän parhaimmassa tapauksessa.

Yksi organisaatioista uskoi sen tulevan enemmän ja enemmän osaksi yritysten ja organisaatioiden jatkuvaa tietoturvan hoitoa. Toinen organisaatioista sanoi viranomaisten tietojärjestelmien tarkastusvelvoitteiden ja hyväksymismenettelytapojen kehittyvän, jolloin järjestelmät joissa käsitellään kansallista tai kansainvälistä salassa pidettävää aineistoa, tulee arvioida. Säädökset siitä, kuka on hyväksytty arvioija, tulee järjestämään auditointipalvelumarkkinoita huomattavasti.

Kolmas organisaatio sanoo tietoturva-auditointien ja niissä käytettyjen menetelmien kehittyvän samalla, kun tekniikka ja toteutukset kehittyvät. Paras kehitys olisi heidän mielestään se, että auditointia ei tehtäisi vasta sitten, kun on tehty uusi järjestelmä, vaan ja heti alkuun suunnitelmien pohjalta paperilla. On ikävää kahden vuoden sovelluskehitystyön jälkeen tulla toteamaan, että ”huonon teitte, ja tuotantoonkin pitäisi mennä eilen”.

Neljännen organisaation mielestä on selvästi havaittavissa, että turvallisuusasioihin on alettu panostamaan yhä enemmän. Tämän johdosta myös auditoinnit tulevat yleistymään ja muuttuvat vaativimmiksi. Auditointeja tehdään useamman tahon toimesta. Valtionhallinnon tietoturva-asetuksen mukaiset tasovaatimukset perus-, korotetulle- ja korkealle tasolle määräävät heidän organisaatiotaan ohjautumaan vuoden 2015 loppuun mennessä oikealle tielle. Auditoinnit tulevat tulevaisuudessa todennäköisesti pohjautumaan tasovaatimuksiin liittyvän tietoturvallisuustyökalun käytön osoittamiin ongelmakohtiin.

Viidennen organisaation mukaan ulkoiset vaatimukset tietoturvallisuuden varmistamiselle tulevat kasvamaan. Tietoturvan varmistaminen organisaatioissa ja tuotekehitysprosesseissa tulevat tulevaisuudessa olemaan tarkemmin säädeltyjä valtionhallinnon ja eri toimialojen toimesta (esim. energia-ala ja SCADA, tai maksukortit ja PCI). Auditointien viitekehykset, standardit ja menetelmät kehittyvät ja syntyy uusia kansainvälisiä viitekehyksiä, standardeja ja menetelmiä eri toimialoille. Sovellustietoturva-auditointien painopiste siirtyy vähitellen tuotekehityksessä pois prosessin loppupäästä kohti alkupäätä, ja integroituu osaksi prosessia. Vaatimustenmukaisuus organisaatioissa tulee lisääntymään ja tätä myöten myös tarve tietoturva-auditoinneille lisääntyy.

Tietoisuus tietoturvallisuudesta ja varsinkin sovellustietoturvallisuudesta tulee kasvamaan tietojärjestelmiä ostavissa organisaatioissa. Tätä myötä myös tietojärjestelmiä toimittavilta organisaatioilta tullaan toteutusprojekteissa vaatimaan parempaa ja tarkempaa näyttöä tietojärjestelmien turvallisuudesta.

Organisaation edustaja toivoo, että "tietoturva" -termistä ja -käsitteestä siirryttäisiin pois kohti tietovastuuta. Tietoturvallisuus sanana assosioidaan usein teknisiin kontrolleihin, kuten palomuureihin, virustorjuntaan tai auditointiin. Karrikoidusti sanottuna usein tietoturva käsitetään asiana, jonka tilasta yrityksen johto ei ole tietoinen, vaan "asiaa meillä hoitaa se palvelinkonesalin palomuuriasiantuntija" tai korkeintaan yrityksen CISO. Suurin osa tietoturvallisuuteen liittyvistä ongelmista johtuu kuitenkin siitä, että yrityksen johto ei ole ottanut vastuuta tietovarojensa hallinnoinnista, jakamisesta ja luokittelusta. Siksi pitäisi puhua ennemmin tietovastuusta kuin tietoturvallisuudesta. Peilaten esimerkiksi julkisuudessa olleisiin viimeaikaisiin tietovuotoihin, eri osapuolet

(tietojärjestelmien tai palvelun omistaja, tietojärjestelmien kehittäjät, tietojärjestelmien ylläpidon palveluntarjoajat jne.) eivät ole kantaneet omaa tietovastuutaan. Toivottu kehityssuunta tässä olisi siis se, että tietovastuu tulisi yrityksen johdon agendalle.

12 POHDINTA

Tietoturva-auditointiin liittyy paljon monipuolista termistöä ja kategoriointia, mutta yleisellä tasolla auditoinnin suoritus noudattaa aina samaa kaavaa. Mikään auditointi ei kuitenkaan ole täysin samanlainen kuin toinen, koska auditoinnin tarkoitus on aina kohdeorganisaation tietoturvan nykytason selvittäminen organisaation parasta ajatellen. Kohdeorganisaation liiketoiminta, siihen kohdistuvat tietoturvariskit, ja kyseessä olevalle auditoinnille asetetut tavoitteet tekevät jokaisesta auditoinnista yksittäistapauksen.

Se, että jokainen auditointi on suunniteltava ja toteutettava yksittäistapauksena, ja että laadukkaan auditoinnin suoritus vaatii auditoijalta ammattitaitoa monelta eri osa-alueelta, tekee auditoijan työstä ajoittain todella haastavan. Auditoijan täytyy tietää paljon tietoturvasta, eri teknologioista, kohdeorganisaation liiketoiminta-alueesta, omata hyvät vuorovaikutus- ja testaustaidot sekä pystyä pysymään puolueettomana arvioijana koko auditointiprosessin ajan.

Vaikka tietoturvan auditointiprosessi on haastava ja vie paljon resursseja, tulisi sen silti olla säännöllinen osa jatkuvaa tietoturvan harjoittamista. Vaikka tietoturvan tärkeys nykypäivänä ymmärretäänkin laajasti, saattaa arkipäiväisten toimien yhteydessä tapahtua sen vähättelyä. Vielä useammin unohdetaan, että tietoturvan taso tulisi auditoida säännöllisesti. Kun organisaation liiketoiminta kehittyy ja sen etuudet muuttuvat, tulee sen näkyä myös muutoksina tietoturvassa, mitä puolestaan tulisi seurata kyseisten muutosten auditointi.

Tietoturvasta huolehtiminen ei ole kuitenkaan ainoastaan organisaation johdon ja eri tietojärjestelmien ylläpitäjien vastuulla, vaan tärkeintä on, että kaikki organisaation työntekijät noudattavat organisaation tietoturvapolitiikkaa ja kantavat kortensa kekoon organisaation kattavan tietoturvan takaamiseksi. Kaikki organisaation työntekijät eivät kuitenkaan välttämättä edes tiedä, missä heidän organisaationsa tietoturvapolitiikka on, tai miten heidän tulisi huomioida se omassa työssään. Täytyy siis toivoa, että tietoturvan – kuten myös sen auditoinnin – tulevaisuudessa myös niin sanottu tavallinen työntekijä ymmärtää vastuunsa organisaation tietoturvan kannalta.

LÄHTEET

[DaS11] Davis C., Schiller M. (2011): *IT Auditing: Using Controls to Protect Information assets*. McGraw-Hill Companies, Yhdysvallat.

[Jac10] Jackson C. (2010): *Network Security Auditing*. Cisco Press, Indianapolis.

[Moe10] Moeller R. (2010): *IT Audit, Control and Security*. John Wiley & Sons Inc., Hoboken.

[Int12] International Organization for Standardization (2008) *ISO/IEC 27001:2005*. International Organization for Standardization, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

[Tie04] Tietokone (2004) *Auditointi tarkastaa tietoturvan tason.* Pertti Hämäläinen, http://www.tietokone.fi/lehti/tietokone_13_2004/auditointi_tarkastaa_tietoturvan_tason_2738.

[Laa10] Laatumatkalla (2010) *Auditointien tuskasta prosessien itsearviointien ahaa elämyksiin.* Jussi Moisio, http://laatumatkalla.fi/2010/10/auditointien-tuskasta-prosessien-itsearviointien-ahaa-elamyksiin.

[Suo11] Suomen Puolustusministeriö (2011) *Katakri*. Suomen Puolustusministeriö, http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf.

[Val12a] Valtionvarainministeriö (2012) *Tietoturvallisuus*. Valtionvarainministeriö, http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp.

[Val12b] Valtionvarainministeriö (2012) *Valtionhallinnon tietoturvallisuus.* Valtionvarainministeriö, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/index.jsp

[Val08] Valtionvarainministeriö (2008) *Tietoturvatasot*. Valtionvarainministeriö, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/02_TTT-kaesikirja-20081029.pdf.

[Tig10] TigerTeam (2010) *Valtion tietoturva-asetus hyväksyttiin – mitä siitä tulee tietää.* Jarkko Holappa, http://www.nixu.fi/blogi/2010/heinakuu/valtion-tietoturva-asetus-hyvaksyttiin/.