BS 7799, Tietoturvan Hallinta

Matti Johansson

Helsingin yliopisto
Tietojenkäsittelytieteen laitos
Seminaari: Tietoturvallisuus
nykyaikaisessa
liiketoimintaympäristössä
Helsinki 20.4.2003

BS 7799, Tietoturvan Hallinta

Matti Johansson

Helsingin yliopisto
Tietojenkäsittelytieteen laitos
Seminaari: Tietoturvallisuus nykyaikaisessa liiketoimintaympäristössä
Helsinki 20.4.2003

Tietoturva on viime vuosina tullut entistä tärkeämmäksi monille organisaatioille. Tähän on vaikuttanut erilaisten (etenkin tietoliikenteen mahdollistamien) tietoturvauhkien lisääntyminen mutta myös organisaatioiden lisääntynyt valveutuneisuus asiassa. Tietoturvan tärkeys on huomattu myös erilaisissa standardointielimissä. Yksi organisaatioiden tietoturvan hallintaan liittyvä tietoturvastandardi on BS 7799. Noudattamalla tätä standardia organisaatio luo itselleen tietoturvan hallintajärjestelmän, joka oikein ylläpidettynä auttaa organisaatiota suojamaan sen liiketoiminnan kannalta tärkeät tietopääomat ja järjestelmät.

Avainsanat: BS 7799, tietoturvan hallintajärjestelmä, organisaatioiden tietoturva

Aiheluokat (The ACM Computing Classification System 1998): K.4.1, K.6

Sisältö

1 Johdanto

Organisaatioiden yksi tärkeimmistä pääomista on tieto kuten esim. pankeilla asiakkaiden tili- ja luottotiedot, maistraateilla niiden ylläpitämät rekisterit sekä ohjelmistoyrityksillä lähdekoodit. Organisaation hallussa oleva tieto on erittäin tärkeässä asemassa, kun ajatellaan liiketoiminnan jatkuvuutta ja kasvua. Ihmiset pitävät yleensä hyvää huolta siitä, että heidän asuntonsa ja omaisuutensa on suojattu luvattomalta käytöltä, varkauksilta sekä vahingoilta. Jokaisen organisaation tulisi suoda tiedolle samanlainen suoja. Tietoon kohdistuvalla rikoksella tai vahingolla saattaa organisaation tulevaisuuden kannalta olla paljon suuremmat vaikutukset kuin etukäteen tulee ehkä ymmärtäneeksi. Tiedon tuhoutuminen tai sen joutuminen vääriin käsiin saattaa vaikuttaa liiketoiminnan kilpailukykyyn, taloudelliseen kannattavuuteen tai vahingoittaa organisaation mainetta. Tärkeän tiedon menetys voi pahimmassa tapauksessa asettaa koko organisaation toiminnan uhatuksi.

Tietoa voi esiintyä monessa eri muodossa. Sitä on tallennettuna tietokoneella, sitä siirretään pitkin verkkoa, tulostetaan tai kirjoitetaan paperille tai se esiintyy esim. keskusteluissa. Oli tieto sitten missä muodossa tahansa, niin organisaation kannalta tärkeän tiedon tulisi aina täyttää seuraavat vaatimukset; tietoon saa päästä käsiksi vain siihen oikeutetut (salassapito), tieto on paikkansapitävää ja eheää (koskemattomuus), valtuutettu henkilö pääsee halutessaan tietoon käsiksi (saatavuus). [BS99a]

Organisaatiot joutuvat nykyään varautumaan moniin erilaisiin tilanteisiin, joissa näitä tiedolle asetettuja vaatimuksia uhataan. Näitä tilanteita ovat sisä- ja ulkoverkosta tulevat hyökkäykset, virukset, tietokoneavusteiset petokset, vakoilu, sabotaasi sekä myös tulipalot ja vesivahinkojen aiheuttamat tuhot. Tiedon turvaamista vaikeuttaa entisestään se, että nykyään organisaatiot ovat entistä enemmän riippuvaisia tietoverkkojen informaatiojärjestelmistä sekä palveluista. Organisaatioiden sisäisten verkkojen sekä julkisten verkkojen yhteenliittyminen sekä resurssien jakaminen verkossa tekevät tiedon turvaamisen vaikeaksi. [BS99a]

Tiedon turvaaminen nykypäivänä on erittäin hankala tehtävä ja organisaatio, joka haluaa turvata liiketoimintansa jatkuvuuden, ei voi olla kiinnittämättä siihen huomiota. Ilman kunnon suunnittelua ja tietoturvaa varmistavia sekä kohottavia toimenpiteitä organisaatio ei voi uskotella, että sen tieto olisi hyvässä turvassa.

Tässä paperissa käsitellään brittiläistä tietoturvastandardia BS 7799, jonka tarkoituksena on opastaa organisaatioita parantamaan tietoturvaa ja varautumaan etukäteen tietoturvauhkiin. Luvussa 2 esitellään tämä standardi ja käydään läpi sen historiaa. Standardin sisältöön

perehdytään tarkemmin luvussa 3. Luvussa 4 käydään läpi standardin noudattamisen vaiheet sekä mahdollinen sertifiointi. Luku 5 sisältää pohdintaa siitä, kuinka tarpeellista sertifiointi organisaatioille on.

2 BS 7799 tietoturvastandardi

BS 7799 on tietoturvastandardi, jota noudattamalla organisaatio pystyy suunnittelemaan ja toteuttamaan tietoturvan hallinnan omien tarpeittensa mukaan. Tietoturva nykyajan organisaatioissa on hyvin laaja käsite ja hyvän tietoturvan rakentaminen ei suinkaan ole helppoa. BS 7799 standardi ottaa kantaa organisaatioiden tämän hetken yleisimpiin tietoturvaan liittyviin ongelmatilanteisiin ja sisältää joukon toimintamalleja kuinka näitä ongelmia voidaan ratkoa. Standardi ei käsittele pelkästään tietoliikennettä vaan keskittyy yleiseen liiketoiminnan turvaamiseen tähtäävään tietoturvaan.

Standardia seuraamalla organisaatio pystyy luomaan itselleen tietoturvan hallintajärjestelmän, jonka tarkoituksena on ylläpitää organisaation toiminta sellaisella tasolla, että halutut tietoturvan vaatimukset pystytään täyttämään. Standardi on tällä hetkellä jaettu kahteen osaan. Ensimmäinen osa on lähinnä kokoelma hyväksi havaittuja toimintamalleja ja tapoja, joita noudattamalla erilaisia tietoturvaan liittyviä riskejä ja uhkia voidaan hallita. Toinen osa taas esittelee prosessin, jolla tietoturvan hallintajärjestelmä tulisi toteuttaa, sekä sisältää toteutukseen liittyvät vaatimukset.

BS 7799 standardin noudattamisessa tärkeä osa on riskienhallinnassa. Organisaation tulee pystyä tunnistamaan liiketoimintaan liittyvät tietoturvariskit, arvioida näiden suuruus ja tämän perusteella suunnitella toimintansa niin, että riskit voidaan minimoida hyväksyttävälle tasolle. Standardi sisältää joukon valvontatoimenpiteitä, joiden tarkoituksena on auttaa organisaatiota varautumaan uhkiin etukäteen. Näistä valvontatoimenpiteistä organisaatio voi valita sopivimmat tunnistettujen riskien minimointia varten. [Ken00]

2.1 Standardin historia

Iso-Britannian Kauppa- ja Teollisuusministeriö (UK Department of Trade and Industry, DTI) perusti 1990-luvun alussa työryhmän, joka koostui kokeneista tietoturva-asiantuntijoista. Tämä ryhmä tuotti tietoturvan hallintaa koskevan menettelytapaohjeen (Code of Practice for Information Security Management), joka julkaistiin syyskuussa 1993. Tämä menettelytapaohje muodosti perustan brittiläiselle standardille (British Standard) BS 7799, joka julkaistiin vuonna 1995 (BS7799:1995). [Gam03b]

Koska standardin ensimmäinen versio ei sisältänyt tarkkoja vaatimuksia siitä kuinka organisaatioiden tietoturva tulisi toteuttaa, ei organisaatioita pystynyt sertifioimaan standardia vasten. Vasta kun standardiin lisättiin toinen osa (BS7799-2:1998, Specification for Information Security Management Systems), joka asetti tarkat vaatimukset standardin noudattamisesta, tuli sertifiointi mahdolliseksi. [Gam03b]

Vuonna 1999 standardi (molemmat osat) tarkastettiin sekä päivitettiin ja siihen lisättiin uusia ohjeistuksia, jotka huomioivat informaatioalan uusimmat kehitykset kuten e-kaupan sekä langattoman tietoliikenteen. Uusi versio standardista julkaistiin nimillä BS7799-1:1999 ja BS7799-2:1999. Samaan aikaan kiinnostus tätä standardia kohtaan lisääntyi myös Iso-Britannian ulkopuolella ja tämän innoittamana standardin ensimmäinen osa päätettiin lähettää ISO:lle (International Organization for Standardization), jotta siitä saataisiin kansainvälinen standardi. ISO käsitteli standardin nopeutetussa käsittelyssä (Fast Track mechanism), ja joulukuussa 2000 se julkaistiin pienin muutoksin kansainvälisenä standardina BS ISO/IEC 17799:2000. Tämän jälkeen standardin toisesta osasta on tullut vielä uudempi versio BS7799-2:2002, joka julkaistiin vuoden 2002 syyskuussa. Tässä uudistuksessa keskityttiin yhtenäistämään standardia muiden hallintajärjestelmästandardien, kuten ISO 9001:2000 ja ISO 14001:1996, kanssa. [Gam03b]

3 Valvontatoimenpiteiden jaottelu

BS 7799 standardi sisältää joukon valvontatoimenpiteitä, jotka toteuttamalla organisaatio pystyy nostamaan tietoturvansa tasoa. Valvontatoimenpiteitä on 127 (versiossa ISO/IEC 17799:2000) ja ne on jaoteltu kymmeneen eri osa-alueeseen, jotta standardia lukevan olisi helpompi tunnistaa kyseiselle organisaatiolle sopivat tai kyseisen henkilön vastuualueeseen kuuluvat toimenpiteet [Gam03a]. Nämä valvontatoimenpiteet jakautuvat vielä pienempiin toimenpiteisiin ja ohjeistuksiin nostamalla toimenpiteiden koko luvun yli viiden tuhannen [Gam03a]. Yhdessä nämä kaikki valvontatoimenpiteet kattavat organisaation koko tietoturvan antaen näin mahdollisuuden turvata koko organisaation toiminta käyttäen vain yhtä standardia.

Standardin ensimmäinen osa sisältää jokaisen valvontatoimenpiteen kuvauksen ja tarkoituksen sekä ehdotuksia hyväksi havaituista tavoista toteuttaa nämä valvontatoimenpiteet (menettelytapaohje). Standardin toisessa osassa taas määritellään tarkemmin mitä eri valvontatoimenpiteillä organisaation tulisi saavuttaa. Tässä luvussa käydään yleisellä tasolla läpi nämä kymmenen standardin osa-aluetta ja kerrotaan minkälaisia käytännön toimintaohjeita etenkin standardin ensimmäinen osa sisältää.

3.1 Tietoturvapolitiikka

Tietoturvapolitiikassa organisaation ylin johto määrittelee yleisellä tasolla miten tietoturva tulisi toteuttaa kyseisessä organisaatiossa. Siinä määritellään tietoturvan yleiset tavoitteet ja vaatimukset, joihin on otettu huomioon myös lainsäädännön sekä mahdollisten asiakassopimusten asettamat vaatimukset. Tietoturvapolitiikassa määritellään myös tietoturvan käytännön hallinnan vastuualueet sekä raportointi toimenpiteet, joita tulee noudattaa havaitessa mahdollisia tietoturvarikkomuksia. Vaikka tämän dokumentin tulisi sisältää kaikki olennainen koskien organisaation tietoturvaa, tulisi sen silti olla melko lyhyt ja helposti omaksuttava.

3.2 Turvallisuuden organisointi

Organisaatiossa tulisi olla johdon vetämä foorumi, jossa tietoturvapolitiikka katselmoidaan ja hyväksytään. Lisäksi tämän foorumin vastuualueisiin kuuluu seurata organisaatiossa tapahtuvia muutoksia, jotka saattavat lisätä tietoturvariskejä, seurata organisaatiossa tapahtuneita tietoturvarikkomuksia sekä hyväksyä hankkeita, joilla organisaation tietoturvaa pyritään parantamaan.

Jokaisessa organisaatiossa tulisi olla tietoturva-asiantuntija, jota tarpeen vaatiessa voidaan käyttää. Organisaatio voi tarpeen vaatiessa käyttää myös ulkopuolista asiantuntija-apua. Asiantuntijoita tulisi käyttää kaikissa tietoturvaan liittyvissä kysymyksissä ja etenkin, kun havaitaan mahdollinen tietoturvarikkomus. Tämän lisäksi organisaation tulisi ylläpitää yhteyksiä poliisiviranomaisiin, palveluntarjoajiin ja teleoperaattoreihin, jotta heiltä saataisiin apua mahdollisimman nopeasti tietoturvarikkeen sattuessa.

Monet organisaatiot tekevät yhteistyötä kolmansien osapuolien kanssa. Näitä ovat esim. liikekumppanit, joiden kanssa vaihdetaan liiketoimintaan liittyvää tietoa, laitteistoiden ja ohjelmistojen tukihenkilöstö, siivous- ja pitopalvelu, vartijat, konsultit ym. Lisäksi osa monen organisaation toiminnoista on ulkoistettu. Näissä tilanteissa organisaation tulee tarkkaan harkita mitä toimenpiteitä tarvitaan, jotta yhteistyö kolmansien osapuolien kanssa olisi mahdollisimman sujuvaa mutta myös turvallista. Kaikki tietoturvaan liittyvät vaatimukset ja ehdot tulisi aina kirjata sopimuksiin.

Jotta organisaation tietoturvaan kiinnitettäisiin tarpeeksi huomiota jokapäiväisessä toiminnassa, tulisi kaikille tietovarannoille ja muille tärkeille organisaation tietoturvaan liittyville prosesseille määrätä vastuuhenkilöt.

3.3 Suojattavien kohteiden luokitus ja valvonta

Organisaation tulee pystyä luetteloimaan sen eri tietojärjestelmät ja tietovarannot sekä määrittelemään niiden suhteellisen arvon ja tärkeyden liiketoiminnan kannalta. Tämä helpottaa omaisuuden suojaamisen suunnittelua, toteutusta ja ylläpitoa. Luettelon perusteella tietovarannot voidaan luokitella niiden arvon ja tärkeyden mukaan. Luokittelu toimii osana organisaation riskien hallintaa ja toimii lähtökohtana sille miten omaisuus tulisi suojata.

Esimerkkejä mahdollisista tietovarannoista ja järjestelmistä ovat:

- tietokannat, tiedostot, järjestelmädokumentit, käyttöohjeet, koulutusmateriaalit jne.
- ohjelmistot
- tietokoneet, reitittimet, faxit ym. fyysiset laitteet
- tietojärjestelmäpalvelut

3.4 Henkilöstöturvallisuus

Organisaation tulisi ottaa huomioon sen oma turvallisuus myös silloin, kun uutta henkilöstöä palkataan tai kun määritellään henkilöstön toimenkuvaa.

Riippuen uuden henkilön työtehtävistä tulisi rekrytointi vaiheessa henkilölle suorittaa jonkinasteinen taustojen tarkistus. Mahdollisia tarkistettavia asioita ovat esim.:

- henkilön CV:n paikkansapitävyys
- opinnäytteiden tarkistus
- henkilöllisyyden todentaminen (esim. passi)

Jos henkilön tulevaan työhön liittyy erittäin luotettavien tietojen käsittelyä, esim. finanssitietoja, tulisi myös henkilön luottotiedot tarkistaa. Henkilöstölle asetetut tietoturvaehdot tulisi sisällyttää sopimuksiin ja niiden noudattamista tulisi seurata työsuhteen aikana.

Työntekijöiden olisi työsopimuksen yhteydessä hyvä kirjoittaa myös luottamuksellisuussopimus. Tällaisten sopimusten käyttö on perusteltua myös väliaikaisten työntekijöiden sekä kolmannen osapuolen henkilöstön kanssa.

Organisaation tulee pitää huoli siitä, että henkilöstö on tietoinen mahdollisista tietoturvauhista, he tuntevat tietoturvapolitiikan sekä turvallisen toiminnan takaavat

menetelmät, ja että heitä on koulutettu käyttämään arkaa tietoa käsitteleviä laitteistoja tietoturvallisella tavalla.

Työntekijät tulisi ohjeistaa raportoimaan nopeasti tietoturvaan liittyvistä häiriöistä, heikkouksista ja tapahtumista käyttäen organisaation tähän tarkoitukseen toteutettua prosessia. Raportoiduista tapahtumista tulisi pitää tilastoa, johon kirjataan tapahtumien tyypit, määrät sekä niiden taloudelliset vaikutukset. Näitä tilastoja voidaan myöhemmin käyttää parantamaan organisaation tietoturvaa. Lisäksi tapahtuneista tietoturvarikkeistä ym. tietoturvaan liittyvistä tapahtumista voidaan tulevaisuutta varten ottaa oppia.

Organisaatiossa tulisi myös olla kurinpidollinen prosessi, jota käytetään, kun henkilö rikkoo laadittuja tietoturvasääntöjä. Tämä voi toimia myös pelotteena sellaisille, jotka eivät muuten säännöistä välittäisi. Prosessin tulee kuitenkin taata oikeudenmukainen käsittely sellaisille henkilöille, joita syytetään vakavasta tietoturvarikkomuksesta.

Henkilöstöturvallisuuden tarkoituksena on vähentää inhimillisen virheen, varkauden, petoksen tai laitteistojen väärinkäytön riskiä organisaatiossa.

3.5 Fyysinen ja toimintaympäristön turvallisuus

Organisaation liiketoiminnan kannalta tärkeät laitteistot tulisi fyysisesti suojata luvattomalta käytöltä, vahingonteolta ja häirinnältä. Tähän päästään eristämällä laitteet tiloihin, joihin pääsyä valvotaan.

Nämä tilat tulisi suojata kulunvalvonnalla, jotta voidaan varmistua siitä, että vain ne henkilöt, joilla on oikeus toimia näissä tiloissa, sinne pääsevät. Kulunvalvonta voidaan toteuttaa käyttämällä esim. magneettisia henkilökortteja ja PIN koodia. Kaikilla henkilöstöön kuuluvilla tulisi olla näkyvillä jonkinlainen henkilöllisyystunniste (esim. henkilökortti). Kaikkia vierailijoita taas tulisi valvoa, heidän tulonsa ja lähtönsä kirjata ylös sekä poistaa heidät alueilta, joissa heillä ei ole oikeus oleskella.

Jos tärkeitä laitteita tai tietoa joudutaan kuljettamaan organisaation toimitilojen ulkopuolelle esim. kotona tai asiakkaan luona tapahtuvan työn vuoksi, tulee näissä tilanteissa ottaa huomioon lisääntyvä tietojen luvattomaan käyttöön ja varkauteen liittyvä uhka.

Henkilöstön tulisi aina noudattaa tyhjän pöydän ja ruudun politiikka etenkin työajan ulkopuolella. Lisäksi tietokoneet tulisi lukita salasanalla, jos niiden ääressä ei työskennellä.

Näin voidaan ehkäistä tärkeän tiedon joutumista vääriin käsiin ja pienentää laitteiden väärinkäytön mahdollisuutta. Tyhjän pöydän politiikka vähentää myös tärkeän tiedon tuhoutumisen riskiä esim. tulipaloissa tai vesivahinkojen sattuessa.

Tärkeätä informaatiota sisältävien laitteiden ja tallenteiden hävittämisessä tulee olla erityisen huolellinen, jotta voidaan varmistua siitä, ettei liiketoiminnan kannalta haitallista tietoa pääse tässä yhteydessä kulkeutumaan vääriin käsiin.

Laitteiden sijoittelussa sekä turva-alueiden suunnittelussa tulisi huomioida myös miten erilaiset ulkopuoliset haittatekijät vaikuttavat laitteiden toimintaan, ja kuinka niitä voitaisiin ehkäistä. Tämänkaltaisia tilanteita ja haittatekijöitä ovat esim. varkaus, tulipalo, savu, vesivahinko, vesikatkos, pöly, sähkökatkos ja elektromagneettinen säteily.

Sähkökatkoksiin organisaatio voi varautua esim. vetämällä liiketiloihin useampia toisistaan riippumattomia sähkölinjoja, hankkimalla UPS laitteita (Uninterruptable Power Supply) sekä sähkögeneraattoreita. Kaikki sähköntuotannon varalaitteet tulisi aika-ajoin testata.

3.6 Tietoliikenteen ja käyttötoimintojen hallinta

Liiketoiminnan kannalta tärkeät toiminnot ja prosessit (ne, jotka on kirjattu tietoturvapolitiikkaan) tulisi dokumentoida. Dokumenttien tulisi sisältää ohjeistus toimintojen suorituksesta sekä neuvoa mahdollisissa virhetilanteissa. Lisäksi kaikki muutokset tärkeimpiin laitteistoihin (laitteiston vaihto, ohjelmistojen päivitys) tulisi olla tiukan valvonnan alla. Riittämätön valvonta laitteistoihin kohdistuvien muutoksien osalta on yleinen syy systeemivirheisiin ja tietoturvapuutteisiin. Muutoksista tulisi pitää kirjaa, niiden vaikutukset toimintaympäristöön käydä läpi ja informoida niitä osapuolia, joihin muutokset vaikuttavat.

Organisaation tulee etukäteen varautua kriittisten laitteistojen vikatilanteisiin ja mahdollisiin tietoturvarikkomuksiin, jotta niistä voitaisiin toipua nopeasti ja tehokkaasti. Tapahtuneiden rikkeiden tai vikojen syyt tulisi analysoida, jotta vastaavilta tilanteilta voitaisiin välttyä tulevaisuudessa. Tapahtumien jäljitysketju tulisi myös tallentaa, jotta sitä voidaan käyttää esim. todisteena oikeudessa tai vaadittaessa korvauksia ohjelmistovalmistajilta tai palveluntarjoajilta. Kaikki toimenpiteet, joita tehdään virhetilanteesta toipumisessa, tulisi myös dokumentoida myöhempää tarkastelua varten.

Henkilöstön työtehtävät tulisi jakaa niin, että vahingossa tapahtuva tai tahallinen järjestelmien väärinkäyttö voitaisiin minimoida. Tällä pyritään esim. siihen, että henkilö ei pysty yksinään toteuttamaan organisaation kannalta haitallisia toimia. Eräs tapa on pitää huoli siitä, että toiset ihmiset hyväksyvät ja toiset suorittavat sellaiset toiminnot, joissa petoksia voisi tapahtua.

Organisaation tulee myös eriyttää mahdollisten tuotteiden kehitys ja testaus sellaisista laitteistoista, joissa ajetaan operatiivisia ohjelmistoja. Kehitys ja testaus saattavat aiheuttaa ei haluttuja muutoksia liiketoiminnallisessa käytössä olevaan dataan. Myös kehitys ja testiympäristöt olisi hyvä eriyttää, jotta voitaisiin helpommin ylläpitää vakaata testiympäristöä.

Organisaation tulee ottaa riittävän kattavat varmuuskopiot tarpeellisin väliajoin. Lisäksi aika-ajoin tulee tarkistaa, että varmuuskopiot ovat onnistuneita. Varmuuskopioiden lisäksi tulee ylläpitää tarkkaa kirjaa otetuista varmuuskopioista sekä ohjeistusta tietojen palauttamisesta. Kaikki tämä tieto (varmuuskopiot ja niihin liittyvät dokumentit) tulisi tallentaa ulkopuoliseen paikkaan, jossa ne ovat turvassa päätoimitiloissa mahdollisesti tapahtuvalta onnettomuudelta.

3.7 Pääsyoikeuksien valvonta

Organisaation tulee huolehtia, että asiattomat henkilöt eivät pääse käsiksi sellaisiin tietoihin, laitteistoihin eikä toimitiloihin, joihin heillä ei ole oikeuksia. Liiketoiminnan ja tietoturvan vaatimusten tulisi olla perustana näille pääsyoikeuksien rajoituksille.

Pääsyoikeuksien hallintaa varten tulisi kehittää menetelmä, joka kattaa käyttöoikeuksien koko elinkaaren uuden henkilön rekisteröinnistä hänen organisaatiosta poistumiseen. Jokaisella henkilöllä tulisi olla yksikäsitteinen tunniste, joka mahdollistaa henkilön toimien seuraamisen. Henkilöiden pääsyoikeudet tulisi pitää ajan tasalla etenkin henkilöiden toimenkuvan muuttuessa tai heidän lähtiessä organisaatiosta.

Koska salasanoja käytetään edelleen monessa tilanteessa käyttäjien henkilöllisyyden varmentamiseen, tulisi organisaation ja käyttäjien huolehtia, että salasanoja käytetään turvallisesti ja oikeaoppisesti. Lisäksi tulisi huolehtia siitä, että valvomatta jätetyt laitteistot (esim. henkilökohtaiset tietokoneet) on asianmukaisesti lukittu.

Organisaation tulee kiinnittää erityistä huomiota myös tietoverkkojen turvallisuuteen esim. jakamalla organisaation erilaiset toiminnot omiin verkkoihin sekä turvaamalla liikenteen

esim. palomuureilla. Erityistä huolellisuutta tulisi noudattaa myös ulkoapäin otettujen etäyhteyksien varmentamiseen.

3.8 Tietojärjestelmän kehittäminen ja ylläpito

Kun organisaatioon suunnitellaan uusia informaatiojärjestelmiä ja informaatiota käsitteleviä ohjelmistoja, tulee jo suunnitteluvaiheessa ottaa huomioon tietoon kohdistuvat uhat ja suunnitella järjestelmä/ohjelmisto siten, että näihin uhkiin on riittävällä tavalla varauduttu jo etukäteen. Etenkin ohjelmistosysteemeissä pitäisi kiinnittää huomiota siihen, että ohjelmiston syötteet ja tulosteet ovat oikeita, ja että sisäinen tiedon käsittely tapahtuu oikein. Erityistä huomiota pitää kiinnittää järjestelmiin, jotka prosessoivat arvokkaita tai kriittisiä organisaation tietovarantoja. Kryptografisia menetelmiä tulisi käyttää tilanteissa, joissa niistä on hyötyä. Erityistä tarkkuutta kuitenkin vaaditaan avainten hallinnassa sekä eri maiden lainsäädännön asettamissa vaatimuksissa kryptografisten systeemien käytössä.

3.9 Liiketoiminnan jatkuvuuden hallinta

Organisaation tulisi pystyä jatkamaan liiketoimintaansa mahdollisimman nopeasti erilaisten onnettomuuksien, laitteistovikojen tai tietoturvahyökkäysten sattuessa. Organisaatio pystyy tunnistamaan mahdolliset ongelmatilanteet riskianalyysin kautta. Tämän pohjalta organisaation tulisi kehittää strategia liiketoiminnan jatkuvuuden takaamiseksi ongelmien sattuessa.

Strategian tulisi toimia pohjana liiketoiminnallisesti tärkeiden toimintojen sekä niiden jatkuvuuden takaamiseksi tarkoitettujen prosessien suunnittelussa. Toiminnot sekä toteutetut prosessit tulee huolellisesti dokumentoida sekä aika-ajoin katselmoida ja testata. Etenkin organisaatiossa ja liiketoiminnassa tapahtuvat muutokset (uuden laitteiston hankita, operatiivisten systeemien päivitys, vaihdokset henkilöstössä ym.) saattavat aiheuttaa muutostarpeita liiketoiminnan jatkuvuuden takaaviin prosesseihin.

3.10 Vaatimustenmukaisuus

Organisaation tulee selvittää mitä vaatimuksia laki, erilaiset säädökset ja mahdollisesti tehdyt sopimukset aiheuttavat organisaation liiketoiminnan harjoittamiseen. Nämä vaatimukset tulisi dokumentoida ja varmistaa, että kyseiset vaatimukset tulee täytettyä. Esimerkkejä näistä vaatimuksista ovat tekijänoikeuksien sekä kryptografisten rajoitusten noudattaminen.

Organisaation tulee pitää hyvää huolta sen toimintaan liittyvistä asiakirjoista. Organisaation tulee huolehtia, että liiketoiminnan kannalta tärkeät asiakirjat ovat turvassa niin häviämiseltä, tuhoutumiselta kuin väärentämiseltäkin. Asiakirjat saattavat olla tärkeässä asemassa, kun organisaation tulee esim. oikeudessa todistaa toimineensa lakien ja säädösten mukaan. Lisäksi organisaation tulisi varmistaa, että mahdollisten tietoturvarikkomusten sattuessa todisteiden keruu sekä tallennus tapahtuu käyttäen sellaisia menetelmiä, että ne voidaan hyväksyä esim. oikeudessa.

Organisaation tulee myös aika-ajoin suorittaa operatiivisille järjestelmille teknisiä vaatimustenmukaisuustarkistuksia, joissa tutkitaan toimivatko järjestelmät teknisesti turvallisesti.

4 Standardin noudattaminen ja sertifiointi

Standardin noudattamisen tarkoituksena on rakentaa organisaatiolle tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS). Standardin noudattamisessa ensimmäinen vaihe (standardin uusimman version mukaan, BS7799-2:2002) on määritellä mitkä liiketoiminnan osa-alueet organisaatio haluaa ottaa mukaan hallintajärjestelmään. ISMS voi kattaa niin koko organisaation kuin pelkästään yhden organisaation tuottaman palvelun. Tämän jälkeen organisaation tulee laatia tietoturvapolitiikka. Tietoturvapolitiikassa organisaation johto määrittää yleisellä tasolla mitä tietoturvalta halutaan (mitä halutaan suojata ja kuinka hyvin), ja kuinka haluttuun tietoturvatasoon aiotaan päästä. [Gam03a]

Kun on saatu määriteltyä ne organisaation tietopääomat, joita halutaan suojella, tulee arvioida pääomiin kohdistuvat riskit. Kaikki mahdolliset uhat tulee tunnistaa, arvioida niiden todennäköisyydet ja vaikutukset toteutuessaan. Tämän arvioinnin pohjalta organisaation tulee päättää mitkä riskit ovat hyväksyttäviä sellaisenaan ja mitä riskejä vastaan täytyy varautua toimenpitein, jotta riskejä voidaan pienentää. [Gam03a]

Riskien arvioinnin jälkeen tulee valita millaisia valvontatoimenpiteitä tullaan toteuttamaan, jotta riskejä voidaan pienentää. BS 7799 standardi sisältää joukon eri tilanteisiin sopivia toimenpiteitä, joista voidaan valita sopivimmat. Esimerkki tämänkaltaisesta toimenpiteestä on sijoittaa tärkeät laitteistot tiloihin, joihin pääsyä rajoitetaan ja valvotaan, jotta voidaan pienentää laitteiden väärinkäytön riskiä. Se mitä toimenpiteitä standardista valitaan riippuu tietoturvallisuuden hallintajärjestelmän rajauksesta, tunnistetuista riskeistä ja tietoturvapolitiikassa määritellystä tietoturvan tasosta. Organisaatio voi käyttää myös

muitakin toimenpiteitä riskien hallitsemiseksi kuin niitä, joita standardi tarjoaa [BS99b]. Toimenpiteitä valittaessa tulisi kuitenkin pitää mielessä, että ne eivät saisi olla kalliimpia toteuttaa kuin mahdollisesti toteutuvan uhkan vaikutukset ovat. Tämän jälkeen organisaation tulee kirjoittaa soveltamissuunnitelma (Statement of Applicability, SoA), johon perustellaan valvontatoimenpiteiden valitsemiset ja valitsematta jättämiset.

Suunnittelun jälkeen tietoturvallisuuden hallintajärjestelmä tulisi toteuttaa. Käytännössä tämä tarkoittaa valittujen valvontatoimenpiteiden toteuttamista ja dokumentointia sekä niiden hallinnan ja ylläpidon vastuun jakamista.

Organisaation tulisi säännöllisin väliajoin tarkistaa, että tietoturvallisuuden hallintajärjestelmä toimii oikein ja tehokkaasti. Tämä tarkoittaa kaikkien hallintajärjestelmään liittyvien dokumenttien katselmointia (kuten tietoturvapolitiikka), riskien uudelleenarvioimista etenkin liiketoiminnassa tapahtuneiden muutosten jälkeen sekä suorittamalla sisäisiä tarkistuksia hallintajärjestelmän ja valvontatoimenpiteiden toimivuudesta. Huomatut puutteet tulisi korjata. [Gam03a]

Jos organisaatio haluaa sertifioida itsensä standardia vasten, tullaan organisaation tietoturvallisuuden hallintajärjestelmä tarkistamaan valtuutetun BS 7799 asessorin toimesta. Saatu sertifikaatti sisältää tiedon siitä, mitkä organisaation toiminnat sertifioitiin sekä muita olennaisia tietoja kuten soveltamissuunnitelman [Gam03a]. Asessori palaa tietyin väliajoin tarkistamaan, että organisaation tietoturvallisuuden hallintajärjestelmä toimii niin kuin sen on tarkoitus. Kolmen vuoden välein organisaation tulee uudelleen sertifioida hallintajärjestelmänsä [TSS02].

5 Sertifioinnin tarpeellisuus

Organisaatiolla on mahdollisuus sertifioida itsensä sen jälkeen, kun sillä on toimiva tietoturvallisuuden hallintajärjestelmä. Sertifiointi on kuitenkin isotöinen ja jatkuva prosessi. Sen jälkeen kun sertifiointi on hyväksytysti suoritettu, käy asessori aika-ajoin tarkistamassa, että organisaation toiminta vastaa edelleen sertifiointia. Lisäksi sertifikaatti on uusittava kolmen vuoden välein [TSS02]. Organisaation tulisikin etukäteen tarkkaan arvioida mitä hyötyä sertifioinnista on ennen kuin siihen ryhdytään.

Sertifiointi kuitenkin esim. lisää asiakkaiden sekä muiden organisaatioiden luottamusta. Näin se voi positiivisesti vaikuttaa esim. organisaation liiketoimintaan. Lisäksi jotkut julkisen

sektorin ja valtion hallinnon virastot saattavat jopa vaatia yhteistyökumppaneiltaan sertifioinnin suorittamista. [TSS02]

Organisaation tietoturvan kannalta itse sertifioinnilla ei käytännössä ole merkitystä. Jo standardin noudattaminen helpottaa organisaatiota paremmin ymmärtämään mahdollisia tietoturvauhkia ja sitä kautta nostamaan tietoturvan tasoa. Standardin noudattamisen vahvuus on siinä, että se vaihe vaiheelta auttaa organisaatiota rakentamaan toimivan tietoturvaa parantavan järjestelmän. Standardia seuraamalla organisaatio pystyy paremmin tunnistamaan liiketoiminnan kannalta kriittisimmät tietoturvauhat, varautumaan niihin ja tätä kautta paremmin ymmärtämään tietoturvan merkityksen organisaation liiketoiminnan jatkuvuuden kannalta.

Lähteet

BS99a British Standard BS 7799-1:1999, ”Information security management – Part 1: Code of practice for information security management”, 1999.

BS99b British Standard BS 7799-2:1999, ”Information security management – Part 2: Specification for information security management systems”, 1999.

Gam03a Gamma Secure Systems Limited, ”How 7799 Works”, *http://www.gammassl.co.uk/bs7799/works.html.* [18.02.2003]

Gam03b Gamma Secure Systems Limited, ”History of 7799”, *http://www.gammassl.co.uk/bs7799/history.html.* [18.02.2003]

Ken00 Kenward, J., ”The Global Development of BS7799”, *http://www.itsecurity.com/papers/bs7799.htm*. [01.03.2003]

TSS02 Trinity Security Services, ”Is BS7799 for you?”, *http://www.itsecurity.com/papers/trinity5.htm.* [15.04.2003]