BS 7799, Tietoturvan Hallinta

(Laajennettu tiivistelmä)

Matti Johansson

Helsingin yliopisto
Tietojenkäsittelytieteen laitos
Helsinki 1.3.2003
Seminaari: Tietoturvallisuus
nykyaikaisessa
liiketoimintaympäristössä

1 Tiedon turvaaminen

Monen organisaation yksi tärkeimmistä pääomista on tieto. Tieto voi esiintyä monessa eri muodossa; paperille kirjoitettuna, elektronisesti tallennettuna, keskusteluissa ym. Tieto on tärkeässä osassa, kun ajatellaan organisaation liiketoimintaa, sen kannattavuutta sekä tulevaisuutta. Jos jostain syystä tärkeää tietoa pääsee vääriin käsiin tai osa tiedosta tuhoutuu, kärsii organisaatio jonkinasteisia tappioita, ja pahimmassa tapauksessa saattaa organisaation liiketoiminnan tulevaisuus olla uhattuna.

Jotta tieto pysyisi tallessa ja että siihen pääsisivät käsiksi vain ne henkilöt, joilla siihen on oikeus, tulee tieto suojata erilaisin menetelmin. Tiedon suojaaminen on tärkeää, jotta organisaatio voi turvallisesti harrastaa liiketoimintaa, minimoida liiketoiminnalliset tappiot, maksimoida investointien tuottavuus sekä liiketoiminnalliset mahdollisuudet.

Jotta tieto on hyvin suojattu, tulee sen täyttää seuraavat vaatimukset:

a) salassapito: tietoon pääsevät käsiksi vain ne, joilla siihen on oikeus;
b) luottamuksellisuus: tieto on paikkaansapitävää ja eheää;
c) saatavuus: valtuutettu käyttäjä pääsee halutessaan tietoon käsiksi

1.1 Tietoturvan hallinta

Nykyään organisaatiot joutuvat kasvavassa määrin erilaisiin tilanteisiin, joissa niiden tieto on uhattuna. Tällaisia tilanteita ovat erilaiset ulkoapäin tulevat verkkohyökkäykset, virukset, tietokoneavusteiset petokset, vakoilu, sabotaasi sekä myös tulipalot ja veden aiheuttamat tuhot. Tiedon turvaamista vaikeuttaa se, että nykyään organisaatiot ovat entistä enemmän riippuvaisia tietoverkkojen informaatiosysteemeistä sekä palveluista. Organisaatioiden sisäisten verkkojen sekä julkisten verkkojen yhteenliittyminen sekä resurssien jakaminen verkossa tekevät tiedon turvaamisen erityisen hankalaksi.

Jotta organisaation tieto olisi asiallisesti turvattu, tulee organisaation tunnistaa ja täyttää tietoon kohdistuvat turvallisuusvaatimukset. Osa turvallisuusvaatimuksista saadaan kartoitettua, kun organisaatio tekee riskianalyysia, mitä tietoa sen tulisi suojata ja miten. Osa vaatimuksista tulee taas erilaisista laista, säädöksistä sekä kolmansien osapuolien kanssa tehdyistä sopimuksista, jotka organisaation tulee täyttää.

Riskianalyysissä organisaation tulee huolellisesti selvittää, mitä erilaisia uhkia sen omaisuuteen (tietoon) kohdistuu. Tämän jälkeen on arvioitava kuinka todennäköisiä uhkat ovat ja millaisia seurauksia niistä toteutuessaan aiheutuu. Tämän arvioinnin perusteella organisaatio pystyy päättämään millaisiin toimenpiteisiin erilaisia uhkia vastaan ryhdytään, jotta niiden mahdolliset vaikutukset pystytään minimoimaan. Toimenpiteitä valittaessa tulee punnita paljonko uhan toteutuminen tulee maksamaan ja paljonko taas toimenpiteet, joilla riskiä pyritään vähentämään.

2 BS 7799

BS 7799 on tietoturvastandardi, jonka tarkoituksena on auttaa organisaatioita tunnistamaan erilaisia tietoturvaan liittyviä riskejä sekä tarjoamaan keinoja riskien hallitsemiseksi. Standardi ei käsittele pelkästään tietoliikennettä vaan keskittyy yleiseen liiketoiminnan turvaamiseen tähtäävän tietoturvaan.

BS 7799 painottaa riskien hallinan tärkeyttä. Lähtökohtana on arvioida tietoturvaan liittyvät riskit, ja sen jälkeen valita sopivat toimenpiteet, joiden avulla riskejä voidaan pienentää taloudellisesti kannattavasti. BS 7799 sisältää listan toimenpiteitä, joista voidaan valita organisaation kannalta sopivimmat eri tilanteisiin. Aika ajoin valitut toimenpiteet tulee tarkistaa ja riskit uudelleenarvioida, jotta organisaatio voi varmistua siitä, että sen omaisuus on turvassa myös muutosten keskellä.

Standardi edellyttää, että päätökset toimenpiteiden valitsemisesta tai valitsematta jättämisestä tulee dokumentoida. Samoin tulee dokumentoida myös valittujen toimenpiteiden toteutus. Organisaatioilla on mahdollisuus sertifioida itsensä tätä standardia vastaan ja saada näin toiminnalleen eräänlainen tietoturvallisuustodistus.

2.1 Historiaa

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 BS 7799, joka julkaistiin vuonna 1995.

Vuonna 1999 standardi tarkastettiin sekä päivitettiin ja siihen lisättiin uusia ohjeistuksia, jotka huomioivat informaatioalan uusimmat kehitykset, kuten e-kaupan sekä langattoman tietoliikenteen. Uusi versio standardista julkaistiin nimellä BS 7799-1:1999.

Samaan aikaan kiinnostus tätä standardia kohtaan lisääntyi myös Iso-Britannian ulkopuolella ja tämän innoittamana se 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.

Lähteet

BSI02 British Standards Institution, ”BS 7799 History”, *http://www.c-cure.org/7799history.htm.* [01.03.2003]

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, ”IS 17799:2000”, *http://www.gammassl.co.uk/topics/hot1.html.* [18.02.2003]

Gam03b Gamma Secure Systems Limited, ”How 7799 Works”, *http://www.gammassl.co.uk/bs7799/works.html.* [18.02.2003]

Gam03c Gamma Secure Systems Limited, ”History of 7799”, *http://www.gammassl.co.uk/bs7799/history.html.* [18.02.2003]

Gam03d Gamma Secure Systems Limited, ”The Future of 7799”, *http://www.gammassl.co.uk/bs7799/future.html.* [18.02.2003]

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