JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Valtiovarainministeriö

Pvm
5.8.2014

673/00.01.05.00/2014

VM047:21/2007
1862/00.01.00.01/2012

Asia:
Jyväskylän yliopiston lausunto tietoturvallisuuden arviointiohjeesta

Pyydettynä lausuntona tietoturvallisuuden arviointiohjeesta Jyväskylän yliopisto esittää seuraavaa:

Valtiovarainministeriön tietoturvallisuuden arviointiohjeluonnos antaa hyvän perustan valtionhallinnon viranomaisille, joiden tulee arvioida organisaationsa tietoturvallisuuden tilaa sekä toteutettujen tietoturvatoimenpiteiden asianmukaisuutta ja riittävyyttä.

1. Arvioinnin perusteet

Ohjeluonnoksessa on kattavasti esitetty kansallinen lainsäädäntö ja tietoturvallisuuden arviointiperusteet. Kansainvälinen yhteistoiminta erityisesti EU-tasolla edellyttää valtionhallinnon viranomaisilta kykyä arvioida tietoturvallisuutta myös laajemmasta näkökulmasta. Ohjeeseen olisi hyvä kuvata EU-tason säännöstö ja tärkeimmät toimijat, joilla on merkitystä tietoturvallisuuden arvioinnissa.

Tällaisia EU-organisaatioita ovat mm. ENISA (European Network and Information Security Agency) ja Europol/EC3. Erityisesti ENISA julkaisee ohjeita ja raportteja, jotka käsittelevät tietoturvallisuutta ja sen arviointia. Esimerkiksi ENISA on julkaissut vuonna 2010 ohjeen *"The new users' guide: How to raise information security awareness"*, joka on suunniteltu organisaatioille kokonaisvaltaisen tietoturvallisuusarvioinnin ja analyysin toteuttamiseksi.

2. Arvioinnin toteuttaminen

Ohjeluonnoksessa mainitaan, että tietoturvallisuuden arviointiperusteina voidaan käyttää julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita taikka vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia, kuten tietoturvallisuuden hallintajärjestelmiä koskeva kansainvälinen standardi ISO/IEC 27001.

Postiosoite: PL 35, 40014 Jyväskylän yliopisto
Postal address: P.O. Box 35, FI-40014 University of Jyväskylä, Finland
Puh./Tel.: +358 (0)14 260 1211 • Fax: +358 (0)14 260 1021
www.jyu.fi • Business ID, VAT-code: FI02458947

Em. standardin lisäksi **Common Criteria** ISO/IEC 15408 on tietotekniikkatuotteiden tietoturvallisuustason määrittely- ja evaluointistandardi, jota ovat kehittäneet eri maiden kansalliset turvallisuus- ja standardointiorganisaatiot. Common Criteria sisältää joukon vaatimuksia, joita voi käyttää määritettäessä jonkin tietotekniikkatuotteen tietoturvavaatimuksia. Lisäksi se määrittelee evaluointimenettelyn, jonka avulla voidaan arvioida tietotekniikkatuotteiden tietoturvan tasoa. Common Criterian tarkoituksena on tarjota yhtenäinen menettelytapa, jonka avulla tietotekniikkatuotteiden tietoturvatasoa voidaan evaluoida. Common Criteria soveltuu tietojärjestelmien kehityshankkeissa, joissa suurta tietoturvallisuustasoa vaativia tietojärjestelmiä hankitaan sekä räätälöidyillä ohjelmistoilla että valmisohjelmistoilla. Common Criteria -järjestelmä määrittelee joukon tietoturvavaatimuksia, joita voidaan käyttää hyväksi evaluoitaessa tuotteita ja rakennettaessa omia vaatimusmäärittelyjä. Common Criteria määrittelee myös erityiset tietoturvavaatimusten toteutumistasot (Evaluation Assurance Levels, EAL).

3. Tietoturvallisuuteen liittyvät standardit

Ohjeen yhdeksi liitteeksi olisi hyvä koota tietoturvallisuuteen, riskien hallintaan ja arviointiin liittyvät standardit. Tällaisia standardeja ovat mm:

- ISO/IEC Standard 13335 - Information technology -- Security techniques -- Management of information and communications technology security
- BS 25999 – Business continuity management
- ISO/IEC Standard 15443 - Information technology -- Security techniques -- A framework for IT security assurance
- ISO/IEC Standard 17799 - Information technology -- Security techniques -- Code of practice for information security management
- ISO/IEC Standard 18028 - Information technology -- Security techniques -- IT network security
- ISO/IEC Standard 27001 - Information technology -- Security techniques -- Information security management systems
- BS 7799-3 – Information security management systems -- Guidelines for information security risk management
- ISO/IEC TR 18044 – Information technology -- Security techniques -- Information security incident management
- Initiatives of the Information Security Forum, including the Standard of Good Practice and their auditing standards
- ISO Standard 13569 - Financial services -- Information security guidelines
- ISO/IEC Standard 15816 – Information technology -- Security techniques -- Security information objects for access control
- ISO/IEC TR 15947 - Information technology -- Security techniques -- IT intrusion detection framework
- ISO/IEC Standard 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security
- ISO/IEC TR 15446 – Information technology -- Security techniques -- Guide for the production of Protection Profiles and SecurityTargets
- ISO/IEC 18045 – Information technology -- Security techniques -- Methodology for IT security evaluation

Lisäksi omaksi liitteeksi voisi koota kansallisen ja kansainvälisen lainsäädännön, direktiivit ja ohjeet, jotka liittyvät tietoturvallisuuteen ja sen arviointiin.

Rehtori Matti Manninen