Lausuntopyyntö Dnro VM047:21/2007, 1862/00.01.00.01/2012

Tietoturvallisuuden arviointiohje

Tampereen teknillinen yliopisto (TTY) kiittää saamastaan lausuntopyynnöstä ja haluaa kommentoida seuraavia suosituksen kohtia tarkemmin.

Huomioita

Tekstin alussa ohjeen tavoite jää puutteelliseksi. Mitä käytännössä tarkoittaa "tietoturvallisuuden arviointi"? Tämä puute yhdessä hallintajärjestelmän korostamiseen (kts. alla) luo raskaan ja byrokraattisen mielikuvan erittäin tarpeellisesta toiminnasta. Ehdottamme, että dokumentin alussa lukee selkeästi esimerkiksi seuraavaa:

"Tietoturvallisuuden arviointi tarkoittaa käytännön toiminnan vertaamista toimintaa sääteleviä normeja vastaan. Vertailu voidaan tehdä hyväksyttyjä kriteeristöjä ja toimintatapakuvauksia käyttäen. Mahdollisuuksien salliessa suositetaan numeerista tai laadullista mittaamista."

Näin lukija ymmärtää ohjeluonnoksen tarkoituksen heti ensimmäiseltä sivulta alkaen.

Johdanto

Tietoturvallisuuden hallintajärjestelmä korostuu tekstissä. Hallintajärjestelmä-termi on kuitenkin haastava, koska se mielletään tietotekniikan yhteydessä tietojärjestelmäksi. Tästä syystä ohjeen viesti vinoutuu kohti "tietoturvallisuuden hallintajärjestelmän" pakollista hankintaa. Koska ohje on kuitenkin taustaluvussa esitetty suositukseksi, ehdotamme tietojärjestelmämielikuvan poistamiseksi käyttämään termiä kehys tai malli. Suosituksen tavoitteena lienee kuitenkin oikeiden asioiden tekeminen riittävällä perusteellisuudella, ja valtiohallinnon nykyinen suuntaus on kohti selkeää ja yksinkertaista esitystapaa.

Edellytykset tietoturvallisuuden arvioinnille

Itseisarvioinnin toteuttaminen vertaisarviointina on tietoturva-arviointikokemuksemme mukaan hyvä toimintatapa myös sisäiseen tietoturva-arviointiin, ja ehdotamme sen toimintatavan korostamista. Tämä tapa motivoi ja tuo ryhtiä arviointiin, koska sitä ei tee vain oman organisaation jäsen.

Tietoturvallisuuden tasovaatimukset

Luonnoksessa olisi hyvä mainita selkeästi, että arviointi tietylle tasolle tarkoittaa vain niitä järjestelmiä ja toimintatapoja joiden avulla käsitellään luokiteltua tietoa. Tekstissä korostetaan kokonaisuutta ja annetaan käsitys, että suojaustaso on joko kaikki-tai-ei-mitään -periaatteella. Käytännössä tämä ei kuitenkaan ole näin, vaan suojaustasoarvio/-toteutus tehdään erityisesti teknisessä mielessä vain niille osajärjestelmille, joissa suojaustason mukaista tietoa käsitellään.

Tietojärjestelmähankkeiden arviointi

Arviointikehikossa olisi hyvä listata myös luotettavuus.

Tietojärjestelmähankkeissa on erittäin tärkeä arvioida toiminnan luotettavuus jatkuvuuden kannalta. Esimerkkinä yrityksen luotettavuusarviointiin kuuluvista asioista: "tietoturvatoteutus on selkeästi uusi ja kansainvälisesti merkittävä toteustapa, jonka patentin omistaa yksi suomalainen yritys. On siis hyvin mahdollista että yritys ostetaan, jonka seurauksena toteutus siirtyy Suomen lakien ulkopuolelle. Tähän riskiin tulee varautua jatkuvuussuunnittelussa.

Tietoturvallisuus sisältyy merkittävästi myös kohtaan 3, koska ihminen on kriittinen tietoturvan toteuttaja.

Ohjelmistojen ja järjestelmien tietoturvan arviointi tulee aina tehdä elinkaarimallin kautta (idea, esiselvitys, ..., suunnittelu, toteutus, testaus, tuotanto, poistaminen). Sovelluskehitys ja ennen käyttöönottoa ei riitä, koska usein latentit virheet ovat järjestelmän tietoturvan kannalta kaikkein vaikeimmin korjattavia. Lisäksi nykyisten tietomäärien mukana tulee myös kriittiseksi järjestelmän käytöstäpoisto tietokantoineen ja tietoturvaan liittyvine tietoineen (salasanat säilytyspaikkoineen, sähköiset avaimet, suunnittelumateriaalit yms.).

Tietoturvallisuuden arvioinnin toteuttaminen

Tarkoitetaanko tässä auditointia vai arviointia, vai tarkoittavatko ne samaa? Tekstissä oleva kuvaus vaiheineen on erittäin lähellä normaalin auditoinnin kuvausta. Koska terminologia on haastavaa ja tulkinta usein kuulijan/lukijan mielikuviin pohjautuva niin ehdottamme kuvan piirtämistä. Kuvassa olisi eri vaiheet, niiden liittyminen toisiinsa sekä lisäksi muutkin termit olisi hyvä piirtää tähän kuvaan (katselmointi/sertifiointi, miten liittyvät kokonaisuuteen ja mihin vaiheisiin).

Kriteeristöjen vaatimusten tulkinta

Tässä kohdassa erotutaan normaalista auditointiprosessista, koska siinä auditoijalla on usein oikeus tehdä tulkinta kriteeristön toteutumisesta. Tässä ohjeesta jää mielikuva että tulkinta on omistajalla. Asiaa olisi hyvä selkeyttää, koska auditointi on kuitenkin tapa jolla kriteeristöjä käytetään.

Liite 3 CASE-esimerkkejä

Elinkaarimallin merkityksellisyys tuleen esiin vasta liitteessä 3, vaikka se on tietoturvallisen toiminnan tärkeimpiä lähestymistapoja.

Tiina Aijälä
hallintojohtaja