TERVEYDEN JA
HYVINVOINNIN LAITOS

THL/645/4.00.00/2012

24.5..2012

Valtiovarainministeriö
PL 28
00023 Valtioneuvosto

valtiovarainministerio@vm.fi

Viite: Lausuntopyyntönne, VM047:14/2007, 25.4.2012

Sovelluskehityksen tietoturvaohje

Valtiovarainministeriö on pyytänyt Terveyden ja hyvinvoinnin laitokselta (THL) lausuntoa luonnoksesta sovelluskehityksen tietoturvaohjeeksi. THL:n mielestä opas on tarpeellinen ja varsin kattava.

Olemme koonneet oheiseen listaan kommentteja sekä ohjeen luettavuutta ja käytettävyyttä parantavia kehittämisehdotuksia:

Sivulla 5, toisessa kappaleessa on teksti "Sovelluksen ja tietoaineiston tulee tarvittaessa olla myös käytettävissä". Tämä on mielestämme itsestään selvyys ja siksi virke on tarpeeton.

Sivulla 5 viimeisessä kappaleessa oleva ohjeen tarkoitus ja sivulla 6, ensimmäisessä kappaleessa kuvattu ohjeen tavoite poikkeavat tiivistelmässä olevista ohjeen tarkoituksesta ja tavoitteesta.

Sivulla 9 on teksti " Sovelluskehityksen prosessissa tietoturvallisuuden huomioon ottaminen kaikissa vaiheissa koetaan hidastavana tekijänä. Jälkeenpäin tietoturvallisuuden huomioon ottaminen tulee usein kalliimmaksi ja on vaikea toteuttaa." Tämä kohta tulisi ohjeessa mielestämme nostaa korostetusti esille.

Sivun 9 ensimmäisessä kappaleessa edellytetään, että sovelluskehittäjiltä tulee vaatia näyttöä tietoturvaosaamisesta. Tämän vaatimuksen toteuttaminen saattaa olla vaikeaa: millaista näyttöä edellytetään ja miten se todennetaan, jos osaaminen on syntynyt aikaisemmissa kehitystehtävissä, jotka saattavat olla salassa pidettäviä. Lisäksi tulee ratkaista, mitä tehdään sovelluskehitystyötä tekevälle henkilöstölle, joka jo työskentelee viranomaisessa ja jolla ei ole tietoturvaosaamista tai näyttöä osaamisesta.

Sivut 10 ja 11, kuvat 1 ja 2: Roolit ja tapahtumat tulisi mielestämme esittää samalla tavalla riippumatta käytetäänkö lineaarista tai inkrementaalista prosessimallia.

Luvuissa 2.3., 3.1.2., 3.3.4. ja 3.3.6. on ulkopuolisten tahojen ylläpitämiä linkkejä. Vaarana on, että oppaan käyttöaikana (useita vuosia) linkkien takana oleva tieto muuttuu tai se poistetaan, jolloin linkit eivät ole enää käyttökelpoisia lukijoille. Toivottavaa on, että joko linkkejä referoidaan riittävästi tekstissä, linkkien takana oleva tieto liitetään oppaan liitteeksi, linkeistä kootaan lista oppaan liitteeksi tai linkit poistetaan oppaasta kokonaan.

Luvussa 2.4. oleva lause "Organisaatioista riippuen voidaan käyttää projekti- tai hanke-termiä" on mielestämme turha.

Luvussa 2.4. sivu 12, ensimmäinen kappale: koodaus-, testaus ja hyväksyminen suositellaan eri henkilöiden tekemäksi. Testaus on melko laaja käsite ja osa testauksesta kuuluu koodaajan tehtäviin. Testauksesta puhuttaessa ja kirjoitettaessa tulisi ottaa huomioon mm. yksikkötestaus, integraatiotestaus, järjestelmätestaus, käytettävyystestaus, suorituskykytestaus, hyväksymistestaus, automatisoidut käyttötapaustestit. Voisiko oppaan tekstissä tarkentaa, mitkä testaukset tulee eriyttää koodauksesta.

Luvussa 2.4., sivulla 12 olevassa kuvassa 3. tulisi mielestämme korostaa tietoturvavastaavan roolia myös määrittely ja suunnitteluvaiheessa. Kuvassa oleva tietohallintovastaavan rooli on ristiriidassa oppaan tekstin kanssa. Vaikka kuva onkin vain esimerkki, sen tulisi mielestämme noudattaa oppaassa kuvattua käytäntöä. Kuvan projektirooleista puuttuvat myös Scrum-mallissa tunnistetut Product Owner- ja Scrum Master -roolit, joista ensimmäinen on omistaja siinä mielessä, että hän edustaa käyttäjäryhmiä ja tilaajan etua sovelluskehitysprosessin ajan. Scrum master taas on vastaava rooli tuottajan puolella. Näiden roolien ja niiden välisen suhteen tarkoituksena on viestiä, kuinka tärkeää on, että tilaaja osallistuu projektiin täydellä panoksella koko kehitysprojektin ajan.

Luvussa 2.7, sivulla 15 luetellaan dokumentoitavia asioita. Luvun ensimmäisessä lauseessa tulisi kappaleen alussa mielestämme korostaa tietoturvan kannalta keskeisten asioiden dokumentointia. Lause voisi alkaa "Alla on listattu tietoturvallisuuden kannalta tärkeimmät asiat....". Samassa kappaleen listassa käytetään termiä 'turvakuvaus'. Termiä tulisi selittää tarkemmin, jotta lukija ymmärtäisi, mitä ko. kuvauksella tarkoitetaan.

Voisiko luvussa 2.9. huomioida moniasiakasympäristöinä ne suuret organisaatiot, joissa samaa sovellusta käytetään esimerkiksi eri osastoilla tai toimialoilla. Tämä onnistuisi vaikkapa lisäämällä ensimmäisen virkkeen loppuun sanat "... tai suuren organisaation eri osastoilla / toimialoilla."

Luvussa 2.10., sivulla 17 ei mainita lainkaan immateriaalioikeuksia, jotka ovat mielestämme merkittävä osa sovellusten tietoturvaa koko sovelluksen elinkaaren ajan. Jos immateriaalioikeuksista ei huolehdita ajoissa, saatetaan joutua, etenkin räätälöidyissä sovelluksissa, vendor lock-in –tilanteeseen. Tämä tilanne voi johtaa merkittävien riskien toteutumiseen ja/tai sovelluksen rappeutumiseen. Tässä kohdassa tietoturva on määriteltykin melko suppeasti eikä siinä oteta huomioon sovelluksen käytettävyyttä koko elinkaaren ajan. Mikäli immateriaalioikeuksia ei haluta mainita luvussa 2.10., tulisi siinä mielestämme ainakin viitata lukuun 4.1., jossa asiaa käsitellään lisää.

Luku 3. Osa vaatimuksista on sellaisia, jotka on jo esitetty muissa Vahti-ohjeissa. Voisiko tällaisten vaatimusten osalta tarkentaa, mitä ne merkitsevät sovelluskehityksen kannalta. Tällaisia vaatimuksia ovat mm. POL-001 ensimmäinen kappale, POL-003 sekä JTH-vaatimukset. Esimerkiksi vaatimus OSK-001 on mielestämme tarkennettu hyvin sovelluskehitykseen sopivaksi.

Vaatimus STA-001 merkitsee erittäin suurta työmäärää monissa valtionhallinnon organisaatioissa. Sitä ja sen merkitystä tulisi mielestämme korostaa ja selkiyttää oppaassa.

Vaatimus TSK-002: lähdekoodin muutoksen jäljitettävyys myös muutosaikaan on tärkeää. Voisiko sen lisätä vaatimukseen.

Vaatimus SNT-014: Salasanan vahvuuden määrittämisessä tulisi mielestämme käyttää mielummin entropia-arvoa eikä yksinkertaisia pituus ja erikoismerkkisääntöjä. Lisäksi salasanojen tallennuksessa tulisi mielestämme painottaa, että vain tiivistearvot saa tallentaa ja että tiivistefunktion tulee olla hidas, kuten bcrypt.

Vaatimus TOT-002: Vaatimuksessa viitataan kriittiseen tietoon. Voisiko termiä kriittinen tieto selvittää lukijalle. Tietoturva-asetuksessa edellytetään mm. että " Arkaluonteisten tai biometristen henkilörekisteriin talletettujen henkilötietojen käsittelytapahtumien tulee kirjautua lokiin (TTA 20 § 1 mom.).

Vaatimus TOT-005: Vaatimusta lokien puskuroimattomuudesta tulisi mielestämme tarkentaa. Joissakin sovelluksissa lokimerkintöjä tulee jopa satoja tuhansia sekunnissa. Puskuroimattomuus johtaa helposti suorituskykyvaikuksiin ja vähentää siten palvelun saavutettavuutta.

Opas vaatii vielä kielenhuoltoa. :

- Oppaassa käytetään yhdyssanoissa sekä muotoa tietoturva- että tietoturvallisuus- (esimerkiksi kappaleessa 2.4.). Yhdyssanoissa lyhyt muoto tietoturva- on selkeämpi.
- Sivu 3, kappale 1, terminologia: "yhteiskunnan toiminta on yhä verkottuneempaa". Tarkoitetaanko tässä verkostomaista toimintaa vai tietoverkkojen käyttöä?
- Sivu 3, kappale 1, kirjoitusvirhe: "internetin kautta, jossa " - väärä viittaussuhde, tulisi olla missä
- Sivu 5, kappale 1, terminologia: internet kirjoitettu isolla - tulee kirjoittaa yhtenäisesti pienellä
- Sivu 6, kappale 1, terminologia: ohjeessa puhutaan tietoturva-asetuksesta (oikein), lausuntopyynnössä taas puhutaan tietoturvallisuusasetuksesta

Oppaassa on lisäksi vielä jonkin verran kirjoitusvirheitä, joita emme tässä yksilöi.

Pääjohtaja Pekka Puska

Tietoturvapäällikkö Tuija Lehtinen