OIKEUSMINISTERIÖ

Tietohallinnon vastuualue
Tietohallintoyksikkö

LAUSUNTO

23.5.2012

10/043/2012

VALTIOVARAINMINISTERIÖLLE

LAUSUNTO SOVELLUSKEHITYKSEN TIETOTURVAOHJEESTA

Tietoturvaohjeessa sovelluskehitystä lähestytään pääosin perinteisen vesiputousmallin mukaisesti. Vesiputousmallia käytetään edelleen sovelluskehitysprojektien yleisenä ohjausmallina, joskin ketteriä kehitysmenetelmiä sovelletaan varsin yleisesti ulkopuolisen it-toimittajan kanssa tehtävässä yhteistyössä. Asiakirjan sisällysluettelossa luvussa 3.2 mainitaan ketterät menetelmät vain otsikkotasolla, jolloin lukuun tulee vain yksi alaluku. Myös perinteinen vesiputousmalli olisi hyvä mainita, koska siitä kuitenkin puhutaan tekstissä jopa enemmän kuin ketteristä menetelmistä.

Palveluorientoitunutta arkkitehtuuria (SOA) ei mainita ollenkaan. Myös koko ohjeen painopiste on vanhassa maailmassa - ei ketterissä tai SOA-tekniikassa tms. joita kuitenkin lähes kaikki nykyään käyttävät. Ohje ei siis käytännössä anna ohjeita nykyajan vaatimuksiin, jolloin päädytään esim. seuraavanlaisiin kysymyksen asetteluihin

- miten eri turvaluokkaa olevat SOA-komponentit toimivat
- saako sama palikka toimia eri turvaluokissa
- pitääkö komponenttien sertifikoitua toisilleen jne..,
- miten varmistetaan palveluväylän tietoturva ja onko siinä jotain erityiskysymyksiä
- ovatko SOA:ssa käytetyt tekniikat ja protokollat turvallisia (UDDI, jne...)

Nykypäivänä hankinnat ovat usein keskeisessä asemassa sovelluskehityshankkeiden toteuttamisessa julkishallinnossa. Vaikka ohjeen tekstissä korostetaan hankintoja ja myös todetaan ohjeen tukevan hankintojen tekoa, niin käytännössä ohje ei paljoakaan käsittele hankintoja, hankintojen muotoja, menettelytapoja ja toteuttamista. Asiasta on ihan uusi Vahdin ohje (3/2011), joten asiaa ei sovi unohtaa tässäkään, vaikka sitten paljossa viitattaisiinkin tähän uuteen hankintaohjeeseen. Kun näin ei ole

Käyntiosoite	Postiosoite	Puhelin	Telekopio	Sähköpostiosoite
Kasarmikatu 42	PL 25	09 160 03	09 1606 7731	oikeusministerio@om.fi
HELSINKI	00023 VALTIONEUVOSTO			

tehty, paljon olennaista sovellushankkeeseen vaikuttavaa jää ulkopuolelle, joka haittaa ohjeen käytettävyyttä.

Ohjeen kuvassa neljä (s.29) määritellään (ilmeisesti sovelluskehityksen) elinkaaren joka vaihe ja vaiheiden tehtävät.

Esitutkimusvaiheen osalta todetaan seuraavat tehtävät:

Strategian mukaisuus

Projektin riskianalyysi

Jatkuvuussuunnitelmat

Turvallisuussuunnitelma

Projektiohjeet

Näistä tehtävistä voidaan todeta seuraavaa:

Strategian mukaisuus lienee hyväksyttävissä, joskin voisi tarkentaa mistä kaikista strategioista on tässä kyse. (esim. toiminnan strategiset suunnitelmat, tietohallinnon strategiset suunnitelmat, tietoturvastrategia)

Projektin riskianalyysi: onko kyse projektin oman toiminnan riskianalyysistä vai projektin toimintaympäristön riskianalyysistä. Jälkimmäinen voisi olla parempi ja sitä sitten täydennetään myöhemmin.

Jatkuvuussuunnitelmat: Ei kannata tehdä tässä vaiheessa, koska sisältö selviää elinkaaren myöhemmissä vaiheissa. Riskianalyysin yhteydessä voisi määritellä jatkuvuuden yleiset tavoitteet esim. sovelluksen tulee toimia aina, tulee toimia pääsääntöisesti työpäivinä, tulee toimia työpäivinä, työpäivän- kahden katkot kuitenkin mahdollisia jne.. sekä arvioita siitä onko sovelluksen osalta luottamuksellisuus, eheys, saatavuus millä tavalla tärkeitä. Itse projektin osalta voidaan mennä syvemmälle riskiarvion pohjalta.

Turvallisuussuunnitelman osalta menettelyt kuten jatkuvuussuunnitelmien osalta. Eli tässä yhteydessä käydään läpi vain keskeiset periaatteet.

Tarkemmat jatkuvuus- ja turvallisuussuunnitelmat kannattaa tehdä myöhemmässä vaiheessa esim. projektin suunnittelun yhteydessä.

Projektiohjeet. O.k.

Asiakirja sisältää suhteellisen runsaasti linkkejä muuhun materiaaliin. Osa linkeistä viittaa kaupallisten toimittajien tuotoksiin (esimerkiksi tietoturvan huomioiminen ketterissä menetelmissä). Linkkien sisällyttämistä tekstiin voisi vielä uudelleen harkita asiakirjan ylläpidon näkökulmasta: hyperlinkkien osoitteet eivät välttämättä ole pysyviä. Vähintäänkin osoitteiden yhteyteen tulisi laittaa merkintä, milloin linkin kohde on haettu, eli milloin sen sisältö on ollut saatavilla.

Luvussa 2.4. puhutaan sovelluskehityksen rooleista. Projektin asettajasta mainitaan, että hän "toimii ohjausryhmässä puheenjohtajana". Näin voi usein ollakin, mutta ei aina.

Käsitteistö tulisi pitää yhdenmukaisena koko asiakirjassa. Esimerkiksi tietoturvavastaava ja tietoturvallisuusvastaava tarkoittanevat samaa roolia.

Monitoimittajuus (luku 2.8) on nykyisin normaalitilanne sovelluskehitysprojekteissa. Näin ollen monitoimittajuuteen liittyvät tietoturvahaasteet tulisi sisällyttää muun tekstin joukkoon, esimerkiksi arkkitehtuurilukuun.

Sovelluskehityksen vaiheita tarkasteltaessa tietoturvallisuuden näkökulmasta huomioon voisi ottaa myös käytöstä poistuvien järjestelmien sisältämän tiedon konversioon liittyvät tietoturvatarpeet. Konversionäkökulmaa tulisi miettiä jo esitutkimusvaiheessa. Samoin jo tällöin tulisi pohtia, onko kehitettävässä järjestelmässä pitkäaikaissäilytettävää tai pysyvästi säilytettävää aineistoa. Näiden osalta tulisi huomioida SÄHKE2-vaatimukset. Ohjeluonnoksessa näitä asioita käsitellään kohdassa 3.3.8 (käytöstä poisto), mikä on aivan liian myöhäistä.

Sovelluskehityksen vaiheisiin liittyvien tietoturvatasovaatimusten sijoittelu ei kaikilta osin vastaa OM:ssä olevaa käsitystä eri vaiheiden tehtävistä. Nyt toteutusvaiheeseen sijoitetut vaatimukset ovat suurelta osin sellaisia, jotka on otettava huomioon jo sovellusta suunniteltaessa. Toteutusvaiheessa virheiden käsittelyn ja lokituksen miettiminen on jo liian myöhäistä. Testausvaiheeseen oli sijoitettu toteutusvaiheeseen liittyviä tietoturvavaatimuksia (TOT-008 - TOT-011). Myöskään koodikatselmointi (TST-004) ei ole osa testausta vaan tehdään toteutusvaiheen aikana.

Monessa kohtaa kuvat ja siihen liittyvä teksti eivät vastaa toisiaan. Esim. s. 12 tietohallintovastaava tai tietoturvavastaava. Kuvassa tietoturvavastaavaa informoidaan esitutkimuksessa mutta ei sen jälkeen ennen kuin käyttöönotossa, Kuitenkin koko ohje käsittelee juuri väliin jääviä asioita. Eikä tietoturvavastaavan tarvitse olla mukana näissä?

Voisiko kuvan notaatio/kuvaustapa olla toisenlainen tai selkeämpi esim. RACI -matriisin mukainen. Nyt kuvan esille tuomat asiat voidaan ymmärtää väärin.

s. 17 Monitoimittajuutta ja asiakkuutta koskevissa luvuissa ei ole huomioitu ollenkaan sisäisiä toimittajia/palvelusopimuksia. Monella hallinnonalalla toimii palvelu- tai tietotekniikkakeskus tilaaja-tuottajamallin mukaisesti. Tilaajan vastuita ei ole käsitelty ollenkaan.

s. 17 kohta 2.10 Sopimukset

Tulkintanne mukaan sovelluskehitysohje koskee uutta sovelluskehitystä eikä tarkoitus ole avata vanhoja, mahdollisesti jo lähiaikoina käytöstä poistuvia sovelluksia. OM:n hallinnonalalla on paljon vanhoja sovelluksia ja niiden muuttaminen ohjeen mukaisiksi ei ole mahdollista ilman tuntuvia investointeja. Eräin osin vanhoja järjestelmiä ei teknisistä syistä edes pystytä muokkaamaan vastaamaan ohjeen vaatimuksia.

Toivomme, että ohjeen tarkoitusta määriteltäessä tuotaisiin selkeästi esiin se, että ohjetta pyritään soveltamaan vain uusien tai uusittavien järjestelmien kehittämiseen.

Tekijänoikeudet luvussa 4.11: Asia on mainittu JIT:ssä ja sen tulisi olla aina mukana tarjouspyynnössä ja sopimuksissa.

Avoimet verkot luvussa 4.2: Olemme olettaneet, että tulevaisuudessa kaikki kytkennät menevät Kytkyn kautta, joten tähän liittyviä tietoturvaratkaisuja ei tarvitse erikseen toteuttaa muuta kautta.

Luku 5,2. Julkisuus: Tulee huomioida, että salassapito voi koskea vain osaa asiakirjasta. Toisaalta vaikka asiakirja on lain mukaan julkinen se voi sisältää arkaluonteista tietoa, kuten henkilötunnuksia tms., jolloin suojaustarpeita on.

Asiakirjan ulkoasusta:

Tietoturvaohjeessa käytetty kirjasintyyppi vaihtelee asiakirjan osien välillä.

Kuvassa 3 ohjaus- ja toteutus- toiminnot eivät helposti erotu toisistaan.

Kuvan 4 tekstit ovat epäselviä.

tietohallintojohtaja Max Hamberg

erityisasiantuntija Timo Erjansola