Lausunto sovelluskehityksen tietoturvaohjeesta (lausuntopyyntö 26.4.2012, VM047:14/2007)

Työskentelemme tietoturvatehtävissä, jotka tukevat tietoturvallisten tietoteknisten tuotteiden ja palvelujen tuottamista. Halusimme antaa lausunnon, koska ohje tulee todennäköisesti vaikuttamaan yksityisen sektorin palvelutuottajiin. Aikataulullisista syistä annamme kommentin yksityishenkilöinä. Yhdessä kuitenkin edustamme 29 vuotta tietotekniikka-alan kokemusta, josta 15 vuotta tietoturva-alan kokemusta.

Tietotekniset ratkaisut turvallisten ja saatavilla pysyvien palvelujen mahdollistajina

Sovelluskehitysprojektia koskevat huomiot luonnoksessa ovat arvokkaita ja ne on johdettu sovelluskehityksestä käsin. Ohje voisi syvemmin heijastella kautta linjan *palvelun* toimintaprosessien kokonaisvaltaisempaa huomioon ottamista sovelluskehitysprojektiin liittyvissä tehtävissä sekä tarvittavissa rooleissa. Tästä esimerkkinä kappaleessa 3.2 kuva 4, jossa Määrittely – vaiheessa todetaan yhden tehtävän olevan käyttäjäroolien määrittely. Palvelun osalta on tavallisesti tarve määritellä toimintatavat palvelun antamisessa. Toimintatavat antavat viitteitä mahdollisista käyttäjärooleista, joita järjestelmällä tulisi voida toteuttaa. Palvelu on tavallisesti jotain laajempaa kuin siinä käytettävät sovellukset ja joskus palvelua tuotetaan sovelluksista huolimatta.

Kappaleessa 2 palvelut määritellään kapea-alaisesti teknisiksi komponenteiksi. Niin valtion- ja kuntahallinnon organisaatiot sekä yksityisen sektorin organisaatiot ovat käytännössä erilaisista palveluista muodostuvia yksikköjä, joiden organisaatiorakenne, hallintomalli ja tietojärjestelmät tukevat palveluryppään toimintaa, palvelun tuottamista. Sitä se on silloinkin, kun palvelulla ei ole ulkoisia asiakkaita.

Tällaisessa ympäristössä tavoitteita tukevat parhaiten sovelluskehitysprojektit, jotka rakentavat ensi sijassa palvelua ja siinä sivussa myös sitä turvallista työkalua. Sovelluksen turvallisuus on osa koko palvelun turvallisuutta.

Sovelluskehitysprojektin turvallisuusvastuut

Kappaleesta 2.4 kuvasta 3 puuttuu merkintä ohjausryhmän vastuullisuudesta. Lisäksi tekstiosuudessa olisi hyvä syventää, mikä vastuu ohjausryhmällä on projektin tavoitteiden (esimerkiksi tietoturvallisuuden toteutumisen) saavuttamiseksi ja miten se eroaa esimerkiksi projektipäällikön vastuusta.

Sovelluskehitysprojektin riskinhallinnan vieminen osaksi koko organisaation riskinhallintaa

Luonnoksessa voisi kautta linjan selkeämmin tuoda esiin riskinhallinnan kohdalla sitä, miten ja kuka projektissa huolehtii siitä, että projektin

riskinhallintatyössä esiin tulleet seikat viedään osaksi koko organisaation riskinhallintaa.

Standardoinnin tila

Ohjeessa on runsaasti viitteitä muihin sovellus- ja ohjelmistoturvallisuushankkeisiin. Ohje mainitsee sovelluskehityksen turvallisuuden standardisarjan ISO 27034. Sen ensimmäinen osa, ISO/IEC 27034-1:2011, on jo valmis, joten ohjeen ja standardin käsitteiden ja terminologian vertailu ja vastaavuuksien taulukointi voisi olla hyödyllistä – erityisesti, jos uusi standardi saavuttaa 27-sarjan muiden standardien suosion.

Vaatimusten kustannusvaikutukset ohjelmistotuotantoon

Puhtaasti tietoturvamielessä ohjeen vaatimukset ovat tervetulleita, mutta vaatimuksilla tulee olemaan mahdollisesti merkittäviä kustannusvaikutuksia ohjelmistotuotantoon, erityisesti pienille yrityksille.

Tällä hetkellä todennäköisesti ainoa julkinen lähde eri yritysten ohjelmistoturvallisuusaktiviteeteista on yhdysvaltalaisen Cigital-yhtiön BSIMM (Building Security In Maturity Model, http://www.bsimm.com/facts/). Hankkeessa on kartoitettu yli sata ohjelmistoturvallisuusaktiviteettia ja tutkittu niiden käytännön toteutumista tätä kirjoittaessa 49 (tyypillisesti suurehkossa) yrityksessä. Suomesta tutkimuksessa ovat tällä hetkellä mukana Nokia, Nokia Siemens Networks ja F-Secure, kaksi viimeksi mainittua seuraavassa versiossa.

Ohjeen vaatimuksia voisi ehkä peilata BSIMM-tutkimuksessa havaittuun aktiviteettien yleisyyteen, koska niiden perusteella voi alustavasti arvioida, mikä ohjelmistokehitysprosessin muutostarve yrityksissä todellisuudessa olisi.

Ketterä ohjelmistokehitys ja sen turvallisuus

Ketterän ohjelmistokehityksen nostaminen ohjeessa erikseen esille on erinomainen asia. Ketterien menetelmien ja turvallisuuden ristiriidasta liikkuu usein epäilyjä, joten ohjeen selkeä vaatimus samojen tehtävien ja vaatimusten täyttämisestä on tervetullut. Ketterien menetelmien huomiointi ei kuitenkaan ole täysin läpileikkaavaa, koska esimerkiksi kappaleen 2.4 suositus tiukasta työnjaosta toteuttajien ja testaajien välillä on suorassa ristiriidassa esimerkiksi testausohjatun kehityksen (TDD, test driven development) kanssa. Pikemminkin tulisi puhua ohjelmistotuotannon ja vaatimustenmukaisuuden hyväksymisen erottamisesta kuin ohjelmistokehityksen vaiheiden erottamisesta.

Ketteriä menetelmiä käytettäessä turvallisuuden näkökulmasta yksi olennaisimmista rooleista on tuoteomistajan (product owner) rooli. Tuoteomistaja on mainittu kappaleen 2.3 kuvassa ja rooli selitetään kappaleessa 3.2.1, mutta sitä ei ole mainittu muissa rooliluetteloissa. Ohjeen soveltuvuutta ketteriin menetelmiin voisi parantaa, mikäli tuoteomistajan vastuita selkeytettäisiin esimerkiksi kappaleissa 2.4 ja vaatimuksessa OSK-005. Tämä

toisi ketterät menetelmät myös ehkä hieman tasa-arvoisemmaksi vaihtoehdoksi ohjeen näkökulmasta.

Kappaleessa 2.3 viitataan Agile Finlandin seminaariin. Seminaarin jälkeen aiheen tutkimista on jatkettu ja aiheesta on olemassa paperi herättämään keskustelua (http://www.fokkusu.fi/agile-security/) . Kappaleen 3.2.1 kuvaus tuoteomistajan rooleista on varsin yhdenmukainen tämän kanssa, joten tämä paperi voisi toimia lisäviitteenä.

Kunnioittaen,

Antti Vähä-Sipilä
Tietoturva-asiantuntija (CISSP, CSSLP, CISM)
avs@iki.fi

Tuuli Siiskonen
Tietoturva-asiantuntija
tuuli.miettinen@gmail.com