Pääesikunta
Johtamisjärjestelmäosasto
HELSINKI

Lausunto

AI10390

22.5.2012

Valtiovarainministeriö (toimitus sähköpostilla osoitteeseen valtiovarainministerio@vm.fi)

PL 28
00023 VALTIONEUVOSTO

Viitteet

LAUSUNTO VAHTI SOVELLUSKEHITYKSEN TIETOTURVAOHJEESTA

Puolustusvoimat vastaa tällä asiakirjalla 25.4.2012 Valtionvarainministeriöltä tulleeseen lausuntopyyntöön SOVELLUSKEHITYKSEN TIETOTURVAOHJEESTA. Lausunto koskee ohjeistuksen versiota 0.9.

Puolustusvoiminen edustajat tekivät seuraavia huomioita ohjeluonnoksesta:

Koko ohjetta kokonaisuutena tarkasteltaessa ohjeen tulee ottaa enemmän kantaa normaalin ohjelmistojen laadunvarmistamiseen, jonka osa tietoturvakin on. Kaikki ohjelmistovirheet ovat mahdollisia hyökkäysvektoreita ja tietoturvahaavoittuvuuksien ensimmäinen puolustuslinja on normaalin ohjelmistokehitysprosessin laadunvarmistamismenetelmät. Näiden lisäksi ohjelmistoon voidaan kohdistaa erityisiä tietoturvaa testaavia/parantavia toimenpiteitä. Ohjelmistotestauksen eri kerrokset (esim. V -malli) on hyvä käydä läpi ohjeen alussa taustatietona. Lisäksi voi pohtia olisiko hyödyllistä käydä läpi sitä että minkälaisia tietoturvaongelmia saadaan torjuttua eri testauskerroksilla ja millaisilla menetelmillä. Lisäksi voi pohtia minkälaisia tietoturva-ongelmia voidaan torjua eri testauskerroksilla.

Toinen asia mihin tulee kiinnittää huomiota, on vaatimustenmäärittely. Mikäli ohjelmiston vaatimukset on määritelty huonosti, niin tietoturva-vaatimuksia ei ole tai niitä ei ole mietitty loppuun saakka. Tämä johtaa siihen että normaali ohjelmistotestausprosessi ei saa tuollaisia virheitä kovin helposti kiinni.

Ohjeen loppu on kovin taulukkomainen ja tekee lopun lukemisesta raskaampaa. Lopun liitteisiin kannattaa tehdä lyhyitä tarkastuslistoja tuomaan lisää käytännön esimerkkejä ja konkretiaa ohjeeseen (esim. tunnetut ”testausstandardit” OWASP, PTES, framework, jne), lyhyt tarkastuslista onko organisaatiosi sovelluskehitys tietoturvallista?, jne.

Muut kommentit:

Sivu 3

” Tietoturvallisuusasetuksen (681/2010) mukaan organisaatioiden tulee saavuttaa tietoturvallisuuden perustaso 1.10.2013 mennessä.”

Onko tuo päivämäärä oikea, esimerkiksi Vahti 2/2010 (s. 7) ohje antaa määräpäiväksi 30.9.2013?

Sivu 11 (ja muut samankaltaiset kohdat)

Linkkiviittaukset tarvitsevat lisää tekstiä. Puhtaat linkkilistaukset ilman yhteenvetoa mitä linkin takana on, ei sovellu ohjeen tyyliin, koska ohjeen tarkoitushan on kertoa miten sovelluskehityksessä pitäisi tietoturva-asioita huomioida ja auttaa erilaisten muiden ohjeiden tulkinnassa. Toivottavaa on että ohje vetää yhteen erilaisten linkkien takana olevia parhaimpia käytäntöjä tms. Jos lukija haluaa lisätietoja niin tämän jälkeen hän voi siirtyä ohjeen ulkopuolelle lukemaan linkkien takana olevaa tietoa. Tämä on erityisen tärkeää juuri kappaleessa kerrotuista ketterissä menetelmistä, koska niitä käytetään pääsääntöisest/yleisesti.

Sivu 12

”Esi-merkiksi sovelluksen koodaus, testaus ja hyväksyminen suositellaan vahvasti eri henkilöiden toimesta suoritettavaksi.”

Ohjelmistotestaus hyötyy siitä että testiryhmässä on mukana erilaisia ihmisiä erilaisine taustoineen. Osa voi olla ohjelmiston kehittäjiä, koska ohjelmiston hyvä tuntemus (esim. ohjelmistokehityksessä saatu) edesauttaa ohjelmiston ohjelmistovirheiden löytymistä. Tärkeää on kuitenkin muistaa se että jokaisella testauskerroksella (esim. V -mallin kerrokset) on huomioitu riittävästi vaarallisten työyhdistelmien syntyminen. Lisäksi ohjelmistokehittäjät tulevat usein sokeaksi omille virheilleen.

Sivu 15

”tulee sovelluksen kriittisyys arvioida ennen kehitysprosessin aloittamista. Kehitettävän sovelluksen merkityksen arviointiin on käytettävä kahta eri näkökulmaa: sovelluksen käsittelemän tiedon asettamat vaatimukset sekä sovelluksen itsensä kriittisyys organisaation toiminnalle.”

Hienoa on jos tässä samassa yhteydessä voidaan määrittää tavoitteita tietoturvan osalta ja määrittää niihin yksikäsitteisen validointikriteerit joihin voidaan palata esim. hyväksymistestausvaiheessa. Tämä selventää kaikille osapuolille sitä että minkälaisia tietoturva-asioita tulee kehityksessä

huomioon ja mikä on niissä hyväksyttävä taso. Tietoturvavaatimusten kartoitus tulee ottaa osaksi alussa tehtävää sovelluksen vaatimusmäärittelyä. Kaikki testauksen vaiheet pohjautuvat enemmän tai vähemmän vaatimusmäärittelyssä tulleisiin vaatimuksiin. Esim. vaatimus ”Tiedon tulee olla saatavissa” on hyvin ylimalkainen ja se varaan on vaikea rakentaa yksikäsitteistä validointikriteeriä.

Sivu 24

Vastaavanlaisia esimerkkejä saisi olla ohjeessa runsaammin. Ne tuovat konkretiaa hyvin ylätasolla olevaan ohjeeseen.

Sivu 30

Ketterien menetelmien tietoturvatestauksen ohjenuorana on testaussuunnitelma ja vaatimusten määrittelyvaiheessa määritelty tavoitteiden validointikriteerit. Testaussuunnitelman mukaisesti nämä kohdat testataan suunnitelmassa riittäväksi katsotulla tekniikoilla (esim. test caseilla, yksikkötestaus, katselmoinneilla, erikoistyökalut). Näiden lisäksi tietoturvaan ketterissä menetelmissä voidaan käyttää sivulla 30 esitettyjä menetelmiä. Tärkeää tässä on kuitenkin se että tietoturvatestaus on leivottu esim. testaussuunnitelman kautta prosessiin sisään eikä vain yksistään luoteta siihen että joku tekee työjonoon tietoturvaan liittyviä tehtäviä.

Suositeltavaa on että organisaatio luo omasta ohjelmistokehitysprosessistaan prosessikaavion ja miettii miten kehittäjän kirjoittama koodirivi päätyy lopulliseen tuotteeseen ja mitä laadunvarmistuskeinoja sen tulee ensin käydä läpi ennen kuin se päätyy valmiiseen tuotteeseen. Tietoturvatestausta ei voida erottaa kunnolla normaalista ohjelmistotestauksesta, koska yksi ohjelmistovirhe on aina mahdollinen hyökkäysvektori. Testauksen tarkoituksena on vähentää ohjelmistovirheitä ja siis mahdollisia hyökkäysvektoreita.

Sivu 38 (ja muut samankaltaiset kohdat)

Linkit wikipediaan on hyvä laittaa esim. alaviitteisiin.

Osastopäällikön sijainen
Eversti Mikko Heiskanen

Sektorin johtaja
TkT Catharina Candolin

Tämä asiakirja on sähköisesti allekirjoitettu.

JAKELU

TIEDOKSI