#tuki2018 #stöd2018

Sisäänrakennettu tietosuoja ja ohjelmistokehitys

Petri Strandén

—

14. kesäkuuta, 2018

Petri Strandén

#tuki2018 #stöd2018

Manager
Cyber Security Services
Application Technologies
Petri.stranden@kpmg.fi

Petri vastaa KPMG:n Technology Advisoryn ohjelmistokehityksestä.

Agenda

#tuki2018 #stöd2018

- Johdanto
- Ohjelmistokehitys
- Ohjelmistokehitys vs. konsultointi
- Vaatimukset
  - Käyttötapaukset
  - Toiminnalliset vaatimukset
  - Ei-toiminnalliset vaatimukset
- Tietosuoja ohjelmistokehityksessä
- Tietosuoja ohjelmistokehityksessä kiteytettynä
- Hankinnan haasteita

Johdanto

#tuki2018 #stöd2018

- Esitys käsittelee ohjelmistokehitystä ns. kehittäjän näkökulmasta
- Kehittäjän tuntemus tilaajan toimialasta sekä toimintaympäristöstä ei useinkaan ole syvällistä
- Tilaajalle on olennaista kyetä kertomaan ja kuvaamaan tarpeensa mahdollisimman hyvin
- Ohjelmistokehityksen näkökulmasta ei oteta kantaa onko tietyn ohjelmiston kehittäminen järkevää vai ei
- Olemassa olevien ohjelmistojen sopivuutta tulee arvioida omia tarpeita ja vaatimuksia vasten

Ohjelmistokehitys

#tuki2018 #stöd2018

- Ohjelmistoja kehitetään tarvelähtöisesti ja tarve voi tulla esimerkiksi:
  - Lainsäädännöstä
  - Yksittäiseltä asiakastaholta
  - Kokonaisen markkinasegmentistä
  - Asian tekemisestä tietyllä tavalla
- Erilaisista tarvelähtökohdista kehitetyt ohjelmistot eroavat toisistaan yleisesti
  - sopivuudessa tiettyyn tehtävään
  - muokattavuudessa
  - ylläpidettävyydessä

Ohjelmistokehitys vs. konsultointi

- Jos omiin tarpeisiin sopivaa ohjelmistoa ei löydy, joudutaan tilanteeseen jossa:
  - Muokataan omia prosesseja ja toimintatapoja, jotta voidaan käyttää valmista ohjelmistoa
  - Tilataan ohjelmiston kehitys omien prosessien ja toimintatapojen tueksi
- Hankintaa valmistellessa on tärkeää hahmottaa omien prosessien vaikutus ohjelmistolle asetettaviin vaatimuksiin
  - Riippumatta siitä onko hankittava ohjelmisto valmis vai räätälöity
- Ohjelmistokehityksentarjoajan on haastavaa ottaa kantaa asiakkaan prosesseihin ja toimintatapoihin
  - Kaikki tilaajat **eivät halua** tai **voi** muuttaa prosessejaan
- Kaikki ohjelmistokehitystarjoajat eivät välttämättä osaa tai edes halua ehdottaa kokonaisratkaisua (mikä voi olla esimerkiksi prosessimuutos ilman ohjelmistokehitystä) tulonmenetyksen pelossa

Ohjelmiston hankinta

- Ennen hankintaa on olennaista huomioida kuinka aiottu ohjelmisto sopii olemassa olevaan arkkitehtuuriin
- Hankintaprosessia itseään on hyvä arvioida jo etukäteen
  - Kehitettävän ohjelmiston hankintaa tulee arvioida kirjattuja vaatimuksia vasten.
  - Olemassa olevien ohjelmistojen sopivuutta tulee arvioida omia tarpeita ja vaatimuksia vasten.
- Jo etukäteen on hyvä miettiä eri vaatimusten välisiä painoarvoja arvioinnin helpottamiseksi

Vaatimukset 1/3
Käyttötapaukset

#tuki2018 #stöd2018

Käyttötapaukset

- Hankintaa varten tulee määritellä prosessit, joissa ohjelmistoa käytetään

Käyttötapauksen tiedot	
Käyttötapauksen nimi	Aloita esimerkki-ilmoitus
Käyttötapauksen numero	1
Tekijä	Matti Meikäläinen
Päivämäärä	13.6.2018
Versio	1
Viimeksi muokattu	13.6.2018 – Matti Meikäläinen
Lyhyt kuvaus	Järjestelmä näyttää aloitusnäytön, josta käyttäjä valitsee organisaation, jonka ilmoituksen haluaa tehdä.
Aktori	Ilmoittaja
Toissijainen aktori	Tarkastaja
Esiehdot	Käyttäjällä on toimivat tunnukset järjestelmään Käyttäjällä on pääsy järjestelmään Käyttäjä on kirjautunut järjestelmään ja näkee etusivun, organisaatiovalinnan sekä painikkeet.

Vaatimukset 2/3
Toiminnalliset vaatimukset

#tuki2018 #stöd2018

Toiminnalliset vaatimukset

- Mitä ohjelmiston tulee pystyä tekemään?
- Vaatimukset koskien ohjelman ominaisuuksia
- Liiketoimintavaatimukset
- Yleensä tehdään määrämuotoisesti esim. käyttäjätarinoina:
  - As <person>, I can <what?> so that <why?>

Esimerkki

- As preparer I want to be able to upload my accounts information in Microsoft Excel format so that I can use my available software to fill the file.

Vaatimukset 3/3
Ei-toiminnalliset vaatimukset

#tuki2018 #stöd2018

Ei-toiminnalliset vaatimukset

- Miten ohjelmiston tulee toimia?
- Vaatimukset koskien ohjelman suoriutumista, esimerkiksi:
  - Suorituskyky
  - Saatavuus
  - Käytettävyys
  - Yms

Esimerkkejä

- Järjestelmän tulee olla käytettävissä 99% ajasta
- Järjestelmän tulee olla STIII –luokituksen mukaisesti sertifioitu
- Järjestelmästä tulee ottaa varmuuskopio päivittäin

Tietosuoja ohjelmistokehityksessä

- Tietosuoja määrittelee kuinka prosesseissa käsitellään tietoja ja asettaa vaatimuksia prosesseissa käytettäville ohjelmistoille ja niiden käyttötavoille.
- Ohjelmiston toimintaympäristö ja prosessit tulee avata toiminnallisten ja ei-toiminnallisten vaatimusten kautta
  - Asiakas tietää oman toimintaympäristönsä tietosuojaan kohdistuvat vaatimukset ja säädökset parhaiten
- Vaatimusten kirjaamisen lisäksi suora vuorovaikutus kehityksen aikana edesauttaa vaatimusten täyttymistä
- Tietosuoja vaikuttaa ohjelmiston elinkaaressa etenkin palvelun käytön aikana, mutta vähemmän itse kehityksen aikana
- Tietosuojaa tuleekin arvioida koko ohjelmiston elinkaarta ajatellen
  - Kehitys: käyttäjien tunnistaminen, todentaminen ja käyttövaltuudet, lokitietojen sisältöjen määrittäminen, kehitys ja testaus tekaistulla tiedolla
  - Käyttö: ylläpitäjien vs. käyttäjien oikeudet, ylläpito-oikeuksien hallinnointi, lokitietojen lukeminen, virhetilanteiden selvittäminen, oikeassa käytössä on oikeaa tietoa

Tietosuoja ohjelmistokehityksessä kiteytettynä

#tuki2018 #stöd2018

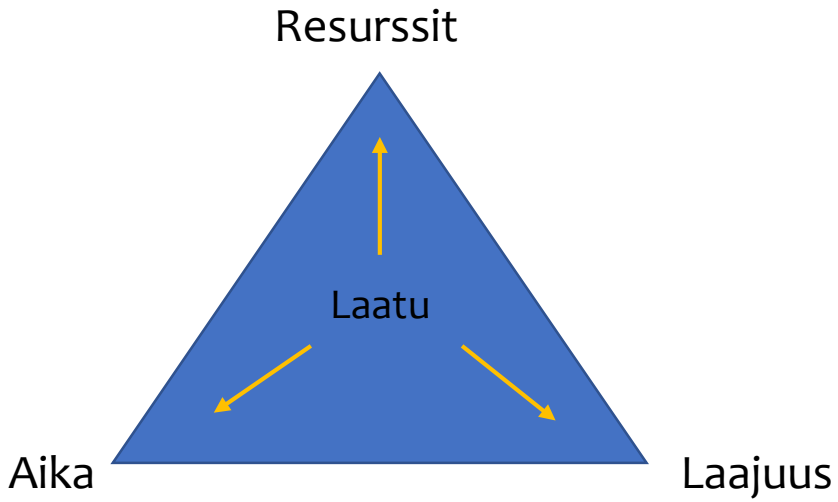
- Ohjelmistokehityksessä on tietoturvan osalta valmiita ohjelmistokehitysviitekehyksiä esimerkiksi OWASP:n ASVS*
  - Määrittävät ja asettavat vaatimuksia kuinka toiminnallisuus toteutetaan
- Tietosuojan osalta vastaavia viitekehyksiä ei oikein ole
  - Yleisillä käytänteillä päästään jo pitkälle (ei oikeaa tietoa testeihin, käyttäjät pääsevät vain omiin tietoihin)
  - Tietosuojasta johdetut vaatimukset määrittävät mitä toiminnallisuuksia toteutetaan ja kuinka niitä käytetään
- Esimerkiksi tekstinkäsittelyohjelma:
  - On vaikea edes tehdä vaatimuksia ohjelmalle tietosuojan osalta, mutta on helppo määritellä prosessit ja toimenpiteet kuinka tekstinkäsittelyohjelmalla tuotettuja tiedostoja voidaan ja saadaan käsitellä, kenen toimesta jne.

* OWASP = Open Web Application Security Project
ASVS = OWASP Application Security Verification Standard

Hankinnan haasteita

#tuki2018 #stöd2018

- Keskitetty hankinta:
  - Hankinnassa ei välttämättä ole tarkkoja vaatimuksia ja tietoa lopullisista prosesseista kuinka työkalua käytetään
  - Kyky vuoropuheluun tarpeista ja vaatimuksista ensisijaisen tärkeää
- Kehitysprosessin kolminaisuus: aika, resurssit ja toteutuksen laajuus – jos yksi lukitaan niin muiden täytyy joustaa
- Hankintaprosessin joustamattomuus etenkin ohjelmiston kehityksen aikana voi pahimmassa tapauksessa johtaa kehitysprojektin epäonnistumiseen



#tuki2018 #stöd2018

Kysymyksiä?

#tuki2018 #stöd2018

KIITOS

#tuki2018 #stöd2018

Kuntaliitto
Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto