

Ohjelmistojen valinta turvallisuuskriittisissä järjestelmissä

Jouni Rosenlöf
KTM, CISA, CISSP
JRComplex Oy
www.jrcomplex.fi
jouni.rosenlof@jrcomplex.fi
GSM: 050 363 9002



Kuka?

JRCComplex

- Jouni Rosenlöf
 - JRCComplex Oy:n perustaja ja toimitusjohtaja
 - lähes 9 v IT ja tietoturvakonsulttina
 - Linux käyttäjä vuodesta 95 alkaen, työpöydällä 98 alkaen
- JRCComplex Oy
 - Auditointiosaamista
 - Open Source ja Linux osaamista
 - toiminta alkanut keväällä 2003
 - Asiakasreferenssinä mm. Valtiovarainministeriö, Kesko, TietoEnator, Yleisradio jne.

Esityksen rakenne

JRCComplex

- Määrittely
- ICT-hankintojen ihmeellinen maailma
- Perspektiiviä
- Uhkakuvia
- Omia kokemuksia
- Miten Open Source ratkaisu valitaan
- Yhteenveto

- Kriittinen järjestelmä?
 - Liiketoiminnan näkökulma (yritysmaailma)
 - Tiedon käsittelyn näkökulma (julkishallinto)

- Turvallisuuskriittinen järjestelmä?
 - Liiketoiminnan näkökulma
 - Tietoturvallisuuden näkökulma
 - Tiedon käsittelyn näkökulma
 - Juridinen näkökulma

- Ohjelmistojen valinta (hankinta)?
 - Virallinen hankintamenettely
 - Vahti 6/2001 Valtion Tietotekniikkahankintojen Tietoturvallisuuden Tarkistuslista
 - Vyse
 - Keittiön kautta

ICT-hankintojen ihmeellinen maailma

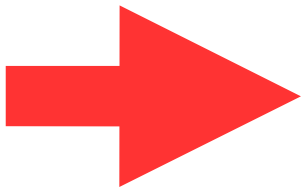
JRComplex

ICT hankinnat pohjaavat perusteelliseen kustannushyöty arviointiin, ratkaisujen teknisten ominaisuuksien vertailuun sekä riskiarviointiin - Niinkö???

ICT-hankintojen ihmeellinen maailma

JRComplex

- Onnistunut järjestelmähanke on...
 - Onnistunut esiselvitys ja evaluointi
 - Onnistunut valinta
 - Onnistunut projekti
 - Onnistunut tekninen käyttöönotto ja integrointi
 - Onnistunut käyttäjäkoulutus ja henkilöstön mukaantulo
 - Onnistunut ylläpito ja hallinta
 - Onnistunut jatkokehitys
 - Onnistunut siirtyminen seuraavaan järjestelmään - versioon
 - Tarvittaessa onnistunut palveluntuottajan, sovelluskehittäjän, kumppanin, teknisen komponentin, konsultin tms. vaihto



Tietoturvatavoitteen saavuttaminen edellyttää kaikkien osa-alueiden onnistumista

ICT-hankintojen ihmeellinen maailma

JRCComplex

- Eräs vaatimusmäärittely
 - Toimintavarmuus
 - Kustannustehokkuus
 - Integroitavuus
 - Skaalautuvuus
 - Liiketoimintaprosessien tehostaminen
 - Uuden sukupolven ratkaisut
 - Keskitetty hallinta
 - Tiedon-, sisällön- ja dokumenttien hallinta
 - Mobiilivalmius
 - Tietoturva

ICT-hankintojen ihmeellinen maailma

JRCComplex

- Tietoturvallisuusmäärittely
 - Valvontaominaisuudet
 - Kontrollit
 - Järjestelmähallinta
 - Käyttövaltuushallinta
 - Kompleksisuus
 - Teknologian kypsyys - uutuus
 - Dokumentointi
 - Testaus ja laadunvarmistus
 - Muutosnopeus
 - Tietoturvaominaisuudet
 - toimittajan tietoturvaosaaminen

ICT-hankintojen ihmeellinen maailma

JRCComplex

- Näkökulmia riittää organisaatiossa
 - Busineksen näkökulma
 - Tietohallinnon näkökulma
 - Loppukäyttäjien näkökulma
 - Sidosryhmien näkökulma
 - Tietoturvaihmisten näkökulma

ICT-hankintojen ihmeellinen maailma

JRComplex

- Softaa ja ratkaisuja ei voi hypistellä, kaikki on vain mielikuvia (powerpointwarea)
- Saavutettuja hyötyjä ei voi mitata etukäteen
- Päätöksiä tekevät ihmiset eivät yleensä ymmärrä tekniikkaa
- Riippumatonta vertailutietoa on hyvin vähän saatavilla
- Päätös tehdään ensin ja sitten etsitään sille sopivat perustelut
- Mitä suurempi hanke, sen abstraktimmaksi se muuttuu

ICT-hankintojen ihmeellinen maailma

JRComplex

- Väitän vahvasti että...
 - Mielikuvat ratkaiset 85% hankintapäätöksestä
 - Asiakas tehdään tietoiseksi ajankohtaisesta ongelmasta, jonka myyjän ratkaisu tuntuu ratkaisevan
 - Myyjän ratkaisu sisältää sopivasti ”trendisanoja”, jotka ovat ostajalle tuttuja
 - Myyjän ratkaisu sisältää sopivasti ko. liiketoiminta-alueen avainsanoja
 - Menestyvän ratkaisun- ja ratkaisutoimittajan tunne (=kivaa olla aallonharjalla ratsastajien mukana)

ICT-hankintojen ihmeellinen maailma

JRCComplex

- Mielikuvat ratkaisevat 85% hankintapäätöksestä
 - Ostajan henkilökohtainen miellyttämisen tarve (luontainen tarve olla takaisinpäin ystävällinen, mukavien lätkämatsi-, oopperajuhla-, tms. reissujen jälkeen)
 - Ostajan hintamielikuva vastaa myytävän ratkaisun kustannuksia ”tämän tason business ratkaisun” kustannuksista
 - Toimittajan ja ratkaisun koko vastaa ostajan ”pelikenttää”

ICT-hankintojen ihmeellinen maailma

JRComplex

- Mielikuvat ratkaisevat 85% hankintapäätöksestä
 - Mielikuva uskottavan tuntuista referensseistä, markkinatutkimuksista, analyyseistä, konsulttilausunnoista tms.
 - Ostajan mielikuva edullisesta tai ”voitetusta” sopimusneuvottelusta, kun myyjä on suostunut pitkän väännön jälkeen johonkin ”alennukseen”
 - Ostajan tunne sellaisesta valinnasta, josta ei voi moittia jälkeenpäin (= varmanpäälle pelaaminen - Best Practise toteutus – Alan seminaarien listahitti jne.)

ICT-hankintojen ihmeellinen maailma

JRComplex

- Hinta ja asiakkaan maksuvalmius 10%
- Tekniset arvioinnit ja muut riippumattomat selvitykset 5%

ICT-hankintojen ihmeellinen maailma

JRComplex

- Microsoftin mainos MikroPC 13/2005:
 - *Halusimme suorituskykyä, tietoturvaa ja luotettavuutta kohtuullisin kustannuksin ja Linux olisi merkinnyt ylimääräisiä riskejä kaikilla näillä osa-alueilla. Teknisesti Linux saattaa olla kiinnostava, mutta liiketoiminnallisesta näkökulmasta tämä ei riitä...*

- Erään tietohallintopäällikön määrittely järjestelmävalinnalle:
 - Riittävän pieni ja hallittava kokonaisuus, hyödyt saadaan nopeasti näkyviin
 - Helppo tehdä muutoksia pienin askelin ilman mummultiprojekteja ja konsulttilaumaa
 - Joustavasti räätälöitävissä, saadaan muokattua eri roolien vaatimuksiin ja toimintaprosesseihin (tässä tapauksessa ITIL)
 - Softan voi konfiguroida aivan minkänäköiseksi haluaa, ts. systeemi pystyy elämään liiketoiminnan mukana (nykyisin palkattu yksi henkilö tekemään järjestelmään omaa kehitystä, isommat hankkeet ostetaan projekteina)

- Kysely kuudelle päättäjälle, joista neljä vastasi
 - Teollisuus
 - PK sektori/palvelut
 - Valtionhallinto
 - IT palvelutuotanto

- Onko organisaatiossasi käytössä Open Source ratkaisuja tietoturvakriittisessä ympäristössä? [kyllä/ei]
 - 4 x kyllä
- Onko suljetun koodin (lähdekoodia ei ole saatavilla) ratkaisut mielestäsi paremmin suojassa tietoriskeiltä (esim. haittaohjelmat, virhetoiminnot, käyttövaltuus/oikeus virheet jne.) kuin Open Source ratkaisut, joiden koodi löytyy Internetistä? [perustelu]
 - 4 x ei, kaikki vastaajat uskoivat avoimuuden tuottavan parempaa laatua

- Jos valitsisit järjestelmää puhtaasti tietoturvaperusteilla, mikä olisi mielestäsi painavin argumentti ratkaisun tietoturvalaadusta? [valitse yksi ja perustelu]
- A) Iso tunnettu toimittaja, kaupallinen ratkaisu ja tukipalvelut
- B) Riippumaton auditointi
- C) Toimittajan laatu/tietoturvasertifiointi
- D) Laajan loppukäyttäjäjoukon toimittajasta riippumaton informaatio ratkaisun tietoturvaominaisuuksista, esim. keskustelufoorumi tms.
 - 3 x D
 - 1 x A

- Jos valitsisit tietoturvakriittistä järjestelmää ja vaihtoehtoina olisi kaksi teknisiltä ominaisuuksiltaan samanlaista ratkaisua, toinen Open Source ja toinen kaupallinen suljetun koodin ratkaisu, kumman valitsisit? [perustelu]
 - 4 x Open Source
 - Muokattavuus
 - Hinta ja kustannushyödyt
 - Yksi edellytti, että ratkaisutoimittajat ovat samantasoisia

- Onko avoimen Open Source kehityksen tai suljetun kaupallisen ohjelmistokehityksen ja koodin tietoturvalaadussa (esim. lopputuotteeseen läpipäässeet ohjelmointi- ja/tai suunnitteluvirheet) mielestäsi eroja? [valitse yksi ja perustelu]
- A) kaupallinen kehitys on laadukkaampaa
- B) Open Source kehitys on laadukkaampaa
- C) ei eroa
 - 1 x C ei eroa
 - 3 x B
 - kypsissä projekteissa laatua, pienissä heittoja
 - Julkisuuteen tulleet virheet ovat olleet kriittisempiä kaupallisissa tuotteissa
 - tieto huonosta laadusta leviää nopeammin Open Source puolella

- Korjataanko julkistetut tietoturvaongelmat mielestäsi nopeammin [valitse yksi]
- A) Kaupallisessa ohjelmistokehityksessä
- B) Open Source projekteissa
 - 4 x B

- Mitkä ovat kolme tärkeintä kriteeriä, joihin kiinnittäisit huomiota ohjelmiston valintatilanteessa, jos organisaatioosi olisi ehdolla Open Source ratkaisu tietoturvakriittiseen ympäristöön?
 - Yleisesti käytetty ja koeteltu teknologia
 - Tekeekö vain sen mitä on tarkoitus
 - Onko kustomoitavissa juuri omaan tarpeeseen
 - Toimii omissa testeissä kuten halutaan
 - Toimittajan luotettavuus
 - Muilta käyttäjiltä saatu vastine ja aktiiviset käyttäjäryhmät
 - Hinta
 - Tuki, päivitykset ja elinkaari kohdallaan

- Ovatko Open Source vaihtoehdot organisaatiossasi tasavertaisesti mukana kaupallisten vaihtoehtojen kanssa kartoitettaessa mahdollisia uusia ratkaisuvaihtoehtoja? [kyllä/ei ja perustelu]
 - 2 x kyllä
 - 2 x ei
 - sovellushistorialliset syyt
 - ostajien (rahasta päättäjien) ennakkoluulot
 - ei tarjontaa

- Jos toimittaja tarjoaa organisaatiollesi Open Source vaihtoehtoa, onko tämä tietoturvamielessä [valitse yksi ja perustelu]
- A) kilpailuetu
- B) ei vaikutusta
- C) negatiivinen asia
 - 2 x B
 - 2 x A
 - Edellyttäen että...
 - osaava tarjoaja
 - uskottavat referenssit

- Mikä on arviosi Open Source ratkaisujen leviämisestä kriittisiin järjestelmiin lähitulevaisuudessa [valitse yksi ja perustelu]
- A) Open Source osuus kasvaa
- B) Open Source osuus pienenee
- C) Open Source ei pysty kilpailemaan kaupallisten kanssa
 - 4 x A
 - tiukkeneva kustannuskuri

- Edellisen kyselyn perusteella...
 - Ovi on auki Open Source ratkaisuille kriittisissä järjestelmissä
 - Open Sourcella on asiantuntijoiden parissa positiivinen laatumielikuva
 - Hinnalla on väliä
 - Vahvan oman teknisen osaamisen omaavat organisaatiot ovat valmiimpia ottamaan keittiön kautta Open Source ratkaisuja, mikäli tekniset ominaisuudet ja laatu ovat kohdallaan muille se pitää myydä ulkopuolisen toimittajan pakettina

- Vastaako kukaan Open Source projektin kehityksen jatkuvuudesta ja laadusta?
- Jääkö asiakas yksin Open Source ratkaisunsa kanssa, vai löytyykö tukea?
- Löytyykö Open Source ratkaisulle valmiita Best Practise malleja, vai onko asiakas tuotekehittäjä?
- Löytyykö uskottavia kotimaisia referenssejä?
- Voiko GPL lisenssi olla riski Open Source ratkaisua käyttävälle loppuasiakkaalle?

- Miksi asiakkaani ovat valinneet Open Source ratkaisuja
 - Omaa *nix osaamista
 - Halutaan tehdä paljon omia pieniä viilauksia tai optimointeja
 - Halutaan säilyttää riippumattomuus toimittajista
 - Tiedon saannin helppous
 - Testaamisen ja kokeilun helppous
 - Kehitysympäristöjen mukaantulo
 - Valtava valmiiden komponenttien saatavuus
 - Integrointi
 - Pyrkimys pieniin ja nopeisiin projekteihin
 - Luottamus vakauteen ja suorituskykyyn
 - Luottamus tietoturvallisuuteen
 - TCO hyödyt

Miten Open Source ratkaisu valitaan

JRComplex

- Onko hanke uskottava ?
 - Hanke on ollut olemassa riittävän pitkään
 - Hanketta tuetaan taloudellisesti tai siitä on olemassa liiketoimintamalli
 - Hankkeella on selvästi laaja ja aktiivinen käyttäjäfoorumi
 - Ratkaisua käytetään riittävässä laajuudessa
 - Ratkaisua käytetään yritysmaailmassa
 - Ratkaisu on mukana kaupallisissa Linux distribuutioissa
 - Ratkaisusta on saatavissa kirjallisuutta

Miten Open Source ratkaisu valitaan

JRComplex

- Onko ohjelmistokehitys uskottavaa?
 - Selkeä versiosykli
 - Selkeä päivitysmenettely
 - Päivitysten julkaisemisen nopeus
 - Uusien versioiden vakaus
 - Ratkaisua käytetään jonkin kaupallisen ratkaisun osana

Miten Open Source ratkaisu valitaan

JRCComplex

- Millaista käyttäjäpalautetta ratkaisu on saanut
 - Omien asiantuntijoiden palaute
 - Käyttäjäfoorumien palaute
 - Ratkaisun esiintyminen lehdistössä
 - Ratkaisun esiintyminen messuilla tms. tilaisuuksissa
 - Ratkaisun saamat julkiset tunnustukset, palkinnot tms.

- Jonkun pitää myydä ratkaisu (sisäinen tai ulkoinen)
- Pitää pystyä osoittamaan uskottavat referenssit
- Pitää pystyä osoittamaan uskottava laatu ja luotettavuus
- Hyödyt pitää pystyä osoittamaan nopeasti ja etenemään vaiheittain halutun kokoisin askelin
- Ratkaisun pitää integroitua ympäristöönsä ja toimintatapoihin
- Ratkaisun pitää pystyä kasvamaan ja skaalautumaan
- Jonkun pitää kyetä/haluta ottaa ratkaisu hallintaansa (sisäinen tai ulkoinen) ja viedä sitä eteenpäin

Kiitoksia