Lausunto

15.05.2012

Viite: Lausuntopyyntö_VAHTI_Sovelluskehityksen_tietoturvaohje_2012.pdf

VAHTI_Sovelluskehityksen_tietoturvaohje_2012 TEM/TIE-lausunto

Ohje on hyvä lisä VAHTI-ohjeiden sarjaan. Osa sisällöstä on jo ohjeistettu muissa VAHTI-ohjeissa, esim. käyttäjätunnus/salasana-asiaa lienee turha toistaa tässä muodossa vaan todeta, että asiaa on käsitelty VAHTI-ohjeessa. Sovelluskehityksessä voisi käyttäjätunnus/salasanan pituuden sijaan ohjeistaa ns. vahvoihin tunnistusmenetelmiin ja SSO-käytäntöön.

Salasanakäytännöissä on myös syytä viitata käyttäjäorganisaation omaan ohjeistukseen asiassa.

Väheksymättä tietoturvaa ja sen ehdotonta huomioimista valtionhallinnon tietojärjestelmien olennaisena osana kiinnittyy huomio siihen, että onko syytä ohjeen antamisen lisäksi tehdä kartoitus ohjeen kustannusvaikutuksista sovellushankinnoissa sekä järjestelmäylläpidossa.

Onko tietoturvaosaamiseen sekä hankkijalla että toimittajilla riittävät ja samalla tasolla olevat toimijat – ja pysytäänkö tavoitetila riittävän yksiselitteisesti määrittelemään?

Substanssisovelluksen hankkijalla on paine saada sovellus käyttöön mahdollisimman nopeasti ja edullisesti. Tämä paine on ja tulee olemaan aina ristiriidassa tietoturva- ja lokitusvaatimusten kanssa.

On mietittävä rajaukset, miten vaatimukset ulotetaan koskemaan valmisohjelmistojen koodia tai valmiskoodin komponentteja, joiden osuus on yhä kasvava. Kokonaisarkkitehtuurin yhtenä tavoitteena on tuottaa yleiskäyttöisiä komponentteja valtiohallintoon.

Tietoturva on prosessi, jossa tietoturvan taso on sen heikoimman lenkin vahvuinen. Esim. jos käyttöjärjestelmän TCP/IP-pino sisältää mahdollisuuden DDoS-hyökkäykseen, ei sovellustasolla ole mitään tehtävissä sen estämiseen.

Tietoturvaohjeiden noudattaminen ei ole käytännössä mahdollista vanhoihin jo olemassa oleviin sovelluksiin kuin yksittäisiltä osiltaan.

165010

TYÖ- JA ELINKEINOMINISTERIÖ
PL 32 (Aleksanterinkatu 4)
00023 Valtioneuvosto • Puh. 010 606 000
Faksi (09) 1606 2160 • www.tem.fi

ARBETS- OCH NÄRINGSMINISTERIET
PB 32 (Alexandersgatan 4)
00023 Statsrådet • Tfn 010 606 000
Fax (09) 1606 2160 • www.tem.fi

MINISTRY OF EMPLOYMENT AND THE ECONOMY
P.O. Box 32 (Aleksanterinkatu 4)
FI-00023 Government • Tel + 358 10 606 000
Fax + 358 9 1606 2160 • www.tem.fi

Ohjelmistot eivät muutu uuden ohjeistuksen mukaiseksi itsestään, vaan tarvitaan myös taloudellis-tekninen perustelu, mihin muutosta tarvitaan ja miksi. Muutos pitäisi hyväksyttää tai hylätä riskien hallinnan kautta. Hanketeknisesti on erittäin vaikea perustella olemassa olevan sovelluksen muuttamista ilman toiminnallisuuden muutoksia vain siksi, että v. 2012 osataan ohjeistaa asiat laajemmin kuin 1990-luvulla sovelluksen pääosien kirjoittamisen aikaan.

Sovelluksen lokitukseen kohdistetaan merkittäviä vaatimuksia jo tietoturvatasosäädöksissä. Esimerkiksi keskitetty lokien keräyksen vastuu etenkin ulkoistetuissa sovelluksissa on hankala toteuttaa varsinkin jo toteutetuille sovelluksille. Kyseenalaiseksi jää, kuuluuko ulkoistetun sovellustoimittajan vastuulle toimittaa lokit organisaation keskitettyyn lokivarastoon.

Lokivarantojen pitäminen järkevässä muodossa siten, että asiantuntijalla on pääsy lokien säilytyspaikkaan ja hän osaa hakea oikean lokin, avata sen, lukea sitä ja tehdä oikeat johtopäätökset tapahtuneesta niin, että lukemisesta jää merkintä, vaatii oman lokijärjestelmän. Tähän taas välttämättä kaikkien tietojärjestelmien lokit eivät sovellu sellaisenaan.

Data varastoidaan tietokantaan. Tietokannan omistaja pääsee käyttöjärjestelmätasolta muuttamaan halutessaan datan sisältöä ohi sovelluslokin. Erityistä huomiota on kiinnitettävä siihen, että kenellä on oikeus ja missä tilanteessa muuttaa tietokannan sisältöä ohi sovelluksen.

tietohallintopäällikkö Jaakko Jokela

LIITTEET

JAKELU

TIEDOKSI