

Asia: 888/00.01.00.01/2015

VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohje

Lausunto - VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus-ohjeluonnokseen - yleistä

Yleinen palaute

Lausunnolla oleva ohje sähköisen asioinnin tietoturvallisuus on sisällöltään varsin tiivis ja laaja kokonaisuus. Sen pääkohderyhmä ovat asiantuntijat(ict-arkkitehdit, sovelluskehittäjät, ohjelmistojen hankkijat jne.). Kovin helppolukuiseksi yleisohjeeksi tätä ei voi kuvailla. Luettavuuden ja ohjeiden sisäistämistä olisi voinut helpottaa jopa jakamalla tämän ohjeen sisältö useampaan eri ohjeeseen. Nyt tulos on oppikirjamainen.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ytimekäs tiivistelmä alussa olisi tarpeen niille, jotka haluavat muodostaa nopean yleiskäsityksen sähköisen asioinnin tietoturvallisuudesta

Mitkä olivat ohjeen parhaita asioita?

Parhaita kohtia ovat yksityiskohtaiset ohjeet toimenpiteistä sähköisen asioinnin turvaamiseen liittyvistä keinoista.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Johdanto on sinällään tarkka kuvaus ohjeen sisällöstä, mutta siihen kaivataan tiivistystä, jos sen tarkoitus on toimia myös tiivistelmänä esim. johdolle.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Tavanomainen osa VAHTI-ohjeesta. Ei lisättävää.

Luku 3 Sähköiset asiointipalvelut

3.1: Hyvät määritelmät ja raja. Havainnollistamiskuvan esittämistapaa voisi ehkä hioa. Kuvasta tulee mieleen tehtaan tuotantoprosessi.

3.2: Helppolukuinen kuvaus ja kattava luettelo uhkaluettelo.

3.3: Hyvä muistilista sähköisen asioinnin turvaamiseen liittyvistä toimenpiteistä ja keinoista. Esimerkkikuva tässä kappaleessa on hyvä.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

4.1: Tietoturvaperiaatetaulukko on kattava ja avattu yksityiskohtaisesti asiantuntijalle.

4.2: Sama havainto kuin edellä suunnattuna ensisijaisesti järjestelmän suunnittelijoille.

4.3: Tämä kappale suunnattuna organisaation tietoturvallisuuden hallinnasta vastaaville.

Tämän luvun eri osiot voisi "korvamerkitä" kohderyhmittäin vielä selkeämmin.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

5.2.1: Alun tekstiosa ei oikein aukea mutta paranee kuvan ja esimerkin voimalla.

5.2.2: Samoin tässä kuva ja esimerkit valaisivat asiaa

5.2.3: Selkeä kokonaisuus

5.3: Tiivis kokonaisuus, johon on koottu paljon tietoa. Vaatii perusteellista paneutumista eri kontrolleihin. Koko ohjeen keskeisin osa tietoturvallisuuden varmistamisen näkökulmasta.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

6.3: Kuva 5 :Esimerkki sähköisen tunnistamisen menetelmän valintaprosessista hyvä selkeyttävä kuvio. Samoin selkeyttävä Taulukko 4.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Selkeä melko helppolukuinen kappale. Lisäksi hyviä esimerkkejä soveltamisesta viranomaisen toiminnassa.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

8.1: Hyvä muistilista tukipalveluiden käytön oikeuksista ja velvoitteista.

8.2. -> 8.8.3 Suomi.fi palveluväylän yksityiskohtainen kuvaus. Voisi olla ihan omana ohjeena (14 sivua).

Liite 1: Keskeinen sanasto

Ei lisättävää

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Hyvä tarkistuslista, ei lisättävää.

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

Ei lisättävää.

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Kattava tarkastuslista, ei lisättävää.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Ei lisättävää.

Liite 6: Case-esimerkit

Case A hyvä käytännön esimerkki.

Case B perustietoturvaa, jonka hallinta pitäisi olla jo hallussa organisaatiolla, mutta siitä huolimatta käytännössä esim. tietoturvapäivitysten asennuksissa ongelmia, vaikka prosessit niiltä osin ovat kunnossa.

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Tuli todettua jo lausunnon alkuvaiheessa, että tämä ohje on sisällöltään erittäin kattava, jopa oppikirjamainen. Jalkauttaminen kannattaa pilkkoa pienempiin kokonaisuuksiin ja kohdentaa eri asiantuntijaryhmille. Tästä ohjeesta riittää koulutusmateriaalia useampaan tilaisuuteen.

Muuta palautetta ohjeesta tai VAHTille?

Tämä on esimerkki siitä, kuinka Vahti-ohjeet ovat kehittyneet yhä konkreettisemmiksi. Ohjeen pituus ja tiivis sisältö asettavat haasteita sen omaksumiselle. Ohje alkaa muistuttaa tietoturvastandardia.

Lappalainen Päivö
KEHA tieto- ja viestintäyksikkö