

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

Tarpeellinen, hyvä ja kattava ohje.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ohjeen kirjoitusasuun olisi hyvä kiinnittää huomiota (varsinkin alkuosassa on useissa paikoissa esimerkiksi turhia välilyöntejä).

Ohje on hyvä kohderyhmän asiantuntijoille, mutta rinnalle kaipaa jonkinlaista lyhyempää/kevyempää versiota niille henkilöille, jotka eivät ole varsinaisia palvelun kehittäjiä, mutta ovat kuitenkin sähköisten palveluiden kanssa eri tavoin tekemisissä.

Mitkä olivat ohjeen parhaita asioita?

Ohjeessa ei käsitellä pelkkää tietoturvaa, vaan kokonaisuutta mihin kuuluu organisaation ydintoimintojen riskit sekä palvelusta ja sen toimintaympäristöstä tunnistetut uhkatekijät kokonaisuutena.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

-

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

On hyvä asia, että kukin säädös on avattu ja sen ydinsisältö on kuvattu lyhyesti, mikä helpottaa lukijaa huomattavasti verrattuna siihen, että vain säädökset olisi mainittu.

Luku 3 Sähköiset asiointipalvelut

Määrittelyt ovat hyviä ja ymmärrettäviä. Kuvat ja kaaviot avaavat hyvin kyseisiä asiakohtia ja toimivat "tarkastuslistoina".

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

On tärkeä ohjata myös asiakkaiden tietoturvallista käyttäytymistä. Tätä kohtaa voisi ehkä vielä hieman laajentaa konkreettisilla esimerkeillä.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Kaaviot ovat erittäin havainnollistavia myös sellaiselle lukijalle, jolla ei ole asiasta ennestään tietämystä tai vain vähän tietoa.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

6.2 s. 37 toisessa kappaleessa kirjoitusvirhe (määrittellään) ja taulukon alapuolella toinen (toimintan)

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

7.1.3 s. 43 kirjoitusvirhe: tiivistealgoritmilla -> tiivistealgoritmilla

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

-

Liite 1: Keskeinen sanasto

On tärkeää, että eri toimijat käyttävät ”samaa kieltä”. Tämän vuoksi sanasto on merkittävä osa kokonaisuutta. Useammassa sanassa on vain viitattu muihin VAHTI ohjeisiin ilman sanan selittämistä. Olisi parempi, jos lyhyt selitys löytyisi suoraan tämän ohjeen taulukosta (vaikka silti olisi viittaus toiseen VAHTI ohjeeseen). Pari viestintävirastoon liittyvää kohtaa oli linkitetty alaviitteillä, joten olisi hyvä jos myös nämä viittaukset toisiin VAHTI ohjeisiin olisi linkitetty, jolloin lukija pääsisi halutessaan nopeasti siirtymään niihin.

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Olisiko tarpeen huomioida taulukossa yhtenä osa-alueena tukipalvelun käyttöehdot. Esimerkiksi onko kyseinen palvelu edes sallittua käyttää ajatellussa käyttötarkoituksessa (esim. jos tukipalvelu on tarkoitettu vain vaikkapa yksityiskäyttöön, mutta ei kaupalliseen tai hallinnolliseen käyttöön).

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Hyvä kooste, helppo ja nopea käyttää tarkastuslistana.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

-

Liite 6: Case-esimerkit

-

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Sähköisten palveluiden kehittäjille on syytä kouluttaa koko ohje perusteellisesti. Myös sellaisilla henkilöillä pitäisi olla asiasta perustiedot, jotka ovat tavalla tai toisella sellaisessa asiakasrajapinnassa, missä palveluita käytetään.

Muuta palautetta ohjeesta tai VAHTille?

-

Koivisto Juha
Tampereen kaupunki