Vieremän kunta

Lausunto

16.02.2017

Asia: 888/00.01.00.01/2015

VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohje

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

Yleinen palaute

Ohje on monipuolinen, kattava ja rakenteeltaan selkeä. Pienen kuntaorganisaation näkökulmasta ohjeen käyttökelpoisuutta rajaa, että ohjeen kohderyhmäksi on määritelty syvällisemmän ict-asiantuntemuksen omaavia henkilöitä, joita ei pienestä kunnasta välttämättä löydy. Teksti onkin paikoitellen melko vaikeaselkoista it-jargonia puhumattomalle. Voisiko kenties laatia selkokielisen tiivistelmän kuntien käyttöön perustyötä ajatellen? Hienoa että mukaan on otettu viitearkkitehtuuri ja suomi.fi.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Eri yhteyksissä saatetaan käyttää samasta asiasta eri termejä, ja toisessa yhteydessä samalla termillä saatetaan tarkoittaa eri asioita. Esimerkiksi palvelun omistaja, palvelun tuottaja, palvelun käyttäjä – termit olisi syytä määritellä selkokielisesti ja käyttää niitä yhdenmukaisesti. Kuntaorganisaatiossa ohjeen soveltamista auttaisi myös selkeä vastuunjakotaulukko esimerkiksi edellä mainittujen tahojen rooleista. Ks. myös kommentti yleiseen palautteeseen.

Mitkä olivat ohjeen parhaita asioita?

Ohje on kattava ja paikoin hyvinkin yksityiskohtainen. Kuvat ja esimerkit konkretisoivat tekstiä mainiosti. Suomi.fi – palveluiden kuvaus on hyvä.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Ohje toteuttaa johdannossa asetetut tavoitteet. Jos ohje on tarkoitus jalkauttaa myös kuntien perustyöhön, kannattanee tarkastella kohderyhmiä hieman maanläheisemmällä tasolla ja

huomioida, että varsinkin pienissä kunnissa esimerkiksi tietohallintovastaavan tehtäviä hoidetaan muiden töiden ohessa, eikä ict-osaaminen välttämättä ole asiantuntija-tasoista.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Hyvä yhteenveto. Eikö laissa julkisen hallinnon tietohallinnon ohjauksesta säädetä mitään tähän ohjeeseen liittyvää?

Luku 3 Sähköiset asiointipalvelut

Ymmärrettävä kuvaus ja hyviä huomioitavia seikkoja asiointipalvelun tarkoituksenmukaisesta suojaamisesta.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Perusteellisen oloinen listaus periaatteista eri tasoilla (asiakkaiden opastuksesta teknisiin ratkaisuihin). Onko esitetty/eritelty velvoittavat vaatimukset ja toisaalta ”pelkät” suositukset? Jos kuvauksen mukaan palvelun omistajan ”tulee tehdä jotakin”, onko kyseessä velvoite vai kehotus? Jos velvoite, niin viittaus siihen mihin perustuu olisi hyvä.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Laaja kokonaisuus, jota kuvat ja esimerkit selkeyttävät. Teksti monine lyhenteineen on kuitenkin paikoitellen melko vaikeaselkoista.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Hyvä ohje soveltuvan tunnistusmenetelmän valintaan, sekä kuvaus nykyhetkellä käytettävissä olevista ratkaisuista.

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Olisi hyvä lisätä käytännön esimerkkejä tilanteista, milloin minkäkin tyyppistä ratkaisua voitaisiin käyttää; ei niinkään teknisestä vaan palvelun sujuvuuden näkökulmasta.

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Palveluiden nimet muuttuneet.

Palveluiden kuvaukset ja kuvat ovat hyviä, jonkin verran taas it-jargonia hankaloittamassa maallikon luetun ymmärtämistä. Miten esimerkiksi tiedämme, onko organisaatiomme tiedonsiirtotarve synkronista sanomaliikennettä?

Liite 1: Keskeinen sanasto

Sanat tulisi selittää sanastossa, selitykseksi ei riitä pelkkä viittaus johonkin toiseen ohjeeseen. Lisäksi ohjeessa esiintyy paljon lyhenteitä ja termejä, joita ei ilmeisesti ole katsottu keskeisiksi sillä suurin osa puuttuu sanastosta. Toivotaan kattavampaa sanastoa.

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

Lista on aika lyhyt, mutta nostaa olettavasti esille tärkeimmät huomioitavat seikat. Olisiko hyvä määritellä tarkemmin ne vaatimukset, joille on olemassa selkeä velvoite. Esimerkiksi yksityisyydensuojan osalta voisi edes mainita ne lait, jotka tulee huomioida.

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Olisiko syytä eritellä tarkistuslistalle selkeästi mahdolliset velvoitteet? Onko esim. lokeista säädetty jotain velvoitteita, vai onko kyseessä suositus.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

Taulukko vaikuttaa olevan keskeneräinen? Lisäksi olisi mielenkiintoista saada esimerkkejä miten käytössä olevat tunnistusvälineet toimivat milläkin varmuustasolla, ja miten tunnistus käytännössä toteutettaisiin.

Liite 6: Case-esimerkit

Esimerkit eri tasolla ohjeen sisältöön ja laajuuteen nähden. Loppukäyttäjän tietoturvaohjeiksi suunnatut case-esimerkit eivät selvennä sähköisen asioinnin tietoturvallisuuden toteuttamista kokonaisuutena.

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Ohje opitaan parhaiten käytännön työn yhteydessä. Ohjeelle tulee varmasti käyttöä, kun otamme käyttöön sähköisiä asiointipalveluja. Siinä vaiheessa todennäköisesti olisi tarvetta koulutuksellekin. Verkko-opetus lienee toimiva vaihtoehto. Voisikohan lisäksi laatia selkokielisen tiivistelmän kuntien käyttöön perustyötä ajatellen?

Voisikohan tätä kokonaisuutta jotenkin yhdistää mahdollisiin EU:n tietosuoja-asetuksen myötä järjestettäviin koulutuksiin?

Muuta palautetta ohjeesta tai VAHTIlle?

-

Koho Jenni
Vieremän kunta