Elisa Oyj

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

Ohjeistus on kattava ja kuvaa hyvin eri osa-alueita.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ohjeistuksessa on yhteneviä piirteitä esim. ISO27001 määrittelyjen tai sertifiointien kanssa. Onko näiden välistä suhdetta pohdittu kuten esimerkiksi, jos täyttää ISO27001 määrittelyt, missä määrin tulee täyttäneeksi myös tämän ohjeiston määrittelyt?

Mitkä olivat ohjeen parhaita asioita?

Sisällön kattavuus ja kokonaiskuva, jonka ohjeisto muodostaa.

Yksityiskohtaiset kommentit

Luku 1 Johdanto

Olisiko johdanto-osassa hyödyllistä todeta, että ohjeistus ei sellaisenaan ole tarkoitettu hankintojen (ainakaan yksinomaiseksi) vaatimusmäärittelyksi. Sisältö toki palvelee eri osa-alueet huomioivan määrittelyjen laadintaa.

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

Ei kommentoitavaa

Luku 3 Sähköiset asiointipalvelut

Luku 3.1 Sähköisen asiointipalvelun määritelmä ja rajaus. Rajauksen perusteella sähköinen asiointipalvelu kattaa mm. viranomaisen ja asiakkaan välisen vuorovaikutteisen asioinnin

mahdollistavat palvelut. Sisältyvätkö tähän rajaukseen myös kaupallisten tukipalvelujen (esim. kuvassa 1 sininen osa) vuorovaikutuskanavat asiakkaiden suuntaan kuten puhepalvelut?

Luku 3.2 Sähköisen asioinnin uhkaympäristö. Ehdotetaan lisättäväksi listaan uusi kohta: Palveluntuottajilla tulee olla riittävä kyky hallita häiriöitä ja tietoturvapoikkeamia.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

Luku 4.1 Tietojen luokittelua ja turvallista sähköistä käsittelyä ohjaavat periaatteet. Taulukossa kohtaan "Sitouta palvelutoimittajat ja yhteistyökumppanit asiointipalvelun tietoturvatavoitteisiin ja -vaatimuksiin" ehdotetaan kuvauksen tarkentamista: "Usean organisaation vastuulle jakaantuvan sähköisen asioinnin suunnittelussa palvelun omistajan tulee varmistua siitä …"

Luku 4.3 Tietoturvapoikkeamien hallintaa koskevat periaatteet. Kohtaan "Kerää asiointipalvelun tapahtuma- ja lokitietojen riittävän kattavasti"

ehdotetaan tarkennettavaksi, mitä tarkoittaa ”lokitiedot ovat tarvittaessa palvelun omistajan saatavilla”? Esimerkiksi, millä aikataululla ja tavalla lokitiedot ovat saatavilla? Voiko vaihtoehtoisesti palvelun omistaja pyytää tukipalvelun tuottajaa tarkistamaan pyydettyjä asioita?

Ehdotetaan myös lisättäväksi: Lokitietojen luovutuksessa tulee ottaa huomioon voimassa oleva henkilötietojen käsittelyn lainsäädäntö.

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

Luku 5.2.3 Tukipalveluiden tietoturvallisuus. Ehdotetaan täsmennystä asioinnin tukipalveluiden valintalistaan kohtaan 3). Vrt. tilanne, jossa vaatimukset täyttävä ratkaisu on kaupallisesti saatavissa, miksi tehdä itse? Ehdotuksena, että poistetaan kohdan 3. alusta sanat "Muussa tapauksessa".

Ehdotetaan kappaleessa "Edellä kuvattujen palveluiden käyttöönotto …" toisen lauseen täydentämistä: "Asiointipalvelun suunnittelussa tulee kuitenkin pitää kaupallisia palveluita, oletusarvoisesti ei-luotettuja ellei sertifiointeja tai auditointeja ole todennettavissa".

Luku 5.3 Kontrolliympäristö. Tämä on erinomainen malli ja kuva. Kokonaisympäristön merkitystä tulee korostaa, koska yhden osa-alueen tietoturvaratkaisut helposti menettävät merkityksensä, jos kokonaisuus ei toimi yhteen.

Luku 5.3.1. Yleiset kontrollit. Kommentti 1: Saatavuus on keskeinen sähköisen asiointipalvelun ominaisuus, mitä on syytä korostaa.

Kommentti 2: Nykypäivänä lokien valvonta automaattisesti tulee olla ehdottomasti osana palvelua.

Kohdassa ” …lokitietoja, jotka ovat tarvittaessa asiointipalvelun omistajan käytettävissä” saattaa olla ristiriidassa vuoden 2018 EU tietoturva-asetuksen kanssa, jos lokeissa on henkilötietoja. Tätä olisi hyödyllistä tarkentaa.

Ehdotetaan täydentävää muutosta "- lokitietoja ei kerätä tarpeettoman laajasti ja suunnittelematta vaan rekisterinpitäjän tarpeisiin ja teknisten vikatilanteiden havaitsemiseksi ja korjaamiseksi suunnitelmien mukaisesti"

Ehdotetaan täydentävää muutosta, koska nykyinen muoto ei salli mitään muuta käyttötarkoitusta lokeille kuin tietoturvallisuuden valvonta: ” – lokeihin ei kirjoiteta tietoturvallisuuden valvonnan, käytön varmistamisen, laadun valvonnan tai vian hallinnan kannalta tarpeetonta tietoa, esimerkiksi asiointipalvelussa käsiteltäviä arkaluonteisia henkilötietoja”.

Luku 5.3.6 Palvelurajapinnat, integraatioratkaisut ja sanomaliikenne. ”Tarkoituksenmukaisimman integraatioratkaisun valinta on aina tapauskohtaista …” Tämä on tärkeä ja hyvä huomio.

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

Ei kommentoitavaa

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

Ei kommentoitavaa

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

Ei kommentoitavaa

Liite 1: Keskeinen sanasto

-

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

-

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

-

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

-

Liite 6: Case-esimerkit

-

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Erittäin paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

-

Muuta palautetta ohjeesta tai VAHTIlle?

Blockchain yms. murrosten huomiointi tai arviointi tarpeen?

Lehtinen Kari
Elisa Oyj - Yritysasiakkaat