Verohallinto

Lausunto

16.02.2017 A6/00 00 01/2017

Asia: 888/00.01.00.01/2015

VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohje

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

Yleinen palaute

Kattava ja tarpeellinen ohje. Tämän ohjeen käyttöönottoon koko julkishallinnon laajuisesti pitää panostaa erityisen voimakkaasti.

Mitä kehittämistä mielestäsi ohjeessa vielä on?

Ohjeelle tulee tehdä vielä kielentarkistus; jonkin verran on kielioppi- ja kirjoitusvirheitä, joista ainakin osa lienee syntynyt tekstin muokkauksessa.

Mitkä olivat ohjeen parhaita asioita?

-

Yksityiskohtaiset kommentit

Luku 1 Johdanto

- Sivu 4; Internet-verkon uhkatekijät " ...yhdenmukaista tietoturvallisuuden tasoa." KOMMENTTI: Käytännön tasolla toteutuva tietoturvan taso määräytyy heikoimman lenkin perusteella. Vaikka palvelu olisi tietoturvallinen, niin palvelun käyttäjä voi omalla toiminnallaan jopa täysin tietämättään synnyttää tilanteen, jossa syntyy tietoturvauhka. Onko itse asiassa niin, että samaa kykyä kuin palvelujen omistajilta edellytetään myös kansalaisilta ja yrityksiltä? Uhkatekijät eivät siten kohdistu ainoastaan asiointipalvelujen omistajiin. Tärkeää olisi ymmärtää kenellä on esim. vastuu kansalaisten ja yritysten ohjaamisesta tietoturvallisiin toimintatapoihin, jos heitä ohjataan voimakkaasti käyttämään sähköisiä palveluita? Tämä tulisi viestiä myös palvelujen hyödyntäjille. Tästä syntyy myös kustannuksia, jotka muodostuvat esteeksi kansalaisille tai yrityksille, joilla talous ei ole kunnossa, mutta heillä on velvollisuus palvelujen käyttöön.

- Sivu 5 "auttaa muodostamaan kokonaisnäkemys sähköisen asioinnin keskeisistä tietoturvauhista" KOMMENTTI: Mikä taho huolehtii siitä, että asiakkaalle muodostuu riittävän hyvä kokonaiskuva vai onko se täysin asiakkaan vastuulla? Mikä on palvelun omistajan vastuu asiakkaisiin nähden?

- Sivu 5 "Ohjeen kohderyhmä" KOMMENTTI: Kilpailutusvaiheen merkitystä olisi hyvä korostaa, sillä monet tässä dokumentissa esitetyistä vaatimuksista on myöhäistä huomioida toimitussopimuksen allekirjoituksen jälkeen.

- Sivu 6 "Käyttäjien tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa; kuvaa sähköisen tunnistusmenetelmän varmuustasot sekä päätöksentekoprosessin, jota noudattaen palvelun omistaja määrittelee palvelun käytön edellyttämän varmuustason." KOMMENTTI: Identiteettivarkauksien, kalastelun (phishing) ja koneiden kaappausten estäminen?

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

- Sivu 8 "Henkilötietojen siirtäminen EU-maiden ulkopuolelle on kielletty" KOMMENTTI: Eikös tästä ole poikkeus tai poikkeuksia (Fatca / Beps?)

Luku 3 Sähköiset asiointipalvelut

- Sivu 9 "yritysten edustajat, jotka yritys on valtuuttanut asioimaan puolestaan" KOMMENTTI: Edustaja voi olla käytännössä mistä tahansa maasta myös EU:n ulkopuolelta.

- Sivu 9: "Sähköinen asiointipalvelu rakentuu tyypillisesti seuraavista kerroksista ja elementeistä:" KOMMENTTI: Mikäli kyseessä on pilvipalvelu, ei välttämättä tiedetä rakenneosista mitään.

- Sivu 9: "...verkkoselaimella käytettävät sovellukset ja päätelaitteille asennettavat natiivisovellukset" KOMMENTTI: Ympäristö, johon nämä asennetaan on käytännössä asiakkaan tai asiakkaan valtuuttaman (jopa ulkomailla EU:n ulkopuolella olevan) tahon vastuulla.

- Sivu 10: "Sähköinen asiointipalvelu tukeutuu useimmissa tapauksissa seuraaviin ulkoisiin palveluihin:" KOMMENTTI: Pilvipalvelut osana palvelukokonaisuutta?

- Sivu 10: "toteuttavat riittävän vahvan tieto- ja sanomaliikenteen salauksen," KOMMENTTI: Toteutus täytyy olla päästä päähän.

- Sivu 10: "mahdollistavat tietoliikenteen seurantatietojen tallentamisen tietoturvaloukkausten tai vika- ja häiriötilanteiden selvittämiseksi" KOMMENTTI: Myös niissä tapauksissa, joissa esim. kaksi eri omistajan (esim. viranomainen ja yritys) Enterprise Service Bus –ratkaisua (ESB) on kytketty toisiinsa. Näistä ratkaisuistahan toinen saattaa sijaista fyysisesti missä tahansa maassa (Kiinassa, Intiassa,

Tsekissä, USAssa). Onko nyt selvää miten tällaiset mahdolliset selvittämiset selvitettäisiin tällaisissa tilanteissa?

- Sivu 11: "Toisen osapuolen omistamien tietojen hyödyntäminen sähköisessä asiointipalvelussa edellyttää palvelun omistajalta kykyä suojata tietojen luottamuksellisuutta tiedon omistajan edellyttämällä tasolla" KOMMENTTI: Sama koskee myös asiakasta.

- Sivu 11: "Palveluiden käyttäjien tulee lisäksi ymmärtää palveluiden mahdollisista häiriöistä ja poikkeamatilanteista omaan toimintaansa aiheutuvat jatkuvuusriskit, ja toisaalta välttää itse käyttämiensä asiointipalveluiden tarpeetonta kuormittamista" KOMMENTTI: Mikäli tässä käyttäjillä tarkoitetaan tässä asiakasta, niin mikä taho huolehtii viestinnästä ja mahdollisesta kouluttamisesta?

- Sivu 11: "Sähköisen asiointipalvelun keskeiset uhkatilanteet kohdistuvat palvelun ja siinä käsiteltävien tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen" KOMMENTTI: Eikö uhkatilanteita synny myös siitä ettei jommallakummalla ole riittävästi tietoa mahdollisista uhkista?

- Sivu 11: "Hyökkääjä, tai palvelun yksittäinen valtuutettu käyttäjä, muuttaa sähköisen asiointipalvelun haavoittuvuutta hyödyntämällä sen sisältämiä tietoja. Motiivina voi olla esimerkiksi taloudellinen hyötyminen (ks. Oman edun tavoittelu) tai viranomaisen maineen tahraaminen." KOMMENTTI: Viranomaiseen kohdistuva identiteettivarkaus?

- Sivu 11: "...uhkatekijät huomioiden riittävät mutta eivät ylimitoitetut" KOMMENTTI: Voisiko tässä olla esimerkki tai esimerkkejä, joissa alla mainittujen kysymysten perusteella on helpompaa hahmotta suhteuttaminen?

- Sivu 13: "Palvelussa jaetaan yleisölle julkista tietoa. Keskeistä on tiedon hallittu päivittäminen ja julkaistun tiedon eheys. Palvelulta voidaan edellyttää lisäksi korkeaa saatavuutta" KOMMENTTI: Joskus vaatimukset tietosisällön oikeellisuudelle määrittyvät hyödyntämisen pohjalta. Esimerkiksi Sää- ja olosuhdetietoihin liittyy hyödyntäjillä turvallisuuskysymyksiä.

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

- Sivu 14: "palvelun omistajan, palvelutuottajan tai palvelua kehittäjän tahon mahdolliset pääkäyttäjä- ja muut hallinta- sekä kehittämistilanteet" KOMMENTTI: ...Kehittävän ja ylläpitävän tahon...

- Sivu 14: "Arvioi ja hallitse säännöllisesti asiointipalveluun kohdistuvia uhkia" KOMMENTTI: Voisiko tässä olla joku maksimiaikaväli esim. vähintään kerran vuodessa, puolivuosittain tms.?

- Sivu 14: "Sitouta asiointipalvelun suunnittelijat ja toteuttajat tietoturvatavoitteisiin ja -vaatimuksiin" KOMMENTTI: Mikäli kyseessä on kaupallinen palveluntuottaja, olisi syytä huomioida nämä vaatimukset jo hankintavaiheessa ja viimeistään sopimusta tehdessä.

- Sivu 15 "Sitouta palvelutoimittajat ja yhteistyökumppanit asiointipalvelun tietoturvatavoitteisiin ja -vaatimuksiin" KOMMENTTI: (Sama kommentti kuin edellä) Mikäli kyseessä on kaupallinen palveluntuottaja, olisi syytä huomioida nämä vaatimukset jo hankintavaiheessa ja viimeistään sopimusta tehdessä.

- Sivu 15 "Varmista tietoturvallisuuden riittävä koordinointi ja seuranta" KOMMENTTI: Pitääkö tämän olla kuvattuna johonkin? Jos pitää, niin missä sen pitäisi olla kuvattuna (huomioiden sekä projektivaihe että sovellushallinta)

- Sivu 15 "Palvelun omistajan tulee tarjota palvelun käyttäjille riittävät ohjeet ja tuki palvelun turvalliseen käyttöön" KOMMENTTI: Missä menevät vastuun rajat omistajan ja asiakkaan välillä?

- Sivu 15 "Minimoi riskialttiit toiminnot ja pääsy tietoon" KOMMENTTI: Tämän vaatimuksen toteutuminen pitää minusta myös todentaa testein.

- Sivu 16 "Sovella modulaarista arkkitehtuuria" KOMMENTTI: Tähän on joissakin tapauksissa käytännössä vaikea vaikuttaa, sillä asia on valmiita ratkaisuja/ohjelmistoja hyödyntävissä toimitusprojekteissa ja valmiissa pilvipalveluissa usein toimittajan vastuulla.

- Sivu 16 "Arvio säännöllisesti asiointipalvelun tietoturvallisuuden tasoa" KOMMENTTI: Joskus alun perin turvallinen ratkaisu voi tosiaan muuttua ajan myötä turvattomaksi. Kuinka paljon on mahdollista vaikuttaa silloin ulkoiseen palveluntuottajaan, jos tätä ei huomioida myös palvelun elinkaaren kattavissa sopimuksissa (ylläpito)?

Nykyisin sovelluskehityksessä käytetyt ketterä kehittäminen ja jatkuva integraatio asettavat erilaisia vaatimuksia tietoturvan hallinnan menettelyille ja prosesseille. Erityisesti tämä on huomioitava toiminnan sykleissä.

- Sivu 18 "Varaudu tietoturvapoikkeamiin ja niistä palautumiseen" KOMMENTTI: Pitäisikö tällä olla joku talotasoinen ”kattosuunnitelma” jatkuvuuden turvaamiseksi, johon voisi liittää yksittäisiä suunnitelmia/sopimuksia?

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

- Yleinen kommentti; voisiko esimerkit siirtää liitteeseen jolloin tekstiä saisi tiivistettyä?

- Kpl 5.3 eteenpäin; Kaikissa taulukoissa sarake "Kontrolli" ei kuvaa kontrolleja, pikemminkin tavoitteita tai päämääriä. Sen sijaa sarake "Toteuttamisohje" sisältää kontrolleja.

- Sivu 18 "Käyttöpalveluympäristön ja asiointisovelluksen arkkitehtuuriin tulee kiinnittää erityistä huomiota jo palvelua suunniteltaessa" KOMMENTTI: Tämä tulisi huomioida jo hankintavaiheessa, sillä sopimuksen allekirjoitusvaiheessa kiinnitetään usein myös rakenne ja toimeenpanovaiheessa korjaaminen tulee usein myös kalliiksi.

- Sivu 19 "Viitearkkitehtuuri ei ohjaa palvelun omistajia käyttämään tiettyjä ohjelmistotuotteita- tai teknologioita." KOMMENTTI: Julkishallinnon kokonaisarkkitehtuurin (JHS 179) periaatteisiin on kirjattu suositus käyttää avoimen lähdekoodin ohjelmistoja.

- Sivu 19 "5.2.1 Modulaarinen ratkaisuarkkitehtuuri" KOMMENTTI: Tämä pätee vain niihin tilanteisiin, joissa ratkaisuarkkitehtuuriin on mahdollista vaikuttaa. Trendi on kuitenkin tänä päivänä valmisohjelmistoja suosiva. Taustalla mahdollisuus hyödyntää laajoja kehittämisresursseja sekä jakaa kehittämiskustannukset muiden asiakkaiden kanssa.

- Sivu 20 kuva 2 KOMMENTTI: Onko tämä JHS 179-suosituksen mukainen kuvaustapa ns. kerroskaaviolle?

- Sivu 21 kuva 3 KOMMENTTI: Pitäisikö tämän kuvan sisällön esittämisessä noudattaa JHS 179-suositusta?

- Sivu 22 "Edellä kuvattujen palveluiden käyttöönotto on usein houkuttelevan helppoa ja edullista mikäli palveluille ei aseteta erityisiä vaatimuksia" KOMMENTTI: Oliko kuitenkin niin, että valtionhallinnolle on määritetty taso, joka kaikkien palvelujen tulee täyttää?

Sivu 23 "Ellei tietoturvallisuuden ja vaatimuksenmukaisuuden varmistaminen ole mahdollista, palvelun omistajan tulee rajoittaa tietojenkäsittely ei-luotetussa tukipalvelussa julkisiin tietoihin" KOMMENTTI: Myös henkilötietojen käsittelyä voi olla syytä rajoittaa vaikka ne olisivat julkisiakin

Sivu 23 "Analytiikkavälineiden valinnassa ja konfiguroinnissa tulee varmistua, etteivät ne paljasta asiointipalvelun käyttäjistä tietoja osapuolille, jotka voivat käyttää tietoja muuhun kuin niiden alkuperäiseen käyttötarkoitukseen." KOMMENTTI: Mikä on sopimusten rooli, joissa esim. velvoitetaan rajaamaan käyttö & hävittämään aineisto?

- Sivu 24 kuva 4 KOMMENTTI: Onko tarkoitus kuvata nämä myös JHS 179-suosituksen mukaisesti?

- Sivu 25 "Palvelun saatavuusajan ohella palvelun omistajan tulee määritellä poikkeamatilanteiden RPO- ja RTO-vaatimukset. Palvelutoimittajien vastuulla olevien palveluiden osalta sopimuksissa tulee määritellä vaatimukset häiriöiden ratkaisuajoille." KOMMENTTI: Nämä pitää kiinnittää jo tarjouspyynnössä, sillä niillä on yleensä merkittävä kustannusvaikutus

- Sivu 26 "Lokienhallinta" KOMMENTTI: Lokitiedon hävittäminen?

- Sivu 27 "Kayttäjät" KOMMENTTI: Tekstiin olisi hyvä tarkentaa kuuluuko käyttäjiin muita kuin asiakkaita esim. virkailijoita.

- Sivu 29 "Internetin kautta asiointipalvelua käyttävien asiakkaiden kohdalla asiointipalvelun omistajalla on hyvin rajalliset keinot vaikuttaa asiakkaiden omien päätelaitteiden tietoturvallisuuteen." KOMMENTTI: Onko kuitenkin velvollisuus ohjeistaa tai muistuttaa tietoturvallisuudesta huolehtimisen tarpeellisuudesta?

- Sivu 30 "Toteutuksen, operoinnin ja kehittämisen tietoturvallisten menettelyjen tulee kattaa palvelun koko elin-kaari siten, että haavoittuvuuksien synty esimerkiksi uhkaympäristön muuttuessa tai palvelun merkittävissä muutostilanteissa on ehkäisty." KOMMENTTI: Edelleen tämä on huomioitava pääasiassa jo tarjouspyyntöjä laadittaessa.

- Sivu 31 "Tietoturvapäivitysten ja haavoittuvuuksien hallinta" KOMMENTTI: Organisaatiolla täytyy olla tästä vastaava prosessi (oli se sitten kuvattu tai ei) ja siitä vastaava(t) henkilö(t).

- Sivu 33: "Suomi.fi-palveluväylää" Onko Suomi.fi –palveluväylä sama kuin kansallinen palveluväylä? Mikä on ko. ratkaisun suojaustaso?

- Sivu 33 "Valtorin VIA-integraatiopalvelua integroituessaan muun valtionhallinnon sisäverkkojen tietojärjestelmiin" KOMMENTTI: Mikä on ko. ratkaisun suojaustaso?

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

- Sivu 36 "Esimerkiksi julkisissa tietopalveluissa kansalaisia ei ole yleensä tarpeen tunnistaa lainkaan," KOMMENTTI: Onko jopa niin, että joidenkin tietojen osalta ei edes saisi tunnistaa kansalaista?

- Sivu 37 "Virheelliseen tunnistukseen liittyy merkittävä riski" KOMMENTTI: Yhdenmukaisuuden vuoksi olisi hyvä laittaa myös tämä termi englanniksi

- Sivu 38 kuva 5 KOMMENTTI: Pitäisikö tämä kuvata JHS 179-suosituksen edellyttämällä tavalla?

- Sivu 40 6.4.1 viimeinen kappale "Asiointipalvelun omistaja määrittelee ..." KOMMENTTI: Onko tässä dokumentissa tarpeen kuvata tätä ratkaisua?

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

-

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

- Kannattaisiko luku 8 sisältö siirtää liitteeksi, jolloin se mahdollisesti olisi helpommin ylläpidettävissä?

- SIvu 49 "Taulukko 5 kuvastaa tilannetta tämän ohjeen julkaisuhetkellä. Sähköisen asioinnin järjestämisestä vastaavien tahojen on syytä seurata aktiivisesti tukipalveluiden kehittymistä." KOMMENTTI: Korvaako tämä JHS 179-suosituksessa esitetyn palvelukartan?

- Sivu 51 "Palveluväylä" KOMMENTTI: Onko tätä hyödynnettävä vain niissä tapauksissa, joissa sen tietoturvataso on riittävä? Muutoinhan voi syntyä ristiriita.

- Sivu 52 "8.2 Suomi.fi -palveluväylä" KOMMENTTI: Tuoko tämä jotain erityistä hyötyä turvallisuuden näkökulmasta?

- Sivu 53 "1.1.1 Tarkistuslista asiointipalvelun omistajalle" KOMMENTTI: Omistajuus määritetään usein vasta hankintapäätöksen ja jopa vasta toimitusprojektin jälkeen. Tämä tieto listasta pitäisikin saada jo hankintaprosessissa mukana oleville.

- Sivu 53, 8.3 viimeinen kappale "Tämän ohjeen julkaisuhetkellä..." KOMMENTTI: Kannattaisiko nämä laittaa liitteeseen?

- Sivu 56 kuva 11 KOMMENTTI: Pitäisikö tässä käyttää prosessikartan- ja prosessikuvauksen välimaastoa (=sidosryhmien vuorovaikutusta) kuvaavaa toimintamalli-kuvaustapaa, joka on esitetty JHS 152 –suosituksessa?

Liite 1: Keskeinen sanasto

Sanasto pitäisi ehdottomasti saada keskitetysti yhteen paikkaan. Nyt jokaisessa uudessa ohjeessa luetellaan muutama termi eikä kukaan huolehdi niiden yhdenmukaisuudesta.

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?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

Mahdollisimman laajasti. Koulutuksia pitää markkinoida ja räätälöidä erilaisille kohderyhmille kuten tietohallintojohto, järjestelmien omistajat, hankinnoista vastaavat, projektipäälliköt, tietoturvavastaavat jne.

Muuta palautetta ohjeesta tai VAHTIlle?

-

Kinnunen Erja
Verohallinto - Verohallinto, Turvallisuusyksikkö