Terveyden ja hyvinvoinnin laitos THL

Lausunto

16.02.2017 THL/97/4.00.00/2017

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 perusolemukseltaan hyvä ja selittävä. Ohjeen käyttötarkoitusta ja kohderyhmää voisi olla hyvä vielä kerran tarkastella. Ohjeessa on nykyisellään paljon selittävää ja perusperiaatteita avaavaa tekstiä, mutta yksityiskohtaisempia toteutusreferenssejä on vähemmän. Mikäli ohjeessa vahvemmin halutaan painottaa toimintavaatimuksia ja luoda ohjeesta vahvempi referenssilista, niin vaatimuksia olisi hyvä hieman tarkentaa. Jos toisaalta ohjeen halutaan olevan yleissivistävä yleiskatsauksen luova, niin silloin ohjeen kohderyhmät voisi olla hyvä tarkistaa.

Ohjeessa on paljon selittävää tekstiä, mikä sinänsä on hyvä, mutta ohje kaipaisi hieman määrämuotoisempaa struktuuria, jotta sitä olisi mahdollista nopeasti ja helposti käyttää referenssinä eri toiminnoissa ja projekteissa. Lisäksi tuota referenssitoteutusten/ohjeiden tarkentamista voisi jatkaa. Esimerkkinä voisi käyttää OWASP:in ASVS standardia tai muuta vastaavaa, jossa eri verkkopalveluluokille on valmiiksi luokkien mukaan kirjoitetut vaatimukset. Varsinkin vaatimusmäärittelyssä, suunnittelussa sekä lopputuloksen verifioinnissa vastaavanlaiset varsin yksityiskohtaiset referenssilistat/tarkemmat luokkakohtaiset ohjeet olisivat todella hyödyllisiä. Lisäksi ASVS:ään on linkitetty aihekohtaisesti OWASP:in ”Cheat Sheeteja”, josta helposti ja pienellä vaivalla voi tarkistaa parhaita käytäntöjä.

Lisäksi OWASP:in suunnitteluperiaatteita (tai vastaavia voisi nostaa selvemmin esille) hyvän suunnittelun ja toteutuksen lähtökohtana (OWASP - Secure Coding Principles):

- Hyökkäyspintojen minimointi (Mimimize Attack Surface Area)
- Turvallisten oletusasetusten käyttö (Security Default)
- Tehtävien eriyttäminen (Separation of Duties)

- Vähäisimpien oikeuksien periaate (Least Privilege)
- Syvyyssuuntainen puolustus (Defense in Depth)
- Virheiden turvallinen käsittely (Secure Failure)
- Ei luoteta tietoturvamekanismien salassa pysymiseen/piilottamiseen (Security by Obscurity)
- Yksinkertaiset turvallisuusrakenteet (Keep Security Simple)
- Älä luota keneenkään (Trust no one)
- Heikoimman alueen suojaaminen (Securing the Weakest Link)

Mitä kehittämistä mielestäsi ohjeessa vielä on?

-

Mitkä olivat ohjeen parhaita asioita?

-

Yksityiskohtaiset kommentit

Luku 1 Johdanto

-

Luku 2 Lainsäädäntö ja tietoturvallisuutta ohjaavat viitekehykset

-

Luku 3 Sähköiset asiointipalvelut

-

Luku 4 Sähköisen asiointipalvelun tietoturvaperiaatteet

-

Luku 5 Sähköisen asiointipalvelun viitearkkitehtuuri

-

Luku 6 Tunnistaminen ja valtuuttaminen sähköisissä asiointipalveluissa

-

Luku 7 Suostumusten, tahdonilmausten ja viranomaispäätösten sähköinen käsittely

-

Luku 8 Sähköisen asioinnin kansalliset tukipalvelut

-

Liite 1: Keskeinen sanasto

-

Liite 2: Kaupallisten tukipalveluiden tietoturvallisuuden tarkistuslista

-

Liite 3: Tunnistusmenetelmän luotettavuuteen vaikuttavat tekijät

-

Liite 4: Tietoturvallisen sähköisen asiointipalvelun suunnittelun tarkistuslista

Tämä kohta on aika suppea eikä ota kantaa läheskään kaikkeen mitä pitää ottaa huomioon. Parempi olisi tarjota jotain hieman yksityiskohtaisempaa listaa jos halutaan tällaista tarjota. ks. esim. OWASP ASVS.

Liite 5: Sähköisen tunnistamisen menetelmien varmuustasot

-

Liite 6: Case-esimerkit

Valittujen Case-esimerkkien tarkoitus jäi hieman epäselväksi ohjeen muuta sisältöä ajatellen (kuvaavat käyttäjän näkökulmaa ei palvelun tarjoajan/kehittäjän)

Miten paljon organisaatiollesi on hyötyä tästä ohjeesta?

Paljon

Miten ohjetta tulisi kouluttaa ja jalkauttaa käyttöön?

-

Muuta palautetta ohjeesta tai VAHTIlle?

Nämä ohjeet ovat tarpeellisia ja hyviä, mutta kohderyhmä ja ohjeen rakennetta/sisältöä ollisi syytä vielä edelleen miettiä ja jos mahdollista sitoa entistä tiukemmin kiinni VAHTI-tasovaatimuksiin (perus, korotettu ja korkea) jos mahdollista. Nyt vaikuttaa siltä, että yritetään miellyttää sekä noviisia, että teknistä kehittäjää jonka seurauksena kumpikaan ei välttämättä ole täysin tyytyväinen. Mutta tästä huolimatta ohje on tarpeellinen ja siihen osoitettu työpanos perusteellisen hyvä.

Esimerkeissä viitataan useammassakin kohdassa sosiaali- ja terveydenhuollon palveluihin. Kuitenkin puuttuvat viittaukset ko. kohdealueen keskeisiin lakeihin, mm. ”Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä”.

Samoin tekstissä viitataan useaan otteeseen kansalliseen palveluarkkitehtuuriin KaPAan ja palveluväylään, mutta ei kuitenkaan vastaavaan sosiaali- ja terveydenhuollon KanTA-palveluihin ja -arkkitehtuuriin.

Integraatioiden osalta mainitaan useaankin otteeseen VIA-ympäristö, ikään kuin teksti olisi peräisin ajalta jolloin kansallista palveluväylää ei vielä ollut keksittynä. Tosin Suomi.fi palveluväylä on myös nostettu rinnalle, mutta sen todetaan (sivu 35) soveltuvan korkeintaan ST IV -aineistoille. Kanta-palvelujen viestinvälitysarkkitehtuuria ei mainita.

Tunnistamisen yhteydessä ei mainita terveydenhuollon ammattivarmenteita (sivu 36).

Kaiken kaikkiaan, sosiaali- ja terveydenhuollon näkökulma näyttää ikään kuin jääneen vähemmälle huomiolle tekstistä, esimerkkejä lukuun ottamatta!

Jämsen Christian
Terveyden ja hyvinvoinnin laitos THL