Jämsen Christian

8.5.2015

Valtiovarainministeriö
VAHTI

Lausuntopyyntönne VM047:18/2007

Valtionhallinnon salauskäytäntöjen tietoturvaohje

Yleiset kommentit

Ohje on verrattaen yleinen ja tarjoaa yleiskatsauksen salauskäytäntöihin ja tarpeisiin. Mitään erityisen isoja tai periaatteellisia asiaan kohdistuvia huomioita, joita olisi syytä pohtia tarkemmin ei huomattu.

Yleisesti kuitenkin kiinnitettiin huomiota ohjeen tarkoituksen kirkastamisen tarpeeseen ja kohderyhmän määrittelyyn. Ohjeen alussa on suhteellisen paljon yleistä tietoa salauksen historiasta, yleisestä periaatteista, yleisistä käyttökohteista ja muusta vastaavasta, joka ei välttämättä tuo lisäarvoa halutulle kohderyhmälle. Jos kohteeksi on ajateltu salausratkaisuja suunnittelevia ja implementoivia tahoja, yleistä tietoa paljon kiinnostavampaa olisi lukea siitä miten eri salauskäytännöt tulee soveltaa eri suojaustason vaativiin ympäristöihin. Ohjeessa on viitteitä joistain konkreettisesti sovellettavista hyvistä salauskäytännöistä ja käytäntoihin liittyvistä prosesseista (esim. luku 5. avaintenhallinta ja luku 6.7 esimerkkejä), mutta ne jäävät kokonaisuuteen nähden pienemmälle huomiolle.

Jos taas kyseessä on yleisohje, kohdentaminen on varmaankin tämänkaltaisena hyvä, mutta samalla herää kysymys ohjeen käyttötarkoituksesta, kun iso osa informaatiosta on sellaisenaan löydettävissä muista lähteistä eikä ohje tuo sitä lisäarvoa, jota sille on ajateltu.

Jonkin verran yleistä huomiota tulee kiinnittää ohjeen kielelliseen ulkoasuun ja viestin yleiseen selkeyttämiseen.

Voisi kenties mainita, että ohjetta voitaneen soveltaa myös muualla kuin julkisessa hallinnossa.

Lukukohtaiset kommentit

Esipuhe

Lunnashaittaohjelmien esille ottaminen heti alussa voi olla hieman ”irrallista”. Esimerkki on vain yksi uhkatyyppi monesta, joka aihepiiriä sivuaa, mutta ei välttämättä sellaisenaan ole ohjeen pääasiallisessa fokuksessa. Esimerkki jää ehkä hieman irralliseksi kontekstista.

Viidennessä kappaleessa puhutaan liike- ja ydintoiminnan vaatimuksista, mutta koska myös tukitoiminnoilla on omat vaatimuksensa ehdotetaan, että kohdassa käytettäisiin termiä ”toiminnan vaatimukset”.

Laskentatehon nopea kehittyminen heikentää salausta

Viimeisessä virkkeessä on maininta kyberturvallisuuskeskuksen toiminnasta ja yhteystiedot. Mainінta vaikuttaa olevan irrallaan otsikon aiheesta?

Tietoturvallisuusasetus toi mukanaan salausvaatimuksen

Ensimmäisen kappaleen ensimmäisessä virkkeessä todetaan, että ” Valtaosa julkishallinnossa käsiteltävästä tiedosta on julkista”. Muotoilu ko. lauseen osalta on hyvä tarkistaa. Jos tarkoituksena on tuoda esille Julkisuuslain mukainen asiakirjojen julkisuusolettama, niin lausetta tulee muotoilla paremmin yhteyteen sopivaksi.

Ohjeen tavoitteet

Ensimmäisen kuvan kuvatekstin viimeinen lause liittyen saatavuuteen. Tekstissä mainittu sopimus on ”vain” sopimustekninen tapa varmistaa saatavuutta. Ehkä olisi hyvä ottaa käytännön esimerkki mitä keinoja käytetään teknisesti (vikasietoisuus, kahdennus, hajautus, varajärjestelmät ja varajärjestelyt yms)

Toisen kappaleen ensimmäisessä virkkeessä on maininta ”luokituksen noustessa” – mitä tällä tarkoitetaan?

Kuva kolme. Kuvan sana ”koska” esitetään korvattavan sanalla ”jos”.

Sivu 9 ensimmäinen kappale, ensimmäinen virke. Kohdassa mainittu, että ”Tietoaineiston eheyden osalta voidaan edellyttää…”. Asian voisi muotoilla jollakin toisella tavalla. Nyt asia ilmaistu ”lievästi”. Lähtökohtana kai on, että eheys on perusedellytys ja vaatimus. Yleensä perusvaatimus minkä tahansa aineiston hallinnassa. Se, että sallittaisiin hallitsematon muuttuminen, lienee poikkeus.

Sivu 9, 4 kappale. Mainitaan, että perustietotekniikkapalvelut jatkossa keskittyy Valtorille. Tämä tosin on jo suhteellisen pitkälle tapahtunut. Voisi ehkä vain todeta, mitä palveluita Valtori tuottaa. Lisäksi on hyvä samassa kappaleessa huomioda, että Valtori tuottaa vain osan tukitoimintojen tietotekniikkapalveluista ja ohjetta on tältä osin myös noudatettava muissa kuin mainituissa substanssi- ydin- ja liiketoiminnassa. Ohjeen noudattamiskehtoukseen liittyen jää epäselväksi mitä ohjeessa tarkalleen ottaen on noudatettava, kun se luonteltaan on hyvin yleinen ja tuo esille vain vähän selkeitä ohjeita, joita voi noudattaa tai soveltuvat noudatettaviksi.

Kohderyhmä

Ks. yleiset kommentit.

Tietoturvallisuusasetus, tietoturvtasot ja muut viitekehykset

Luku 3.1, sivu 13 viimeinen kappale. Mitä kohdassa tarkoitetaan kohteeseen pääsyllä? Tarkoitetaanko myös mahdolllista paikallista lähiverkkoa (joka voi olla irti muista verkoista)?

Tiedon salaaminen – tekninen viitekehys

Ensimmäinen kappaleessa määritellään mitä eheydellä tarkoitetaan. Eikö eheydellä tarkoiteta ensisijaisesti sitä että tieto on ”ehjää”, siis oikein (suhteessa todellisuuteen tai todellisuutta mahdollisesti kuvaaviin asiakirjoihin tai havaintoihin). Muutosten havaitseminen ja kirjaaminen lienee toissijaista?

VPN-ratkaisu organisaation kahden toimipisteen välillä

Sivu 38, kuva 6. Kuvan pitäisi paremmin kuvata se, että tiedon salaaminen tapahtuu turvallisen alueen sisäpuolella. Nyt kuvasta joku saattaa saada käsityksen, että salaus tapahtuu ”rajalla”.

Etäkäyttölaitteiston sekä muiden päätelaitteiden kiintolevyn ja apumuistien salaus

Sivu 38, viimeinen kappale, viimeinen lause. Lause antaa hyvin paljon tulkinnan varaa. Mitä on suositeltavaa, missä pitää toteuttaa ja mitä voidaan mahdollistaa?

USB-muistien salaus

Pitäisi yleistää erilaisiin muihinkin ulkoisiin muistivälineisiin. USB on vain yksi väylätyyppi.

Liite 3

Liiteessä mainitaan VAHTI 3/2008 Valtionhallinnon salauskäytäntöjen tietoturvaohje. Mainittu ohje ei kuitenkaan ole voimassa sen jälkeen kun lausunnolla oleva ohje julkaistaan.

Tietoturvapäällikkö Christian Jämsen

JAKELU: valtiovarainministerio@vm.fi