ILMATIETEEN LAITOS

LAUSUNTO

7.5.2015 30/020/2015

Lausunnon pyytäjä

Lausuntopyyntö 21.4.2015, VM047:18/2007

Ilmatieteen laitoksen lausunto salausohjeen luonnoksesta

Valtiovarainministeriö on pyytänyt lausuntoa valtionhallinnon salausohjeen luonnoksesta. Ilmatieteen laitos on perehtynyt VAHTIn Salauskäytäntöjen tietoturvaohjeen luonnokseen ja toteaa seuraavaa:

Organisaatiolle tulee yhä enemmän haasteita hallita tietoturvallisuus kattavasti ympäristössä, jossa organisaation yhteistyö on laajasti verkostoitunutta ja tarpeet eri tietoteknisten välineiden ja ohjelmistojen käyttöön sekä tiedon jakamiseen kasvavat. Samalla tietoturvauhkat ovat myös kehittyneet ja tulleet yhä vaikeammin hallittaviksi. Tässä ympäristössä salaustuotteiden käytölle on tilausta ja on hyvä, jos valtionhallinnon linjauksilla ja ohjeella edistetään organisaation salausratkaisuihin liittyvää päätöksentekoa ja oikeansuuntaisten valintojen tekemistä sekä hallinnollisissa että teknisissä ratkaisuissa.

Hyvää ohjeessa on, että siinä tuodaan esille salassa tietoturvallisuusasetuksesta, tietoturvatasosta ja muista viitekehyksistä (KV, KATAKRI, ...) tulevia perusteita ja velvoitteita salassa pidettävän tiedon käsittelylle ja tietojärjestelmien suojaamiselle. Vaatimusmäärittelyjä oli poimittu suoraan VAHTI 2/2010 -ohjeen taulukoista. Lopullisessa ohjeessa kyseiset kohdat olisi hyvä olla selvemmässä formaatissa ja paremmin luettavissa. Kopioidussa taulukossa ST II tietoaineiston siirto avoimessa verkossa ei ole sallittu, mutta ST II salassa pidettävän tietoaineiston käsittely avoimissa tietoverkoissa vahvasti salattuna tai suojattuna on sallittu (s.13 ja s.14). Määrittelyt vaatinee lisäselvitystä.

Ohjeeseen oli koottu kattavasti myös tiedon salaamisen teoriaa ja salauskäytäntöjen teknistä viitekehystä sekä ohjeistetaan, millä salauksen toimenpiteillä suojataan tietoturvan eri osa-alueita luottamuksellisuutta, eheyttä ja saatavuutta. Salausratkaisuja valittaessa teoriatietojen ja tarkistuslistojen saatavuus yhdestä ja samasta ohjeesta on hyvä asia.

Kappaleeseen (2.1) Huoneentaulu oli koottu keskeisiä asioita, mitä organisaation tulee ottaa huomioon tiedon salausasioiden suunnittelussa ja käyttöönotossa. Salaustuotteiden käyttö liittyy kiinteästi organisaation arkkitehtuuriin, tietoaineistojen luokitteluun ja kriittisen salassa pidettävän tiedon elinkaaren hallintaan ja suojaamiseen. Ohjeessa voisi olla enemmänkin teknisiä ratkaisuja esittäviä kuvia, koska ne selventävät heti toteutukseen liittyviä vaatimuksia.

Ohjeesta puuttui kappale, jossa käsiteltäisiin salattujen tietoaineistojen varmistuksiin sekä avainten vanhenemisiin ja versiohallintaan liittyviä asioita. Voisi olla hyvä, että nämäkin asiat huomioitaisiin.

Salausratkaisujen käytössä riittää haasteita kuten ohjeessa niistä olikin mainintaa. Laajempi salaustuotteiden käyttö organisaatiossa vaatii keskitettyä avaintenhallintaa, mikä tulee olla huolella suunniteltu ja ylläpidetty. Luotettaviksikin ilmoitetuista salaustuotteista löytyy aika ajoin tietoturva-aukkoja. Valtionhallinnossa on suuntauksena, että yhä enemmän palveluja ulkoistetaan, mikä tuo lisähaasteita kyseiselle aihealueelle, kun vastuu tietoturvasta on aina kuitenkin organisaatiolla itsellä.

Alla vielä kohdennettuja kommentteja ohjeeseen:

*1.1 Mukaan pilvilaskennan mukanaan tuoma erittäin tehokas hashien vertaaminen esim. rainbow-tableihin on nykyään helppoa ja halpaa. Samoin bruteforcettaminen on todella nopeaa pilvilaskennan ansiosta. Näille on olemassa halpoja valmiita palveluita saatavilla.

*4.2.2 Epäsymmetristen menetelmien heikkoudesta: ”Ne saattavat olla myös alttiimpia tietyille hyökkäystyypeille. Tarkoitetaanko esim. mitm- tai side-channel hyökkäyksiä?

*4.2.2 Epäsymmetrisessä menetelmässä on ”yleensä” käytettävä -> on käytettävä. Tai sitten esimerkkejä, missä näin ei ole.

*4.2.3 ”Näin symmetrinen avain voidaan välittää turvallisesti: Kahta kappaletta aiemmin todettiin että epäsymmetriset menetelmät ovat tietyille hyökkäystyypeille alttiita. Pitäisikö sanoa että ”suhteellisen turvallisesti”

*4.3 Vaikka tässä kohdassa tiivisteistä puhutaankin eheyden varmistamisessa, pitäisi ottaa niin kovasti aina huomioon kun puhutaan tiivisteistä SUOLAUS. Suolaamattomat hashit on täysin vapaasti murrettavissa (pilvilaskenta + rainbow-tablet)

*4.6 Tietoliikenneprotokollat kappale kaipaa ehdottomasi mainintaa SSL:n turvattomuudesta.

*4.6.2 IPsec on ainoastaan niin turvallinen kuin millaiseksi se on konffattu. On paljon ihmisiä jotka luulevat sen tuovan automaattista turvaa, ja valitsevat esimerkiksi sen päällä ajettavaksi turvattomia ratkaisuja. Tosin tässä taidetaan puhua vain L2:lla käyttämisestä.

*4.7 TrueCryptin tuen päättyminen johti siihen, että joukkorahoituksella haalittiin rahat kasaan ja tuote auditoitiin NSA:n pelossa. Viimeisin versio on todistetusti turvallinen ja käyttö lisääntynyt.

*5.1.1 Satunnaislukujen luomisessakin ollut vähän hikkaa (RDRAND, PadLock) eli näihinkin keinoihin pitää suhtautua kriittisesti.

Liite 1, Tiedot (www.ficora.fi/ xxx) olisi hyvä olla saatavilla.
Liite 2, Keskeistä sanastoa, joita ohjeessa on käytetty, on hyvä täydentää.

Helsingissä 7.5.2015

Matti Keränen
Yksikön päällikkö / Sääpalvelujen tuotantojärjestelmät

Valmistelija:

Pirkko Kilpeläinen
tietoturvapäällikkö