Valtiovarainministeriön lausuntopyyntö VM047:18/2007

PUOLUSTUSHALLINNON RAKENNUSLAITOKSEN LAUSUNTO SALAUSOHJEEN LUONNOKSESTA

Valtiovarainministeriö pyysi 21.4.2015 päivätyssä asiakirjassaan lausuntoa Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI:n alaisuudessa toimivan teknisen jaoston valmistelemasta luonnoksesta valtionhallinnon salausohjeeksi.

Puolustushallinnon rakennuslaitos on tutustunut ohjeluonnokseen ja laatinut lausunnon tietoturvallisuuden ja tietohallinnon yhteistyönä. Lausunnossa otetaan kantaa ohjeen yleisluonteeseen ja teknisiin yksityiskohtiin.

1 Yleistä

Lausuntokierroksella oleva salausohje on tarpeellinen ja selkeyttää valtion virastojen toimintamalleja suojattavan tietoaineiston käsittelyssä. Lopullisessa salausohjeessa tulisi mielestämme kiinnittää enemmän huomiota seuraaviin yleisluonteisiin asioihin.

- Salausohjeen sitovuutta ja velvoittavuutta tulisi korostaa.

- Valtorin roolia tulisi korostaa ja harkita siitä näkökulmasta, että Valtori kilpailuttaisi salaustuotteet ja tarjoaisi niitä asiakkailleen. Valtori voisi myös paketoida salausratkaisut esim. PÄKÄ- kokonaisuuteen ja näin ”pakottaa” asiakasviraston salaustuotteen hankkimiseen.

- Esimerkit luvussa 6.7 voisivat olla kattavampia ja tarkempia.

- Salaustuotteen mainitseminen nimellä luvussa *Esimerkkejä,* johtaa suurella todennäköisyydellä tilanteeseen jossa ohjeen lukija valitsee ohjeessa mainitun tuotteen. Salausohjeen elinkaaren kannalta voisi olla turvallisempaa jättää tuotenimet pois ja viitata NCSA:n hyväksyttyjen salausratkaisujen listaan tai Valtorin kilpailuttamiin/tarjoamiin ratkaisuihin.

2 Yksityiskohtaiset havainnot

Luvussa 4.3 mainitaan tiivistefunktioiden vaatimuksena sen, että niiden laskennan tulee olla mahdollisimman nopeaa. Tämä on kuitenkin ristiriidassa käytännön kanssa, sillä salasanojen tallentamiseen tarkoitetut tiivistefunktiot (esim. bcrypt, scrypt) tulisi nimenomaan olla vapaasti parametroitavissa siten, että niiden laskeminen on riittävän hidasta. Tämä tehdään siksi, jotta ns. rainbow-taulujen luonti salasanojen brute force-murtamiseen olisi laskennallisesti mahdollisimman vaikeaa.

Luvussa 4.6.1. suositellaan käyttämään TLS-salauksen uusinta versiota. Olisi syytä mainita myös kaikkien vanhempien TLS / SSL-versioiden nimenomaisesta poistamisesta käytöstä, ellei jokin toiminnallinen vaade edellytä jotain vanhempaa versiota. Tämäkin toiminnallinen vaatimus olisi syytä kuvata organisaation toimesta, siitä tulisi esittää riskiarvio sekä laatia aikataulu ongelman korjaamiseksi.

Luvussa 4.6.2 kuvataan TLS-protokollan toimivan sovellustasolla. Tämä pitää paikkansa ainoastaan Internet Protocol Suiten mukaan, OSI-mallissa **TLS initialisoidaan sessiokerroksella ja toimii esityskerroksella**. Salausta käsiteltäessä OSI-malli on suuremman tarkkuutensa vuoksi hyödyllisempi viitekehys.
.

Luku 4.7, kannattaako Wikipediaa oikeasti käyttää lähteenä tämän tason ohjeistuksissa? Lisäksi, mitä ihmettä tarkoittaa ”tietoturvadomainien rajojen fraktalisoituminen” kohdassa ”Salaustekniikoiden sijainti”?

Luku 5.5, pitäisikö forward secrecy-ominaisuutta vaatia eikä vain suositella? Lisäksi, tulisiko ottaa kantaa digitaalisten avainten revokaatiomekanismeihin (CRL vs. OCSP)?

Luku 6.3.2. ”On syytä ottaa huomioon time-memory-tradeoff-hyökkäykset”. Varmasti onkin, mutta millä tavalla? Miten ko. hyökkäykset vaikuttavat järjestelmävalintaan? Pitäisikö tässä yhteydessä vielä korostaa avaintenhallinnan merkitystä, joka epäonnistuessaan voi pahimmassa tapauksessa mahdollistaa online- viestinnän murtamisen kaikilla algoritmeilla ja toteutuksilla?

Ohjeessa ei oteta myöskään kantaa siihen, tulisiko kryptografian mahdollistamia erilaisia kiellettävyyden lajeja huomioida valtiohallinnan toiminnassa, eikä siihen, että voisiko OTR-viestimiä kuten Pidgin käyttää jossain viestinnän erikoistilanteessa. Ohjeen tulisi ottaa kantaa myös siihen, että voiko TrueCryptin / VeraCryptin / CipherShedin mahdollistamia piilotettuja datasäilöjä käyttää? Tai jos ei voi niin tulisi perustella, että miksi ei voi?

Henri Lehtelä
Tietoturvapäällikkö

JAKELU Valtiovarainministeriö, kirjaamo

TIEDOKSI Aarne Hummelholm