Valtiovarainmisteriö
VM047:18/2007/

OPETUSHALLITUKSEN LAUSUNTO SALAUSOHJEEN LUONNOKSESTA

Tämä on Opetushallituksen (myöhemmin OPH) lausunto koskien Valtiovarainministeriön lausuntopyyntöä salausohjeen luonnoksesta. Opetushallituksen toiminta on Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttämällä perustasolla ja korotetulla tasolla sitä edellyttävissä toiminnoissa.

OPH pitää salausohjetta tervetulleena päivityksenä joka toimii hyvänä kertauksena teoriaan ja aiemmin julkaistuihin Vahti-ohjeisiin. Ohjeistuksen parhaimpana antina toimivat tarkistuslistat, jotka tarjoavat konkreettisen työkalun organisaation prosessinhallintaan ja toimintojen tarkastamiseen.

OPH pyytää huomioimaan vielä seuraavat asiat ennen ohjeen julkaisemista:

- Varmenteiden/sertifikaattienhallinnan tulisi näkyä ohjeessa selkeämmin
- Liite 1. Kryptografiset vahvuusvaatimukset luottamuksen suojaamiseen puuttui. Esimerkiksi kappaleessa 4.6.1 TLS-protokollan osalta mainittava, ettei suositella tuettavaksi heikkoja salausmenetelmiä ("cipher suite"). Heikkojen salausmenetelmien tukemiseen ei yleensä ole tarvetta, koska nykyaikaiset selaimet, sovellukset ja muut teknologiat tukevat parempiakin salausmenetelmiä
- Korostettava, että vain vahvat salausalgoritmit tulisi sallia
- Tarkistuslistoihin voisi tarvittaessa lisätä kappaleen järjestelmän ylläpitäjän näkökulmasta (tekninen näkökulma)
- Lisättävät maininta esim. tarkistuslistoihin tai liitteeseen 1, ettei esimerkiksi seuraavia salausalgoritmejä ja allekirjoitusavaimia tulisi enää käyttää, niissä olevien heikkouksien takia:
    - 128 bittisillä avaimilla (tai alle)
    - Poikkeuksena AES-128 ja Camellia-128
    - 3DES:n, jonka efektiivinen avainkoko on alle 128 bittiä johtuen ns. meet-in-the-middle -hyökkäyksestä
    - DSS-autentikointia käyttävät salakirjoitusmenetelmät (cipher suite)
    - RC4-salausalgoritmi
    - Salakirjoitusmenetelmät, joissa on käytössä MD5-pohjainen MAC
    - Anonymous Diffie–Hellman (aDH) avaintenvaihtoa käyttävät
    - Null- tai export-salausalgoritmiä käyttävät salakirjoitusmenetelmät
    - SHA-1. (selaintuki loppunee 2017)

Opetushallitus
Hakaniemenranta 6, PL 380, 00531 Helsinki, puhelin 029 533 1000, faksi 029 533 1035, etunimi.sukunimi@oph.fi, www.oph.fi
Utbildningsstyrelsen
Hagnäskajen 6, PB 380, 00531 Helsingfors, telefon 029 533 1000, fax 029 533 1035, fornamn.efternamn@oph.fi, www.oph.fi

- Salausalgoritmeistä tulisi suosia niitä, jotka toteuttavat Perfect Forward Secrecy (PFS) -ominaisuuden. PFS-salaukset ovat niitä, joissa käytetään Ephemeral Diffie–Hellman (EDH) –avaintenvaihtoa
- Ohjeeseen voisi lisätä kappaleen tai viittauksen tarjolla oleviin salaustyökaluihin, joilla voi selvittää ympäristönsä vaatimuksenmukaisuutta:
  - https://www.ssllabs.com
  - http://nmap.org/
- Liite 2. Keskeisestä sanastoa tulisi päivittää mm. mitä tarkoittaa x.509V3, S/MIME, SSH
- Hyviä mainintoja tietoturvan sipulimaisuudesta ja ettei kaikkia tietojärjestelmiä kannata auditoida
- 802.1x:ää ei ole mainittu ollenkaan; liittyy avainten hallintaan
- Vahva salaus/salaus epämääräisesti määritelty. Olisi jo syytä määritellä, mitä se on käytännössä.
- Ei käsitellä riittävästi organisaation sisäisiä tietoturvaloukkauksia ja niihin varautumisia tieto salaamalla esim. tietokantojen ja sovellusten kannalta
- Luvussa 4.3 käsitellään myös autentikointia, vaikka sille on oma luku (4.4). Vaarana on käsitteiden sekoittuminen
- On syytä mainita, ettei SSL:n mitään versiota tule käyttää
- Kryptovaluutat eivät koske julkista hallintoa, joten niitä on turha käsitellä. Samaa kategoriaan menee kvanttilaskenta.
- Turhaa toistoa esim. avainten eri tyypeistä ja siirtometodeista tulee välttää
- OSI -malli liitteenä ja kerroksiin viittauksia kuten IPSec (verkko) ja TLS (sovellus), koska ovat eri tasolla. On tarpeen lisätä esimerkkejä myös siirtokerroksen salauksista.
- SS7-verkon väärinkäytösmahdollisuudet syytä mainita

Tietohallintojohtaja Erja Nokkanen

Tietoturvavastaava Esa Keränen