Viestintävirasto
Kommunikationsverket
Finnish Communications
Regulatory Authority

Päivämäärä/Datum/Date
31.1.2012

Nro/Nr/No.
1979/04/2012

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI)
valtiovarainministerio@vm.fi

Viite
Ref.
Ref.
Lausuntopyyntö (2125/00.01.00.01/2011 - VM047:13/2007)

Asia
Ärende
Subject
Viestintäviraston lausunto teknisen ICT-ympäristön tietoturvataso-ohjeluonnokseen

Viestintävirasto on tutustunut VAHTI:n valmistelemaan teknisen ICT-ympäristön tietoturvataso-ohjeeseen ja sen tukimateriaaleihin. Ohje on tukimateriaaleineen tärkeä osa valtioneuvoston antaman valtionhallinnon tietoturva-asetuksen (681/2010) maastouttamisesta. Viestintävirasto on osallistunut ohjeen valmistelutyöhön.

Ohjeluonnos

Sivu 12, kohta 1.2 "Rajaukset"

Kappaleessa mainitaan, että käsiteltäessä kansallista tai kansainvälistä turvallisuusluokiteltua tietoaineistoa, sovelletaan suojauksilta edellytettävänä tasona Kansallista turvallisuusauditointikriteeristöä (KATAKRI).

Sekä kansainvälisen, että kansallisen turvallisuusluokitellun tiedon suojaamisessa sovelletaan KATAKRI:a jo laajasti, ja ohje selkeyttää tätä entisestään. Ohjeen linjaus tukee hyvin myös käynnissä olevaa työtä, jossa tietoturva-asetuksen, -tasojen ja KATAKRI:n vaatimuksia yhtenäistetään.

Edelleen samassa kappaleessa mainitaan, että kansallisten verkkojen tietoliikenteen osalta pitää noudattaa VAHTI:n valmistelemassa sisäverkko-ohjeessa (3/2010) olevia tasovaatimuksia.

Sisäverkko-ohje ei ole velvoittava. Tietoturva-asetuksen (681/2010) maastouttamisen selkiyttämiseksi kaikki sen toimeenpanon tukemiseksi laaditut keskeiset ohjeet tulisi käytännön syistä osoittaa velvoittaviksi.

Sivu 54, kappale 4.4.3, kohta 8: "Toimittajan tuottama jaettu kapasiteetti usealle eri asiakkaalle..."

Kappaleen mukaan olisi mahdollista, että pilvipalveluihin, joiden osalta asiakas ei tiedä käytännössä lainkaan, mistä, millä tavalla ja kenen toimesta palvelua tuotetaan tai ylläpidetään, voitaisiin tästä huolimatta tallentaa suojaustaso IV:n mukaista tietoaineistoa muutamaa poikkeusta lukuun ottamatta.

Itämerenkatu 3 A, PL 313
00181 Helsinki
Puhelin 09 69 661
Faksi 09 6966 410
Y-tunnus 0709019-2

Östersjögatan 3 A, PB 313
FI-00181 Helsingfors, Finland
Telefon +358 9 69 661
Fax +358 9 6966 410
FO-nummer 0709019-2

Itämerenkatu 3 A, P.O. Box 313
FI-00181 Helsinki, Finland
Telephone +358 9 69 661
Fax +358 9 6966 410
Business ID 0709019-2

www.ficora.fi

Suojaustaso IV:n mukaiset tietoaineistot ovat salassa pidettävää tietoa, joiden suojaamiseksi on toteutettava ko. tasolle osoitetut suojamekanismit. Näitä vaatimuksia ei voida jättää toteuttamatta missään tietojärjestelmäympäristössä, jossa ko. tietoa käsitellään.

Sivu 69, Liite 9: "Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje"

Kappaleessa ei mainita kansallista turvallisuusauditointikriteeristöä, KATAKRI:a, vaikka se on keskeinen työkalu vaatimuksien mukaisten toteutuksien todentamisessa.

Liitteet

Liite 7, Etäkäyttö - tekniset vaatimukset

Koska etätyö ja -käyttö muodostavat yleisesti tavanomaista suuremman riskien suojattavan tiedon käsittelylle, on niiden turvaamiseksi kiinnitettävä erityistä huomiota ottaen huomioon myös fyysisen turvallisuuden vaatimukset. Viestintävirasto esittää, että:

Kaikille tasoille (erityisesti perustasolle ja soveltuvin osin myös ylemmille tasoille) pakollisina määritetään seuraavat vaatimukset:

1) Organisaatiossa on käytössä periaatteet ja turvamekanismit etä- ja matkatyön riskejä vastaan.
2) Periaatteista ja vaadittavista mekanismeista on tiedotettu henkilöstölle.
3) Turvallisesta etä- ja matkatyöskentelystä on henkilöstön saatavilla ohje.
4) Laitteita, tietoaineistoja tai ohjelmia ei siirretä pois työpaikalta ilman ennalta saatua valtuutusta.
5) Järjestelmien etähallinnassa tai -käytössä käytetään vahvoja (kahteen tekijään pohjautuvia) todennusmenettelyjä. Ts. edellytetään vähintään vahvaa käyttäjätunnistusta. (Kts. kohta 8).
6) Suojattavaa tietoa sisältävät välineet on suojattu luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle.
7) Toimitilojen ulkopuolelle vietyjä laitteita ja tietovälineitä ei jätetä valvomatta julkisille paikoille, kannettavat tietokoneet kuljetetaan matkustaessa käsimatkatavarana.
8) Vain luotettavia ja käyttöympäristöön hyväksyttyjä laitteita (esim. työnantajan tarjoama kannettava tietokone) ja etätyöyhteyksiä käytetään.
Etäkäyttö sidotaan teknisesti työnantajan tarjoamaan etäkäyttölaitteistoon (esim. laitetunnistus).
9) Etähallinnassa huomioidaan etähallintapisteen looginen ja fyysinen sijainti (rajaukset esim. tiettyihin IP-osoitteisiin ja/tai fyysisiin tiloihin).
Etäkäytössä edellä mainitut rajaukset suosituksina.
10) Siirrettäessä suojaustason IV-aineistoa, liikenne tai aineisto salataan luotettavasti.

Korotetulle tasolle pakollisina määritetään (suosituksina perustasolle) seuraavat vaatimukset:

11) Suojaustason III järjestelmien etähallinta on lähtökohtaisesti estetty. Etähallinta on sallittu vain viranomaisen erikseen hyväksymällä menettelyllä. Suojaustasolla III hyväksyttävä etähallintamenettely huomioi mm. etähallintapisteiden fyysisen ja loogisen pääsynvalvonnan, hallintaan käytetyt laitteistot ja ohjelmistot, hallintaliikenteen salauksen, ja edellä mainittujen elementtien luotettavuuden erityisesti luottamuksellisuuden ja eheyden suhteen.

Korkealle tasolle määritetään pakollisena seuraavat vaatimukset:

12) Suojaustason II järjestelmien etähallinta on estetty. Viranomaisten suojaustason II järjestelmissä voidaan tapauskohtaisesti kuitenkin hyväksyä rajattu etähallinta. Tapauskohtaisesti hyväksyttävällä etähallinnalla tarkoitetaan tässä yhteydessä lähes poikkeuksetta turvapäivitysten ja haittaohjelmatunnistekantojen keskitettyä jakelua. Jotta etähallinta voidaan hyväksyä, tulee viranomaisen tekemässä järjestelmällisessä ja kokonaisvaltaisessa riskienarvioinnissa päätyä aina tulokseen, jossa etähallinta on paikallista hallintaa merkittävästi pienempi riski. Tällaisen etähallinnan hyväksyminen edellyttää aina myös päivityspalvelimen sisällyttämistä samaan tietojärjestelmään ja sen fyysistä eristämistä muista järjestelmistä.

Allekirjoitukset,

Timo Lehtimäki
Johtaja

Jani Arnell
Turvallisuuspäällikkö