451/01/2012

23.11.2012

VALTIOVARAINMINISTERIÖ

Julkisen hallinnon ICT-toiminto

Valtiovarainministeriön lausuntopyyntö VM047:19/2007

Lausunto Toimitilojen tietoturvaohjeesta

Valtiokonttori toteaa, että lausunnolla oleva Toimitilojen tietoturvaohje on tarpeellinen ja konkretiaan painottuva ohje. Valtiokonttori pitää tärkeänä, että toimitilojen tietoturvallisuudesta saadaan päivitetty ohjeistus, joka vastaa muuttuneeseen uhkatilanteeseen sekä toimitilojen ja työtapojen osalta muuttuvaan valtionhallintoon. Tietoturvallisuuteen liittyvät vaatimukset ovat tiukentuneet viimeisten vuosien aikana, sekä kansallisesti että kansainvälisesti, joka edellyttää myös tietoaineistojen käsittelyn ja tietojen käsittelyssä käytettyjen toimitilojen (mukaan lukien tekniset laitetilat) kehittämistä.

Lausunnoilla olevassa ohjeessa esitetään merkittävää muutosta siten, että suojaustaso III ollaan jakamassa kahteen eri kategoriaan toimitilojen suhteen. Toinen näistä soveltuisi suojaustasomerkinnällä olevien tietojen käsittelyyn ja toinen turvallisuusluokitusmerkinnällä olevien tietoaineistojen käsittelyyn vaikka tietoturvallisuusasetuksessa niiden salassa pidettävyys ja mahdollinen vahinko on kuvattu samalle tasolle. Toisena muutoksena ehdotetaan käyttöön otettavaksi turvallisuusvyöhykkeiden määrittelemiseksi uudenlainen värikoodaus, jota ei käsittääksemme ole yleisesti käytetty.

Pidämme näitä ehdotuksia epäloogisina sekä hämmennystä ja merkittäviä kustannuksia aiheuttavana ratkaisuna, etenkin jos ST III taso jaetaan kahteen osaan.

Ehdotamme, että suojaustasot pidetään kuten tähänkin saakka määrittelevänä tekijänä tietoturvallisuusasetusten mukaisesti eikä ST III suojaustasoa jaeta kahtia. Tarvittaessa sellaisten vaatimusten osalta, jotka saattavat aiheuttaa toimitilojen osalta merkittäviä kustannuksia, arvioitaisiin niihin liittyviä riskejä. Riskien pienentämiseksi voitaisiin tehdä lisäkontrolleja sellaisiin toimitiloihin, joissa käsitellään säännöllisesti ST III tietoja. Lisäkontrollivaatimuksissa voitaisiin hyödyntää aiemmista VAHTI-ohjeista tuttua jaottelua: ”pakollinen vaatimus”, ”vahva suositus” ja ”suositus”.

Ohjeeseen tulisi kuvata selkeämmin sekä prosessi riskienarvioinnin suorittamiseksi niihin kohteisiin, joissa sitä tarvitaan, että tiettyjen kohteiden riskienarvioinnin tueksi yleiset huomioitavat tai toimintaa mahdollisesti uhkaavat seikat.

Valtiokonttori
Statskontoret
State Treasury

Sörnäisten rantatie 13, Helsinki | PL 14, 00054 VALTIOKONTTORI
Puh. (09) 77251, Faksi (09) 7725 208, www.valtiokonttori.fi

Ohjeen tehtävänä on myös päivittää vanhentuneet tietoteknisten laitetilojen vaatimukset. Koska vanhempaa ohjetta on sovellettu ja käytetty jo pitkään valtionhallinnon ja sen palvelutoimittajien keskuudessa, tulisi tästä laatia yhteenveto, jossa käydään läpi keskeiset muutokset ja kustannusanalyysi toteuttamisesta mahdollisuuksien mukaan verrattuna vanhempaan ohjeeseen.

Valtiokonttorin huolena on se, että ohjeessa ei ole tehty riittävää kustannusvaikutusanalyysia tulevista pakollisista vaatimuksista toimitiloille. Lisäksi ohjeen jalkautukseen tarvitaan tarkempaa soveltamisohjeistusta, sillä ohje voi pahimmillaan luoda merkittäviä lisäkustannuksia valtionhallinnon toimitilojen saneeraus- ja uudisrakennushankkeisiin.

Yksityiskohtaiset kommentit ohjeesta

1.1 Ohjeen tausta, tarkoitus ja tavoite
Lauseet "Ohje ei ota kantaa työ- tai palo- ja pelastusturvallisuuden erillisratkaisuihin, joista vastuuviranomaiset ohjeistavat erikseen. Nämä ratkaisut on kuitenkin syytä huomioida myös turvallisuusrakentamisessa osana rakenne- ja rakennussuunnittelun perusteita" voisi korvata paremmin kuvaavalla lauseella: Tässä ohjeessa keskitytään toimitilojen tietoturvavaatimuksiin, kun taas mm. henkilö- ja rakenneturvallisuuden vaatimukset määräytyvät eri lakien, määräysten ja ohjeiden nojalla.

Sivulla 6 olevan kuvan merkitys ei kaikille aukea. Tulisi tarkemmin kuvata prosessi, miten organisaation tulisi jalkauttaa ohje omaan toimintaansa.

2.5 ICT-varautumisen vaatimukset (VAHTI 2/2012)
Tietoteknisten ympäristöjen varautumista ja jatkuvuuden hallintaa ohjaamaan laadittu VAHTI-ohje 1/2012 kuvaa erityisesti varautumiseen pohjautuvia vaatimusperusteita eri tietoturvallisuustasojen toteuttamista silmällä pitäen. Lauseessa viitattu ohje on 2/12. Samalla tulee huomioida että, ICT-varautumisessa ei perusteeksi oteta tietoturvatasoja vaan se pohjautuu kohteen tärkeysarviointiin. Sen taustalla voi olla sen yhteiskunnallinen, huoltovarmuuskriittinen tai muu sen merkitys kriittisen infrastruktuurin suojaamisessa.

3.1.1Luokittelu
Samassa yhteydessä tulisi käydä läpi myös suojaustaso-luokittelu tai sitten poistaa tämä kohta kokonaan.

3.1.2 Valtionhallinnon toimitilojen turvallisuusvyöhykejako
"Toimitilassa, jossa muutoin kuin tilapäisesti käsitellään tai säilytetään suojaustasoon III luokiteltuja tietoja, jotka on turvallisuusluokiteltu (TTA 11§) perustuen joko kansalliseen tai kansainväliseen suojaustarpeeseen, tulee täyttää liitteessä 1 esitetyt KELTAISEN vyöhykkeen vaatimukset. "
Todetaan, että selkeämpi jako olisi pelkkä kansallinen vs. kansainvälinen – ei kansallisiin tietoaineistoihin ole enää tarpeen tehdä lisää tasoja eikä siten eroavia käsittelysääntöjä/-tiloja.

Ei koske tällä hetkellä toimittajia, joiden tiloissa on paljon valtionhallinnon tietoa.

3.1.3 Turvallisuusvyöhykkeiden yleiset vaatimukset
Todetaan, että tulee synkronoida Sähkötieto ry:n suuntaan myös valtionhallinnon uudet vyöhykkeet/suojaustasot jne.

Kansallisessa KATAKRI:ssa esitetään huomattavasti – lauseesta tulee ottaa pois sana kansallinen.

Kappale Henkilöiden tunnistus, tulisi avata lukijalle, esimerkiksi mitä tarkoitetaan tunnistamisen lisäksi, esim. sähköisen kulunvalvontaa lokeihin tehdään kirjaukset ja lokitietoja käytetään sovitusti säännöllisesti läpi.

Kappale Hajasäteily; hajasäteilyn vastatoimet voidaan jakaa karkeasti kahteen menetelmään: laitteiden suojaaminen metallikoteloinnilla tai työskentelytilan suojaaminen rakenteellisilla ratkaisuilla (esim. ns. Faradayn häkki). Tavoitteena on, ettei salassa pidettävää tietoa sisältävää sähkömagneettista säteilyä pääse vuotamaan tilasta ulos vaimennusvaatimukset ylittävällä tasolla.

-karkeampi jako olisi laitteen tai tilan TEMPEST-suojauksella esim. metallikoteloinnilla.

- lyhyesti jos eri menetelmiä avaa: standardin täyttävät TEMPEST-suojatut laitteet, olemassa olevien laitteiden sisään laitettavat suojaukset, olemassa olevien laitteiden ulkoinen suojaaminen metallikoteloinnilla, TEMPEST-suojatuilla lisätarvikkeilla tai työskentelytilan suojaamisella rakenteellisilla ratkaisuilla (esim. ns. Faradayn häkki).

3.2 Alueet ja toimitilat
Näillä korvaavilla menettelyillä voidaan joissakin tapauksissa saavuttaa merkittäviä kustannussäästöjä. Todetaan, että käytännössä harvemmin saavutetaan kustannussäästöjä.

3.5 Merkitseminen
Otsikon pitää olla sisältöä kuvaava.

3.6 Etätyo
Lauseessa "Kuljetettaessa luokiteltuja tietoja pääasiallisen.." tulisi luokiteltuja tietoja vaihtaa salassa pidettäviä tietoja. Toisena kohtana tulee asianmukainen salaus määrittää, riittääkö esim. muistitikun oma ohjelmallinen salaus vai vaaditaanko ns. laitetason salaus ja FIPS tai vastaavan hyväksynnän?

4.2 Ulkopinnat
Työmenetelmiä harkittaessa on huomattava, että esimerkiksi oikein raudoitettu valuharkkoseinä antaa paremman suojan, kuin vääriä menetelmiä käyttäen metallilevyllä päällystetty tavanomainen valuharkkoseinä. Ei paras esimerkki, jos jokin väärä menetelmä ei olekaan parempi. Tulisiko antaa enemmän ohjeita työmenetelmien valintaan? Lisäksi tulisi ainakin perustella mihin rakenteiden paremmuuden/vahvuuden järjestys perustuu.

4.5 Ovirakenteet
Ylimpään kappaleeseen tuli lisätä Finanssialan keskusliiton vaatimukset.

4.5.3 Lukitusjärjestelmät
Korotetun ja korkean tason tiloihin (ST III/ST II) johtavat, turvallisuusvyöhykkeiden väliset luukut tai hätäpoistumistiet on varustettava avattavin kalterein ja valvottava rikosilmoittimilla. Suluissa oleva ST III/ST II tulisi poistaa tekstistä, sekä korvata rikosilmoitin rikosilmoitinjärjestelmällä.

5.2 Valvontajärjestelmät
Lauseessa "...vyöhykkeelle ja sieltä ulos voidaan myöhemmin todentaa (järjestelmäloki) ehdotetaan vaihdettavaksi lokitietojen avulla.

Todetaan, että FKL käyttää termiä murtohälytysjärjestelmä. Samalla ehdotetaan kohtaan lisättäväksi myös LVI-järjestelmä osaksi kokonaisuutta.

Huom! Vaatimussetissä kohdassa 33-> käytetään asiasta eri termiä
Vaatimus kohta 34: tunkeutumisen ilmaisinjärjestelmän testaus: Teksti ja vaatimussetti antavat eri ajan testaamissykliin

5.3 Vartiointi
Vartiointihenkilöstö ei käytä turvallisuusluokiteltujen tilojen avaimia muuten kuin poikkeustilanteissa –lauseen selkeämpi muoto olisi tiettyjen turvallisuusvyöhykkeiden tai niiden rajalla olevien ovien kohdalla vain poikkeustilanteissa.

Toisena huomiona avainten säilytys suljetussa kuoressa, missä itse kuorta tullaan säilyttämään.

6 Toimeenpano ja ohjeistaminen
Otetaanko käyttöön uusia rakennuksia suunniteltaessa versus remontointitarpeet ja kustannukset? – tulisi kirjata selkeästi mikä on velvoittavuus tai mahdollinen siirtymäaika.

Perustaso on 1.10.2013, mutta korotettu ja korkea taso riippuvat siitä, milloin organisaatio on tehnyt luokituspäätöksen tietoaineistojen luokittelemisesta tietoturvallisuusasetuksen mukaisesti, mutta tiloille oli 5 vuoden siirtymä tietoturvallisuusasetuksessa.

Kommentit liitteisiin
Liite 1

Korkean riskitason toimintaympäristössä ei sallita lainkaan vakavia poikkeamia. Vakavien poikkeamien korjaamatta jättäminen edellyttää työpisteen johtajan kirjallista ja perusteltua erillispäätöstä. Pisteiden antoperusteet ovat:
- ei työpisteen johtajan vaan organisaation johdon.

Korotettu taso ST III Oranssi ja Korotettu taso TL III Keltainen
- Nämä tulisi yhdistää yhdeksi turvallisuusvyöhykkeeksi ja kontrollien kohdalla jaottelu pakollisiin ja riskien arvioinnin kautta vahvasti suositeltaviin.

3. Aidat*
- voidaanko aitaa käyttää aitaa korvaavana elementtinä?

7. Seinärakenne
- lujuudet tulisi perustua esitettyyn vahvuusjärjestykseen ja arvoihin

9. Salakuuntelun estäminen
kohta 2) Henkilöstölle on koulutettu, että taukopaikoilla (tupakkakopit, lounasravintolat, jne.) ei saa keskustella suojattavista asioista.
- suojattavista asioista sijaan tulisi käyttää termiä "salassa pidettävistä" kaikkialla ohjeistuksessa.

11. Lattia ja kattorakenteet
Olemassa olevissa toimitiloissa: katto-, välipohja- ja lattiarakenne vahvistetaan viranomaisten erillisvaatimusten mukaisesti (esim. erillinen pintavalu lattiassa), mikäli kohteen riskiarviointi tätä edellyttää (seinänaapureiden ja toimintaympäristön arviointi jne.).
- tällaisia riskiarvioinnissa huomioitavia, tiloihin liittyviä ohjeita/mahdollisia riskitekijöitä – näitä tulisi olla useissa muissakin kohdissa, etenkin kaikki ohjeen kohdat joissa on käytetään riskiarviointia.

16. Halliovet tai ajo-ovet, jotka johtavat turvallisuusvyöhykkeen sisään.*
"Palo-oven EI60-tyyppinen vahvennettu läpiajon estävä rakenne. "
EI60-tyyppinen ovi tarkoittaa sitä, että ovi kestää TULIPALOA (ei läpiajoa!) 60 min (E=tiiviys, I=Eristävyys). Ks. http://www.finlex.fi/data/normit/37126-E1_2011-fi.pdf s.5 "paloluokitus".

26. Huoltohenkilöstön pääsynhallinta
Keltainen turvallisuusvyöhyke: Työajan ulkopuolella tapahtuvien huoltokäyntien on kirjauduttava sähköiseen kulunvalvontalokiin.
- tulisi kirjautua (tai olla yhdistetty johonkin lokissa) työaikanakin tapahtuneet.

36. Kameravalvontajärjestelmä
Ehdotetaan että vyöhyke korvataan turvallisuusvyöhyke sanalla.

38. Vartiointi
Vasteajan voi määritellä myös tarkemmin, koska nykyään vartiointipalvelut myydään vasteajan perusteella, mitä pienempi vasteaika, sitä suuremmat kustannukset. Jos SLA ei toteudu, voidaan saada hälytyskäynnit edullisemmin.

Liite 2.1
Rakentamispalvelun turvallisuussopimus sekä 2.2 sekä muut turvallisuussopimusmalli, onko näitä verrattu sisällöllisesti esimerkiksi Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011?

Liite 3.3

Tiedon hallintaprosessi rak hankkeissa v03 solu 7C: ”…tarvittaessa auditoi hankekohtaiset erityisvaatimukset.” Erityisvaatimusten auditointi?

Pääjohtaja Timo Laitinen

Yksikönjohtaja Juha Pietarinen