Jakelussa mainitut

VM:n lausuntopyyntö

Sisäasiainministeriön lausunto koskien teknisen ICT-ympäristön tietoturvataso-ohjetta

Valtiovarainministeriö on pyytänyt sisäasiainministeriön hallinnonalalta lausuntoa teknisen ICT- ympäristön tietoturvataso-ohjeesta.

Yleistä

Tietoturva-asetuksen toimeenpanon tueksi on Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTIn ohjauksessa valmisteltu Teknisen ICT -ympäristön tietoturvataso-ohje ja sen tukimateriaalit.

Yleisesti ottaen luonnosasiakirja kattaa sille asetetut vaatimukset ja on pääosiltaan looginen. Perustelua ja hyvää on myös se, että ohjeessa määritelty keskeiset käsitteet ja annettu ohjeen lukuohjeet. Ohjeen hyvänä puolena mainittakoon vielä liitteissä kuvatut apuvälineet ja työkalut.

Sisäasianministeriö näkemyksen mukaan ohjeen tulisi olla mahdollisuuksien mukaan tiivis, jolloin siitä saadaan eniten konkreettista tukea toiminnalle. Parannusehdotuksena voisi olla joko erillinen peruskäyttäjän ohje tai että nykyiseen ohjeluonnokseen kirjoitettaisiin auki keskeiset ohjeet peruskäyttäjälle. Tulisi myös arvioida voitaisiinko ohjetta jakaa useampaan osaan kuten esimerkiksi tietojärjestelmän luokittelu ja järjestelmille asetettavat yleiset tekniset vaatimukset, jotka saattaisivat olla lukukelpoisemmat eri ohjeissa.

Ohjeesta ei ole kuvattu selkeästi mitä vaatimuksia tulee noudattaa. Ohjeluonnoksessa on runsaasti viittauksia KATAKRIin ja muihin VAHTI –ohjeisiin.

Ohjeeseen pitäisi lisätä määritelmät seuraaville asioille:
- Kansainvälinen tietoturvallisuusvelvoite
- Tietoaineiston selväkielinen käsittely
- SLA - palvelutaso.

Tietoturvavaatimukset tulisi voida suhteuttaa myös arvioituun riskiin. Mikäli riski on korkeampi, noudatettaisiin tiukempaa vaatimusta. Tämä ajattelutapa/ malli mahdollistaa kustannustehokkaamman toiminnan. Tietoturvallisuuden toteuttamissuunnitelmien/ ohjeiden määrittelyssä tulisi huomioida hallinnonalojen virastosten ja laitosten taloudelliset edellytykset toteuttaa tiukkenevia tietoturvavaatimuksia ja huomioitava, että vaatimusten toteuttaminen ei saa vaarantaa operatiivista toimintaa.

Postiosoite:
PL 26
00023 Valtioneuvosto

Käyntiosoitteet:
Kirkkokatu 12
Helsinki
Vuorikatu 20
Helsinki

Puhelin:
Vaihde 071 878 0171
Faksi:
071 878 8555

Virkasähköpostiosoite:
kirjaamo(at)intermin.fi
Sähköpostiosoite:
etunimi.sukunimi(at)intermin.fi
www.intermin.fi

Yksityiskohtaiset havainnot

Asiakirjojen suojaustason on esitelty kahteen kertaan; sivuilla 10 ja 18. Toinen esittely on tarpeeton.

Ohjeluonnoksen sivun 12 kappaleessa 1.2 kuvataan kansainvälisen turvallisuusluokiteltavan tietoaineiston vaatimuksista suhteessa KATAKRIin. Ohjeen rajaukset tulisi tarkistaa voimassa olevan lainsäädännön mukaiseksi erityisesti kansallisen turvallisuusluokitellun tietoaineiston osalta.

Sivun 14 kappale 2.1 asetuksen vaatimusten konkretisointi on erittäin tarpeellinen ja hyvä osa ohjetta. Sisäasiainministeriö ehdottaa kuitenkin seuraavaa tarkennusta kappaleeseen.

- Kohta 3 asiakirjojen käsittelyä koskevat tehtävät ja vastuiden määrittelyssä lienee erittäin keskeistä, jopa luokitteluakin keskeisempää asiakirjahallinnon, diaarin ja tiedonohjaussuunnitelman määrittely.

Sivulla 15. Kohdan 2.1 alakohta 5. ”Mikäli tietoaineisto turvallisuusluokitellaan tietoturvallisuusasetuksen 11 §:n mukaisesti, kohdistuu siihen tällöin pelkillä suojaustasomerkinnöillä varustettuja kansallisia tietoaineistoja tiukemmat käsittelyvaatimukset”. Samoin myöhemminkin ohjeessa mainitaan, että turvallisuusluokitusmerkinnän sisältävän tietoaineiston suojausvaatimukset olisivat kovemmat kuin vastaavan suojaustasovaatimuksen omaavilla asiakirjoilla.

- Kansallisten turvallisuusluokitusmerkinnän omaaville tietoaineistojen tiukemmille käsittelyvaatimuksille ei löydy perustetta lainsäädännöstä. Kansainvälisen tietoturvallisuusvelvoitteen perusteella saattaa joissain tapauksessa olla tiukemmat käsittelyvaatimukset, jotka perustuvat Suomen ja toisen valtion tekemään turvallisuussopimukseen. Edellä mainittuun perustuen KATAKRIn velvoittavuus turvallisuusluokiteltuja asiakirjoja sisältävän tietojärjestelmän arviointien suhteen ei ole tältä osin selkeä.

- Kysymyksenä myös: Onko kansainvälistä tietoturvallisuusnormistoa noudattava, myös silloin kun on tietojärjestelmissä suoria integraatioita esim. Schengen järjestelmiin?

Sivun 18 viimeisessä kappaleessa on käsitelty tietoaineistojen luokittelemista. Tässä yhteydessä tulisi nostaa korostetusti esille se, että vaatimus suojaustasoluokittelusta koskee kaikkea salassa pidettävää tietoaineistoa eikä vain turvallisuusluokiteltavaa aineistoa. Selvyyden vuoksi kappaleen loppuun asti jatkuvan kohdan, joka alkaa ”Osaan salassa pidettävistä asiakirjoista voidaan tehdä…” voisi siirtää seuraavalle sivulle suojaustasoerittelyn jälkeen omaksi kappaleekseen.

Päätelaitteet ja niitä koskevat vaatimukset oli järkevästi otettu esille yhtenä kokonaisuutena eikä puhuta enää erikseen erityyppisistä päätelaitteista.

Merkittävä muutos aikaisempien ohjeiden malliin on se, että palvelimilta vaaditaan samoja asioita kun päätelaitteilta lisättynä palvelimien erityisvaatimuksilla.

Päätelaitteiden osalta on otettu selkeästi esille vaatimus peruskomponenttien tietoturvallisuuden ylläpidosta päivittämällä komponentit ja asettamalla pakotetusti asetuksia päälle.

Edellä mainitussa kokonaisuudessa puuttui kuitenkin maininnat kokonaisista tietojärjestelmistä. Jos työaseman peruskomponentit kuten Adobe Reader ylläpidetään uusimmassa versiossa, se vaatii tietojärjestelmien päivittämistä siten, että ne tukevat uusimpia Adoben versioita. Tähän toivoisimme, siis lisäystä vaatimuksena tietojärjestelmien ylläpitoon. Lisäksi huomiona se, että mainintaa yleisen turvallisuustilanteen seurannasta ei ohjeluonnoksessa ole, mikä mielestämme olisi hyvä lisäys. Esim. Cert.fi tiedotteiden seurannan vastuutus organisaatiossa.

Luonnoksen mukaan työasema voi olla liitettynä alemman turvallisuustason ratkaisuun hyväksytyn yhdyskäytävän välityksellä. KATAKRIssa puhutaan datadiodista eli yksisuuntaisesta tietoliikenteestä. Yksisuuntainen tietoliikenne on lähinnä sovellus-sovellustason yhdyskäytävä. Mutta toisaalta on kuva, jossa päätelaitteella saa olla suorayhteys ST IV ja ST III tason tietojärjestelmään?

Pääteistunto tai VDI pohjaisten työasemien toteuttamisessa haasteeksi tulee tietojärjestelmän käytön lokittaminen, kuka käyttää mitä käyttää jne. Tämä vaatisi käyttäjäpohjaisen palomuuriratkaisun (SSLVPN) toteuttamista pääteistunto tai VDI laitteesta tietojärjestelmään, jotta voidaan eriyttää se, ketkä pääsevät järjestelmään ja ketkä ei. Muutoinhan päätepalvelimella tai VDI laitteella on sama osoite riippumatta siitä kuka sitä käyttää. Huomioitakoon myös, että ensimmäiset pääteistuntojen välityksellä tarttuvat virukset on jo julkaistu.

Tietojärjestelmien hankinnan ja asiakkaille toimitettavien sisäisten palveluiden osalta voidaan ottaa esille tärkeä huomioitava asia palveluiden tuottamisen kannalta. Eli näiden vaatimusten mukaan palveluntuottajan pitää pystyä toteuttamaan asiakkaille seuraavanlainen raportointi, jonka toteuttaminen vaatii sopimuksia ja resursointia:

- Perustasolla organisaation tulee saada vähintään neljännesvuosittainen raportti.
- Korotetulla tietoturvatasolla kuukausittainen raportti toimittajalta hankittujen tietoturvallisuuteen liittyvien palveluiden toiminnasta ja poikkeamista.
- Kriittisistä poikkeamista tai muista uhkatilanteista raportointi pitää olla sovittuna, pääsääntöisesti näistä tulee tapahtua yhteydenotto välittömästi, vaikka organisaatiolla ei olisikaan kykyä tai tarvetta itse ryhtyä toimenpiteisiin. Organisaation tulee kuitenkin saada välittömästi tieto tapahtuman ajankohdasta ja sen perusteella liikkeelle laitetuista toimenpiteistä.

Sivulla 22 organisaation tietoturvallisuuden hallinta ja tietojenkäsittely-ympäristöt luokitellaan kolmeen tietoturvatasoon; tietoturvallisuuden perustaso, korotettu taso ja korkea taso. Alin valtionhallinnon viranomaisille sallittu taso on tietoturvallisuuden perustaso. Tämän toteuttavassa

ympäristössä voidaan käsitellä suojaustason IV edellyttävää tietoaineistoa selväkielisessä muodossa toimivaltaa käyttävän viranomaisen päätöksellä. Korotetun tietoturvallisuustason ympäristössä voidaan vastaavasti käsitellä tietoa selväkielisessä muodossa aina suojaustasoon III asti ja korkean tietoturvallisuustason täyttävissä ympäristöissä suojaustasoon II ja I asti.

- Antaako tämä mahdollisuuden olla salaamatta tietokantoja esimerkiksi TUVE:ssa? Sama mahdollisuus toistuu sivuilla 24 - 25, 33 ja 63. Jos näitä mahdollisuuksia puolestaan verrataan viitedokumentteihin, niin mikä on tulkinta?, koska mm. Katakri edellyttää salausta tietyllä tasolla.

Sivulla 27 olevaan kuvaan nro:11 tulisi lisätä www -selain, koska se on käytännössä keskeinen tunkeutumisreitti ja osa viestintäpalveluita.

Ohjeluonnoksen sivulla 29 on kuvattu kahden erillisen teknisen ympäristön rakentaminen. Mainittu ratkaisu vaatii usein merkittäviä rahallisia lisäresursseja, joten käytännössä sen toteuttaminen ei läheskään aina tiukan taloudellisen tilanteen vuoksi ole mahdollista, vaikka tietoturvallisuuteen liittyvät seikat tätä edellyttäisivät. Lisäksi kuvaa olisi perusteltua tarkentaa siten, että samalla työasemalla ei voida liikkua molemmissa ympäristöissä ilman, että erotetaan ympäristöt työasemassa esimerkiksi eri käyttäjätunnuksilla.

Sivulla 35 kohdassa ”Esimerkkejä tietoliikenneyhteyteen liittyvistä teknisistä ratkaisuista…” on mainittu ”tarvittava lokitus ja hälytysten tuottaminen sekä niihin reagoiminen”. Tässä yhteydessä olisi tärkeää ilmaista, että lokiin tulee kirjata nimenomaan onnistuneet yhteydet eikä ainoastaan palomuurin estämiä yhteyksiä. Tietoturvapoikkeamat syntyvät erityisesti onnistuneista tunkeutumisista, joten juuri niiden tulee kirjautua lokiin.

Sivun 36 kohtaan ”Esimerkkejä palvelinympäristöön liittyvistä teknisistä ratkaisuista…” olisi perusteltua lisätä kaksi kohtaa:

- Viranomaisen tiedon suojaaminen pääkäyttäjäoikeuksin toimivilta (ulkoistetuilta) ylläpitäjiltä silloin, kun se on käytännössä mahdollista esimerkiksi tietokannan sisällön salakirjoittamisella.

- Lokitiedon siirtäminen automaattisesti palvelimen ulkopuolelle keskitettyyn ja suojattuun lokipalvelimeen.

Sivulle 51 kohtaan ”3. Dedikoitu ympäristö - toimittajan ylläpitämä ympäristö - palvelu tuotetaan Suomesta” tulisi huomioitavien seikkojen listaan lisätä seuraavat kohdat:

- Ulkoistava organisaatio saattaa menettää oikeuden käsitellä lokitietoa tietoturvapoikkeaman selvittämiseksi. Ellei muuta sovita, palveluntarjoaja saattaa myös laskuttaa lokitiedon käsittelystä asiantuntijapalkkion.

- Uuden pakkokeinolain voimaantullessa ei ulkoistavalla organisaatiolla, ulkoistetun palvelun tarjoajalla eikä esitutkintaviranomaisella ole lähtökohtaisesti oikeutta selvittää lokitiedoista ulkoistetun palveluntarjoajan työntekijän tekemää salassa pidettävän viranomaistiedon päätymistä oikeudettomasti ulkopuolisille.

Sivulle 52 huomioitaviin seikkoihin tulisi lisätä maininta siitä, että henkilötietoja ei saa siirtää ETA -alueen ulkopuolelle prosessia tarkastamatta ja ettei suomalaisten viranomaisten toimivalta ulotu Suomen rajojen ulkopuolelle.

Sivulla 54 puhutaan julkiseen lähteeseen (FB, Twitter) tallennettavasta materiaalista.

- Mitä merkitystä on vaikka tieto siirrettäisiinkin suojaamattomalla yhteydellä? Materiaali on joka tapauksessa julkisesti saatavilla.

Ohjeen sivulla 64 oleviin vaatimuksiin tulisi lisätä lokien käsittelyoikeuden toteuttaminen siten, ettei palveluntarjoajalla ole oikeutta pyytää palkkiota jokaisesta lokitietoihin liittyvästä käsittelytoimenpiteestä.

Liitteet

Liite 1. Salassa pidettävien asiakirjojen ja tietojen käsittelyvaatimukset:

- Liitteessä on erittäin suuri määrä vaatimuksia, joiden toteuttaminen kirjaimellisesti on erittäin haastavaa/ aiheuttaa valtavasti työtä ja vaatii lisää henkilöresursseja. Pitäisi arvioida ovatko kaikki vaatimukset järkeviä suhteessa edellytettävään työmäärään.

- ”Organisaation kulunvalvontajärjestelmä tallentaa lokitustietoa kuka ja milloin on käsitellyt salassa pidettävää tietoa”: Kyseinen vaatimus on mahdoton toteuttaa. Kulunvalvontajärjestelmällä ei pysty hoitamaan tällaisia asioita.

- Salassa pidettävän tietoaineiston tilojen tulee sisältää automaattinen hälytysjärjestelmä luvattomien tunkeutumiskeinojen yritysten tunnistamiseen: Tarpeettoman kova vaatimus, etenkin jos tietoaineistot säilytetään kassakaapissa. Pitäisi perustua riskiarvioon.

- Kohdan 4.4 vaatimuksilla ei ole perusteita. (leimasinten säilyttäminen, käyttöön erikseen oikeutettavat henkilöt, leimasimessa päivämäärä ja leimasimessa hologrammit yms.)

Liitteet 2 ja 3. TTT Tietoturvallisuuden ja tietojärjestelmien hallinnan vaatimukset:
- Vaatimukset päällekkäisiä tietoturvatasovaatimuksia kanssa.
- Sarakkeessa ”kriittisyys” olevat luokittelut eivät ole yhtenäisiä ”JHS 174 ICT-palvelujen palvelutasoluokitus”-suosituksen kanssa.

Liite 4. Suojattavien kohteiden tärkeysluokittelija, ei huomautettavaa.

Liite 5. Järjestelmien väliset riippuvuudet:
- Taulukossa viittausvirheitä. Ei toimi kuvatulla tavalla, eli ei näytä ongelmien värikoodeja.

Liite 6. Palveluiden tuottamisen valinta:
- Ohjeista ei selvinnyt miten taulukkoa tulisi käyttää. Käyttäminen edellyttää lisäohjeistusta.

Liite 7. Etäkäytön tekniset vaatimukset:
- Kohta 1.2. loogisuus puuttuu, sillä korkealla tasolla löysemmät vaatimukset kuin korotetulla tasolla.
- Kohta 3.8. ei avaudu. Miksi kohdassa ”korkea taso” on Ei?

Tietohallintojohtaja Kaarlo Korvola

Tietoturvapäällikkö Mika Kuronen

Asiakirja on sähköisesti allekirjoitettu asiankäsittelyjärjestelmässä. Sisäasiainministeriö SM 30.01.2012 klo 08.57. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Jakelu Valtiovarainministeriö

Tiedoksi Kansliapäällikkö Ritva Viljanen, hallinnonalan virastot