28.10.2015

Ohje arviointikriteeristöjen tulkinnasta

Kansalliset arvioinnit

1 Arviointikriteeristöt

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (Tietojärjestelmien tarkastuslaki 1406/2011) 3 §:n mukaan:

"*Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain tässä laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) mukaan.*"

Kansallista salassa pidettävää tietoa käsittelevien tietojärjestelmien viranomaisarvioinneissa voi arviointikriteeristönä käyttää Katakria (Tietoturvallisuuden auditointityökalu viranomaisille, 2015), VAHTI:a (valtiovarainministeriön tietoturvallisuutta koskevat ohjeet) tai molempia. Viestintävirasto suosittelee kansallista salassa pidettävää tietoa käsittelevien järjestelmien arviointikriteeristöksi Katakria.

Käytännön tasolla vaatimustasoeroa ei VAHTI:n ja Katakrin välillä ole, vaan eroavaisuus ilmenee lähinnä esitystavassa. Katakri on yksi kokonaisuus, jossa kaikki vaatimukset sisältyvät samaan dokumenttiin. VAHTI-ohjeet on annettu eri aikoina erillisissä julkaisuissa, joita on kertynyt useita. Sekä Katakria että VAHTI:a tulkitaan yksittäisten vaatimusten[1] osalta eroavasti riippuen siitä, onko kyse kansallisen turvallisuusluokitellun (JulkL 24 §:n 1 momentin 2 ja 7–10 kohdat) vai muun salassa pidettävän tiedon suojaamisesta.

2 Tietoturvallisuuden arviointi VAHTI-ohjeiden mukaan - Viestintäviraston tulkintalinja

Tässä luvussa selvitetään, kuinka Viestintävirasto tulkitsee käsitettä "tietoturvallisuuden arviointi VAHTI-ohjeiden mukaan".

VAHTI 2/2014 (Tietoturvallisuuden arviointiohje) kuvaa tietoturvallisuuden arvioinnista seuraavaa:

"*Tietoturvaturvallisuusasetuksen 4 §:ssä säädetään kymmenen vaatimusta tietoturvallisuuden perustasolle. Näitä vaatimuksia täsmentää ja täydentää VAHTI-ohje 2/2010, jossa tietoturvatasojen kaikkien kolmen tason vaatimukset on kuvattu yksityiskohtaisesti. Nämä vaatimukset kohdistuvat*

[1] Turvallisuusluokitellun ja muun salassa pidettävän tiedon suojausvaatimusten tulkinnat eroavat salauksen ja tietojen fyysisen suojaamisen osalta.

menettelytapoihin ja prosesseihin eikä niiden perusteella voida tehdä päätöksiä teknisistä yksityiskohdista ja ratkaisuista, joiden avulla tasovaatimukset voidaan täyttää. Tämän seikan korjaamiseksi tietoturvatasot on huomioitu kaikissa asetuksen voimaantulon jälkeen julkaistuissa VAHTI-ohjeissa, joissa annetaan vaatimuksia ja suosituksia eri tietoturvatasoilla sovellettavista ratkaisuista.

Tietoturvatasovaatimuksia toteutettaessa ja arvioitaessa on huomioitava VAHTI 2/2010 -ohjeen lisäksi erityisesti seuraavat ohjeet:
VAHTI 3/2010 Sisäverkko-ohje
VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje
VAHTI 3/2012 Teknisen ympäristön tietoturvataso-ohje
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje
VAHTI 2/2013 Toimitilojen tietoturvaohje
VAHTI 4/2013 Henkilöstön tietoturvaohje
VAHTI 5/2013 Päätelaitteiden tietoturvaohje".

Viestintävirasto soveltaa edellä mainittua ohjeistusta nykytilassa siten, että **VAHTI-kriteeristöä vasten arvioitaessa arviointi kattaa VAHTI-ohjeissa 2/2010, 3/2010, 3/2012, 1/2013, 2/2013 ja 5/2013 kuvatut vaatimukset soveltuvin osin.** Tilanteissa, joissa vaatimukset ovat keskenään ristiriitaisia, tulkitaan vaatimusten täyttämisen olevan mahdollista siten, että tiukin vaatimus täyttyy[2].

3 Esimerkkejä Katakri- ja VAHTI-kriteeristöjen soveltamisesta

Tässä luvussa kuvataan esimerkkejä eri suojaustasojen vaatimuskehikoista Katakri- ja VAHTI-kriteeristöissä. Viittaukset kohdistuvat Katakrin vuoden 2015 versioon, ellei erikseen toisin mainita. Luvussa kuvataan myös joitain yleisiä tulkintakäytäntöjä sekä niiden perusteita.

3.1 Verkon rakenne

Vaatimus	Lähde	Suojaus-tasot
"*Organisaatiossa on tunnistettu ja eriytetty tietoverkon eri suojaustasoa vaativat osat ja eri suojaustason verkkojen välistä liikennettä rajoitetaan ja suodatetaan.*"	VAHTI 2/2010	IV-II
"*Verkko on suunniteltu ja rakennettu siten, että se tukee tiedon suojaamista tiedon luokittelun mukaisesti siten, että kriittisemmät tiedot on suojattu paremmin.*"	VAHTI 3/2010	IV-II
Mikäli korkeamman tietoturvatason päätelaitteella halutaan käyttää alemman tietoturvatason järjestelmiä, tulee käytön riskejä arvioida, ja käyttö tapahtua yhdyskäytäväratkaisun kautta. (vertaa KATAKRI, ks. erityisesti I 401.0[3])."	VAHTI 5/2013	IV-II
"*Tietojenkäsittely-ympäristön kytkeminen muiden*	Katakri	IV

[2] Esimerkiksi kilpailutuksiin voidaan laatia myös oma järjestelmäkohtainen vaatimusmäärittely. Järjestelmäkohtaisissa vaatimusmäärittelyissä asetetaan usein VAHTI-vaatimuksia tiukempia vaatimuksia niiltä osin, kuin ne ovat järjestelmän toiminnallisten tarpeiden näkökulmasta perusteltuja.
[3] KATAKRI:n II-version vaatimus I 401.0 on Katakrin vuoden 2015 versiossa vaatimus I 01.

suojaustasojen ympäristöihin edellyttää vähintään palomuuriratkaisun käyttöä."	/ I 01	
"Tietojenkäsittely-ympäristön kytkeminen muiden suojaustasojen ympäristöihin edellyttää viranomaisen ko. suojaustasolle hyväksymän yhdyskäytäväratkaisun käyttöä."	Katakri / I 01	III-II

3.2 Etäkäyttö

Vaatimus	Lähde	Suojaus-tasot
"Etäkäyttö työnantajan tähän käyttöön antamilla välineillä ja yhteydellä edellyttäen, että käyttöympäristö täyttää tiedon suojaukselle asetetut vaatimukset: sallittu suojattua yhteyttä käyttäen, käyttäjän vahva todentaminen."	VAHTI 2/2010	IV-II
"Käyttäjä käsittelee tietoa vain sellaisissa fyysisissä tiloissa, jotka vastaavat käsiteltävän tietoaineiston vaatimuksia."	VAHTI 3/2012	IV-II
"Huomioitava, että esimerkiksi ST III tietoaineistojen käsittely edellyttää sitä, että myös käytettävät fyysiset tilat täyttävät ST III-tason käsittelyn edellytykset."	VAHTI 3/2012	III
"Turvallisuusluokitellun tiedon osalta etäkäyttö soveltuu lähinnä IV-tasolle, sillä ST III (LUOTTAMUKSELLINEN) -tason aineiston käsittely edellyttää aina viranomaisen hyväksymää fyysisesti suojattua tilaa, tai tietyissä erityistapauksissa korvaavia suojausmenetelmiä (esim. tietyt poliisioperaatiot). Kansallisten tietoaineistojen osalta etäkäyttö on mahdollista toteuttaa ST III-tietoaineistoja käsitteleviin järjestelmiin esimerkiksi henkilön kotoa tai muusta sovitusta, turvallisesta fyysisestä sijainnista."	VAHTI 3/2012	IV-III
"Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle."	VAHTI 3/2010	IV-II
"Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja."	VAHTI 3/2010	IV-II
"Tietojen välitys ja käsittely fyysisesti suojattujen alueiden välillä on mahdollista vain viranomaisen ko. suojaustasolle hyväksymien korvaavien menettelyjen mukaisesti."	Katakri / I 22	IV-II
"Järjestelmien etäkäyttö-/-hallintaratkaisu edellyttää viranomaisen ko. suojaustasolle hyväksymää liikenteen salausta."	Katakri / I 22	IV-II
"Järjestelmien etäkäyttö/-hallinta rajataan viranomaisen hyväksymälle fyysisesti suojatulle alueelle."[4]	Katakri / I 22	III-II

[4] Muun kuin turvallisuusluokitellun suojaustason III aineiston etäkäyttö/-hallinta on mahdollista toteuttaa esimerkiksi henkilön kotoa tai muusta ennalta määritellystä fyysisestä sijainnista riskienarvioinnissa määriteltyjen korvaavien suojausten tukemana.

3.3 Liikenteen salaus

Vaatimus	Lähde	Suojaus-tasot
"Kansallisen ja kansainvälisen turvallisuusluokitellun tiedon siirrossa käytetään salausta aina, kun verkko menee viranomaisen valvoman tilan ulkopuolelle."[5]	VAHTI 3/2010	IV-II
"Salaukseen tulee käyttää vähintään siirrettävän aineiston suojaustasolle hyväksyttyjä salausratkaisuja."	VAHTI 3/2010	IV-II
"Kun salassa pidettävää aineistoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolella, aineisto/liikenne salataan viranomaisen ko. suojaustasolle hyväksymällä menetelmällä."	Katakri / I 15	IV-II

3.4 Yleisiä tulkintakäytäntöjä

3.4.1 Suojaustasojen eriyttäminen ja yhdyskäytäväratkaisut

Internet-palvelujen[6] käytön sallivat ympäristöt ovat haavoittuvia nykypäivän yleisiä hyökkäysmenetelmiä vastaan. Ympäristöjen riskitasoa voidaan laskea käyttämällä useita eri suojauksia[7], mutta edes suojausten yhdistelmillä ei saavuteta kovinkaan luotettavaa suojausta nykypäivän hyökkäysmenetelmiä vastaan.

Nykypäivän hyökkäysmenetelmien käyttö ei edellytä syvällistä osaamista tai merkittäviä resursseja. Esimerkiksi työasemaan suunnatun, sähköpostin ja/tai web-selaimen kautta tapahtuvan hyökkäyksen onnistuneeseen toteuttamiseen tarvittavat menetelmät ovat kotikäyttäjän resursseilla saatavilla.

Viranomaisen salassa pidettävää tietoa käsittelevien tietojärjestelmien suojausten arvioinnissa tulee huomioida järjestelmäkohtaisesti arvioitu riskitaso sekä vaatimuskriteeristöissä kuvatut yleiset suojausvaatimukset. Esimerkiksi suojaustason IV tietoa käsittelevien ympäristöjen riskienhallinnassa voi olla perusteltua hyväksyä Internet-palvelujen käyttö.

Toisaalta suojaustason III tietoa käsittelevän järjestelmän kytkemistä matalamman suojaustason ympäristöön ei yleensä nähdä riskienhallinnallisesti perustelluksi ilman hyväksyttyä yhdyskäytäväratkaisua[8]. Poikkeuksina ympäristöt, joissa aiheutuu luottamuksellisuuden menetystä suurempi riski (tyypillisesti ihmishenkien menetys), jos tietoa ei saada välitettyä järjestelmään/järjestelmästä

[5] Vaatimusta sovelletaan muulle salassa pidettävälle tiedolle siten, että salaukselle ei edellytetä turvallisuusluokitellulle tiedolle vastaavia vahvuuksia.
[6] Internet-palveluilla tarkoitetaan tässä web-selailua, sähköpostia, ja vastaavia Internet-verkkoa käyttäviä palveluja.
[7] Yleisesti käytettyjä suojauksia ovat muun muassa palomuuraus, järjestelmäkovennus, päivitysmenettelyt, haittaohjelmantorjuntaohjelmistojen käyttö sekä esimerkiksi web-liikenteen suodatus välityspalvelimen (proxy) avulla.
[8] Hyväksyttävien yhdyskäytäväratkaisujen suunnitteluperiaatteita ja yleisiä toteutustapoja on kuvattu yksityiskohtaisemmin Viestintäviraston yhdyskäytäväratkaisuohjeessa. URL: https://www.viestintavirasto.fi/attachments/Yhdyskaytavaratkaisuohje.pdf.

nopeasti. Tällaisia järjestelmiä ovat esimerkiksi tietyt pelastustoimeen liittyvät erityisjärjestelmät.

3.4.2 Etäkäyttö/-hallinta ja salaus

Etäkäytöllä/-hallinnalla tarkoitetaan perinteisessä merkityksessään organisaation toimitilojen ulkopuolelta tapahtuvaa tietojärjestelmien käyttöä/hallintaa tätä tarkoitusta varten hankitulla päätelaitteella. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone.

Turvallisuusluokitellun tiedon osalta etäkäyttö/-hallinta soveltuu perinteisessä merkityksessään vain suojaustasolle IV. Suojaustasolta III lähtien turvallisuusluokitellun aineiston käsittely edellyttää viranomaisen hyväksymää fyysisesti suojattua aluetta/tilaa, ellei viranomainen ole hyväksynyt korvaavia menettelyjä, joilla saavutetaan vastaavat fyysisen turvallisuuden olosuhteet (esimerkiksi tietyissä viranomaisoperaatioissa). Muun kuin turvallisuusluokitellun suojaustason III aineiston etäkäyttö/-hallinta on mahdollista toteuttaa esimerkiksi henkilön kotoa tai muusta ennalta määritellystä fyysisestä sijainnista riskienarvioinnissa määriteltyjen korvaavien suojausten tukemana.

Käyttäjätunnistus ja -todennus tulee toteuttaa riskeihin nähden riittävän vahvalla menetelmällä. Suojaustasosta IV lähtien etäkäytössä/-hallinnassa riittävän vahvaksi menetelmäksi tulkitaan vähintään kahteen tekijään perustuva, niin sanottu vahva käyttäjätunnistus. Etäkäyttöön/-hallintaan tulee käyttää vain hyväksyttyjä laitteita ja etäyhteyksiä. Suojaustasosta III lähtien edellytetään lisäksi käytön teknistä sitomista hyväksyttyyn etäkäyttölaitteistoon (esimerkiksi laitetunnistus).

Hallintayhteyksien suojaus on eräs kriittisimmistä tietojärjestelmien turvallisuuteen vaikuttavista tekijöistä. Erityisesti suojaustason IV järjestelmiä voi kuitenkin olla perusteltua pystyä hallinnoimaan myös fyysisesti suojattujen alueiden ulkopuolelta. Tilanteissa, joissa etähallinta nähdään perustelluksi, suositellaan se suojattavan etäkäyttöä kattavammilla turvatoimilla. Esimerkiksi suojaustason IV järjestelmän etähallintayhteydet voidaan rajata yksittäisiin fyysisiin ja loogisiin pisteisiin.

Etäkäyttö/-hallinta on mahdollista toteuttaa tiivistetysti seuraavankaltaisella rakenteella: Ko. suojaustason työasema - ko. suojaustason liikennesalaus - ko. suojaustason järjestelmä. Siten esimerkiksi suojaustason IV tietoa sisältävää järjestelmää voi olla perusteltua etäkäyttää/-hallita suojaustason IV työasemalta suojaustason IV liikennesalauksen suojaamana. Vastaavasti ei-turvaluokiteltua suojaustason III tietoa sisältävää järjestelmää voi olla perusteltua etäkäyttää/-hallita suojaustason III työasemalta suojaustason III liikennesalauksen suojaamana. Turvaluokitellulle suojaustason III tiedolle on lisävaatimuksena hyväksytty fyysisesti suojattu alue, ei-turvaluokitellun osalta hyväksyntäprosessissa on enemmän liikkumavaraa riskienarvioinnissa määriteltyjen korvaavien suojausten kautta.

Jotta kunkin suojaustason tieto saisi yleisiin riskeihin nähden riittävän suojauksen, ylemmän suojaustason järjestelmän etäkäyttöä/-hallintaa ei tule sallia matalamman suojaustason päätelaitteelta käsin. Siten esimerkiksi suojaustason III tietoa käsittelevän järjestelmän etähallintaa suojaustason IV työasemalta ei tule sallia, ellei käytössä ole hyväksyttyä

yhdyskäytäväratkaisua, jolla estetään suojaustason III tiedon kulkeutuminen matalamman suojaustason ympäristöön.

3.5 Yhteenveto ja suositukset

Internet-palvelujen käytön sallivien ympäristöjen suojaukset on ohitettavissa ilman syvällistä osaamista tai merkittäviä resursseja. Viestintäviraston näkemyksen mukaan viranomaisten salassa pidettäviä tietoa käsittelevät ympäristöt tulee eriyttää Internet-palveluista. Erityisesti suojaustason III ja sitä korkeammalle luokiteltujen tietojen käsittely-ympäristöt tulee eriyttää muiden suojaustasojen ympäristöistä hyväksytyillä yhdyskäytäväratkaisuilla tai fyysisen tason erottelulla.

Etäkäyttö ja -hallinta tulee toteuttaa vastaavia periaatteita noudattaen. Lisäksi tulee varmistua erityisesti siitä, että ketju etäkäytön/-hallinnan päätelaitteelta kohdejärjestelmään asti on suojattu kyseisen suojaustason mukaisesti.

Viestintävirasto suosittelee organisaatioita myös pohtimaan, minkä tasoisen tiedon vuotaminen on organisaation riskienhallinnassa hyväksyttävissä, sekä kuinka todennäköiseksi kyseisen uhkan realisoituminen arvioidaan. Viestintävirasto suosittelee myös varmistumaan tiedon luokittelun tarkoituksenmukaisuudesta ennen suojausmenetelmien yksityiskohtaista suunnittelua ja toteutusta.