CSC-Tieteen tietotekniikan keskus Oy

Lausunto

19.04.2022

Asia: VN/10182/2022

Tiedonhallintalautakunnan suositus julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri), kommentointipyyntö

Julkri-suositus

Voit kommentoida tähän Julkri-suositus dokumenttia.
Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi suosituksen sivunumerolla.

CSC kiittää mahdollisuudesta lausua tiedonhallintalautakunnan suosituksesta julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri). CSC –

Tieteen tietotekniikan keskus Oy on Suomen valtion ja korkeakoulujen omistama erityistehtäväyhtiö. Palvelemme laajasti koko yhteiskuntaa tuottamalla teknologiapalveluja ja -ratkaisuja TKI-toiminnalle, koulutukselle, kulttuurille ja julkishallinnolle.

Kriteeristö (Liite 1A ja 1B)

Yleiset kommentit kriteereistä
Seuraavassa voit antaa yleisiä kommentteja kriteeristöön. Tulevissa kohdissa pyydämme kommentteja osa-alueisiin erikseen.

Kriteeristö on kauan toivottu ja odotettu ohjeistus henkilötietojen sekä ei-turvallisuusluokiteltujen tietojen suojaamiseen. Kriteeristön rakenne on selkeä ja johdonmukainen suhteessa esim. Katkari 2020 –kriteeristöön. Kriteeristö niveltyy myös hyvin tunnettuihin kansainvälisiin tietoturvanormeihin, esim. ISO 27001. Lisäksi Katakri-kriteeristön liittyvät panostuksen on hyödynnetty normistossa hyvin.

Mielestämme kriteeristön roolia ja tarkoitusta tulisi määritellä selkeämmin. Normisto tulisi ennen kaikkea olla suostus vaatimusmäärittelyksi.

Mikäli vaatimusmäärittelyä ei ole tehty tai sovittu, on epäjohdonmukaista soveltaa arviontikriteeristöjä.

Mielestämme on merkittävä puute, että Julkri ei ota kantaa harkinnanvaraisesti annettaviin tietoihin. Suurin osa suojattavasta tiedosta kuulu kuitenkin tähän kategoriaan. Toinen puute on, että normisto ei tunnista toimittajien ei-turvallisuusluokiteltujen sisäisten ja luottamuksellisten tietojen suojaamistarpeita. Näitä tietoja ovat mm. liikesalaisuudet, yrityksen kriittinen infrastrukturi sekä toimittajien toisten asiakkaiden tiedot.

Normisto asettaa myös selkeät käytännön vaatimus- ja arviointikriteerit henkilötietoja ja erityisiä henkilötietoja aineistoja sisältäville palveluille.

Julkri-kriteeristön 1A rakenne on selkeä mutta yksittäisten vaatimusten lukumäärä on massiivinen, verrattuna olemassaoleviin kansainvälisiin normistoihin. Esimerkiksi Iso 27001 standardissa on vain 114 pakollista vaatimusta. Toisaalta vaatimuksissa on selkeää jatkumoa jo VAHTI-ohjeista lähtien.

Liite 1B:ssä on mielestämme lueteltu selkeästi henkilötietojen suojaamiseen liittyvät organisaation velvoitteet.

Kommentit hallinnollisen turvallisuuden osa-alueeseen - Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi kriteerin tunnisteella.
Voit arvioida kriteerien ymmärrettävyyttä, kriteerien luokittelun tasojen sopivuutta sekä mahdollisia puutteita kriteeristössä tai voiko jonkun kriteerin jättää tarpeettomana pois?

Hallinnollisen turvallisuuden määrittelyt perustuvat tunnetuihin kansainvälisiin tietoturvanormeihin ja käytäntöihin. Kotimaisilla pienyrityksillä tulee kuitenkin olemaan vaikeuksia toteuttaa k.o. vaatimuksia. Kritteeristö tulee ohjaamaan hankintoja isommille ja kansainvälisille toimittajille.

Vaatimuksessa todettu kohteiden merkitseminen ei ole mielekästä, jos tietovälineet ovat massamuisteja tai tallennusalustoja.

Kommentit fyysisen turvallisuuden osa-alueeseen - Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi kriteerin tunnisteella.
Voit arvioida kriteerien ymmärrettävyyttä, kriteerien luokittelun tasojen sopivuutta sekä mahdollisia puutteita kriteeristössä tai voiko jonkun kriteerin jättää tarpeettomana pois?

On epäselvää, miten kriteeristö tulee soveltaa ei-turvallisuusluokiteluihin tietoihin ja tiloihin. Esim. Tempest-suojauksen soveltaminen on kaukaa haettu vaatimus useimmille toimittajille ja virastoille.

FYY-11 Tietojen fyysinen tuhoaminen: fyysisen tuhoamisen rinnalle pitäisi myös hyväksyä digitaalisille tallennusvälineille TL-IV luokkaan asti riittävän sertifioinnin saavuttaneet medioiden pyyhkimis-ohjelmistot.

Kommentit teknisen turvallisuuden osa-alueeseen - Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi kriteerin tunnisteella.
Voit arvioida kriteerien ymmärrettävyyttä, kriteerien luokittelun tasojen sopivuutta sekä mahdollisia puutteita kriteeristössä tai voiko jonkun kriteerin jättää tarpeettomana pois?

Teknisen tietoturvallisuuden vaatimukset velvoittavat osittain ottamaan käytännössä käyttöön Katakri 2020-vaatimukset myös henkilötietojen suojaamiseen. Tämän toteuttamien tulee vaatimaan merkittävästi resursseja sekä virastoissa että toimittajin osalta. Kotimaisilla pienyrityksillä tulee kuitenkin olemaan vaikeuksia toteuttaa k.o. vaatimuksia. Kritteeristö tulee ohjaamaan hankintoja isommille ja kansainvälisille toimittajille.

TEK-13: Ohjelmistojen turvallisuuden varmistaminen on erinomainen ja tarpeellinen vaatimus panostaa ohjelmistotuotannon automaattiseen testaukseen

TEK-01.4 Verkon rakenteellinen turvallisuus: salaaminen turva-alueiden ulkopuolella TL-IV, riitävän turvallinen salausratkaisu tulisi määritellä, esim. taho, jonka suosituksia pitää noudattaa.

TEK-05.1 Langaton tiedonsiirto: salaaminen TL-IV, riittävän turvallinen salausratkaisu tulisi määritellä, ks. TEK-01.4

Kommentit varautumisen ja jatkuvuudenhallinnan osa-alueeseen - Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi kriteerin tunnisteella.
Voit arvioida kriteerien ymmärrettävyyttä, kriteerien luokittelun tasojen sopivuutta sekä mahdollisia puutteita kriteeristössä tai voiko jonkun kriteerin jättää tarpeettomana pois?

Mielestämme on erinomaista Suomen kyberturvallisuuden kannalta, että varautumisen ja jatkuvuudenhallinnanvaatimukset ovat nyt asianmukaisesti ja kohtuullisesti määritelty.

Kommentit tietosuojan osa-alueeseen - Yksilöi vastauksessasi mahdollisuuksien mukaan esimerkiksi kriteerin tunnisteella.
Voit arvioida kriteerien ymmärrettävyyttä, kriteerien luokittelun tasojen sopivuutta sekä mahdollisia puutteita kriteeristössä tai voiko jonkun kriteerin jättää tarpeettomana pois?
Tietosuojan osa-alueen kommentit välitetään arvioitavaksi Tietosuojavaltuutetun toimistoon.

Mielestämme vaatimuksissa lueteltu selkeästi, asianmukaisesti ja lainsäädännön mukaisesti henkilötietojen suojaamiseen liittyvät organisaation velvoitteet.

Julkri-työkalu ja ohje (Liite 2 ja Liite 3)

Julkri-työkalu (Liite 2)
Voit arvioda seuraavassa kriteeristön käyttöä tukevan työkalun toimivuutta ja ymmärrettävyyttä?

Työkalu on sinänsä erittäin tarpeellinen ja se tuo ilmi myös vaatimusten massiivisuduen (217 vaatimusta!). Työkaluun tulisi lisätä katergoria "Harkiten annettava/Toimittajan liikesalaisuus".

Julkri-työkalun ohjeistus (Liite 3)Voit arvioida seuraavassa onko ohjeistus riittävä ja ymmärrettäväsekä ovatko käyttötapaukset tarkoituksenmukaisia tai puuttuuko joku keskeinen käyttötapaus?

Kohtaa ”SaaS-pilvipalvelun arviointi” tulisi avata huomattavasti selkeämmin, millä kriteereillä turvallisuussertikaateilla voi kuitata vaatimuskriteeristöjä.

Muita kommentteja ja kehitysideoita kriteeristön kehittämiseksi

Voit kirjoittaa kommentit alla olevaan tekstikenttään.

-

Lindell Miia
CSC-Tieteen tietotekniikan keskus Oy