Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä - Muutokset

1 Lausuntokierrosversio -> Versio 1.0

Versiolla 1.0 tarkoitetaan lausuntokierroksen pohjalta korjattua versiota, joka on julkaistu kyberturvallisuuslain vahvistuksen yhteydessä.

1.1 Merkittävimmät muutokset

Uusia suosituksen kohtia ovat 3.1.1 ja 11.1.1. Suosituksen kohdan 3.7 sisältö on siirretty kohtaan 3.1.1. Suosituksen kohta 3.7.1 on poistettu ja sen sisältö siirretty kohtaan 3.7.

Suosituksen osiota 11, joka käsittelee perustason tietoturvakäytäntöjä, on yksinkertaistettu ja sen kohdista on siirretty sisältöä niitä vastaaviin kohtiin muualla suosituksessa.

1.2 Muutokset kohdittain

1.2.1 Suosituksen tausta ja tarkoitus

Kohtaan on tehty tarkennuksia suosituksen antajasta ja suosituksen tarkoituksesta sekä korjattu mm. luonnoskierroksella tarkentuneen kyberturvallisuuslain nimi. Kohtaan on lisätty maininta siitä, että suosituksen kohtien täyttäminen ei välttämättä takaa sitä, että toimija täyttäisi kyberturvallisuuslaissa säädetyt velvoitteet.

Kohtaan on lisätty yhteenveto lausuntopalautteesta, joka saatiin suosituksen lausuntokierroksella.

Määritelmiä on lisätty ja tarkennettu.

Suosituksen lukuohjetta on tarkennettu korkeamman kypsyystason osalta.

1.2.2 1 Kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteet vaikuttavuuden arviointi

Osion otsikkoa on muutettu. Lakiviittaukset on päivitetty.

Kohtaa 1.1 on tarkennettu lausuntopalautteiden pohjalta.

Kohdassa 1.2 pieniä lisäyksiä.

Kohdassa 1.4 "uhka" muutettu muotoon "kyberuhka".

Kohdassa 1.4.1 korjattu sanamuotoja ja sujuvoitettu tekstiä.

Kohdassa 1.5 tarkennettu johdon velvollisuutta riskien hyväksyntään.

Kohtaa 1.6.1 tarkennettu erityisesti komission täytäntöönpanoasetuksen vaatimusten suuntaiseksi. Mittaristo-termin tilalle otettu raportointijärjestelmä.

1.2.3 2 Viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet

Lakiviittaukset on päivitetty.

Kohtaa 2.1 tarkennettu komission täytäntöönpanoasetuksen vaatimusten suuntaiseksi.

Kohtaan 2.1.1 lisätty kappale turvallisuutta koskevien toimintaperiaatteiden luomisesta turvallisuuden eri osa-alueittain.

Kohdasta 2.3 poistettu viittaus toimijan liiketoimintastrategiaan.

1.2.4 3 Viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi

Osion otsikkoa on muutettu. Lakiviittaukset on päivitetty.

Kohdasta 3.1 poistettu viittaus ARP-tauluihin.

Kohta 3.1.1 luotu ja sen sisältö siirretty sellaisenaan kohdasta 3.7 "Kehittämisen turvallisuus".

Kohdassa 3.4 lisätty todennusmenetelmiä.

Kohtaa 3.5 tarkennettu turvallisuustestauksen selitystä sekä korvattu menettelyt ja toimintatavat toimintaperiaatteella.

Kohdassa 3.6 lisätty tarkennus kansallisista CVD-menettelytavoista.

Kohta 3.7 poistettu ja teksti siirretty kohtaan 3.1.1.

Kohta 3.7.1 uudelleennumeroitu kohdaksi 3.7. Poistettu laajennetun ohjeistuksen määritelmä. Komponenttilista uudelleennimetty materiaaliluetteloksi.

Kohtaan 3.8 lisätty kohtia kyberhygieniakäytäntöjen kohdasta 11.3 sekä komission täytäntöönpanoasetuksen liitteestä. Tarkennettu todentamismenetelmiä.

Kohtaan 3.9 lisätty kohtia kyberhygieniakäytäntöjen kohdasta 11.3 ja 11.5. Tarkennettu todennusmenetelmien 3-tasolle palveluntarjoajan lupa.

1.2.5 4 Toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt

Osion otsikkoa on muutettu. Lakiviittaukset on päivitetty.

Kohtaan 4.2 lisätty maininta toimintaperiaatteista ja korjattu sanamuotoja.

1.2.6 5 Omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

Lakiviittaukset on päivitetty.

Kohtaan 5.1 lisätty viittaus toimintaperiaatteisiin ja tehty muita lisäyksiä sekä korjattu sanamuotoja.

Kohtaan 5.2 lisätty viittaus toimijan sopimussuhteiden kautta hallinnassa oleviin laitteisiin.

1.2.7 6 Henkilöstöturvallisuus ja kyberturvallisuuskoulutus

Lakiviittaukset on päivitetty.

Kohdassa 6.5 sanamuodon korjauksella laajennettu suositus henkilöstökoulutuksesta koskemaan turvallisuutta yleisemmin.

Kohtaan 6.6 korjattu sanamuotoja ja lisätty tavoite toteutusesimerkkiin.

1.2.8 7 Pääsynhallinnan ja todentamisen menettelyt

Lakiviittaukset on päivitetty.

Kohtaan 7.1 lisätty viittaus toimintaperiaatteisiin ja korjattu nollaluottamuksen periaatteen suomennos, joka oli luottamattomuuden periaate.

Kohdassa 7.3.1 lisätty valvottavia tapahtumia toteutusesimerkkiin.

Kohtaan 7.5 lisätty viittaus toimintaperiaatteisiin ja maininta hallintaverkoista ja hallintatyöasemista.

Kohtaan 7.6 lisätty ja tarkennettu toteutusesimerkkejä.

1.2.9 8 Salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi

Osion otsikkoa on muutettu. Lakiviittaukset on päivitetty.

1.2.10 9 Poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

Lakiviittaukset on päivitetty.

Kohtaan 9.1 lisätty viittaus toimintaperiaatteisiin.

Kohdassa 9.3 korjattu sanamuotoja ja todennusesimerkin viittaus säilytysajan pituudesta.

Kohdassa 9.4 korjattu sanamuotoja ja lisätty maininta toteutusesimerkkeihin vanhojen poikkeamien uudelleenarvioinnista.

Kohtaan 9.5 lisätty maininta merkittävien poikkeamien käsittelystä.

Kohtaan 9.7 lisätty toteutusesimerkkejä merkittävän poikkeaman käsittelystä.

1.2.11 10 Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

Lakiviittaukset on päivitetty.

Kohtaan 10.1 lisätty toteutusesimerkkejä.

Kohtaa 10.2 tarkennettu lausuntopalautteen pohjalta. Lisätty toteutusesimerkkejä.

Kohtaa 10.4 tarkennettu lausuntopalautteen pohjalta.

1.2.12 11 Perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

Tarkennettu perustason tietoturvakäytäntöjen määritelmää ja yksinkertaistettu tekstiä.

Kohtaa 11.1 tarkennettu ja siihen lisätty viittaus kyberturvallisuustietoisuuden parantamisesta.

Kohta 11.1.1 luotu. Sisältö yhdenmukaistettu komission täytäntöönpanoasetuksen kanssa.

Kohtaa 11.3 yksinkertaistettu.

Kohtaa 11.4 yksinkertaistettu.

Kohtaa 11.5 yksinkertaistettu.

Kohdasta 11.6 poistettu toisen tason todennusesimerkki.

Kohtaan 11.9 lisätty viittaus haavoittuvuusskannaukseen. Todennusesimerkkejä yksinkertaistettu.

Kohdasta 11.10 poistettu toisen tason todennusesimerkki.

1.2.13 12 Toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi

Lakiviittaukset on päivitetty. Kohtiin lisätty viitteet Rakennusten digitaalinen turvallisuus -ohjeistoon.

Kohtaan 12.1 lisätty toteutusesimerkkiin kohta maantieteellisesti laaja-alaisista yhteyksistä.

Kohdan 12.2 toteutusesimerkkiä tarkennettu.

Kohtaan 12.3 lisätty maininta ulkoisista kumppaneista ja sopimussuhteista.