

Katakri 2020 / Liite IV: Naton turvallisuusluokitellun tiedon suojaaminen

Johdanto

Tämä liite on julkaistu tukemaan niitä julkishallinnon ja elinkeinoelämän organisaatioita, jotka tulevat käsittelemään Pohjois-Atlantin liiton eli Naton tietoa. Liite on tarkoitettu tukemaan myös Naton tiedon suojaamiseen edellytettävien turvallisuustoimenpiteiden täyttymisen arviointia. Liite perustuu Suomelle 2022 Nato-jäsenyysprosessin aikana luovutettuihin tarkentaviin turvallisuussäntöihin ja -ohjeisiin, joista on tehty vertailuanalyysi Katakri 2020:een. Liite on valmisteltu Naton turvallisuusluokiteltujen tietojen suojaamisen lakisäätteisten asiantuntijaviranomaisten (DSA, Designated Security Authority, 588/2004, 4 §) yhteistyönä. Ulkoministeriön Kansallinen turvallisuusviranomainen (NSA, National Security Authority) on hyväksynyt liitteen osaksi Katakria 1.1.2023.

Naton turvallisuussäännöistä vastaava turvallisuustoimisto (NOS, Nato Office of Security) on Suomeen 2022 tehdyssä tarkastuksessa todennut Katakri 2020:n olevan arvokas työkalu Naton turvallisuussäntöjen jalkauttamiseksi ja arvioimiseksi. Tämä liite ei siten tuo merkittäviä muutoksia Katakri 2020 sisältöön tai sen soveltamiseen, vaan pyrkii esittämään ainoastaan huomionarvoiset eroavaisuudet kansallisten, EU:n ja Naton turvallisuusvaatimusten välillä. Naton turvallisuusvaatimukset ovat joissakin tilanteissa lievemmat ja joissakin tilanteissa tiukemmat, kuin kansalliset tai EU:n vastaavat. Katakri ja tämä liite yhdessä käytettynä käsittelee Naton turvallisuusluokitellun tiedon luokkien NATO RESTRICTED, NATO CONFIDENTIAL ja NATO SECRET suojaamista. Naton COSMIC TOP SECRET -luokan tietoihin kohdistuvat turvallisuusvaatimukset pohjautuvat NATO SECRET -luokan vaatimuksiin. COSMIC TOP SECRET -luokan lisävaatimuksia ei ole kyseisen tiedon rajoitetun käsittelytarpeen vuoksi esitetty tässä liitteessä. COSMIC TOP SECRET -luokan turvallisuusvaatimukset tulee varmistaa kansalliselta turvallisuusviranomaiselta tai määrätyiltä turvallisuusviranomaisilta (588/2004, 4 §) tapauskohtaisesti. Tässä liitteessä sivutaan lisäksi Naton turvallisuusluokittelemattoman, jakelurajoitetun NATO UNCLASSIFIED -tiedon suojaamisen yleisiä periaatteita.

Jakelurajoitetun tiedon suojaaminen

Naton jakelurajoitettu tieto merkitään turvallisuusluokan sijasta jakelurajoitemerkinä NATO UNCLASSIFIED. Tällaista tietoa käsittelevällä henkilöllä tulee olla viranomaisen hyväksymä, työtehtävään liittyvä tiedonsaantitarve ja hänen tulee ymmärtää asiakirjan jakelurajoitteisuuden merkitys. Tällaista tietoa käsitteleviin tietojärjestelmiin ei kohdistu hyväksyntävelvoitetta, ja tiedon käsittely on mahdollista myös fyysisesti suojattujen turvallisuusalueiden ulkopuolella.

Kunkin NATO UNCLASSIFIED -asiakirjan kohdalla tulee erikseen arvioida, onko asiakirjassa esitetty tieto julkisuuslain mukaan salassa pidettävää. Asiakirjan mahdollisen salassapidon kansallisesti tulee perustua julkisuuslakiin, esimerkiksi julkisuuslain 24 §:n 1 momentin 2 kohtaan. NATO UNCLASSIFIED -tiedon suojaamista on käsitelty kattavammin kansallisen turvallisuusviranomaisen julkaisemassa kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohjeessa¹.

¹ Kansallinen turvallisuusviranomainen. 2020. Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje. URL: <https://um.fi/turvallisuusluokitellun-tiedon-kasittelyohje>.

Turvallisuusjohtaminen

Katakri 2020:n turvallisuusjohtamisen osa-alueeseen ei kohdistu lisäyksiä tai muutoksia tässä päivitysliitteessä. Katakriin seuraavassa kokonaisuudistuksessa tullaan kuitenkin huomioida vaatimuskokonaisuuksien sijoittelun eri vaihtoehdot turvallisuusjohtamisen, fyysisen turvallisuuden ja teknisen turvallisuuden osa-alueiden välillä.

Fyysinen turvallisuus

Katakri 2020:een kootut fyysisen turvallisuuden vähimmäisvaatimukset (F-01 – F-07) ovat sellaisenaan Naton turvallisuusäntöjen mukaiset, joten päivitysliitteessä on pyritty esittämään ainoastaan selvemmin Naton turvallisuusaluejaon ja käsittelysääntöjen rinnasteisuudet Katakriin. Esitetyt rinnasteisuudet pohjautuvat Naton turvallisääntöjen fyysistä turvallisuutta käsitteleviin kokonaisuuksiin.

Suomella ja EU:lla on käytössä kaksiportainen fyysisesti suojattujen turvallisuusalueiden luokitus (1101/2019, 9§; 2013/488/EU liite II, 12), joka sisältää hallinnollisen alueen ja turva-alueen (Katakri 2020, F-04). Natolla on käytössä samankaltainen luokitus, joka sisältää kuitenkin hallinnollisen alueen (Administrative Zone) lisäksi kaksi erilaista turva-aluetta (NATO Class I Security Area ja NATO Class II Security Area). Katakriissa (F-05) määritelty hallinnollinen alue vastaa sellaisenaan Naton hallinnollista aluetta. Katakriissa määritelty turva-alue (F-06) vastaa toteutus- ja käyttötavasta riippuen Naton molempia turva-alueita (Class I ja Class II). Nämä erilaiset toteutus- ja käyttötavat sekä eri vaatimukset on otettu sellaisenaan huomioon jo Katakri 2020:n F-osa-aluetta laadittaessa, joten uusia vaatimuksia ei ole. Tässä liitteessä rinnasteisuudet on kuitenkin osoitettu Naton kaksiportaisen turva-aluejaon mukaisesti, jotta tietoa käsittelevillä organisaatioilla on mahdollisuus tarvittaessa luoda Naton vaatimusten mukaisia turva-alueita eri käyttötarkoituksiin ja arvioida niiden vaatimustenmukaisuus. Käytännössä Naton turva-alueiden ero liittyy siihen, että turva-alueelle Class I sisäänpääsy tarkoittaa myös pääsyä alueella käsiteltäviin ja säilytettäviin tietoihin. On tärkeä huomioida, että turva-alueiden ero liittyy edellä mainitulla tavalla turva-alueiden toteutus- ja käyttötapaan, eikä tiedon turvallisuusluokkaan tai esimerkiksi vaarantavalta hajasäteilyltä (TEMPEST) suojautumisen vaatimukseen (vrt. Katakri 2020, I-14). Lisäksi on huomioitava, että vaikka turva-alue perustettaisiinkin Naton turvallisuusluokiteltujen tietojen suojaamiseksi, turva-aluetta ei tarvitse nimetä ja merkitä Naton turva-aluejaon mukaisesti nimellä Class I tai Class II. Naton turvallisuusääntö käsittelevät lisäksi turva-alueisiin sisältyvää teknisesti suojattua turva-aluetta (Technically Secure Area). Katakriissa (F-07) määritelty teknisesti suojattu turva-alue vastaa sellaisenaan Naton teknisesti suojattua turva-aluetta.

Naton turvallisuusääntöjen soveltamista arvioiva turvallisuusauditointi tulee suorittaa F-osa-alueen johdannossa esitetyn arviointiprosessin mukaisesti. On tärkeä huomioida, että myös Nato korostaa turvallisuusjärjestelyjen suunnittelussa ja arvioinnissa riskien arviointia ja kustannustehokkuutta. Fyysinen turvallisuus on vain yksi osa-alue, jonka ratkaisuja tulee tukea ja jonka ratkaisuja voi kompensoida muiden turvallisuuden osa-alueiden kuten I-osa-alueen turvallisuusratkaisujen avulla. Edes turva-alueen (NATO Class I Security Area) vähimmäisvaatimuksena ei ole alueen fyysisten rajojen rakenteellinen vahventaminen, vaan rakenteellinen murto suojaus ja sen mahdollinen parantaminen perustuu aina turvallisuusalueiden monitasoiseen suojaukseen ja riskiarvioon. Naton fyysistä turvallisuutta koskevan politiikan mukaan järkevä riskien hallinta onkin oikeassa suhteessa vaikuttava ja kustannustehokas yhdistelmä eri osa-alueiden vaatimusten soveltamista. Naton tietojen suojaksi suunniteltuja turvallisuusratkaisuja auditoivan asiantuntijan ei tulisi kaan

rajoittaa toimintaansa ja tarkastella seikkaperäisesti kaikkia yksityiskohtia Katakrista, vaan tarkastella että fyysisen turvallisuuden kokonaisuus täyttää vähimmäisvaatimukset ja muodostaa riittävän suojan turvallisuusluokitelluille tiedoille yhdessä muiden turvallisuusjärjestelyjen kanssa.

Katakri 2020:n F-osa-alueessa esitetyt tietoaineistoturvallisuuden vähimmäisvaatimukset (F-08) ovat muutamia yksityiskohtia lukuun ottamatta Naton turvallisuussääntöjen mukaiset. Nämä yksityiskohtaiset eroavuudet on esitelty kohta-kohdalta. Myös tietoaineistoturvallisuuden osa-alueella jotkin yksittäiset kansalliset vaatimukset ovat tiukemmat, kuin Naton turvallisuussääntöjen vähimmäisvaatimukset. Näitä pieniä eroja ei ole kuitenkaan tuotu esiin tässä liitteessä. Osa-alueen merkittävin muutos on lievennys, joka koskee NATO CONFIDENTIAL -luokan asiakirjojen tuhoamistodistusmenettelystä luopumista (F-08.4).

F-04 – Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella

Turvallisuusluokiteltujen tietojen käsittely fyysisesti suojatuilla turvallisuusalueilla on kuvattu Katakri 2020:n kohdassa F-04. Tämän liitteen taulukko 1 on tarkoitettu sovellettavaksi niihin tilanteisiin, joissa käsiteltävänä on Naton turvallisuusluokiteltua tietoa. Taulukkoa 1 tulee soveltaa yhdessä taulukossa 2 esiteltävän Naton turvallisuusalueita koskevan rinnastuksen kanssa.

Naton ja kansallisen tiedon käsittelyn merkittävimmät erot kohdistuvat turvallisuusalueiden ulkopuolella liittyvään tiedon käsittelyyn sekä tiedon käsittelyyn hallinnollisella alueella. Hallinnollisella alueella saa käsitellä korkeintaan NATO RESTRICTED -luokan tietoja. Naton turvallisuusluokittelun tiedon käsittely ei ole sallittua fyysisesti suojattujen turvallisuusalueiden ulkopuolella. Organisaation toimitilojen ulkopuolella on kuitenkin mahdollista perustaa tilapäinen hallinnollinen alue NATO RESTRICTED -luokan tiedon käsittelyyn, esimerkiksi etätyötä varten. Taulukossa 1 on myös esitetty sijoitussuositukset niille palvelimille, verkon hallintalaitteille ja muille verkkolaitteille, jotka käsittelevät Naton turvallisuusluokiteltua tietoa. Nämä suositukset on tuotu esiin taulukon Säilytys-sarakkeessa kohdissa ”Palvelimet, verkkolaitteet ja vastaavat”.

Naton turvallisuusluokiteltuja tietoja on kaikissa tilanteissa käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin estetään sivullisilta. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen tietoon että laittomalta tiedustelulta. Suojaaminen tarkoittaa käytännössä esimerkiksi suoran näkö- tai kuuloyhteyden estämistä turvallisuusluokiteltuun tietoon sekä tiedon tai tietoa sisältävän päätelaitteen riittävän turvallista säilyttämistä. Tietojen käsittelyssä on huomioitava lisäksi toiminta työskentelytaukojen aikana, jolloin paperiasiakirjat ja päätelaitteet on turvallisuusluokan perusteella sijoitettava soveltuvalle turvallisuusalueelle ja/tai säilytysyksikköön tauon ajaksi. Tiedon säilytyksellä viitataan tilanteeseen, jossa tieto ei ole sen käsitelijän välittömässä valvonnassa. Katakriassa käytettävällä termillä ”pätelaitte” tarkoitetaan tietojärjestelmää tai sen osaa, jota henkilö käyttää työtehtäviensä hoitamiseen liittyvään sähköiseen tietojenkäsittelyyn. Vaatimukset täyttävällä päätelaitteella tarkoitetaan päätelaitetta, joka täyttää teknisen tietoturvallisuuden osa-alueessa (I) kuvatut vaatimukset.

Taulukko 1. Tiedon käsittely ja säilytys turvallisuusalueilla ja niiden ulkopuolella.

F-04 – TIEDON KÄSITTELY JA SÄILYTYS TURVALLISUUSALUEILLA JA NIIDEN ULKOPUOLELLA								
NATON TURVALLISUUSLUOKITELLUN TIEDON KÄSITTELY JA SÄILYTYS								
	Käsittely				Säilytys			
Turvallisuusluokka	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue (Administrative Zone)	Turva-alue (NATO Class II Security Area)	Turva-alue (NATO Class I Security Area)	Turvallisuusalueiden ulkopuolella	Hallinnollinen alue (Administrative Zone)	Turva-alue (NATO Class II Security Area)	Turva-alue (NATO Class I Security Area)
NATO SECRET	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Kyllä , jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa	Paperiasiakirjat: Ei Päätelaitteessa: Ei Palvelimet, verkkolaitteet ja vastaavat: Ei	Paperiasiakirjat: Ei Päätelaitteessa: Ei Palvelimet, verkkolaitteet ja vastaavat: Ei	Paperiasiakirjat: Kyllä , soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä , mikäli ne on erikseen suojattu fyysisesti. (**)	Paperiasiakirjat: Kyllä Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä
NATO CONFIDENTIAL	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Ei Päätelaitteessa: Ei	Paperiasiakirjat: Kyllä , jos pääsy tietoihin on suojattu sivullisilta Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa	Paperiasiakirjat: Ei Päätelaitteessa: Ei Palvelimet, verkkolaitteet ja vastaavat: Ei	Paperiasiakirjat: Ei Päätelaitteessa: Ei Palvelimet, verkkolaitteet ja vastaavat: Ei	Paperiasiakirjat: Kyllä , soveltuvaksi arvioidussa säilytysratkaisussa Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä	Paperiasiakirjat: Kyllä Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä
NATO RESTRICTED	Paperiasiakirjat: Ei* Päätelaitteessa: Ei*	Paperiasiakirjat: Kyllä , jos pääsy tietoihin on suojattu sivullisilta	Paperiasiakirjat: Kyllä , jos pääsy tietoihin	Paperiasiakirjat: Kyllä	Paperiasiakirjat: Ei* Päätelaitteessa: Ei*	Paperiasiakirjat: Kyllä , soveltuvassa lukitussa toimistokalusteessa	Paperiasiakirjat: Kyllä , soveltuvassa lukitussa	Paperiasiakirjat: Kyllä

		Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	on suojattu sivullisilta Päätelaitteessa : Kyllä , vaatimukset täyttävässä laitteessa, jos pääsy tietoihin on suojattu sivullisilta	Päätelaitteessa : Kyllä , vaatimukset täyttävässä laitteessa	Palvelimet, verkkolaitteet ja vastaavat: Ei	Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä (**)	toimistokalusteessa Päätelaitteessa: Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä	Päätelaitteessa : Kyllä , vaatimukset täyttävässä laitteessa Palvelimet, verkkolaitteet ja vastaavat: Kyllä
--	--	------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------	----------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------

* NATO RESTRICTED-luokan tiedon käsittely ja säilytys turvallisuusalueiden ulkopuolella on mahdollista, mikäli perustetaan tilapäinen hallinnollinen alue, joka täyttää Katakriin F-05-vaatimukset ja tiedon käsittelijä:

- kuljettaa tietoja F-08.1 mukaisesti
- on sitoutunut noudattamaan Suojelupoliisin tai Pääesikunnan ja päätelaitteen osalta Traficomien NCSA-toiminnon antamissa turvallisuusohjeissa määrättyjä korvaavia toimenpiteitä sen varmistamiseksi, että pääsy tietoihin on suojattu sivullisilta

** Suojaustarve ja -toteutus arvioidaan järjestelmäkohtaisesti tiedon turvallisuusluokkaan perustuen. NATO RESTRICTED- tai NATO CONFIDENTIAL-luokan tietoa käsittelevät palvelimet, verkon hallintalaitteet tai muut verkkolaitteet suositellaan sijoitettavan turva-alueelle (NATO Class II Security Area). NATO SECRET-luokan tietoa käsittelevät palvelimet, verkon hallintalaitteet tai muut verkkolaitteet suositellaan sijoitettavan turva-alueelle (NATO Class I Security Area).

Turvallisuusluokitelluista tiedoista keskusteleminen turvallisuusalueilla ja niiden ulkopuolella: Tiedoista keskusteleminen on mahdollista turvallisuusalueilla ja niiden ulkopuolella, jos estetään että sivulliset eivät pääse kuulemaan henkilöiden turvallisuusluokiteltuun tietoon liittyviä keskusteluja. Estämisellä tarkoitetaan tiedon suojaamista sekä henkilöiltä, joilla ei ole tiedonsaantitarvetta (need-to-know) kyseiseen keskusteltavaan tietoon että laittomalta tiedustelulta.

TEMPEST-riskien arviointi: Arvioitaessa tiedon käsittelyä päätelaitteessa ja turvallisuusalueiden sijaintia on riittävässä määrin otettava huomioon myös I-14-kohdassa käsiteltävä TEMPEST-riski, jota voidaan yleensä pienentää muuttamalla tiedon käsittelypaikan sijaintia kiinteistössä.

Taulukko 2. Katakri 2020:n ja Naton turvallisuusalueiden rinnastus - Perustamistarve ja käyttötarkoitus.

KATAKRI 2020:N JA NATON TURVALLISUUSALUEIDEN RINNASTUS – PERUSTAMISTARVE JA KÄYTTÖTARKOITUS

NATO C-M(2002)49- REV1	KATAKRI 2020	ALUEEN PERUSTAMISTARVE	TIETOJÄRJESTELMISTÄ JOHTUVA ALUEEN PERUSTAMISTARVE- SUOSITUS (**)	ALUEEN KÄYTTÖTARKOITUS	ESIMERKKIKÄYTTÖTAPAUS
Technically Secure Area	Teknisesti suojattu turva-alue (F-07)	Organisaation tulee perustaa teknisesti suojattu turva-alue, mikäli se järjestää NATO SECRET -luokan tietoihin liittyviä kokouksia tai keskustelee SECRET-luokan tiedoista säännöllisesti toimitiloissaan. Alue voidaan tilapäisesti perustaa hallinnolliselle alueelle turvallisuusluokiteltua kokousta tai muuta vastaavaa tarkoitusta varten.	-	Alue, jolla voidaan keskustella turvallisuusluokitelluista (NATO SECRET) tiedoista avoimesti.	Tällaisia alueita ovat neuvottelutilat. Suojelupoliisi tai Pääesikunta päättää alueeseen liittyvästä uhka-arvioinnista, riskien hallintatoimenpiteistä ja mahdollisen tilapäisesti perustettavan alueen turvallisuusjärjestelyjen hyväksynnästä tapauskohtaisesti.
NATO Class I Security Area	Turva-alue* (F-06)	Organisaation tulee perustaa turva-alue esitetyillä lisävaatimuksilla (NATO Class I Security Area), mikäli alueelle pääsy tarkoittaa pääsyä myös alueella käsiteltäviin ja/tai säilytettäviin tietoihin.	Suositus**: Organisaation tulee perustaa turva-alue esitetyillä lisävaatimuksilla (NATO Class I Security Area) niitä palvelimia, verkon hallintalaitteita tai muita verkkolaitteita varten, jotka käsittelevät NATO SECRET -luokan tietoa.	Alue, jolla voidaan käsitellä ja/tai säilyttää turvallisuusluokiteltuja tietoja avoimesti.	Tällaisia alueita voivat olla esimerkiksi kirjaamot, arkistot, konesalit ja tilannekeskukset sekä tiettyjen tietojärjestelmien sijoituspaikat.

			Perustamistarvetta ei ole, mikäli laitteet on sijoitettu turva-alueelle (NATO Class II Security Area) ja laitteet on erikseen suojattu fyysisesti. Perustamistarvetta ei myöskään ole, mikäli käytetään päätelaitteita, jotka ottavat ainoastaan yhteyden NATO SECRET-tietoa sisältäviin palvelimiin.		
NATO Class II Security Area	Turva-alue (F-06)	Organisaation tulee perustaa turva-alue (NATO Class II Security Area), mikäli se käsittelee vähintään NATO CONFIDENTIAL-luokan tietoa toimitiloissaan. Alueelle pääsy ei tarkoita pääsyä alueella käsiteltäviin tai säilytettäviin tietoihin.	Suositus**: Organisaation tulee perustaa turva-alue (NATO Class II Security Area) niitä palvelimia, verkon hallintalaitteita tai muita verkkolaitteita varten, jotka käsittelevät NATO RESTRICTED- tai NATO CONFIDENTIAL -luokan tietoa. NATO SECRET -luokan tietoa käsitteleviä palvelimia, verkon hallintalaitteita tai muita verkkolaitteita voi sijoittaa alueelle, mikäli laitteet on erikseen suojattu fyysisesti.	Alue, jolla voidaan käsitellä ja säilyttää turvallisuusluokiteltuja tietoja siten, että tiedot säilytetään säilytysyksikössä. Päätelaitteet tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa, mikäli mahdollista.	Tällaisia alueita voivat olla esimerkiksi toimistotilat tai neuvottelutilat.
Administrative Zone	Hallinnollinen alue (F-05)	Organisaation tulee perustaa hallinnollinen alue (Administrative Zone), mikäli se käsittelee NATO RESTRICTED-luokan tietoa toimitiloissaan. Alueelle pääsy ei	-	Alue, jolla voidaan käsitellä ja säilyttää enintään NATO RESTRICTED-luokan tietoa siten, että tiedot säilytetään soveltuvassa lukitus- toimistokalusteessa.	Tällaisia alueita voivat olla esimerkiksi toimistotilat ja aidatut ulkoalueet. Alue voi olla osa turva-alueiden monitasoista suojausta.

		tarkoita pääsyä alueella käsiteltäviin tai säilytettäviin tietoihin. Alue voidaan tilapäisesti perustaa etätyötä tai muuta vastaavaa tarkoitusta varten.		Päätelaitteet tulee säilyttää soveltuvaksi arvioidussa säilytysratkaisussa, mikäli mahdollista.	
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------	--	-------------------------------------------------------------------------------------------------	--

* Turva-alueen (NATO Class I Security Area vastaava) perustamisessa tulee toteuttaa muiden turva-alueen (F-06) vaatimusten lisäksi seuraavat vaatimukset Katakri 2020:sta:

- Turva-alueella säilytettyjen ja käsiteltyjen Naton tietojen korkein turvallisuusluokka ja alueelle pääsyn edellytyksenä olevan Nato-PSC-todistuksen tarve on ilmoitettava selkeästi (F-06.4)
- Turva-alueen vierailijoilla on oltava erityisen luvan (F-06.3) ja Nato PSC:n lisäksi saattaja, paitsi jos on varmistettu, ettei vierailijoilla ole pääsyä turvallisuusluokiteltuihin tietoihin (F-06.4)
- Mikäli turva-alueella ei ole tiedon säilytykseen riittäväksi arvioitua säilytysratkaisua, on alueen seinien, lattian, katon, ikkunoiden ja ovien tarjottava tietojen säilytyksen edellyttämä turvallisuustaso murtoriskien arviointiin perustuen (F-06.1).

** Suojaustarve ja -toteutus arvioidaan järjestelmäkohtaisesti tiedon turvallisuusluokkaan perustuen. Palvelimet, verkon hallintalaitteet ja muut verkkolaitteet suositellaan sijoitettavan sarakkeessa mainituille turvallisuusalueille.

F-08 – Tietoaineistoturvallisuus

Tässä luvussa eritellään keskeisimmät täydennykset ja tarkennukset Katakri 2020:n tietoaineistoturvallisuuden osa-alueeseen koottuihin vaatimuksiin. Erittelyssä ei ole toistettu sellaisia Naton turvallisuusluokiteltuun tietoon kohdistuvia suojausvaatimuksia, jotka on jo kuvattu Katakri 2020:n vaatimus- tai toteutusmerkikentissä. Osa-alueen merkittävin muutos on lievennys, joka koskee NATO CONFIDENTIAL -luokan asiakirjojen tuhoamistodistusmenettelystä luopumista (F-08.4).

F-08.1 - Tietojen välitys postilla ja kuriirilla

Ei oleellisia muutoksia. Täydennykset:

- Toteutusmerkikenttä kohta 5: NATO SECRET -luokan tietoa sisältävän lähetyksen kulku on varmistettava kuittausmenettelyllä. NATO CONFIDENTIAL-luokan tietoa lähetettäessä lähetyksen kulku on varmistettava kuittausmenettelyllä, mikäli tiedon laatija sitä erikseen vaatii. Kuittauslomakkeisiin tai vastaaviin ei tule kirjata turvallisuusluokiteltua tietoa, niiden tulee sisältää viitetieto asiakirjaan (esimerkiksi numero), kopion numero, asiakirjan kieli sekä otsikko, mikäli otsikko ei sisällä turvallisuusluokiteltua tietoa.
- Toteutusmerkikenttä kohta 5 ja 8: sisäkuoren tulee olla sinetöity ja merkitty asianmukaisella Naton turvallisuusluokkaa osoittavalla leimalla, kuten myös muilla määrävillä merkinnöillä. Sisäkuoren tulee olla varustettu vastaanottajatiedoilla. Uloimmassa kuoressa tulee olla vastaanottajatiedot sekä mekanismi lähetyksen kuljetuksen kuittaamiseksi. Mikäli tietoa kuljetetaan kuriirin välityksellä, uloimmassa kuoressa on oltava selkeä merkintä "vain kuriiritoimitus".

F-08.2 - Turvallisuusluokiteltujen tietojen kopioiminen

Ei oleellisia muutoksia. Täydennykset:

- Vaatimuskohta 2): Kopioiden ja niiden käsittelijöiden lisäksi kopionumerot on merkittävä asiakirjoihin ja kopionumerot on luetteloitava asiakirjoista vastaavassa rekisterissä.

F-08.3 - Turvallisuusluokiteltujen tietojen kirjaaminen

Ei oleellisia muutoksia. Täydennykset:

- Vaatimuskohta 1): Kirjaamon asiakirjojen käsittely- ja toimintatavasta riippuen, kirjaamo on määriteltävä turva-alueeksi, joka täyttää joko NATO Class I tai Class II Security Area -vaatimukset.
- Vaatimuskohta 2): NATO SECRET -luokan asiakirjojen jatkuvasta hallinnasta on varmistuttava määräjain tehtävin pistotarkastuksin, jotka kohdistuvat sekä rekisterissä että tiedon käsittelijöillä oleviin asiakirjoihin.

F-08.4 - Ei-sähköisten tietojen tuhoaminen

Ei oleellisia muutoksia. Täydennykset:

- Vaatimuskohta 2): NATO CONFIDENTIAL -luokan asiakirjojen tuhoamisesta ei tarvitse laatia tuhoamistodistusta. Rekisterimerkintä asiakirjan tuhoamisesta on riittävä.

Tekninen tietoturvallisuus

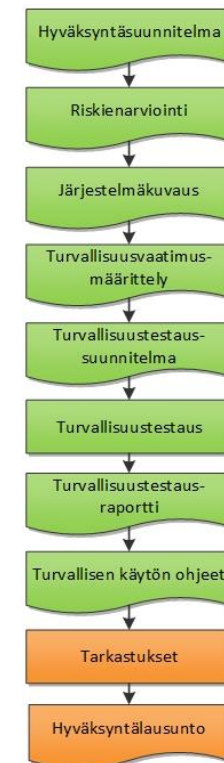
Teknisen tietoturvallisuuden osalta Naton turvallisuusluokitellun tiedon suojaaminen noudattaa suurten linjojen osalta Katakri 2020 -työkalussa kuvattua lähestymistapaa. Eroavaisuuksia löytyy kuitenkin sekä hyväksyntäprosessin rakenteesta, että teknisten suojausten yksityiskohtaisuudesta. Tässä luvussa kuvataan sellaiset Naton turvallisuusluokitellun tiedon suojaamisessa huomioitavat näkökulmat, joita ei ole vielä riittävällä tarkkuudella katettu Katakri 2020 -työkalussa.

Hyväksyntäprosessi

Tietojärjestelmien hyväksyntäprosessi (akkreditointi) mukailee Katakri 2020:ssa kuvattua mallia. Naton turvallisuusluokitellun tiedon suojaamisessa tulee kuitenkin huomioida tietojärjestelmän vastuorganisaatiolta edellytettävä kattavampi valmistelutyö ennen tietojärjestelmän viranomaistarkastusta ja -hyväksyntää. Valmistelutyö on esiehtona sille, että prosessi voi edetä tietojärjestelmän viranomaistarkastukseen ja -hyväksyntään.

Tietojärjestelmän vastuorganisaation valmistelutyö koostuu erityisesti hyväksyntäsuunnitelmasta, riskienarvioinnista, tietojärjestelmäkuvauksesta, turvallisuusvaatimusmäärittelmästä, turvallisuustestauksesta sekä turvallisen käytön ohjeista. Valmistelutyö ja siihen sisältyvien kuvausten laadintavastuu on järjestelmän vastuorganisaatiolla². Valmistelutyöhön sisältyvien kuvausten hyväksyntävastuu on turvallisuusjärjestelyjen hyväksyntäviranomaisella³. Valmistelutyöhön kuuluvia tehtäviä on mahdollista yhdistellä, mikäli se nähdään kyseisen tietojärjestelmän näkökulmasta perustelluksi. Esimerkiksi riskienarviointi ja tietojärjestelmäkuvaus voi olla perusteltua sisällyttää osaksi järjestelmäkohtaista turvallisuusvaatimusmäärittelyä. Kuvausten laadinta on yleensä iteratiivinen prosessi, jossa järjestelmän vastuorganisaatio alihankkijoineen käy aktiivista vuoropuhelua hyväksyntäviranomaisen kanssa.

Tietojärjestelmän hyväksyntäprosessia on havainnollistettu kuvassa 1. Yksityiskohtaisempi kuvaus on saatavilla Kyberturvallisuuskeskuksen NCSA-toiminnolta.



² Vastuorganisaationa on usein tietojärjestelmän omistaja. Tilanteissa, joissa esimerkiksi tietojärjestelmään liittyvää suunnittelu-, rakennus- tai testaustyöhön osallistuu alihankkijoita tai toimittajia, järjestelmän vastuorganisaatio on vastuussa kokonaisuuden hallinnasta.

³ SAA, Security Accreditation Authority. Suomessa Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen NCSA-toiminto.

Turvallisuusmalli

Naton turvallisuusluokitellun tiedon suojaamiseen liittyvä turvallisuusmalli mukailee Katakri 2020:n liitteessä III kuvattua mallia. Naton turvallisuusluokitellun tiedon sähköisen käsittelyn suojaamisessa tulee kuitenkin huomioida, että vähimmäisvaatimukset ja riskiperusteiset lisävaatimukset kootaan järjestelmäkohtaiseen turvallisuusvaatimusmäärittelyyn. Järjestelmäkohtaisessa turvallisuusvaatimusmäärittelyssä huomioidaan tiedon luottamuksellisuuden ja eheyden lisäksi myös tiedon saatavuuteen liittyvät näkökulmat. Vastaavasti kuin kansallisen ja EU:n turvallisuusluokitellulle tiedolle, vaatimusten täyttämässä on rajallinen mahdollisuus hyödyntää myös korvaavia suojauksia tilanteissa, joissa ne ovat riskienhallinnallisesti perusteltuja. Esimerkiksi tietojärjestelmään kohdistuva vaatimus vahvasta, useaan todennustekijään pohjautuvasta tunnistautumisesta voi joissain ympäristöissä olla toteutettavissa myös fyysisen turvallisuuden menettelyin. Naton turvallisuusluokitellun tiedon suojaamiseen liittyvien vaatimusten koostumista on havainnollistettu kuvassa 2.



Kuva 2. Vaatimusten koostuminen

Lähestymistapa tekniseen tietoturvaluuteen

Kansallinen, EU:n ja Naton lähestymistapa tekniseen tietoturvaluuteen on pääosin yhtenevä. Suojaukset pohjautuvat muun muassa monitasoiseen suojaamiseen, vähimpien oikeuksien periaatteeseen, hyökkäyspinta-alan minimointiin sekä kykyyn havaita ja myös sietää erilaisia häiriötilanteita. Naton turvallisuusluokitellun tiedon suojaamisessa painottuu lisäksi tietojärjestelmän kyvykyys suojata itse itseään, mikä tukee myös eri tietojärjestelmien turvallista yhteenliittämistä. Naton turvallisuusluokitellun tiedon suojaamisessa korostuu myös tietojärjestelmän laitteisto- ja ohjelmistokirjanpidon sekä esimerkiksi konfiguraation- ja päivitystenhallinnan roolit koko tietojärjestelmän elinkaaren ajan. Naton turvallisuusluokitellun tiedon suojaamiseen kohdistuu lisäksi lukuisia määriä yksityiskohtaisia vaatimuksia, kattaen sekä teknisen toteutustavan että hallinnointikäytäntöjen järjestämisen. Nämä yksityiskohtaiset vaatimukset tulee huomioida hyväksyntäprosessissa osana järjestelmäkohtaista turvallisuusvaatimusmäärittelyä.

Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien suunnittelussa ja ylläpidossa painottuu myös roolien ja vastuiden selkeä määrittely. Esimerkiksi vastuut tietoturvaluuteen hallintajärjestelmään sisältyvän jatkuva-aikaisen riskienarvioinnin (vrt. osa-alue T) toteuttamisesta tulee olla selkeästi nimettyjä. Vastaavasti myös esimerkiksi tietojärjestelmäkohtaisen turvallisuusvastaavan roolin tulee olla selkeästi nimetty ja vastuutettu.

Hallintatoimien kerrosmalli

Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien teknisen ympäristön hallintatoimet jaetaan turvallisuuskriittisyyden mukaisesti kolmeen kerrokseen (tier). Kerrokseen 0 sisältyvät kaikkein turvallisuuskriittisimmät roolit ja toiminnot. Kerrokseen 0 sisältyy esimerkiksi hallintapääsy organisaation identiteetteihin, kuten domain admin -tunnukset Windows-ympäristöissä. Kerrokseen 1 sisältyy järjestelmän pääkäyttäjät, joilla on hallinnointimahdollisuudet tietojärjestelmän palvelimiin, ohjelmistoihin ja verkkolaitteisiin. Kerroksen 1 oikeuksiin voi sisältyä esimerkiksi rajatut oikeudet palvelinten käyttöjärjestelmiin, verkkolaitteisiin ja ohjelmistoihin. Kerrokseen 2 sisältyvät tiukemmin rajatut pääkäyttäjäoikeudet työasemiin ja laitteisiin, esimerkiksi organisaation päätelaitteiden lähituki.

Eri kerrosten toimenpiteiden ja oikeuksien ei tule sekoittua, vaan ne tulee rajata kyseisen kerroksen hallintatoimiin. Tämä voidaan toteuttaa esimerkiksi siten, että kerrosten 0 ja 1 hallintatoimet rajataan toteutettavaksi vain kyseiselle kerrokselle ja vain kyseiseen käyttöön varattuun, muista verkoista eristettyyn verkkoon. Lisäksi tulee huomioida, että kerrosten 0 ja 1 työasemien tulee olla vain kyseisen kerroksen hallintatoimenpiteisiin rajattuja, kovennettuja ja valvottuja laitteita. Kerroksellisuus tulee huomioida myös käyttäjätunnuksissa siten, että hallintatoimiin käytettävät tunnukset rajataan kerroksittain. Yhden kerroksen hallintatunnuksen käyttö tuleekin rajata vain kyseisen kerroksen hallintatoimiin.

PKI-infrastruktuurin suojaaminen

PKI-infrastruktuurin kohdistuvat vaatimukset ovat linjassa Katakri 2020:ssa kuvattujen kanssa. Koska Katakri 2020 ei kuitenkaan ota teknologiatasolla asiaan erikseen kantaa, kuvataan tässä luvussa keskeiset teknologiatason periaatteet, painottuen PKI-infrastruktuurin suojaamiseen. PKI:hin kohdistuvat vaatimukset riippuvat siitä, mihin PKI:ta hyödynnetään kyseisessä tietojärjestelmässä. PKI:ta voidaan hyödyntää korkeaa luotettavuutta edellyttäviin tarpeisiin, esimerkiksi Internetin yli tapahtuvan liikennöinnin salausavainten luontiin. PKI:ta voidaan toisaalta hyödyntää esimerkiksi käyttäjätunnistukseen tai laitevarmenteisiin. PKI-infrastruktuuriin liittyvien varmenteiden osalta on varmistuttava niiden oikeellisuudesta ja luotettavuudesta.

Automaatiojärjestelmät

Naton turvallisuusluokitellun tiedon suojaamisessa tulee tunnistaa tilanteet, joissa automaatiojärjestelmillä (control systems) voi olla vaikutusta tietojen suojaamiseen suoraan tai epäsuoraan. Tietojen suojaamisessa tulee huomioida erityisesti järjestelmäkomponentit, jotka tai joiden kautta voi olla mahdollisuus vaikuttaa fyysisen turvallisuuden suojauksiin. Tietojärjestelmässä käsiteltävien turvallisuusluokiteltujen tietojen korkeimman luokan suojausvaatimuksia tulee tällaisissa tilanteissa ulottaa myös automaatiojärjestelmiin. Erityistä huomiota tulee kiinnittää automaatiojärjestelmien ja turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien eriyttämiseen. On myös tilanteita, joissa automaatiojärjestelmällä on tarve käsitellä turvallisuusluokiteltua tietoa. Automaatiojärjestelmiin kohdistuu myös erityisuhkia, erityisesti ylläpitotoimintojen myötä. Nämä seikat tulee ottaa huomioon automaatiojärjestelmien suojauksissa.

Täydennykset teknisen tietoturvallisuuden vaatimuskortteihin

Tässä luvussa eritellään keskeisimmät täydennykset ja tarkennukset Katakri 2020:n teknisen tietoturvallisuuden osa-alueeseen koottuihin vaatimuksiin. Täydennykset ja tarkennukset pohjautuvat Naton turvasääntöön ja erityisesti sen teknisen tietojärjestelmäturvallisuuden määrittelyyn. Erittelyssä ei ole toistettu sellaisia Naton turvallisuusluokiteltua tietoa kohdistuvia suojausvaatimuksia, jotka on jo kuvattu Katakri 2020:n vaatimus- tai

toteutusmerkintäkentissä. Muutokset kuvataan ylätasolla. Yksityiskohtaiset, järjestelmäkohtaiset vaatimukset asetetaan hyväksymisprosessissa osana järjestelmäkohtaista turvallisuusvaatimusmäärittelyä.

I-01 - Verkon rakenteellinen turvallisuus

Verkon rakenteelliseen turvallisuuteen liittyvät vaatimukset ovat pääpiirteittäin yhteneväiset. Keskeiset yhdyskäytäväratkaisuille edellytettävät tekniset suojaukset ovat linjassa Katakriissa viitatus, Kyberturvallisuuskeskuksen julkaiseman yhdyskäytäväratkaisuohjeen kanssa. Termistön osalta tulee kuitenkin huomioida, että sekä EU:n että Naton säädöksissä käytetään samansuuntaista termiä kuvaamaan kaikkia eri turvallisuusluokkien välisiä yhdyskäytäväratkaisuja, vaikka kansallisessa termistössä "hyväksyttyä yhdyskäytäväratkaisua" käytetäänkin yleensä vasta turvallisuusluokasta III lähtien.

Naton turvallisuusluokitellun tiedon suojaamisessa tulee huomioida, että kaikkien eri turvallisuusluokkien välisiin yhdyskäytäväratkaisuihin sovelletaan esimerkiksi vikaturvallisuuteen ja käynnistyksen aikaiseen eheyteen liittyviä suojausvaatimuksia. Tämän lisäksi on rajoitettu, millaisia laitteita voi käyttää verkkolaitteina. Virtualisoiuihin ympäristöihin kohdistuu selkeitä teknologiaperustaisia tarkennuksia esimerkiksi fyysisestä erottelusta. Verkon rakenteen osalta on lisäksi huomioitava mahdolliset järjestelmäkohtaiset saatavuusvaatimukset, jotka saattavat edellyttää yhteyksien kahdennuksia tai kuormanjakotoiminnallisuuden toteuttamista. Vrt. myös edellä kuvattu hallintatoimien kerrosmalli, jossa kerrosten 0 ja 1 erotteluun voidaan hyödyntää myös yhdyskäytäväratkaisujen mukaisia teknisiä toteutuksia.

I-02 - Tietoliikenneverkon vyöhykkeistäminen ja suodatussäännöt ko. turvallisuusluokan sisällä

Vyöhykkeistämiseen ja suodatussäännöksiin kohdistuu erityisesti teknologiavalintaan liittyviä tarkennuksia. Nämä koskevat esimerkiksi virtualisoiuja ympäristöjä sekä tekniikoita, kuten nimipalvelut (DNS, Domain Name System) ja IP-puhe (VoIP, Voice over Internet Protocol). Lisäsuojaustarpeet liittyvät erityisesti näiden palveluiden erotteluun ja turvalliseen konfiguraatioon, mitkä tulee huomioida järjestelmäkohtaisessa turvallisuusvaatimusmäärittelyssä.

Kantaa otetaan myös väliverkkoihin (DMZ, demilitarized zone), joita edellytetään palveluille, joihin kohdistuu esimerkiksi muista tietojärjestelmistä tulevia uhkia. Esimerkkinä tästä on muille tietojärjestelmille tarjotut palvelut. Yleisesti tietojärjestelmien väliseen liikenteeseen on kohdistettava analysointityyppistä tarkastelua, niin tulevan kuin lähtevän liikenteen osalta muun muassa haittaohjelmien, virheellisten pakettien tai hajautettujen palvelunestohyökkäysten (DDoS, Distributed Denial of Service) hyökkäysten riskien minimoimiseksi.

I-03 - Suodatus- ja valvontajärjestelmien hallinnointi

Suodatus- ja valvontajärjestelmien hallinnointiin ei tule oleellisia muutoksia.

I-04 - Hallintayhteydet

Hallintayhteyksiin ei tule oleellisia muutoksia.

I-05 - Langaton tiedonsiirto

Langattomaan tiedonsiirtoon ei tule oleellisia muutoksia. Yleisellä tasolla langattomien verkkojen turvallisesta konfiguraatiosta ja minimoidusta kuuluvuudesta on huolehdittava.

I-06 - Pääsyoikeuksien hallinnointi

Pääsyoikeuksien hallinnointiin kohdistuvat muutokset ovat enimmäkseen tarkentavia. Häätätilanteisiin liittyvien pääkäyttäjätunnuksien suojaamiseen on annettu valmiita ratkaisuehdotuksia. Nämä erityistapauksissa käytettävät pääkäyttäjätunnukset voidaan säilyttää esimerkiksi soveltuvaksi arvioidussa säilytysratkaisussa sinetöidyssä kuoressa/pussissa tai vastaavalla menettelyllä.

Kerrosmallin osalta huomioitavaa on paikallisten pääkäyttäjätunnusten rajoitukset eri kerroksilla. Lisäksi tulee huomioida, että pääkäyttäjien turvallisuusselvitystodistuksen (PSC, Personnel Security Clearance) tason tulee lähtökohtaisesti olla korkeampi kuin järjestelmässä käsiteltävän tiedon luokka. Yksityiskohtaiset määritykset kootaan järjestelmäkohtaiseen turvallisuusvaatimusmäärittelyyn.

Hallinnointikäytäntöjen on mahdollistettava se, että on täsmällisesti tiedossa resurssit, joihin kullakin käyttäjällä on pääsy, ja tämä tulee olla yksikäsitteisesti selvitettävissä kirjanpidosta. Lisäksi tietojärjestelmien käyttäjiin ja korotettuihin käyttäjätunnuksiin kohdistuu muodollisia hyväksyntävaatimuksia muun muassa käytäntöihin sitoutumisen ja vastuiden hyväksynnän osalta.

I-07 - Tietojenkäsittely-ympäristön toimijoiden tunnistaminen fyysisesti suojatun turvallisuusalueen sisällä

Tietojenkäsittely-ympäristön toimijoiden tunnistamiseen kohdistuu lukuisia yksityiskohtaisia määrityksiä, kun taas Katakri 2020 lähestyy asiaa korkeamman abstraktiotason tavoitteiden näkökulmasta. Vahvaa, vähintään kahteen todennustekijään pohjautuvaa tunnistautumista edellytetään lähtökohtaisesti kaikkeen tietojenkäsittelyyn. Kerrosmallin osalta on huomioitava, että tunnukset täytyy eriyttää kerroksittain. Siten järjestelmän ylläpitäjille saattaa olla tarvetta luoda kerroskohtaisia eli useita erillisiä ja eriytettyjä tunnuksia. Yksityiskohtaiset, järjestelmäkohtaiset vaatimukset asetetaan osana järjestelmäkohtaista turvallisuusvaatimusmäärittelyä.

I-08 - Järjestelmäkovenus

Järjestelmäkovenukseen ei kohdistu suuria eroavaisuuksia, vain yksittäisiä teknologiakohtaisia tarkennuksia. Olemassa olevia teknologioita tulee hyödyntää siten, että hyökkäyspinta-ala saadaan pidettyä mahdollisimman pienenä ja että teknologian tarjoamia turvallisuusominaisuuksia hyödynnetään soveltuvien osin. Tämä näkyy esimerkiksi turvallisen käynnistyksen (secure boot) käyttövaatimuksena sekä tunnussäilöjen ja mekanismien (credential stores and mechanisms) kovennusvaatimuksena. Kantaa otetaan myös esimerkiksi virtuaalikoneiden mallipohjien (template) sekä tallennusverkkoympäristöjen (SAN, Storage Area Network) suojaamiseen. Kovennustoteutuksissa käsitellään myös ohjelmistojen eheydestä ja autenttisuudesta varmistumista, suorituksen rajoittamista unohtamatta. Kantaa otetaan myös turvallisuusluokitellun tiedon käsittelyyn sekä käsittelyn suojaamiseen käytettävien käyttöjärjestelmien hyväksymiseen.

I-09 - Haittaohjelmasuojaus

Haittaohjelmasuojaukseen kohdistuu kattavampi lähestymistapa, jossa korostetaan muun muassa tallennusmedioiden käsittelyä. Haittaohjelmasuojaukselta edellytetään useaan menetelmään perustuvaa lähestymistapaa, kattaen esimerkiksi tunnistepohjaisen tarkastelun, heuristiikan ja käyttäytymiseen pohjautuvan havainnoinnin. Määrityksissä otetaan kantaa myös tallennusmedioiden käytön tekniseen rajoittamiseen kaikkien turvallisuusluokkien ympäristöissä.

I-10 - Turvallisuuteen liittyvien tapahtumien jäljitettävyys

Jäljitettävyuden toteuttamiseen kohdistuu yksittäisiä täydennyksiä. Kerättävien tallenteiden (lokietojen) tietosisältöön kohdistuu määrittäviä, erityisesti käyttäjiin ja käyttäjätunnuksiin liittyen. Samalla turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellojen tulee olla synkronoituja sovitun ajanlähteen kanssa kaikkien turvallisuusluokkien ympäristöissä. Määrittämissä käsitellään myös jäljitettävyuden toimivuutta ja lokietojen kertymisen teknistä valvontaa ja hälytyksiä. Myös lokietojen tallennukseen käytettävän tilan riittävydestä varmistuminen huomioidaan määrittämissä.

I-11 - Poikkeamien havainnointikyky ja toipuminen

Poikkeamien havainnointikykyyn kohdistuu osin merkittäviäkin täydentäviä määrittäviä. Määrittämissä käsitellään esimerkiksi kattavien havainnointipalvelujen roolia, painottuen erityisesti verkon ulkoreunan liikennöinnistä sekä korotettujen käyttäjätunnusten käytöstä tehtyihin havaintoihin. Tunkeutumisen estämiseen ja havainnointiin käytettäviin järjestelmiin kohdistuu tarkennuksia hälytysten automatisoinnista.

Kantaa otetaan myös poikkeamien selvittämisen edellyttämiin tarpeisiin. Määrittäykset huomioivat myös tietojärjestelmään ja siinä käsiteltäviin tietoihin liittyvien uhkien seurannan ja analysoinnin. Jäljitettävyuden ja jatkuvan valvonnan prosessien tulee olla myös dokumentoituja.

I-12 - Salausratkaisut

Salausratkaisuihin ei kohdistu oleellisia lisätarpeita. Tulee kuitenkin huomioida, että Naton turvallisuusluokitellun tiedon suojaamisessa tulee käyttää Naton turvallisuusluokitellun tiedon suojaamiseen hyväksytyjä salausratkaisuja.

I-13 - Ohjelmistojen suojaaminen verkkohyökkäyksiltä

Ohjelmistojen suojaamiseen liittyvät vaatimukset ovat pääpiirteittäin yhteneväiset. Tulee kuitenkin huomioida, että Naton turvallisuusluokiteltua tietoa käsitteleviin ympäristöihin on mahdollista tuoda vain testattuja tai erikseen hyväksytyjä ohjelmistoja.

I-14 - Hajasäteily (TEMPEST) ja elektroninen tiedustelu

Hajasäteily suojausten osalta tulee noudattaa Naton vaatimuksia, jotka ovat valtaosin yhdenmukaisia esimerkiksi EU:n turvallisuusluokiteltuun tietoon kohdistuvien suojausvaatimusten kanssa⁴.

I-15 - Tiedon sähköinen välitys

Tiedon sähköiseen välitykseen liittyvät vaatimukset ovat pääpiirteittäin yhteneväiset. Määrittämissä otetaan lisäksi kantaa tietojen menetyksen ehkäisyyn (DLP, Data Loss Prevention) käytettäviin menettelyihin.

I-16 - Muutoshallintamenettelyt

Muutoshallintamenettelyihin kohdistuu tarkennettuja vaatimuksia erityisesti konfiguraationhallinnan näkökulmasta. Pohjakonfiguraatioihin (baseline configuration) liittyvät vaatimukset on syytä huomioida erityisesti järjestelmäkovennoissa.

⁴ Lisätietoa: Kyberturvallisuuskeskus. 2022. Kansallinen TEMPEST-ohje. URL:

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Kansallinen_TEMPEST-ohje_20220705.pdf.

Tarkennetut vaatimukset ottavat kantaa muun muassa pohjakonfiguraation määrittämiseen ja sen luotettavaan ylläpitoon koko tietojärjestelmän elinkaaren ajan. Muutoshallintaan kohdistuu myös muodollisia tarkennuksia, joissa otetaan kantaa esimerkiksi turvallisuusvaikutusanalyysin rooliin tavanomaisten muutoshallintatoimenpiteiden osana.

Kantaa otetaan myös tietojenkäsittely-ympäristöön tuotavien uusien tai muutettujen laitteistojen tarkastusprosessiin. Määritykset huomioivat myös dokumentoituidut konfiguraation hallinnan menettelyt, sisältäen kiireellisten muutosten toteuttamisen.

I-17 - Fyysinen turvallisuus

Fyysiseen turvallisuuteen liittyvät eroavat vaatimukset on kuvattu tämän liitteen fyysisen turvallisuuden osa-alueessa. Naton turvallisuusluokitellun tiedon sähköisen käsittelyn osalta keskeisenä eroavaisuutena on se, että säilytyksen lisäksi myös tiedon käsittely on NATO CONFIDENTIAL -luokasta lähtien rajattava turva-alueelle. Tallennusmedioihin ja turvallisuusluokiteltua aineistoa käsitteleviin laitteistoihin kohdistuu lisäksi useampi tarkennus, jotka koskevat muun muassa turvallisuusluokamerkintöjä ja rekisteröintiä. Pääsynhallinnassa tulee huomioida myös hallintatoimien kerrosmalli siten, että esimerkiksi kerroksen 0 palvelimiin ei ole fyysistä pääsyä muilla kuin kyseisen hallintakerroksen ylläpitohenkilöstöllä.

I-18 - Etäkäyttö ja etähallinta

Etäkäyttöön liittyvät vaatimukset ovat pääpiirteittäin yhteneväiset, kattaen kuitenkin muutaman yksityiskohtaisemman tarkennuksen. Määritykset ottavat kantaa esimerkiksi etäkäytön sitomiseen valvottuihin pisteisiin, sekä tarvittaviin toimenpiteisiin yhteyksien hallinnassa ja valvonnassa. Etäkäytössä tulee myös huomioida tämän liitteen kohdassa F-04 käsitelty tilapäisen hallinnollisen alueen perustamistarve.

I-19 - Ohjelmistohaavoittuvuuksien hallinta

Ohjelmistohaavoittuvuuksien hallintaan kohdistuvat vaatimukset ovat pääpiirteittäin yhteneviä, mutta Naton turvallisuusluokitellun tiedon käsittelyyn kohdistuu muutama tarkennus. Määritykset ottavat kantaa esimerkiksi siihen, millaisilla aikaviiveillä eroavien kriittisyysasteiden turvallisuuspäivitykset tulee asentaa.

I-20 - Varmuuskopiointi

Varmuuskopiointiin kohdistuvat vaatimukset ovat pääpiirteittäin yhteneviä.

I-21 - Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoaminen

Sähköisessä muodossa olevien turvallisuusluokiteltujen tietojen tuhoamisen vaatimukset ovat pääpiirteittäin yhteneviä. NATO CONFIDENTIAL -luokan tietojen tuhoamisesta ei kuitenkaan tarvitse laatia tuhoamistodistusta. Rekisterimerkintä tietojen tuhoamisesta on riittävä.