Euroopan unionin
virallinen lehti

FI
C-sarja

C/2026/6013

17.11.2026

KOMISSION TIEDONANTO

Komission ohjeet asetuksen (EU) 2024/2847 (kyberkestävyyssäädös) soveltamisesta

(C/2026/6013)

Sisällys

Sivu

1. JOHDANTO 3
   - 1.1 Kyberkestävyyssäädös 3
   - 1.2 Ohjeiden tarkoitus 3
2. SOVELTAMISALA 4
   - 2.1 Markkinoille saattaminen 4
   - 2.2 Ohjelmisto digitaalisia elementtejä sisältävänä tuotteena 5
   - 2.3 Tietokonekoodi 6
   - 2.4 Laitteiston ja ohjelmiston yhdistelmä, joka on digitaalisia elementtejä sisältävä tuote 7
   - 2.5 Datayhteydet 8
   - 2.6 Kompleksiset järjestelmät 8
   - 2.7 Digitaalisia elementtejä sisältävät tuotteet, jotka on suunniteltu ennen kyberkestävyyssäädöksen soveltamisen aloittamista 9
3. VAPAA JA AVOIMEN LÄHDEKOODIN OHJELMISTO 11
   - 3.1 Sen määrittäminen, kuuluuko vapaa ja avoimen lähdekoodin ohjelmisto tietyn toimijan vastuulle 12
   - 3.2 Sen määrittäminen, onko vapaa ja avoimen lähdekoodin ohjelmisto saatettu EU:n markkinoille 13
     - 3.2.1 Hinnan periminen 13
     - 3.2.2 Tulon saaminen muista palveluista tai vaatimus henkilötietojen käsittelystä 13
     - 3.2.3 Tukipalvelut 14
     - 3.2.4 Lahjoitukset 15
     - 3.2.5 Vapaan ja avoimen lähdekoodin ohjelmiston rahoittaminen 15
     - 3.2.6 Voittoa tavoittelemattomat toimijat, jotka pyrkivät saavuttamaan voittoa tavoittelemattomaan toimintaan liittyviä tavoitteita 16
     - 3.2.7 Integrointi muiden valmistajien toimesta 16
   - 3.3 Avoimen lähdekoodin ohjelmistovastaavat 16
     - 3.3.1 Pitkäjänteinen tuki ja VALOn toimintakelpoisuuden varmistaminen 17
   - 3.4 Osallistujat ja tuotantoketjun loppupään käyttö 18
   - 3.5 Havainnollistavat skenaariot 19
4. MERKITTÄVÄT MUUTOKSET JA VARAOSAT 21
   - 4.1 Fyysiset korjaukset 22
   - 4.2 Varaosat 23
   - 4.3 Ohjelmistopäivitykset merkittävänä muutoksena 24

4.4 Merkittävän muutoksen seuraukset 27
4.4.1 Muun kuin alkuperäisen valmistajan tekemät merkittävät muutokset 28
4.4.2 Alkuperäisen valmistajan tekemät merkittävät muutokset 29
5. TUKIAIKA 29
5.1 Merkittävät muutokset ja tukiaika 31
6. DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT TÄRKEÄT JA KRIITTISET TUOTTEET 32
6.1 Ydintoiminnot 33
6.2 Digitaalisia elementtejä sisältävien tärkeiden ja kriittisten tuotteiden vaatimustenmukaisuuden arviointi. 36
6.3 Vaikutukset vaatimustenmukaisuusolettamaan 38
7. KYBERTURVALLISUUSRISKIEN ARVIOINTI JA DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVIEN TUOTTEIDEN JA KOMPONENTTIEN INTEGROINTI 41
7.1 Kyberturvallisuusriskien arviointi ja käsittely 41
7.2 Digitaalisia elementtejä sisältävien tuotteiden suunnittelu, kehittäminen ja tuottaminen siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin 42
7.3 Riskien arviointi ja asianmukainen huolellisuus ulkoisten riippuvuuksien ja integroitujen komponenttien osalta 42
7.4 Riskien arviointien ja vaatimustenmukaisuusasiakirjojen uudelleenkäyttö digitaalisia elementtejä sisältävien tuoteperheiden osalta 44
8. DATAN ETÄKÄSITTELY 44
8.1 Mitä pidetään digitaalisia elementtejä sisältävän tuotteen datan etäkäsittelyratkaisuna? 45
8.1.1 Ilmaus ”etäältä” 46
8.1.2 Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan? 46
8.1.3 Onko ohjelmisto suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla? 47
8.2 Datan etäkäsittelyratkaisujen ja kolmannen osapuolen ratkaisuihin tukeutumisen käytännön vaikutukset ja tekniset vaikutukset 49
8.3 Datan etäkäsittelyratkaisujen käyttötapaukset 50
8.3.1 Mobiilipankkisovellus 51
8.3.2 Älytermostaatti 52
8.3.3 Sähköinen lukulaite 53
8.3.4 Teollisuusrobotti 53
8.3.5 Matkaviestinverkko 53
9. MUUT ELEMENTIT 54
9.1 Raportointivelvoitteet 54
9.2 Haavoittuvuuksien käsittely 56
9.2.1 Raportointi ketjun alkupäähän ja tietoturvakorjausten jakaminen 56
9.2.2 Tiedossa olevat hyödynnettävissä olevat haavoittuvuudet 57
9.2.3 Tehokkaat ja säännölliset testit ja arvioinnit 58
9.3 Vuorovaikutus muun lainsäädännön kanssa 59
9.3.1 Asetus (EU) 2019/2144 ja asetus (EU) N:o 168/2013 59
9.3.2 EU-tyyppitarkastustodistusten voimassaolo (69 artiklan 1 kohta) 59

1. **JOHDANTO**

1.1 **Kyberkestävyyssäädös**

1. Digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) N:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta 23. lokakuuta 2024 annettu Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847 ([1]), jäljempänä 'kyberkestävyyssäädös', tuli voimaan 10. joulukuuta 2024. Asetuksen tavoitteena on vahvistaa kyberturvallisuuteen liittyvää EU:n toimintamallia, käsitellä kyberkestävyyttä EU:n tasolla ja parantaa sisämarkkinoiden toimintaa vahvistamalla yhdenmukainen oikeudellinen kehys keskeisille kyberturvallisuusvaatimuksille, joita sovelletaan digitaalisia elementtejä sisältävien tuotteiden saattamiseen EU:n markkinoille sekä digitaalisia elementtejä sisältävien tuotteiden elinkaaren aikana.

2. Kyberkestävyyssäädös perustuu EU:n uuteen lainsäädäntökehykseen, joka on vahvistettu akkreditoinnin vaatimusten vahvistamisesta ja asetuksen (ETY) N:o 339/93 kumoamisesta 9. heinäkuuta 2008 annetussa Euroopan parlamentin ja neuvoston asetuksessa (EY) N:o 765/2008 tuotteiden kaupan pitämisen osalta ja tuotteiden kaupan pitämiseen liittyvistä yhteisistä puitteista ja päätöksen 93/465/ETY kumoamisesta 9. heinäkuuta 2008 tehdyssä Euroopan parlamentin ja neuvoston päätöksessä N:o 768/2008/EY ([2]).

3. Markkinavalvonnasta ja täytäntöönpanosta vastaavat kansalliset markkinavalvontaviranomaiset. Kyberkestävyyssäädöksen soveltamisalaan kuuluvat digitaalisia elementtejä sisältävät tuotteet kuuluvat markkinavalvonnasta ja tuotteiden vaatimustenmukaisuudesta sekä direktiivin 2004/42/EY ja asetusten (EY) N:o 765/2008 ja (EU) N:o 305/2011 muuttamisesta 20. kesäkuuta 2019 annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/1020 soveltamisalaan. Komissio ja Euroopan unionin kyberturvallisuusvirasto (ENISA) tukevat talouden toimijoita ja jäsenvaltioita kyberkestävyyssäädöksen soveltamisessa.

1.2 **Ohjeiden tarkoitus**

4. Kyberkestävyyssäädöksen 26 artiklan 1 kohdassa vaaditaan komissiota julkaisemaan ohjeita, joilla autetaan talouden toimijoita soveltamaan kyseistä asetusta ja joilla pyritään erityisesti tekemään sen noudattamisesta helpompaa mikroyrityksille sekä pienille ja keskisuurille yrityksille, jäljempänä 'pk-yritykset'. Saman 26 artiklan 2 kohdassa esitetään kyseisissä ohjeissa käsiteltävät vähimmäisnäkökohdat. Näihin kuuluvat seuraavat: i) kyberkestävyyssäädöksen soveltamisala (erityisesti datan etäkäsittelyratkaisut sekä vapaat ja avoimen lähdekoodin ohjelmistot); ii) tukiaikojen käsite; iii) kyberkestävyyssäädöksen ja EU:n muun lainsäädännön välinen vuorovaikutus; sekä iv) merkittävän muutoksen käsite.

5. Komissio julkaisi 3. joulukuuta 2025 usein kysyttyjä kysymyksiä, joiden tarkoituksena on auttaa talouden toimijoita valmistautumaan kyberkestävyyssäädöksen täytäntöönpanoon ([3]).

6. Näiden ohjeiden tarkoituksena on auttaa talouden toimijoita kyberkestävyyssäädöksen noudattamisessa ja tukea markkinavalvontaviranomaisten, ilmoittamisesta vastaavien viranomaisten ja ilmoitettujen laitosten toimintaa, jotta voidaan varmistaa kyberkestävyyssäädöksen yhdenmukainen täytäntöönpano kaikkialla unionissa. Ohjeiden tarkoituksena ei ole kattaa kyberkestävyyssäädöstä kokonaisuudessaan, vaan pikemminkin selventää tiettyjen keskeisten säännösten perusteita ja sitä, miten ne voidaan panna täytäntöön käytännössä. Ohjeet koskevat kyberkestävyyssäädöstä, eikä niitä sovelleta EU:n muuhun lainsäädäntöön.

([1]) EUVL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Komission vuoden 2026 työohjelmassa esitellään "eurooppalainen tuotesäädös", jolla saatetaan ajan tasalle uusi lainsäädäntökehys sekä markkinavalvontaa ja standardointia koskevat säännöt: https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:52025DC0870.

([3]) Usein kysytyt kysymykset ovat ladattavissa komission kyberkestävyyssäädöksen täytäntöönpanoa koskevan verkkosivuston asiaa koskevalta, usein kysyttyjä kysymyksiä koskevalta verkkosivulta.

7. Ohjeiden valmistelun yhteydessä kuultiin sidosryhmiä, muun muassa digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuutta käsittelevää asiantuntijaryhmää ([4]), laajasti, myös ajanjaksolla 3. maaliskuuta – 13. huhtikuuta 2026 järjestetyssä julkisessa kuulemisessa ([5]).

8. Ohjeet eivät sido talouden toimijoita tai muita kyberkestävyyssäädöksen alaisia toimijoita. Ainoastaan Euroopan unionin tuomioistuin voi antaa sitovia tulkintoja kyberkestävyyssäädöksestä. Ohjeissa esitetään kuitenkin komission tulkinta kyberkestävyyssäädöksestä asetuksen noudattamisen tukemiseksi ja sen tehokkaan täytäntöönpanon edistämiseksi. Lisäksi ohjeissa annetaan useita esimerkkejä, joilla havainnollistetaan yksittäisten säännösten soveltamista. Esimerkkien ei ole kuitenkaan tarkoitus korvata tapauskohtaista arviointia, joka on aina tarpeen kunkin yksittäisen tapauksen erityispiirteiden huomioimiseksi.

9. Kyberkestävyyssäädöksen 26 artiklan mukaisesti komissio voi harkita lisäohjeiden antamista, myös nimenomaisesti valmistajille, jotka kuuluvat kyberkestävyyssäädöksen ja unionin muun yhdenmukaistamislainsäädännön tai muiden asiaan liittyvien unionin säädösten soveltamisalaan. Ohjeissa voidaan käsitellä esimerkiksi kysymyksiä kyberkestävyyssäädöksen ja tekoälyä koskevista yhdenmukaistetuista säännöistä annetun asetuksen (EU) 2024/1689, jäljempänä ’tekoälysäädös’, ja finanssialan digitaalisesta häiriönsietokyvystä annetun asetuksen (EU) 2022/2554, jäljempänä ’DORA-asetus’, välisestä vuorovaikutuksesta.

2. **SOVELTAMISALA**

2.1 **Markkinoille saattaminen**

10. Kyberkestävyyssäädöstä sovelletaan digitaalisia elementtejä sisältäviin tuotteisiin, joita asetetaan saataville EU:n markkinoilla. Käsite ”asettaminen saataville markkinoilla” määritellään kyberkestävyyssäädöksen 3 artiklan 22 alakohdassa, jonka mukaan se tarkoittaa ”digitaalisia elementtejä sisältävän tuotteen toimittamista unionin markkinoille kaupallisen toiminnan yhteydessä jakelua tai käyttöä varten joko maksua vastaan tai maksutta”. Saman säädöksen 3 artiklan 21 alakohdan mukaisesti digitaalisia elementtejä sisältävä tuote saatetaan EU:n markkinoille, kun se asetetaan ensimmäistä kertaa saataville.

11. Vuonna 2022 julkaistussa EU:n tuotesääntöjen täytäntöönpanoa koskevassa sinisessä oppaassa ([6]), jäljempänä ’sininen opas’, annetaan ohjeita, joilla helpotetaan EU:n tuotesääntöjen ymmärtämistä ja niiden yhdenmukaista soveltamista eri alakohtaisissa oikeudellisissa kehyksissä, jotka on mukautettu uuteen lainsäädäntökehykseen, kuten kyberkestävyyssäädökseen. Sinisen oppaan mukaan ”markkinoille saattamisen” ja ”saataville asettamisen” käsitteet on ymmärrettävä viittauksiksi ”kuhunkin yksittäiseen tuotteeseen eikä tuotetyyppiin, riippumatta siitä, onko tuote valmistettu yksittäiskappaleena vai sarjatuotantona” (2.3 kohta).

12. Uuden lainsäädäntökehyksen soveltamisalaan kuuluvien ”perinteisempien” digitaalisia elementtejä sisältävien tuotteiden, kuten digitaalisia elementtejä sisältävien koneiden tai radiolaitteiden, osalta ”markkinoille saattamisen” käsite on vakiintunut, ja sinisessä oppaassa annetaan lisäselvennystä siitä, milloin tällaisten tuotteiden katsotaan olevan saatettuja markkinoille. Sinisen oppaan 2.12 kohdassa on lisää esimerkkejä ”markkinoille saattamisen” käsitteestä.

13. Digitaalisia elementtejä sisältävien aineettomien tuotteiden, kuten itsenäisen ohjelmiston, luonteen vuoksi tarvitaan kuitenkin lisää ohjeita siitä, milloin tällaisten digitaalisia elementtejä sisältävien tuotteiden katsotaan olevan saatettuja markkinoille. Kun ohjelmiston valmistusvaihe on saatu päätökseen ja digitaalisia elementtejä sisältävää tuotetta tarjotaan mahdollisille käyttäjille EU:n markkinoilla, tuotteen valmistajan voidaan katsoa valmistaneen useita kopioita samasta digitaalisia elementtejä sisältävästä ohjelmistotuotteesta ja toimittaneen ne jakelua tai käyttöä varten. Toisin kuin digitaalisia elementtejä sisältäviin konkreettisiin tuotteisiin, itsenäisiin ohjelmistoihin ei

([4]) Digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuutta käsittelevä asiantuntijaryhmä komission asiantuntijaryhmien ja muiden vastaavanlaisten elinten rekisterissä.
([5]) Julkinen kuuleminen kyberkestävyyssäädöstä koskevien komission ohjeiden luonnoksesta.
([6]) Komission tiedonanto: Sininen opas – EU:n tuotesääntöjen täytäntöönpano-opas 2022, 2022/C 247/01 (EUVL C 247, 29.6.2022, s. 1).

kohdistu fyysisiä tuotanto- tai varastorajoituksia: aina, kun ohjelmisto asetetaan saataville ladattavaksi tai jaettavaksi, ohjelmistosta luodaan uusi duplikaatti käyttäjälle. Niin kauan kuin tätä ohjelmistoversiota ei muuteta tavalla, joka vaikuttaa kyberkestävyyssäädöksen noudattamiseen, EU:n markkinoille saattamisen on katsottava tapahtuneen ensimmäisen jakeluun tai käyttöön tarjoamisen ajankohtana. Digitaalisia elementtejä sisältävän ohjelmistotuotteen kyseisen version myöhempää lataamis- tai jakelumahdollisuutta on sen vuoksi pidettävä tilanteena, jossa kyseinen digitaalisia elementtejä sisältävä ohjelmistotuote asetetaan saataville ([7]).

14. Näin ollen olisi katsottava, että digitaalisia elementtejä sisältävä itsenäinen ohjelmistotuote on saatettu markkinoille, kun sen valmistusvaihe on saatettu päätökseen ja kun ohjelmisto toimitetaan ensimmäisen kerran EU:n markkinoille jakelua tai käyttöä varten kaupallisen toiminnan yhteydessä. Olisi katsottava, että valmistaja on saattanut markkinoille useita kopioita samasta digitaalisia elementtejä sisältävästä ohjelmistotuotteesta samanaikaisesti. Vaikka siis saman ohjelmiston useat kopiot ovat digitaalisia elementtejä sisältäviä yksittäisiä tuotteita, katsotaan, että ne on saatettu markkinoille samanaikaisesti riippumatta siitä, milloin kunkin yksittäisen kopion hallussapito tai käyttö on siirretty toiselle luonnolliselle henkilölle tai oikeushenkilölle. Kun valmistaja vastaavasti asettaa saataville ohjelmiston eri variantteina, jotka eroavat ohjelmistoon sisältyvien osien, konfiguraatioiden tai käyttöön otettujen toimintojen osalta (esimerkiksi eri käyttöjärjestelmiin tarkoitetut versiot tai erilaisia ominaisuuksia käsittävät kokonaisuudet), näitä variantteja ei voida pitää saman digitaalisia elementtejä sisältävän ohjelmistotuotteen useina kopioina. Tämän takia niitä olisi pidettävä erillisinä digitaalisia elementtejä sisältävinä tuotteina markkinoille saattamisen kannalta.

Esimerkki 1: Yritys A toimittaa 1. tammikuuta 2028 ensimmäisen kerran jakeluun ohjelmistonsa X version 1.0.0 verkkosivustollaan. Samana päivänä asiakas 1 ostaa kopion ohjelmiston X versiosta 1.0.0. Asiakas 2 ostaa 15. tammikuuta 2028 kopion ohjelmiston X versiosta 1.0.0. Molemmat ohjelmiston X version 1.0.0 kopiot on saatettu markkinoille 1. tammikuuta 2028.

15. Koska ohjelmistokehitys on luonteeltaan iteratiivista, olisi vielä selvennettävä, että digitaalisia elementtejä sisältävän ohjelmistotuotteen myöhempiä iteraatioita pidetään uusina markkinoille saatettuina tuotteina, jos kyseiset iteraatiot katsotaan jo markkinoille saatetun digitaalisia elementtejä sisältävän ohjelmistotuotteen ”merkittäväksi muutokseksi”, kuten kyberkestävyyssäädöksen johdanto-osan 41 kappaleessa todetaan. Iteraatiot, joita ei pidetä merkittävinä muutoksina, eivät edellytä valmistajalta uuden vaatimustenmukaisuuden arviointimenettelyn suorittamista, eikä kyseisen ohjelmiston markkinoille saattamisen ajankohta näin ollen muutu. Merkittävien muutosten käsitteestä annetaan lisätietoja jaksossa *4 Merkittävät muutokset*.

Esimerkki 2: Yritys A toimittaa 1. tammikuuta 2028 ensimmäisen kerran jakeluun ohjelmiston X version 1.0.0 verkkosivustollaan. Asiakas 1 ostaa samana päivänä kopion ohjelmiston X versiosta 1.0.0. Yritys A julkaisee 15. tammikuuta 2028 ohjelmiston X päivitetyn version 1.0.1, jota ei katsota merkittäväksi muutokseksi. Asiakas 2 ostaa 30. tammikuuta 2028 kopion ohjelmiston X versiosta 1.0.1. Ohjelmiston X versioiden 1.0.0 ja 1.0.1 molemmat kopiot katsotaan saatetuiksi markkinoille 1. tammikuuta 2028.

16. Edellä kohdissa 13, 14 ja 15 annettuja ohjeita sovelletaan ainoastaan siltä osin kuin digitaalisia elementtejä sisältävä tuote on itsenäinen ohjelmisto. Näin ei ole esimerkiksi silloin, kun ohjelmisto on yhdistetty laitteistoon, mitä käsitellään jaksossa *2.4 Laitteiston ja ohjelmiston yhdistelmä, joka on digitaalisia* elementtejä sisältävä tuote.

2.2 **Ohjelmisto digitaalisia elementtejä sisältävänä tuotteena**

17. Kyberkestävyyssäädöksen 3 artiklan 1 alakohdassa määritellään, että digitaalisia elementtejä sisältävällä tuotteella tarkoitetaan ”ohjelmisto- tai laitteistotuotetta ja sen ratkaisuja datan etäkäsittelystä, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit”. Tällaiset digitaalisia elementtejä sisältävät tuotteet kuuluvat kyberkestävyyssäädöksen soveltamisalaan, jos niiden käyttötarkoitukseen tai kohtuudella ennakoitavissa olevaan käyttöön sisältyy suora tai epäsuora looginen tai fyysinen tietoyhteys laitteeseen tai verkkoon.

([7]) Asetuksen 13 artiklan 11 kohdan mukaisesti valmistajat voivat ylläpitää julkisia ohjelmistoarkistoja, joilla parannetaan käyttäjien mahdollisuuksia käyttää aiempia versioita. Tällaisissa tapauksissa käyttäjille on tiedotettava selkeästi ja helposti saatavilla olevalla tavalla riskeistä, jotka liittyvät sellaisten ohjelmistojen käyttöön, joita ei tueta.

18. Tämän takia kyberkestävyyssäädös voi kattaa monenlaisia digitaalisia elementtejä sisältäviä tuotteita, kuten i) itsenäiset ohjelmistot, kuten sovellukset ja tietokoneohjelmat, riippumatta siitä, jaetaanko niitä digitaalisesti vai fyysisesti, ii) laitteistot, joissa on sisäänrakennettu ohjelmisto (esim. esineiden internetin laitteet, kannettavat tietokoneet, taulutietokoneet), iii) itsenäiset laitteet (esim. integroidut piirit, emolevyt) ja iv) laitteistojen ja ohjelmistojen yhdistelmät, jotka toimitetaan erikseen mutta jotka on tarkoitettu toimimaan yhdessä.

19. Itsenäinen ohjelmisto kuuluu näin ollen kyberkestävyyssäädöksen soveltamisalaan, kun se saatetaan markkinoille digitaalisia elementtejä sisältävänä tuotteena. On hyödyllistä erottaa toisistaan digitaalisia elementtejä sisältävät ohjelmistotuotteet, jotka kuuluvat kyberkestävyyssäädöksen soveltamisalaan, ja kyberkestävyyssäädöksen soveltamisalan ulkopuolinen palvelujen etätarjonta.

20. Jotta ohjelmisto kuuluisi kyberkestävyyssäädöksen soveltamisalaan, digitaalisia elementtejä sisältävä ohjelmistotuote on toimitettava käyttäjälle, kyseisen käyttäjän on hankittava se ja käytettävä sitä käyttäjän sähköisessä tietojärjestelmässä tai sen osana. Ohjelmisto, joka ladataan, asennetaan tai toimitetaan muulla tavoin käyttäjälle ja joka suoritetaan käyttäjän sähköisessä tietojärjestelmässä, täyttää nämä vaatimukset myös silloin, kun kyse on esimerkiksi selainlaajennuksesta tai sovelluksesta, joka on kehitetty verkkoteknologiaa käyttäen mutta joka toimitetaan paikalliseen käyttöön.

21. Sitä vastoin ohjelmisto, joka suoritetaan etänä ja joita käyttäjä vain käyttää, ei ole pelkästään näillä perusteilla digitaalisia elementtejä sisältävä tuote. Kyberkestävyyssäädöksen johdanto-osan 11 ja 12 kappaleessa tehdään tämä ero selittämällä, että etäkäsittelyyn tai -tallennukseen sovelletaan kyberkestävyyssäädöstä vain sikäli kuin se on välttämätöntä, jotta digitaalisia elementtejä sisältävä tuote voi suorittaa toimintonsa (eli 3 artiklan 2 alakohdassa määritellyn käsitteen, datan etäkäsittelyn, avulla), eikä kyse ole itse digitaalisia elementtejä sisältävästä tuotteesta. Näin on tavanomaisesti verkkosovellusten, myös edistyksellisten verkkosovellusten, tapauksessa, jos niitä käytetään yksinomaan verkkoselaimen kautta. Sama koskee verkkosivustoja: vaikka verkkosivustojen tekninen toiminta ja suorittaminen tapahtuvat vain rajoitetusti käyttäjän laitteella, kyberkestävyyssäädöksen johdanto-osan 12 kappaleesta seuraa, että verkkosivustoja ei itsessään pidetä digitaalisia elementtejä sisältävinä tuotteina ja että ne kuuluvat kyberkestävyyssäädöksen soveltamisalaan vain, jos ne tukevat jonkin digitaalisia elementtejä sisältävän tuotteen toimintoa, eli vain sikäli kuin niiden katsotaan olevan datan etäkäsittelyä (kuten selitetään tarkemmin jaksossa *8* ja erityisesti jaksossa *8.1.2 Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan?*).

Esimerkki 3: Käyttäjän älypuhelimeensa sovelluskaupasta lataama ja asentama mobiilisovellus toimitetaan käyttäjälle ja suorittamaan toimintoja käyttäjän laitteessa, joten se on digitaalisia elementtejä sisältävä tuote. Kun se saatetaan markkinoille kaupallisen toiminnan yhteydessä, se voi kuulua kyberkestävyyssäädöksen soveltamisalaan.

Esimerkki 4: Verkkoteknologioita käyttäen luotu mutta paikalliseen paikallisesti asennettavaksi pakattu työpöytäsovellus toimitetaan käyttäjälle ja suorittamaan toimintoja käyttäjän laitteessa, joten se on digitaalisia elementtejä sisältävä tuote. Kun se saatetaan markkinoille kaupallisen toiminnan yhteydessä, se voi kuulua kyberkestävyyssäädöksen soveltamisalaan.

Esimerkki 5: Käyttäjän ainoastaan verkkoselaimen kautta käyttämä verkkosovellus ei ole digitaalisia elementtejä sisältävä tuote. Jos se ei tue digitaalisia elementtejä sisältävän tuotteen toimintaa, se ei kuulu kyberkestävyyssäädöksen soveltamisalaan. Sen sijaan käyttäjälle paikallisesti asennettuna asiakassovelluksena toimitettu sovellus, joka suoritetaan käyttäjän laitteessa, on digitaalisia elementtejä sisältävä tuote. Kun se saatetaan markkinoille kaupallisen toiminnan yhteydessä, se voi kuulua kyberkestävyyssäädöksen soveltamisalaan.

Jos kyseinen asiakassovellus käyttää yhden tai useamman toimintansa suorittamiseksi datan etäkäsittelyä, joka vastaa datan etäkäsittelyn määritelmää, kyseinen datan etäkäsittely on myös osa digitaalisia elementtejä sisältävää tuotetta.

Esimerkki 6: Verkkosivusto, jolla ainoastaan annetaan tietoja kävijöille ja joka ei tue digitaalisia elementtejä sisältävän tuotteen toimintaa, ei ole itse digitaalisia elementtejä sisältävä tuote. Näin ollen se ei kuulu kyberkestävyyssäädöksen soveltamisalaan.

2.3 **Tietokonekoodi**

22. On hyödyllistä selventää myös, voiko lähdekoodi olla digitaalisia elementtejä sisältävä tuote. Kyberkestävyyssäädöksessä määritellään, että ohjelmistolla tarkoitetaan ”sitä sähköisen tietojärjestelmän osaa, joka koostuu tietokonekoodista” (3 artiklan 4 alakohta). Tietokonekoodi voi olla muodoltaan i) konekoodi, joka on tietokoneen suorittimen suoraan suorittamien ohjeiden sarja, joka on kirjoitettu binäärimuodossa, tai ii) lähdekoodi eli ohjelmointikielellä kirjoitettujen ohjeiden ja väittämien sarja, joka on koottava tai tulkittava tietokoneella suorittamista varten. Kyberkestävyyssäädöksessä vahvistettu ohjelmiston määritelmä kattaa molemmat.

23. Toinen kysymys on, onko tietty tietokonekoodin toimitus digitaalisia elementtejä sisältävän tuotteen saattamista EU:n markkinoille, mikä edellyttää toimitusta kaupallisen toiminnan yhteydessä. Näin ei ole useinkaan lähdekoodin tapauksessa. Esimerkiksi luonnollisen henkilön tai oikeushenkilön, joka jakaa vapaaseen ja avoimeen lähdekoodiin perustuvan tietokonekoodin julkisesti saatavilla olevissa tietokannoissa, ei yleensä katsota saattavan kyseistä koodia EU:n markkinoille kyberkestävyyssäädöksen mukaan (ks. tarkemmat tiedot jaksosta *3 Vapaa ja avoimen lähdekoodin* ohjelmisto). Myöskään digitaalisia elementtejä sisältävän tuotteen suunnittelu- ja kehitysvaiheen aikana (esimerkiksi testausta tai tarkistusta varten) jaettua keskeneräistä koodia ei pidetä markkinoille saatettuna kyberkestävyyssäädöksen mukaan, koska koodin valmistusvaihetta ei ole saatettu päätökseen. Vastaavasti opetusohjelmien tai koulutusmateriaalien osana toimitettua näyte- tai esittelykoodia ei pidetä markkinoille saatettuna kyberkestävyyssäädöksen mukaan ([8]).

24. Jos valmistaja toisaalta toimittaa asiakkailleen tietokonekoodin digitaalisia elementtejä sisältävänä tuotteena, kyseistä koodia pidetään markkinoille saatettuna riippumatta siitä, onko se konekoodi vai lähdekoodi ([9]).

Esimerkki 7: Yritys A myöntää yritykselle B lähdekoodin lisenssin mukautettavaa sisäistä alustaa varten ja antaa kyseisen lähdekoodin tekstitiedostossa. Vaikka lähdekoodia on mukautettava ja koostettava lisää yrityksessä B ennen koodin käyttöä, yritys A saattaa kyseisen lähdekoodin markkinoille ja on siksi kyberkestävyyssäädöksen alainen. Yritys A ei vastaa siitä, ovatko yrityksen B myöhemmät koodin mukautukset ja koostamiset kyberkestävyyssäädöksen mukaisia.

2.4 **Laitteiston ja ohjelmiston yhdistelmä, joka on digitaalisia elementtejä sisältävä tuote**

25. Kun määritetään, onko ohjelmisto osa digitaalisia elementtejä sisältävää tuotetta, ei perustana pitäisi pitää sitä, miten tai milloin ohjelmisto on toimitettu käyttäjälle, vaan sitä, onko ohjelmisto välttämätön digitaalisia elementtejä sisältävän tuotteen aiottujen toimintojen suorittamiseksi tuotteen käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön perusteella. Jos digitaalisia elementtejä sisältävä laitteistotuote on suunniteltu toimimaan yhdessä saman valmistajan toimittaman tietyn ohjelmiston kanssa toiminnan suorittamiseksi, laitteisto ja kyseinen ohjelmisto muodostavat yhdessä digitaalisia elementtejä sisältävän tuotteen. Ohjelmisto, joka on välttämätön digitaalisia elementtejä sisältävän tuotteen toimintaa, asetusten määrittämistä, hallintaa tai käyttämistä varten käyttötarkoituksensa mukaisesti, on siksi osa digitaalisia elementtejä sisältävää tuotetta, vaikka se olisi hankittu erillisen kanavan kautta (esim. sovelluskauppa, latauslinkki tai muu digitaalinen kanava sen jälkeen, kun digitaalisia elementtejä sisältävä laitteistotuote on saatettu markkinoille). Sen markkinoille saattaminen tapahtuu näin ollen samaan aikaan kuin digitaalisia elementtejä sisältävien laitteistotuotteiden yksikköjen markkinoille saattaminen.

Esimerkki 8: Verkkotulostin saatetaan markkinoille digitaalisia elementtejä sisältävänä laitteistotuotteena, kun taas tulostustöiden lähettämiseen, laitteen asetusten määrittämiseen ja laitteen toiminnan hallintaan tarvittavat ohjelmistoajurit on asetettu saataville ladattaviksi valmistajan verkkosivustolta. Vaikka tulostin ja ajurit toimitetaan eri kanavien kautta, ne muodostavat yhdessä yhden digitaalisia elementtejä sisältävän tuotteen, koska tulostin ei pysty täyttämään käyttötarkoitustaan ilman ajureita.

Esimerkki 9: Markkinoille saatetaan kuntoiluun tarkoitettu puettava laite käyttäjän sydämen sykkeen ja aktiivisuuden mittaamiseksi, kun taas valmistajan toimittamaa älypuhelinsovellusta tarvitaan mittausten ja aiempien tietojen näyttämiseen ja laitteen määrittämiseen. Vaikka sovellus ladataan erikseen sovelluskaupasta, puettava laite ja sovellus muodostavat yhdessä yhden digitaalisia elementtejä sisältävän tuotteen, koska ne on suunniteltu ja tarkoitettu toimimaan yhdessä, jotta digitaalisia elementtejä sisältävän tuotteen toiminta toteutuu.

([8]) On myös muistettava, että 4 artiklan 3 kohdassa sallitaan valmistajille mahdollisuus asettaa saataville markkinoilla keskeneräisiä ohjelmistoja, jotka eivät ole asetuksen mukaisia, kuten alfa- tai beetaversioita tai julkaisuehdokkaita, edellyttäen, että keskeneräinen ohjelmisto asetetaan saataville vain rajoitetuksi ajaksi, joka on tarpeen testausta ja palautteen saamista varten.

([9]) Toisaalta on todettava, että tuotevastuulainsäädännön kannalta tietokonekoodi ei itsessään ole tuote, minkä vuoksi valmistajia, jotka saattavat kyseisen koodin markkinoille, ei voida pitää vastuussa direktiivin (EU) 2024/2853 (tuotevastuudirektiivi) nojalla. Kyseisen direktiivin johdanto-osan 13 kappaleessa todetaan, että ”tietoa ei kuitenkaan pidä katsoa tuotteeksi, eikä tuotevastuusääntöjä näin ollen saisi soveltaa digitaalisten tiedostojen, kuten mediatiedostojen tai e-kirjojen, sisältöön tai pelkkään ohjelmiston lähdekoodiin”. Tämä ei estä sitä, että valmistajat voivat olla vastuussa kansallisen vahingonkorvausoikeuden nojalla.

2.5 **Datayhteydet**

26. Kyberkestävyyssäädöksen 2 artiklan 1 kohdassa todetaan, että säädöstä ”sovelletaan kaikkiin markkinoilla saataville asetettuihin digitaalisia elementtejä sisältäviin tuotteisiin, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon”. Kyberkestävyyssäädöksen soveltamisala ei siis liity pelkästään elektroniikan läsnäoloon, vaan digitaalisia elementtejä sisältävän tuotteen kykyyn vaihtaa digitaalista dataa.

27. Kyberkestävyyssäädöksen 3 artiklassa määritellään käsitteet ”looginen yhteys” ja ”fyysinen yhteys”, mutta siinä ei määritellä ”datayhteyttä” eikä ”digitaalista dataa”. Siksi on hyödyllistä esittää tulkinta siitä, mikä datayhteys on, jotta voidaan selventää kyberkestävyyssäädöksen soveltamisalan rajoja. Nämä rajat ovat erityisen tärkeät, jotta voidaan erottaa digitaalisia elementtejä sisältävät tuotteet, joissa käytetään vain sähkösignaaleja, tuotteista, jotka osallistuvat digitaaliseen tietoliikenteeseen ja ovat siksi alttiita kyberturvallisuusriskeille.

28. Perusluonteisesti datayhteydellä tarkoitetaan tiedon välittämistä binäärimuodossa eli nollien ja ykkösten sarjana. Pelkästään lähdön kytkeminen päälle ja pois (eli 0/1) ei sellaisenaan ole datayhteys, jos kyseisiä tiloja ei ole tarkoitettu edustamaan dataa tai jos niitä ei lueta digitaalisella tulolla. Jotta datayhteys olisi olemassa, binääritilat on tarkoituksellisesti koodattava informaatioksi lähteessä, ja ne on voitava purkaa tietona kohteessa. Toisin sanoen on oltava lähettäjä, joka luo tarkoituksellisesti digitaalisia symboleja määritetyn mallin mukaisesti, ja vastaanottaja, joka pystyy tulkitsemaan nämä symbolit dataksi. Jos sähköisiä tai elektronisia signaaleja käytetään yksinomaan toiminnon käynnistämiseen tai käyttämiseen ilman digitaalisesti koodatun informaation välittämistä, kyberkestävyyssäädöksen mukaan ei ole olemassa datayhteyttä eikä digitaalisia elementtejä sisältävä tuote kuulu näin ollen 2 artiklan 1 kohdan soveltamisalaan.

2.6 **Kompleksiset järjestelmät**

29. Kyberkestävyyssäädöksen soveltamisalaan kuuluvia digitaalisia elementtejä sisältävät tuotteet voivat koostua yksittäisten laitteiden tai ohjelmistokomponenttien lisäksi myös kompleksisista järjestelmistä, mukaan lukien järjestelmät, jotka koostuvat useista, yhdessä tietyn toiminnon suorittamiseksi toimivista laitteisto- ja ohjelmistoelementeistä. Jos tällainen järjestelmä saatetaan markkinoille yhtenä digitaalisia elementtejä sisältävänä tuotteena, se on kyberkestävyyssäädöksessä tarkoitettu digitaalisia elementtejä sisältävä tuote.

30. Tällaisille kompleksisille järjestelmille ovat usein ominaisia pitkät suunnittelu- ja kehityssyklit, mahdollisesti ennen kyberkestävyyssäädöksen soveltamista allekirjoitetut sopimukset, toiminnan pitkät elinkaaret sekä suuri tekninen ja organisatorinen monimutkaisuus. Tällaisia järjestelmiä voidaan saattaa markkinoille kyberkestävyyssäädöksen soveltamisen alkamisen jälkeen, mutta niissä voidaan käyttää ennen kyberkestävyyssäädöksen soveltamisen alkamista markkinoille saatettuja komponentteja, vakiintuneita rakenteita tai laajasti sovellettuja yhteentoimivuusstandardeja, mukaan lukien muussa EU:n lainsäädännössä tai alakohtaisissa kehyksissä tarkoitettuja standardeja. Tällaisten järjestelmien tiettyjä teknisiä ominaisuuksia voikin olla vaikeaa tai kohtuutonta muuttaa vaikuttamatta niiden käyttötarkoitukseen, turvallisuuteen, luotettavuuteen tai yhteentoimivuuteen olemassa olevan infrastruktuurin kanssa.

31. Nämä ominaisuudet eivät sinänsä sulje kompleksisia järjestelmiä kyberkestävyyssäädöksen soveltamisalan ulkopuolelle. Ne pikemminkin tuovat esiin kyberkestävyyssäädöksen riskiperusteisen lähestymistavan soveltamisen, minkä avulla vaatimustenmukaisuus voidaan osoittaa eri tavoin riippuen digitaalisia elementtejä sisältävän tuotteen ominaisuuksista ja rajoituksista kyberkestävyyssäädöksen 13 artiklan 3 kohdan mukaisesti. Nämä ominaisuudet ovat osa tuotteen käyttötarkoitusta ja toimintaympäristöä, ja ne ovat siksi merkityksellisiä arvioitaessa olennaisten kyberturvallisuusvaatimusten, jäljempänä ’olennaiset vaatimukset’, noudattamista. Erityisesti johdanto-osan 55 kappaleessa todetaan nimenomaisesti, että tietyt olennaiset vaatimukset eivät välttämättä sovellu digitaalisia elementtejä sisältävään tuotteeseen. Näin voi olla esimerkiksi tilanteessa, jossa vaatimustenmukaisuus vaarantaisi pakolliset yhteentoimivuusvaatimukset tai järjestelmän asianmukaisen toiminnan.

32. Valmistajien olisikin puututtava kyberturvallisuusriskeihin 13 artiklan 2 kohdassa tarkoitetun kyberturvallisuusriskien arvioinnin perusteella. Johdanto-osan 55 kappaleessa selitetään myös, että joissakin tapauksissa erityisiä olennaisia vaatimuksia ei voida soveltaa tai niitä ei voida täyttää toteuttamalla uusimman teknologian

mukaisia turvatoimenpiteitä esimerkiksi järjestelmän sellaisen käyttötarkoituksen vuoksi, joka edellyttää, että digitaalisia elementtejä sisältävä tuote on vuorovaikutuksessa olemassa olevien riippuvuuksien kanssa tai että se noudattaa tiettyjä yhteentoimivuusvaatimuksia. Tällaisissa tapauksissa valmistajien olisi määritettävä ja dokumentoitava kyseiset erityisrajoitteet, arvioitava niihin liittyvät riskit ja toteutettava asianmukaisia vaihtoehtoisia tai korvaavia riskinhallintatoimenpiteitä, jotta digitaalisia elementtejä sisältävän tuotteen turvallisuus ei vaarannu. Tätä varten sekä 31 artiklassa tarkoitetut tekniset asiakirjat että liitteessä II tarkoitetut käyttäjälle annettavat tiedot ja ohjeet ovat tärkeitä, jotta voidaan kuvata läpinäkyvästi tunnistetut rajoitteet, niihin liittyvät kyberturvallisuusriskit ja toteutetut riskinhallintatoimenpiteet. Valmistajat ovat velvollisia päivittämään riskinarvioinnin tukiajan aikana, ja näin ollen niiden olisi myös säännöllisesti arvioitava uudelleen, onko tällaisia rajoituksia edelleen olemassa. Jos tällaisia rajoituksia voidaan poistaa tai lieventää ajan mittaan, valmistajien olisi päivitettävä digitaalisia elementtejä sisältävä tuote vastaavasti, jotta se on kyberturvallisuudeltaan lähempänä asianmukaista tasoa ([10]).

Esimerkki 10: Valmistaja saattaa markkinoille digitaalisia elementtejä sisältävän tuotteen, joka on yhteydessä ulkoisiin järjestelmiin verkkoprotokollan avulla. Osana olennaisten vaatimusten soveltamista valmistaja määrittää kyberturvallisuusriskien arvioinnin perusteella, että suojatun yhteyskäytännön käyttö on tarpeen, jotta varmistetaan digitaalisia elementtejä sisältävän tuotteen vaihtamien tietojen luottamuksellisuus ja eheys.

Tuotteen käyttötarkoitukseen kuuluu kuitenkin yhteentoimivuus sellaisten järjestelmien kanssa, jotka tukevat vain vanhempaa tai vähemmän turvallista yhteyskäytäntöä. Tällaisissa tapauksissa valmistaja voi käyttää kyseistä yhteyskäytäntöä, jos se on tarpeen yhteentoimivuuden saavuttamiseksi, edellyttäen, että asiaan liittyvät kyberturvallisuusriskit määritetään ja niitä vähennetään muilla keinoilla.

Jos on teknisesti mahdollista, että digitaalisia elementtejä sisältävä tuote tukee sekä suojattua yhteyskäytäntöä että vähemmän suojattua yhteyskäytäntöä, valmistajan odotetaan ottavan suojatun yhteyskäytännön käyttöön ja tekevän sen käytöstä oletusarvoista. Vähemmän suojattu yhteyskäytäntö voitaisiin sallia vain, jos yhteentoimivuus sitä edellyttää.

Esimerkki 11: Teollisen automaatiojärjestelmän valmistaja hankkii mikroprosessoreita ennen kyberkestävyyssäädöksen soveltamisen aloittamista. Valmistaja tekee kyberturvallisuusriskien arvioinnin teollisen automaatiojärjestelmänsä saattamiseksi markkinoille sen jälkeen, kun kyberkestävyyssäädöksen soveltaminen on aloitettu. Tämän kyberturvallisuusriskien arvioinnin perusteella valmistaja ei havaitse erityisiä kyberturvallisuusriskejä, jotka liittyvät jonkin tällaisen mikroprosessorin käyttöön. Valmistaja sisällyttää mikroprosessorin teolliseen automaatiojärjestelmäänsä ja varmistaa, että koko digitaalisia elementtejä sisältävä tuote (teollinen automaatiojärjestelmä) täyttää olennaiset vaatimukset.

2.7 **Digitaalisia elementtejä sisältävät tuotteet, jotka on suunniteltu ennen kyberkestävyyssäädöksen soveltamisen aloittamista**

33. Joissakin tapauksissa valmistaja saattaa markkinoille kyberkestävyyssäädöksen soveltamisen alettua 11. joulukuuta 2027 sellaisen digitaalisia elementtejä sisältävän tuotteen yksiköitä, jotka on valmistettu ennen kyberkestävyyssäädöksen soveltamispäivää suunnitellun ja kehitetyn tyypin tai mallin mukaisesti. Tällaisissa tapauksissa kyseisen asetuksen noudattaminen ei välttämättä edellytä digitaalisia elementtejä sisältävän tuotteen yksiköiden uudelleensuunnittelua. Valmistajan on tehtävä kyberkestävyyssäädöksen 13 artiklan 2 kohdan mukainen kyberturvallisuusriskien arviointi määrittääkseen digitaalisia elementtejä sisältävän tuotteen käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön perusteella, mitä liitteessä I olevassa I osassa vahvistetuista olennaisista vaatimuksista sovelletaan kyseiseen digitaalisia elementtejä sisältävään tuotteeseen ja miten nämä vaatimukset pannaan täytäntöön.

34. Jos riskinarvioinnin tulos osoittaa, että digitaalisia elementtejä sisältävään tuotteeseen sisältyy jo asianmukaisia ja tehokkaita turvatoimenpiteitä, joilla puututaan olennaisiin riskeihin, valmistaja voi käyttää kyseisiä käytössä olevia toimenpiteitä osoittaakseen kyberkestävyyssäädöksen vaatimusten täyttymisen. Kyberkestävyyssäädös ei sinänsä velvoita ottamaan käyttöön uusia turvaominaisuuksia tai suunnittelemaan digitaalisia elementtejä sisältävää tuotetta uudelleen, jos tämä ei ole tarpeen tunnistettuihin riskeihin puuttumiseksi.

([10]) On huomattava, että tässä kohdassa esitettyjä näkökohtia voidaan soveltuvin osin soveltaa kaikkiin kyberkestävyyssäädöksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin eikä ainoastaan kompleksisiin järjestelmiin.

35. Valmistajaan sovelletaan kuitenkin edelleen kyberkestävyyssäädöksessä vahvistettuja velvoitteita. Niiden mukaisesti on varmistettava, että ennen digitaalisia elementtejä sisältävän tuotteen markkinoille saattamista suoritetaan sovellettava vaatimustenmukaisuuden arviointimenettely, laaditaan EU-vaatimustenmukaisuusvakuutus ja kiinnitetään CE-merkintä. Näitä vaatimuksia on noudatettava riippumatta siitä, onko digitaalisia elementtejä sisältävän tuotteen suunnittelua pitänyt muuttaa riskinarvioinnin seurauksena. Ennen kyberkestävyyssäädöksen soveltamispäivää suunniteltujen mutta kyseisen päivän jälkeen markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden osalta, joista valmistaja ei pysty osoittamaan, miten riskinarviointi on otettu huomioon digitaalisia elementtejä sisältävän tuotteen suunnittelu- ja kehitysvaiheessa, 13 artiklan 2 kohdan velvoite olisi ymmärrettävä niin, että valmistajien on tehtävä kyberturvallisuusriskien arviointi ja osoitettava tällä perusteella, että digitaalisia elementtejä sisältävässä tuotteessa on asianmukaisia turvatoimenpiteitä kyberturvallisuusriskien minimoimiseksi, poikkeamien torjumiseksi ja niiden vaikutusten minimoimiseksi, myös käyttäjien terveyden ja turvallisuuden osalta.

36. Näin ollen digitaalisia elementtejä sisältävät tuotteet, jotka on suunniteltu ennen kyberkestävyyssäädöksen soveltamisen aloittamista, voidaan mahdollisesti saattaa markkinoille kyberkestävyyssäädöksen nojalla ilman uudelleensuunnittelua edellyttäen, että valmistaja voi kyberturvallisuusriskien arvioinnin ja teknisten asiakirjojen avulla osoittaa, että digitaalisia elementtejä sisältävä tuote on asianmukaisella kyberturvallisuuden tasolla ottaen huomioon sen käyttötarkoitus ja kohtuudella ennakoitavissa oleva käyttö ja täyttää olennaiset kyberturvallisuusvaatimukset.

37. Lisäksi on hyödyllistä selventää vaatimustenmukaisuuden arviointivelvoitteiden soveltamista sellaisten digitaalisia elementtejä sisältävien tuotteiden valmistajiin, jotka saatetaan markkinoille kyberkestävyyssäädöksen soveltamisen alkamisen jälkeen mutta jotka on valmistettu ennen kyseistä päivää suunnitellun ja kehitetyn tyypin tai mallin mukaisesti. Valmistajan on 13 artiklan 12 kohdan mukaisesti osoitettava asiaankuuluvalla vaatimustenmukaisuuden arviointimenettelyllä, että sen digitaalisia elementtejä sisältävä tuote on sovellettavien olennaisten vaatimusten mukainen, ja sisällytettävä tätä koskevat todisteet tuotteen teknisiin asiakirjoihin (liitteessä VII oleva 6 kohta).

38. Tällaisten vaatimusten soveltamista on kuitenkin tulkittava digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskien arvioinnin ja kyberturvallisuusriskiprofiilin valossa. Erityisesti sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, jotka on suunniteltu ennen kyberkestävyyssäädöksen soveltamispäivää (mutta jotka on saatettu markkinoille kyseisen päivän jälkeen) ja joihin sovelletaan 32 artiklan 1 kohdassa säädettyjä vaatimustenmukaisuuden arviointimenettelyjä, jos riskinarvioinnin mukaan digitaalisia elementtejä sisältävään tuotteeseen sisältyy jo asianmukaisia ja tehokkaita, kyseisen tuotteen riskeihin liittyviä turvatoimenpiteitä, velvollisuutta esittää todisteita osana vaatimustenmukaisuuden arviointimenettelyä ei pitäisi tulkita vaatimukseksi siitä, että valmistajalta edellytetään testituloksia, jotka kattavat tällaisten digitaalisia elementtejä sisältävien tuotteiden alkuperäiset suunnittelu- ja kehitysvaiheet. Tällainen olisi tarpeetonta, koska sillä ei parannettaisi itse digitaalisia elementtejä sisältävän tuotteen turvallisuutta. Jos testit ovat kuitenkin tarpeellisia, valmistajien ei odoteta esittävän näyttöä kaikille tuotevarianteille tehdyistä testeistä, vaan ne voivat ryhmitellä tällaiset testit digitaalisia elementtejä sisältävien tuotteiden eri tuoteperheiden mukaan, mitä käsitellään tarkemmin jaksossa *7.4 Riskien arviointien ja vaatimustenmukaisuusasiakirjojen uudelleenkäyttö digitaalisia elementtejä sisältävien tuoteperheiden osalta*.

39. Valmistajan olisi kuitenkin toimitettava todisteet siitä, miten se noudattaa liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyprosesseja, sen olisi päivitettävä riskinarviointinsa 13 artiklan 3 kohdan mukaisesti ja täytettävä kaikki muut kyberkestävyyssäädöksessä säädetyt velvoitteet, myös antamalla käyttäjille tietoja ja ohjeita 13 artiklan 18 kohdan mukaisesti.

Esimerkki 12: Valmistaja saattaa markkinoille mikroprosessorin, joka on suunniteltu ja kehitetty ennen kyberkestävyyssäädöksen soveltamispäivää. Mikroprosessori on tarkoitettu liitettäväksi erilaisiin digitaalisia elementtejä sisältäviin elektronisiin tuotteisiin, myös yhteystoiminnoilla varustettuihin digitaalisia elementtejä sisältäviin tuotteisiin.

Ennen mikroprosessorin uusien yksiköiden saattamista markkinoille kyberkestävyyssäädöksen soveltamisen aloittamisen jälkeen valmistaja tekee kyberturvallisuusriskien arvioinnin 13 artiklan 2 kohdan mukaisesti. Valmistaja määrittää mikroprosessorin käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön perusteella olennaiset kyberturvallisuusriskit, kuten luvattoman pääsyn, ohjelmistojen tai datan manipuloinnin ja käytettävissä olevien rajapintojen väärinkäytön.

Riskinarvioinnin tulokset osoittavat, että alkuperäisen suunnitelman mukaisessa mikroprosessorissa on jo asianmukaisia ja tehokkaita turvatoimenpiteitä, joilla puututaan havaittuihin riskeihin. Valmistaja päättelee näin ollen, että digitaalisia elementtejä sisältävä tuote täyttää liitteessä I olevassa I osassa vahvistetut asiaankuuluvat olennaiset vaatimukset ja että uusia turvatoimintoja ei tarvitse suunnitella tai ottaa käyttöön.

Jos ei ole mahdollista osoittaa, miten kyberturvallisuusriskien arviointi otettiin huomioon alkuperäisen suunnittelu- ja kehitysvaiheen aikana, valmistaja dokumentoi nykyisen kyberturvallisuusriskien arvioinnin ja selittää, miten nykyisellä suunnittelulla ja toimenpiteillä lievennetään havaittuja riskejä. Valmistajan ei tarvitse laatia uudelleen aiempia suunnittelu- tai testiasiakirjoja, koska tämä ei parantaisi digitaalisia elementtejä sisältävän tuotteen kyberturvallisuutta. Jos useat mikroprosessorin variantit perustuvat samaan suunnitelmaan ja niillä on sama kyberturvallisuusriskiprofiili, valmistaja voi käyttää myös edustavia todisteita, jotka kattavat kyseisen tuoteperheen.

Valmistaja varmistaa myös liitteessä I olevassa II osassa vahvistettujen haavoittuvuuksien käsittelyä koskevien vaatimusten noudattamisen muun muassa ylläpitämällä prosesseja haavoittuvuuksiin puuttumiseksi ja niiden korjaamiseksi ja tarkistamalla kyberturvallisuusriskien arviointia 13 artiklan 3 kohdan mukaisesti.

Tällaisessa tilanteessa ennen kyberkestävyyssäädöksen soveltamisen aloittamista suunniteltu mikroprosessori voidaan saattaa markkinoille ilman uudelleensuunnittelua edellyttäen, että valmistaja voi kyberturvallisuusriskien arvioinnin ja teknisten asiakirjojen avulla osoittaa, että mikroprosessori saavuttaa asianmukaisen kyberturvallisuuden tason ottaen huomioon sen käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön ja täyttää sovellettavat olennaiset vaatimukset.

3. **VAPAA JA AVOIMEN LÄHDEKOODIN OHJELMISTO**

40. Kuten jaksossa *2.1 Markkinoille saattaminen* todetaan, kyberkestävyyssäädöstä sovelletaan digitaalisia elementtejä sisältäviin tuotteisiin, joita asetetaan saataville EU:n markkinoilla kaupallisen toiminnan yhteydessä (eli jotka on ”saatettu markkinoille”), sekä kaikkiin myöhempiin tapauksiin, joissa sama digitaalisia elementtejä sisältävä tuote asetetaan saataville markkinoilla. Sinisessä oppaassa (2.2 kohta) selvennetään, että ”kaupallinen toiminta” on ymmärrettävä tavaroiden toimittamiseksi maksua vastaan tai maksutta liiketoimintaan liittyvissä yhteyksissä, ja tämä voidaan selvittää vain tapauskohtaisesti muun muassa toimitusten säännöllisyyden, tuotteen ominaisuuksien ja toimittajan aikeiden perusteella.

41. Kaupallisen toiminnan yhteydessä toteutetulle toimittamiselle ovat ominaisia monenlaiset olosuhteet, jotka on dokumentoitu kattavasti sinisessä oppaassa ja joita on käsitelty kyberkestävyyssäädöksen johdanto-osan 15 kappaleessa. Niitä voivat olla niin hinnan periminen suoraan kuin ”myös hinnan periminen teknisistä tukipalveluista, kun tätä ei käytetä ainoastaan aiheutuneiden kustannusten korvaamiseen, aikomus hankkia tuloja esimerkiksi tarjoamalla ohjelmistoalusta, jonka kautta valmistaja saa tuloja muista palveluista, käytön edellytyksenä oleva vaatimus henkilötietojen käsittelystä muista syistä kuin yksinomaan ohjelmiston tietoturvan, yhteensopivuuden tai yhteentoimivuuden parantamiseksi taikka sellaisten lahjoitusten vastaanottaminen, jotka ylittävät digitaalisia elementtejä sisältävän tuotteen suunnitteluun, kehittämiseen ja tarjoamiseen liittyvät kustannukset” (johdanto-osan 15 kappale) ([11]).

42. Kyberkestävyyssäädöksessä kuitenkin todetaan, että vapaan ja avoimen lähdekoodin ohjelmistojen (VALO), eri kehitys- ja julkaisutavoilla on erityispiirteensä, ja tarjotaan joitakin ohjeita, joilla voidaan määrittää, onko VALO (kaupallisen toiminnan yhteydessä) markkinoille saatettu digitaalisia elementtejä sisältävä tuote kyberkestävyyssäädöksessä tarkoitetulla tavalla. Kuten johdanto-osan 18 kappaleessa todetaan, ”kyseisen toiminnan kaupallista tai ei-kaupallista luonnetta määritettäessä ei saisi ottaa huomioon pelkästään digitaalisia elementtejä sisältävän tuotteen kehittämiseen liittyviä olosuhteita tai sitä, miten kehittäminen on rahoitettu. Tarkennuksena ja jotta kehitys- ja toimitusvaiheet erotetaan selkeästi toisistaan, […] sellaisten digitaalisia elementtejä sisältävien tuotteiden tarjoamista, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja joista niiden valmistajat eivät saa tuloa, ei saisi katsoa kaupalliseksi toiminnaksi.”

([11]) On myös muistettava, että vaikka usein digitaalisia elementtejä sisältävillä tuotteilla hankitaan tuloja (myös) henkilötietojen käsittelyn kautta, henkilötietojen suoja on perusoikeus, ja siksi henkilötietoja ei voida pitää hyödykkeenä, kuten todetaan tietyistä digitaalisen sisällön ja digitaalisten palvelujen toimittamista koskeviin sopimuksiin liittyvistä seikoista 20. toukokuuta 2019 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2019/770 johdanto-osan 24 kappaleessa (EUVL L 136, 22.5.2019, s. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Siksi on hyödyllistä i) selventää, mikä VALO on, ii) selventää, milloin sen katsotaan kuuluvan luonnollisen henkilön tai oikeushenkilön vastuulle, ja iii) antaa esimerkkejä, jotka auttavat sidosryhmiä ymmärtämään, milloin VALOn jakelu on markkinoille saattamista. Jos VALOa ei saateta markkinoille, se ei kuulu kyberkestävyyssäädöksen soveltamisalaan, paitsi jos sen julkaiseva yhteisö on oikeushenkilö, joka täyttää 3 artiklan 14 alakohdan mukaisen ”avoimen lähdekoodin ohjelmistovastaavan”, jäljempänä ’ohjelmistovastaava’, määritelmän. Tällöin siihen sovelletaan ainoastaan 24 artiklassa säädettyjä velvoitteita.

44. Kyberkestävyyssäädöksen 3 artiklan 48 alakohdan määritelmän mukaan VALOlla tarkoitetaan ”ohjelmistoa, jonka lähdekoodi on yleisesti saatavilla ja joka on asetettu saataville vapaalla ja avoimen lähdekoodin lisenssillä, joka tarjoaa kaikki oikeudet, jotta se on vapaasti saatavilla, käytettävissä, muunneltavissa ja uudelleen jaettavissa”. Vaikka näissä ohjeissa ei määritetä erityisiä vapaita ja avoimen lähdekoodin lisenssejä, jotka ovat yhteensopivia 3 artiklan 48 alakohdassa vahvistetun määritelmän kanssa, kyseisen säännöksen sanamuodosta seuraa, että kyberkestävyyssäädöksen mukaan VALOksi katsotaan ainoastaan ohjelmistot, jotka täyttävät seuraavat kaksi edellytystä: i) ohjelmisto on asetettava saataville vapaalla ja avoimen lähdekoodin lisenssillä, jolla myönnetään kaikki 3 artiklan 48 alakohdassa tarkoitetut oikeudet ja ii) sen lähdekoodi on jaettava avoimesti.

45. Vaatimus, jonka mukaan lisenssillä tarjottava ohjelmisto ”on vapaasti saatavilla, käytettävissä, muunneltavissa ja uudelleen jaettavissa” kuvastaa perinteistä käsitystä VALOsta eli sitä, että käyttäjien on voitava päästä lähdekoodiin ilman aiheettomia rajoituksia, muuttaa sitä ja jakaa uudelleen alkuperäisiä tai muutettuja versioita. Lähdekoodiin pääsy on näin ollen välttämätön edellytys muiden oikeuksien käyttämiselle: ilman lähdekoodiin pääsyä ohjelmistoa ei ole käytännössä mahdollista muuttaa tai käyttää mielekkäällä tavalla uudelleen.

46. Kyberkestävyyssäädöksen 3 artiklan 48 alakohdassa ei kuitenkaan viitata pelkästään lisenssiehtoihin, koska siinä nimenomaisesti edellytetään, että lähdekoodi ”on yleisesti saatavilla”. Käsitteellä ”yleisesti saatavilla” tarkoitetaan, että lähdekoodi on asetettava julkisesti saataville (joko toiminnan alkupäässä tai loppupäässä) eikä sitä saa tarjota ainoastaan rajoitetusti tai ehdollisesti. Näin ollen vapaan ja avoimen lähdekoodin lisenssin perusteella jaettavia ohjelmistoja, joiden lähdekoodi on jaettu (tai sallittua jakaa) vain maksavien asiakkaiden tai rajoitetun käyttäjäryhmän kanssa, ei katsota 3 artiklan 48 alakohdassa tarkoitetuksi VALOksi. Kyberkestävyyssäädöstä sovellettaessa VALOna olisi pidettävä ainoastaan ohjelmistoja, joiden lähdekoodi on julkisesti saatavilla ja joiden lisensointi perustuu vapaaseen ja avoimen lähdekoodin lisenssiin, jolla myönnetään kaikki 3 artiklan 48 alakohdassa tarkoitetut oikeudet.

3.1 **Sen määrittäminen, kuuluuko vapaa ja avoimen lähdekoodin ohjelmisto tietyn toimijan vastuulle**

47. Kyberkestävyyssäädöksessä asetetaan keskeisiä velvoitteita talouden toimijoille, jotka toimittavat digitaalisia elementtejä sisältäviä tuotteita EU:n markkinoille. Siinä määritellään valmistaja luonnolliseksi henkilöksi tai oikeushenkilöksi, joka toimittaa omalla nimellään tai tavaramerkillään digitaalisia elementtejä sisältävän tuotteen ja tekee niin kaupallisen toiminnan yhteydessä (saattaen tuotteen siten markkinoille). Samaan tapaan maahantuoja määritellään unioniin sijoittautuneeksi luonnolliseksi henkilöksi tai oikeushenkilöksi, joka toimittaa unionin ulkopuolelle sijoittautuneen henkilön digitaalisia elementtejä sisältävän tuotteen ja tekee niin kaupallisen toiminnan yhteydessä (saattaen tuotteen siten markkinoille). Ohjelmistovastaavien velvollisuudet koskevat oikeushenkilöä, joka toimittaa kaupalliseen toimintaan tarkoitetun VALOn ([12]) mutta ei saata sitä markkinoille kyberkestävyyssäädöksessä tarkoitetulla tavalla.

48. Näin ollen sen määrittämiseksi, saattaako luonnollinen henkilö tai oikeushenkilö VALOn EU:n markkinoille, on ensin selvitettävä, toimittaako kyseinen luonnollinen henkilö tai oikeushenkilö VALOn. Jotta kyberkestävyyssäädöksen nojalla sovellettavat velvoitteet voidaan määrittää asianmukaisesti, on olennaista määrittää, suorittaako luonnollinen henkilö tai oikeushenkilö todellakin VALOn toimittamisen. Kuten johdanto-osan 18 kappaleessa muistutettiin, kyberkestävyyssäädöstä ei sovelleta luonnollisiin henkilöihin tai oikeushenkilöihin, jotka kehittävät lähdekoodia VALOiksi katsottaviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka eivät ole kyseisten henkilöiden vastuulla.

([12]) Tämä on välttämätön mutta ei ainoa edellytys, jotta oikeushenkilö voidaan luokitella avoimen lähdekoodin ohjelmistovastaavaksi, sillä 3 artiklan 14 kohdassa esitetyssä määritelmässä säädetään lisäedellytyksistä, joiden perusteella oikeushenkilö voidaan luokitella ohjelmistovastaavaksi.

49. Kun otetaan huomioon VALOn kehittämisen erityispiirteet, kuten osallistujien usein suuri määrä, hajautetut yhteistyömallit sekä osallistumisen ja päätöksenteon erottaminen toisistaan, on hyödyllistä selventää, että VALOn katsotaan olevan niiden luonnollisten henkilöiden tai oikeushenkilöiden ”vastuulla”, jotka julkaisevat sen ja valvovat ensisijaisesti sen kehittämistä, levittämistä ja jakelua koskevia päätöksiä (usein ”ylläpitäjät”). Henkilöt, jotka tuottavat lähdekoodia mutta eivät hallitse julkaisuja, etenemissuunnitelmia tai hallintopäätöksiä, katsotaan ”osallistujiksi”. VALO ei ole tällaisten henkilöiden vastuulla, vaikka he ovat tuottaneet sen koodia. Pelkkien teknisten lupien, kuten käyttöoikeuksien, omaaminen ei riitä osoittamaan, että VALO on kyseisen henkilön vastuulla; vastuu on niillä, jotka julkaisevat VALOn ja valvovat sitä.

Esimerkki 13: Yksittäinen kehittäjä tai yrityksen työntekijä lähettää VALO-projektiin pull- tai merge-pyynnön, joka sisältää korjaavan tietoturvapäivityksen tai uuden ominaisuuden. Projektin ylläpitäjät tarkistavat, hyväksyvät ja yhdistävät koodin päätietovarastoon ja sisällyttävät sen myöhemmin uuteen versioon. Tässä esimerkissä pull-pyynnön lähettänyt henkilö on ”osallistuja”, eikä häneen sovelleta kyberkestävyyssäädöstä. Vaikka kyseinen henkilö tuotti lähdekoodia, hän ei käytä ensisijaista määräysvaltaa kehitys-, julkaisu- tai jakelupäätöksissä.

3.2 **Sen määrittäminen, onko vapaa ja avoimen lähdekoodin ohjelmisto saatettu EU:n markkinoille**

50. Kun on todettu, että VALO on luonnollisen henkilön tai oikeushenkilön vastuulla, on selvitettävä, toimittaako kyseinen henkilö sitä kaupallisen toiminnan yhteydessä, jolloin on kyse markkinoille saattamisesta.

3.2.1 *Hinnan periminen*

51. Jos VALOn toimittava luonnollinen henkilö tai oikeushenkilö perii itse ohjelmistosta hinnan (esimerkiksi perimällä hinnan valmiiksi käännetyistä binaarituotteista), kyseinen henkilö saattaa digitaalisia elementtejä sisältävän tuotteen markkinoille. VALOn markkinoille saattava henkilö on näin ollen kyberkestävyyssäädöksessä tarkoitettu valmistaja.

52. VALOn valmistajat toimittavat usein maksuttomia ohjelmistoversioita (usein yhteisöversioita), joiden koodipohja on (lähes) sama kuin maksullisessa versiossa. Nämä digitaalisia elementtejä sisältävät tuotteet ovat kuitenkin eri tuotteita: Maksullisesta versiosta saadaan tuloa jollakin tavalla (esimerkiksi veloittamalla maksu tai muulla tässä jaksossa kuvatulla tavalla), minkä vuoksi se katsotaan markkinoille saatetuksi, mikä aiheuttaa valmistajan velvollisuuksia. Maksuttomasta versiosta (tai yhteisöversiosta) ei saada tuloa, minkä vuoksi sitä ei katsota markkinoille saatetuksi kyberkestävyyssäädöstä sovellettaessa. Näin on myös silloin, kun maksullinen versio on ”parannettu” kaupallinen versio, jossa laajennetaan maksutta toimitetun version koodipohjaa tai sisällytetään kyseinen versio laajempaan digitaalisia elementtejä sisältävään tuotteeseen (esimerkiksi open-core-mallissa).

53. Jos yhteisöversion toimittava henkilö on oikeushenkilö, tähän oikeushenkilöön sovelletaan ohjelmistovastaavien velvollisuuksia myös ilmaiseksi toimitetun version (yhteisöversio) osalta. Jos henkilö on luonnollinen henkilö, maksutta toimitettava versio (yhteisöversio) ei kuulu kyberkestävyyssäädöksen soveltamisalaan.

3.2.2 *Tulon saaminen muista palveluista tai vaatimus henkilötietojen käsittelystä*

54. Luonnollinen henkilö tai oikeushenkilö, joka julkaisee VALOn, voi myös saattaa sen markkinoille (eli toimittaa sen kaupallisen toiminnan yhteydessä), jos se tarjoaa ohjelmiston, jonka kautta se saa tuloa muista digitaalisia elementtejä sisältävistä tuotteista tai palveluista, tai jos se edellyttää käyttäjän henkilötietojen käsittelyä muista syistä kuin yksinomaan ohjelmiston tietoturvan, yhteensopivuuden tai yhteentoimivuuden parantamiseksi.

Esimerkki 14: Luonnollinen henkilö tai oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin markkinapaikkasovelluksen. Sovellus on saatavilla maksutta, ja sen kautta käyttäjä voi ostaa tavaroita tai palveluita. Sovelluksen julkaisija saa tuloa muista digitaalisia elementtejä sisältävistä tuotteista ja palveluista, joita se tarjoaa sovelluksen kautta (esim. mainokset, provisiomaksut tai tilausmaksut). Näin ollen sovellus katsotaan kaupallisen toiminnan yhteydessä markkinoille saatetuksi.

Esimerkki 15: Luonnollinen henkilö tai oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin VPN-sovelluksen. Sovellus on saatavilla maksutta, mutta käyttäjät voivat maksaa sovelluksen kautta lisäpalvelimien tai erillisten IP-osoitteiden käytöstä. Sovelluksen avulla kyseinen henkilö saa tuloa muista sen kautta tarjotuista palveluista, minkä vuoksi sovellus katsotaan kaupallisen toiminnan yhteydessä markkinoille saatetuksi.

Esimerkki 16: Luonnollinen henkilö tai oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin fitness-seurantasovelluksen. Sovellus on käytettävissä maksutta, mutta sen käyttö edellyttää käyttäjien henkilötietojen käsittelyä sellaisiin tarkoituksiin kuin kohdennettuun mainontaan tai analytiikkaan, joka ei liity ohjelmiston tietoturvaan, yhteensopivuuteen tai yhteentoimivuuteen. Koska sovelluksen käyttö edellyttää tällaista tietojenkäsittelyä, se katsotaan kaupallisen toiminnan yhteydessä markkinoille saatetuksi.

3.2.3 *Tukipalvelut*

55. Jos luonnollinen henkilö tai oikeushenkilö, joka julkaisee VALOn, myös tarjoaa siihen liittyviä maksullisia tukipalveluja, tämä ei sinällään tarkoita, että digitaalisia elementtejä sisältävä tuote toimitettaisiin kaupallisen toiminnan yhteydessä. Tukipalveluihin voi kuulua esimerkiksi konsultointi-, koulutus- tai asiantuntijapalveluja, jotka liittyvät ohjelmiston käyttöön, dokumentointiin, konfigurointiin ja käyttöönottoon asiakkaan toimesta.

56. Ratkaisevaa on se, edellyttääkö itse VALOon pääsy (eli digitaalisia elementtejä sisältävän tuotteen tarjoaminen), mukaan lukien sen ylläpito, maksua vai onko kyse vain sellaisten ammattimaisten palvelujen tarjoamisesta, jotka liittyvät maksutta saatavilla oleviin digitaalisia elementtejä sisältäviin tuotteisiin, kuten kyberkestävyyssäädöksen johdanto-osan 18 kappaleessa todetaan (”sellaisten digitaalisia elementtejä sisältävien tuotteiden tarjoamista, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja joista niiden valmistajat eivät saa tuloa, ei saisi katsoa kaupalliseksi toiminnaksi”). Jos VALO voidaan ladata ja asentaa maksutta ja käyttäjät voivat halutessaan ostaa ammattilaispalveluja erikseen, kyseistä VALOa ei katsota markkinoille saatetuksi.

57. Joissakin tapauksissa digitaalisia elementtejä sisältävän tuotteen tietty versio, joka sisältää tiettyjä etuja, kuten teknistä tukea tai suorituskyvyn optimoinnin, on sen sijaan saatavilla vain korvausta vastaan. Tällaisissa tapauksissa tuotteen tarjoaminen merkitsee digitaalisia elementtejä sisältävän tuotteen tarjoamista tulon saamiseksi kaupallisen toiminnan yhteydessä, minkä vuoksi se katsotaan markkinoille saatetuksi. Tämä koskee myös tapauksia, joissa maksullinen versio tai yritysversio asetetaan saataville kaupallisen sopimuksen nojalla riippumatta siitä, onko toiminnallisesti vastaavia ohjelmistoja saatavilla maksutta vapaalla ja avoimen lähdekoodin lisenssillä.

Esimerkki 17: Luonnollinen henkilö tai oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin käyttöjärjestelmän ja tarjoaa käyttöjärjestelmästä maksullisen version, joka sisältää tukipalveluja, kuten teknistä tukea tai suorituskyvyn optimointia. Käyttöjärjestelmän maksullinen versio katsotaan kaupallisen toiminnan yhteydessä markkinoille saatetuksi.

Esimerkki 18: Luonnollinen henkilö tai oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin komentorivityökalun. Työkalu on käytettävissä maksutta, ja kuka tahansa voi ladata ja asentaa sen. Kyseinen luonnollinen henkilö tai oikeushenkilö tarjoaa erikseen ammattimaisia palveluja, kuten valinnaisia konsultointipalveluja, kouluttaakseen käyttäjiä ja tukeakseen heitä työkalun asentamisessa ja käytössä. Tätä VALOa ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi.

58. Erityisesti jos on kyse luonnollisesta henkilöstä, joka julkaisee VALOn ja tarjoaa teknistä tukea, joka on suoraan kytköksissä digitaalisia elementtejä sisältävän tuotteen saatavuuteen, julkaisemista ei tässäkään tapauksessa katsota kaupalliseksi toiminnaksi, jos hinnan perimistä käytetään ainoastaan aiheutuneiden kustannusten korvaamiseen, kuten kyberkestävyyssäädöksen johdanto-osan 15 kappaleessa todetaan. Tällaisia aiheutuneita kustannuksia ovat muun muassa kyseisen ohjelmiston suunnitteluun, kehittämiseen ja ylläpitoon liittyvät erilaiset kustannukset, mukaan lukien henkilön kohtuulliset elinkustannukset. Näin ollen jos luonnollinen henkilö julkaisee VALOn ja tarjoaa teknistä tukea kustannustensa kattamiseksi ja kohtuullisen korvauksen saamiseksi, hänen ei katsota yksin tämän perusteella saattavan kyseistä ohjelmistoa EU:n markkinoille.

59. Jos luonnollinen henkilö tai oikeushenkilö tarjoaa teknistä tukea liittyen VALOon, joka ei ole sen vastuulla, kyseisen henkilön ei katsota saattavan kyseistä ohjelmistoa markkinoille, paitsi jos kyseinen henkilö tekee VALOon 22 artiklassa tarkoitetun merkittävän muutoksen osana tällaisen tuen toimittamista.

Esimerkki 19: Palveluntarjoaja ei julkaise VALOa mutta auttaa asiakasta asentamaan sen asiakkaan paikalliselle palvelimelle. Se tekee niin tekemättä VALOon merkittävää muutosta. Palveluntarjoajan ei näin ollen katsota saattavan VALOa markkinoille.

3.2.4 *Lahjoitukset*

60. VALO-hankkeita julkaisevat luonnolliset henkilöt tai oikeushenkilöt tarjoavat ohjelmistojen käyttäjille usein tapoja lahjoittaa vapaaehtoisesti rahaa kiittääkseen hankkeen julkaisijoita ja myös varmistaakseen, että hanketta ylläpidetään aktiivisesti.

61. Kuten kyberkestävyyssäädöksen johdanto-osan 15 kappaleessa todetaan, ”lahjoitusten vastaanottamista ei saisi katsoa liiketoiminnaksi, jos aikomuksena ei ole tehdä voittoa”. Pelkkää lahjoitusalustalle tai vastaavaan työkaluun ohjaavan linkin lisäämistä lahjoitusten keräämiseksi ei pitäisi katsoa aikomukseksi tehdä voittoa, vaikka lahjoituksilla kerätty summa ylittäisi digitaalisia elementtejä sisältävään tuotteeseen liittyvät suunnittelu-, kehitys- ja toimituskustannukset. Tähän sisältyy kohtuullinen korvaus oikeushenkilön palkkaamille osallistujille ja/tai luonnollisen henkilön kohtuulliset elinkustannukset. Lahjoitukset vaihtelevat tyypillisesti ajan mittaan, minkä vuoksi on käytettävä jonkin verran joustavuutta arvioitaessa, katsotaanko VALO, josta saadaan tuloa yksinomaan lahjoituksina, markkinoille saatetuksi. VALOa, jota tuetaan ainoastaan lahjoituksilla, ei sen vuoksi todennäköisesti katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi.

Esimerkki 20: Luonnollinen henkilö tai oikeushenkilö julkaisee VALO-työkalun julkisessa sähköisessä hakemistossa niin, että kuka tahansa voi ladata sen ja käyttää, muokata ja jakaa sitä edelleen vapaan ja avoimen lähdekoodin lisenssillä. Julkaisija pyytää käyttäjiä tekemään vapaaehtoisen lahjoituksen lahjoitusalustan kautta hankkeen jatkuvan kehittämisen ja ylläpidon tukemiseksi. Ohjelmiston, sen lähdekoodin ja päivitysten käyttö ei edellytä lahjoituksen tekemistä. Tätä VALOa ei katsota toimitetuksi kaupallisen toiminnan yhteydessä eikä sitä katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi.

62. Joissakin tapauksissa lahjoituksilla tuettu VALO voidaan kuitenkin katsoa markkinoille saatetuksi. Näin on silloin, kun olosuhteiden kokonaisarvioinnin perusteella lahjoitukset vastaavat tosiasiallisesti hintaa, joka peritään digitaalisia elementtejä sisältävän tuotteen tai joidenkin sen toimintojen käytöstä. Näin voi olla erityisesti silloin, kun VALOn, sen olennaisten toimintojen tai päivitysten käyttö edellyttää käytännössä lahjoituksen tekemistä tai kun lahjoituksiin liittyy sopimusetuja tai yksinomaisia etuja, jotka menevät yhteisön jäsenetuja pidemmälle.

Esimerkki 21: Luonnollinen henkilö tai oikeushenkilö julkaisee digitaalisia elementtejä sisältävän ohjelmistotuotteen vapaalla ja avoimen lähdekoodin lisenssillä mutta tarjoaa ladattavia julkaisuja ja tietoturvapäivityksiä vain lahjoituksen tehneille käyttäjille. Käyttäjät, jotka eivät tee lahjoitusta, eivät voi käyttää ohjelmiston uusinta versiota.

Tässä tapauksessa lahjoitukset ovat tosiasiassa edellytys digitaalisia elementtejä sisältävän tuotteen käytölle, joten ne vastaavat hinnan perimistä. Tämä VALO katsotaan kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi.

Esimerkki 22: Luonnollinen henkilö tai oikeushenkilö asettaa VALOn lähdekoodin julkisesti saataville mutta tarjoaa valmiiksi käännettyjä binaarituotteita, säännöllisiä päivityksiä ja taattuja tietoturvakorjauksia vain lahjoittajille. Tässä tapauksessa lahjoitukset ovat kytköksissä digitaalisia elementtejä sisältävän tuotteen olennaisten toimintojen käyttöön ja muodostavat korvauksen kyseisen tuotteen toimittamisesta. Näin ollen tämä VALO katsotaan kaupallisen toiminnan yhteydessä markkinoille saatetuksi.

3.2.5 *Vapaan ja avoimen lähdekoodin ohjelmiston rahoittaminen*

63. Pelkästään se, että kolmas osapuoli on maksanut VALOn kehittämisen tai sponsoroinut tai muulla tavoin rahoittanut sitä, ei sinällään ratkaise, onko kyseinen VALO saatettu markkinoille. VALOjen ekosysteemissä on yleisenä käytäntönä, että yksittäiset kehittäjät, säätiöt tai yhteisöt saavat rahoitusta yrityksiltä, julkisilta elimiltä tai muilta rahoittajilta tiettyjen ominaisuuksien työstämiseksi, virheiden korjaamiseksi tai kriittisten komponenttien ylläpitämiseksi. Rahoitus voidaan toteuttaa monissa muodoissa, kuten apurahoina, bug bounty -korvauksina, sponsorointina, palvelusopimuksina tai palkallisena kehitystyönä.

64. Kuten kyberkestävyyssäädöksen johdanto-osan 18 kappaleessa jo muistutetaan, ”kyseisen toiminnan kaupallista tai ei-kaupallista luonnetta määritettäessä ei saisi ottaa huomioon pelkästään digitaalisia elementtejä sisältävän tuotteen kehittämiseen liittyviä olosuhteita tai sitä, miten kehittäminen on rahoitettu”.

65. Jos VALO on avoimesti jaettu ja asetettu vapaasti kaikkien saataville käytettäväksi, muunneltavaksi ja uudelleenjaettavaksi, sen, että kaupallinen toimija on saattanut maksaa kyseisestä hankkeesta, ei pitäisi näin ollen vaikuttaa sen määrittämiseen, onko ohjelmisto saatettu markkinoille. Jos kyseisestä VALOsta ei saada tuloa muulla tavoin, sitä ei pidä katsoa markkinoille saatetuksi. Jos VALOn kehittämistä rahoittanut yritys (tai mikä tahansa muu yritys) integroi VALOn digitaalisia elementtejä sisältävään tuotteeseensa, kyseisen yrityksen on noudatettava asianmukaista huolellisuutta kyberkestävyyssäädöksen 13 artiklan 5 kohdan mukaisesti.

Esimerkki 23: Yksittäinen kehittäjä julkaisee VALO-projektin ja ylläpitää sitä aktiivisesti. Valmistaja A pyytää, että yksittäinen kehittäjä lisää kyseiseen VALOon tietyn ominaisuuden ja rahoittaa tämän kehitystyön. Kehittäjä lisää toiminnon VALO-koodipohjaan, jakaa sen avoimesti ja asettaa sen kaikkien vapaasti saataville käytettäväksi, muunneltavaksi ja uudelleenjaettavaksi. Yksittäisen kehittäjän ei katsota saattavan VALOa markkinoille. Jos valmistaja integroi VALOn digitaalisia elementtejä sisältävään tuotteeseensa, sen on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti.

3.2.6 *Voittoa tavoittelemattomat toimijat, jotka pyrkivät saavuttamaan voittoa tavoittelemattomaan toimintaan liittyviä tavoitteita*

66. Jos VALOn julkaiseva oikeushenkilö on voittoa tavoittelematon organisaatio, jonka ”perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen” (kyberkestävyyssäädöksen johdanto-osan 18 kappale), sen julkaisemaa VALOa ei katsota markkinoille saatetuksi. Jos kyseinen oikeushenkilö täyttää ”ohjelmistovastaavan” määritelmän, siihen sovelletaan tätä koskevia velvollisuuksia (kyberkestävyyssäädöksen 24 artikla).

Esimerkki 24: Oikeushenkilö julkaisee vapaan ja avoimen lähdekoodin selaimen, josta saadaan tuloa suoraan hakukonekumppanuuksien kautta, mutta kaikki sen tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan. Selainta ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi. Sen julkaisevaan oikeushenkilöön sovelletaan ohjelmistovastaaviin sovellettavia velvollisuuksia.

3.2.7 *Integrointi muiden valmistajien toimesta*

67. Joissakin tapauksissa VALOn julkaisee selvästi tunnistettava luonnollinen henkilö tai oikeushenkilö, mutta tämä VALO ”on tarkoitettu integroitavaksi muiden valmistajien toimesta niiden omiin digitaalisia elementtejä sisältäviin tuotteisiin”. Tällaisissa tapauksissa VALOa ei katsota saatetuksi EU:n markkinoille, paitsi jos sen julkaiseva henkilö (eli alkuperäinen valmistaja) saa siitä tuloa näiden ohjeiden aiempien jaksojen mukaisella tavalla.

68. Jos kyseistä VALOa ei ole saatettu markkinoille, sen julkaisevaan oikeushenkilöön sovelletaan ohjelmistovastaavalle kuuluvia velvollisuuksia, jos se tarjoaa tukea pitkäjänteisesti ohjelmistovastaavan määritelmän mukaisesti.

Esimerkki 25: Oikeushenkilö julkaisee VALO-kirjaston käyttöliittymien rakentamista varten. Se ei saa tuloa kyseisen kirjaston toimittamisesta vaan integroi sen yhteen digitaalisia elementtejä sisältävistä tuotteistaan (joka sitten saatetaan markkinoille). Kirjastoa ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi, mutta se on tarkoitettu integroitavaksi digitaalisia elementtejä sisältäviin tuotteisiin. Kirjaston julkaissut oikeushenkilö on sen ohjelmistovastaava.

Esimerkki 26: Oikeushenkilö saattaa markkinoille käyttöjärjestelmän ja julkaisee myös VALO-kirjastoja viitesovelluksiksi kyseisen käyttöjärjestelmän käyttäjille. Oikeushenkilö ei saa tuloa VALO-kirjastoista, jotka on tarkoitettu integroitaviksi muihin digitaalisia elementtejä sisältäviin tuotteisiin. VALO-kirjastot julkaiseva oikeushenkilö on niiden ohjelmistovastaava.

3.3 **Avoimen lähdekoodin ohjelmistovastaavat**

69. Kyberkestävyyssäädöksessä säädetään uudesta ”avoimen lähdekoodin ohjelmistovastaavan” oikeudellisesta luokasta, ”koska monilla digitaalisia elementtejä sisältävillä tuotteilla, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi ja jotka julkaistaan mutta joita ei aseteta saataville markkinoilla [kyberkestävyyssäädöksessä] tarkoitetulla tavalla” (kyberkestävyyssäädöksen johdanto-osan 19 kappale).

70. Joissakin tapauksissa VALOn julkaisee mutta sitä ei aseta saataville markkinoilla kyberkestävyyssäädöksessä tarkoitetulla tavalla oikeushenkilö, ”jonka tarkoituksena tai tavoitteena on järjestelmällisesti ja pitkäjänteisesti tarjota tukea sellaisten [VALOjen] kehittämistä varten, [...] jotka on tarkoitettu kaupalliseen toimintaan, ja joka varmistaa kyseisten tuotteiden toimintakelpoisuuden” (kyberkestävyyssäädöksen 3 artiklan 14 kohta). Tällaisissa tapauksissa kyseiseen oikeushenkilöön sovelletaan ohjelmistovastaavien velvollisuuksia.

71. Ohjelmistovastaavalla tarkoitetaan ”muuta oikeushenkilöä kuin valmistajaa”, koska valmistaja on määritelmän mukaan luonnollinen henkilö tai oikeushenkilö, joka saattaa digitaalisia elementtejä sisältäviä tuotteita markkinoille (”pitää niitä kaupan”) omalla nimellään tai tavaramerkillään. Oikeushenkilö voi toimia ohjelmistovastaavana vain sellaisille VALOksi katsottaville digitaalisia elementtejä sisältäville tuotteille, jotka on julkaistu mutta joita ei ole asetettu saataville markkinoilla kyberkestävyyssäädöksessä tarkoitetulla tavalla. Näin ollen ohjelmistovastaavan käsitettä sovelletaan ainoastaan sellaisiin VALOihin, ”jotka on viime kädessä tarkoitettu kaupalliseen toimintaan, kuten integroitavaksi kaupallisiin palveluihin tai digitaalisia elementtejä sisältäviin vastikkeellisiin tuotteisiin” (kyberkestävyyssäädöksen johdanto-osan 19 kappale ([13])) mutta joita ei ole asetettu saataville markkinoilla kyberkestävyyssäädöksessä tarkoitetulla tavalla ja joille kyseisen VALOn julkaiseva oikeushenkilö tarjoaa järjestelmällisesti tukea.

72. Yhden tietyn VALOn ohjelmistovastaavana toimiminen ei tarkoita, että kyseinen oikeushenkilö olisi välttämättä myös muiden julkaisemiensa VALOjen ohjelmistovastaava. Myöskään yhden tietyn VALOn valmistajana toimiminen ei tarkoita, että oikeushenkilö ei voisi olla muiden VALOjen ohjelmistovastaava. Tähän sisältyy saman VALOn yhteisöversioiden toimittaminen, kuten jaksossa *3.2.1 Hinnan periminen* selostetaan.

73. Oikeushenkilö voi näin ollen samanaikaisesti toimia yhden tietyn VALOn ohjelmistovastaavana (tarjotessaan järjestelmällisesti tukea pitkäjänteisesti ja varmistaessaan ohjelmiston toimintakelpoisuuden) ja toisen tietyn VALOn valmistajana (saattaessaan sen markkinoille). Toisin sanoen samaa oikeushenkilöä voidaan vaatia täyttämään eri tehtäviä eri VALO-hankkeissa.

74. Oikeushenkilön on varmistettava kunkin julkaisemansa VALOn osalta, katsotaanko kyseinen VALO markkinoille saatetuksi kyberkestävyyssäädöksessä tarkoitetulla tavalla. Jos katsotaan, se tekee oikeushenkilöstä ohjelmiston valmistajan. Jos VALOa ei katsota markkinoille saatetuksi, oikeushenkilö voi olla sen ohjelmistovastaava, jos ohjelmisto on tarkoitettu kaupalliseen toimintaan ja jos oikeushenkilö ylläpitää sitä ohjelmistovastaavan määritelmän mukaisesti ([14]).

3.3.1 *Pitkäjänteinen tuki ja VALOn toimintakelpoisuuden varmistaminen*

75. Johdanto-osan 19 kappaleessa selitetään, että digitaalisia elementtejä sisältävän tuotteen kehittämistä voidaan tukea pitkäjänteisesti muun muassa seuraavilla tavoilla: i) isännöimällä ja hallinnoimalla ohjelmistokehityksen yhteistyöalustoja; ii) säilyttämällä lähdekoodia tai ohjelmistoa; iii) hallinnoimalla sellaisia digitaalisia elementtejä sisältäviä tuotteita, jotka katsotaan vapaiksi ja avoimen lähdekoodin ohjelmistoiksi; ja iv) ohjaamalla tällaisten digitaalisia elementtejä sisältävien tuotteiden kehittämistä.

76. Tämä voi koskea esimerkiksi oikeushenkilöä, joka kehittää VALOn integroitavaksi omiin digitaalisia elementtejä sisältäviin tuotteisiinsa ja julkaisee sen sitten saattamatta sitä markkinoille. Tätä käsitellään myös jaksossa *3.2.7 Integrointi muiden valmistajien toimesta*. Tässä tapauksessa oikeushenkilö ei ole ohjelmiston valmistaja, mutta saattaa olla sen ohjelmistovastaava. Lisäksi, kuten aiemmissakin jaksoissa on selitetty, oikeushenkilö, joka julkaisee samasta VALOsta maksuttoman version (eli yhteisöversion) ja vastikkeellisen version, katsotaan maksuttoman version (eli yhteisöversion) ohjelmistovastaavaksi ja vastikkeellisen version valmistajaksi.

77. Vastaavasti oikeushenkilö, joka saa VALOsta tuloa mutta on voittoa tavoittelematon yhteisö, jonka tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen (ja näin ollen sen VALOa ei saateta markkinoille kyberkestävyyssäädöksessä tarkoitetulla tavalla, kuten jaksossa *3.2.6 Voittoa tavoittelemattomat* toimijat todetaan), katsotaan julkaisemansa VALOn ohjelmistovastaavaksi.

78. Lisäksi tietyt säätiöt tarjoavat yhteistyöalustoja, joilla on erilaisia hallintomuotoja, joiden avulla valmistajat voivat osallistua säännöllisesti VALOn kehittämiseen ja/tai joita valmistajat rahoittavat säännöllisesti. Tällaiset säätiöt on katsottava sellaisten VALOjen ohjelmistovastaaviksi, jotka on tarkoitettu kaupalliseen toimintaan ja joille säätiö tarjoaa pitkäjänteistä tukea. Kuten jaksossa *3.3 Avoimen lähdekoodin ohjelmistovastaavat* selitetään, tällaiseen säätiöön ei kuitenkaan saa kohdistua kyberkestävyyssäädöksen mukaisia velvollisuuksia muista tietyistä VALOista, joita se isännöi, jos se ei tarjoa järjestelmällistä tukea tietylle VALOlle, se ei varmista sen toimintakelpoisuutta ja/tai jos kyseistä ohjelmistoa ei ole tarkoitettu kaupalliseen toimintaan.

([13]) Tämä käsite sisältyy myös sanamuotoon ”tarkoitettu kaupalliseen toimintaan”, joka sisältyy kyberkestävyyssäädöksen 3 artiklan 14 kohdassa esitettyyn ”avoimen lähdekoodin ohjelmistovastaavan” määritelmään.

([14]) Kyberkestävyyssäädöksen velvollisuuksia ei sovelleta oikeushenkilöön, jos i) tiettyä VALOa ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi ja ii) oikeushenkilö ei täytä ohjelmistovastaavan määritelmää suhteessa kyseiseen VALOon.

79. Säätiöiden ja vastaavien organisaatioiden tietyille VALO-hankkeille tarjoaman ”pitkäjänteisen tuen” tyyppi voi vaihdella suuresti. Esimerkiksi tietyt oikeushenkilöt tarjoavat vain muuta kuin teknistä tukea, kuten hankkeiden brändäyksen hallintaa, hallintosääntöjen vahvistamista, yhteisötapahtumien järjestämistä tai lahjoitusten keräämistä. Muut oikeushenkilöt tarjoavat myös projektin toteuttamiseen tarvittavan tietoteknisen infrastruktuurin, esimerkiksi isännöivät lähdekoodin tietovarastoja, tarjoavat versionhallintajärjestelmiä tai luovat allekirjoitusavaimia. Toiset antavat pidemmälle menevää tukea tarjoamalla hankkeelle aktiivisesti suunnitteluresursseja, esimerkiksi palkkaamalla kehittäjiä, koordinoimalla kehitystyötä, tarkistamalla tai yhdistämällä koodia, hallitsemalla julkaisuja tai käsittelemällä haavoittuvuusraportteja ja tietoturvakorjauksia. Vaikka kaikkien kyberkestävyyssäädöksen nojalla ohjelmistovastaaviksi luokiteltavien oikeushenkilöiden on noudatettava 24 artiklan 1 ja 2 kohdassa säädettyjä velvoitteita, se, missä määrin 14 artiklan 1, 3 ja 8 kohdassa säädettyjä velvoitteita sovelletaan kyseisiin oikeushenkilöihin, riippuu 24 artiklan 3 kohdan mukaisesti siitä, millaista tukea ne tarjoavat.

80. Esimerkiksi ohjelmistovastaava, joka tarjoaa vain muuta kuin teknistä tukea, ei määritelmän mukaan osallistu digitaalisia elementtejä sisältävän tuotteen kehittämiseen, eikä hänen näin ollen tarvitse ilmoittaa aktiivisesti hyödynnetyistä haavoittuvuuksista. Ohjelmistovastaava ei myöskään tarjoa verkko- ja tietojärjestelmiä digitaalisia elementtejä sisältävien tuotteiden kehittämistä varten, eikä sen näin ollen edellytetä ilmoittavan vakavista poikkeamista Euroopan unionin kyberturvallisuusvirastolle (ENISA) ja tietoturvaloukkauksiin reagoiville ja niitä tutkiville yksiköille (CSIRT-yksikkö) tai käyttäjille, joihin poikkeama vaikuttaa. Jos ohjelmistovastaava kuitenkin saa tietoonsa aktiivisesti hyödynnetyn haavoittuvuuden (esimerkiksi ulkoisen tahon, kuten turvallisuustutkijoiden, raportista), sen olisi toimitettava tiedot digitaalisia elementtejä sisältävän tuotteen ylläpitäjille kyberturvallisuusperiaatteidensa mukaisesti. Digitaalisia elementtejä sisältävien tuotteiden ylläpitäjien ja/tai ohjelmistovastaavien olisi myös harkittava haavoittuvuudesta ilmoittamista vapaaehtoisesti 15 artiklan mukaisesti.

81. Toisaalta jos ohjelmistovastaava tarjoaa tiettyjen digitaalisia elementtejä sisältävien tuotteiden taustalla olevan tietoteknisen infrastruktuurin, sen on ilmoitettava ENISAlle ja CSIRT-yksiköille 14 artiklan 3 kohdan mukaisesti kaikista kyseiseen infrastruktuuriin liittyvistä vakavista poikkeamista, jotka vaikuttavat digitaalisia elementtejä sisältävien tuotteiden tietoturvaan. Sen on tarvittaessa ilmoitettava myös kaikille käyttäjille (esim. yleisellä ilmoituksella). Kuten edellisessä kohdassa todettiin, vaikka ohjelmistovastaavalla ei ole velvollisuutta ilmoittaa tietoonsa tulleista aktiivisesti hyödynnetyistä haavoittuvuuksista, sen pitäisi edistää haavoittuvuuksien asianmukaista käsittelyä ja harkita vapaaehtoista ilmoittamista 15 artiklan mukaisesti.

82. Jos ohjelmistovastaava tarjoaa myös suunnitteluresursseja tietyille digitaalisia elementtejä sisältäville tuotteille, sen on i) ilmoitettava 14 artiklan 1 kohdan mukaisesti tietoonsa tulleista aktiivisesti hyödynnetyistä haavoittuvuuksista; ja ii) ilmoitettava tarvittaessa kaikille käyttäjille. Siltä osin kuin ohjelmistovastaavalla on suora suhde käyttäjiin, joihin vaikutukset kohdistuvat, sen on 14 artiklan 8 kohdan mukaisesti myös ilmoitettava asiasta suoraan heille.

83. Jos toimija lopettaa järjestelmällisen tuen pitkäjänteisen tarjoamisen tietylle VALOlle, se ei ehkä enää täytä ohjelmistovastaavan määritelmää eikä sen vuoksi ehkä enää ole sitä koskevien velvoitteiden alainen. Tällaisissa tapauksissa kyseistä toimijaa kannustetaan ilmoittamaan selkeästi asemansa muuttumisesta kyseisen VALOn suhteen.

84. Joissain tilanteissa toimija, joka on aiemmin toiminut tietyn hankkeen ohjelmistovastaavana, voi päättää alkaa saada kyseisestä hankkeesta tuloa suoraan, jolloin se saattaa digitaalisia elementtejä sisältävän tuotteen markkinoille ja siihen aletaan soveltaa valmistajaa koskevia kyberkestävyyssäädöksen velvoitteita. Tällaisessa tilanteessa kyseinen toimija katsotaan digitaalisia elementtejä sisältävän tuotteen valmistajaksi siitä päivästä alkaen, jona se saattaa tuotteen markkinoille (mutta ei sellaisten aiempien versioiden suhteen, joiden ohjelmistovastaavana se toimi).

3.4 **Osallistujat ja tuotantoketjun loppupään käyttö**

85. Kuten jaksossa *3.1 Sen määrittäminen, kuuluuko vapaa ja avoimen* lähdekoodin ohjelmisto tietyn toimijan vastuulle jo mainittiin, kyberkestävyyssäädöksessä selvennetään, että sitä ei sovelleta ”luonnollisiin henkilöihin tai oikeushenkilöihin, jotka kehittävät lähdekoodia vapaiksi ja avoimen lähdekoodin ohjelmistoiksi katsottaviin digitaalisia elementtejä sisältäviin tuotteisiin, jotka eivät ole kyseisten henkilöiden vastuulla” (johdanto-osan 18 kappale).

86. Myöskään digitaalisia elementtejä sisältävien tuotteiden valmistajat, jotka integroivat VALO-komponentteja omiin digitaalisia elementtejä sisältäviin tuotteisiinsa, eivät ole vastuussa siitä, että kyseiset komponentit ovat yksittäin kyberkestävyyssäädöksen vaatimusten mukaisia, vaikka valmistajat tuottaisivat lähdekoodin niiden ylläpitoa varten.

87. Myöskään pelkästään se seikka, että valmistajat integroivat VALO-komponentteja omiin (vastikkeellisiin) digitaalisia elementtejä sisältäviin tuotteisiinsa, ei vaikuta kyseisen VALO-komponentin asemaan kyberkestävyyssäädöksen suhteen. Sellaisten VALO-komponenttien ylläpitäjillä, joita ei ole saatettu markkinoille, ei ole velvoitteita suhteessa muihin toimijoihin, jotka saattavat integroida tällaisia komponentteja digitaalisia elementtejä sisältäviin tuotteisiinsa. Se, sovelletaanko kyberkestävyyssäädöstä tiettyyn VALO-komponenttiin, riippuu yksinomaan siitä, saattaako julkaiseva luonnollinen henkilö tai oikeushenkilö sen markkinoille.

88. Digitaalisia elementtejä sisältävien tuotteiden valmistajien, jotka integroivat VALO-komponentteja, on kuitenkin noudatettava kyberkestävyyssäädöstä digitaalisia elementtejä sisältävien omien tuotteidensa osalta. Niillä on myös 13 artiklan 5 kohdan mukainen asianmukaisen huolellisuuden velvoite integroimiensa VALO-komponenttien suhteen. Lisäksi niiden on ilmoitettava integroitujen komponenttien haavoittuvuuksista ja jaettava tietoturvakorjauksia 13 artiklan 6 kohdan mukaisesti. Lisätietoja tästä aiheesta on jaksossa *9.2.1 Raportointi ketjun alkupäähän ja tietoturvakorjausten jakaminen*.

3.5 **Havainnollistavat skenaariot**

89. Seuraavassa luetellut esimerkit ovat täysin hypoteettisia, ja niiden tarkoituksena on vain havainnollistaa edellä olevissa jaksoissa selitettyjä tapauksia.

Esimerkki 27: Yksittäinen kehittäjä A on kehittänyt VALOn. Kehittäjä A julkaisee VALOn omalla nimellään tai tavaramerkillään mutta ei peri sen käytöstä hintaa. Ohjelmisto on avoimesti jaettu ja vapaasti kaikkien käytettävissä, muunneltavissa ja jaettavissa uudelleen. Kehittäjä A lisää myös linkin alustalle, jolla kerätään vapaaehtoisia lahjoituksia.

Yritykset B, C ja D integroivat VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa. Yritykset B, C ja D tekevät vapaaehtoisia lahjoituksia kehittäjälle A tukeakseen jatkuvaa ylläpitoa. Näiden lahjoitusten avulla kehittäjä A voi ylläpitää hanketta aktiivisesti.

Tätä VALOa ei ole saatettu markkinoille kyberkestävyyssäädöksessä tarkoitetulla tavalla. Kehittäjällä A ei ole velvoitteita kyberkestävyyssäädöksen nojalla. Yritysten B, C ja D on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti integroidessaan kyseisen VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa.

Esimerkki 28: Voittoa tavoittelematon säätiö F julkaisee VALO-komponentin integroitavaksi muihin digitaalisia elementtejä sisältäviin kaupallisiin tuotteisiin. Säätiö F sitoutuu tarjoamaan tälle VALOlle pitkäjänteistä tukea sen toimintakelpoisuuden ja käyttöönoton varmistamiseksi. Yritykset A, B ja C integroivat tämän VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa. Yritykset A ja B antavat vapaaehtoisesti osan kehittäjiensä ajasta VALO-hankkeiden kehittämiseen ja ylläpitoon säätiön F sisällä, myös kyseisen VALOn osalta.

Koska säätiö F on voittoa tavoittelematon järjestö, jonka perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen, VALOa ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi. Säätiö F on VALOn ohjelmistovastaava, ja siihen sovelletaan 24 artiklassa säädettyjä ohjelmistovastaavan velvoitteita. Yritysten A, B ja C on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti integroidessaan kyseisen VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa.

Esimerkki 29: Yritys A on kehittänyt VALO-komponentin integroitavaksi omiin digitaalisia elementtejä sisältäviin tuotteisiinsa. Se julkaisee VALOn myös erikseen omalla nimellään tai tavaramerkillään ja ylläpitää sitä aktiivisesti. Se ei kuitenkaan veloita sen käytöstä eikä saa siitä tuloa muilla tavoilla. Yritykset B, C ja D integroivat VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa ja antavat vapaaehtoisesti osan kehittäjiensä ajasta sen ylläpitoon.

Tätä VALOa ei katsota kyberkestävyyssäädöksessä tarkoitetulla tavalla markkinoille saatetuksi. Yritys A ei ole sen valmistaja vaan sen ohjelmistovastaava. Yritysten B, C ja D on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti integroidessaan kyseisen VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa.

Esimerkki 30: Yritys A julkaisee VALOn omalla nimellään tai tavaramerkillään ja tarjoaa sitä maksullisena versiona, joka sisältää tiettyjä etuja, kuten teknistä tukea tai suorituskyvyn optimointia. Yritysten B, C ja D kehittäjät osallistuvat VALOn ylläpitoon, mutta se pysyy yrityksen A määräysvallassa.

Yritys A katsotaan kyseisen VALOn valmistajaksi ([15]). *Yrityksiin B, C ja D ei sovelleta kyberkestävyyssäädöksen velvoitteita kyseisen VALOn osalta. Jos ne integroivat kyseisen VALOn omiin digitaalisia elementtejä sisältäviin tuotteisiinsa, niiden on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti.*

Esimerkki 31: Yritys A julkaisee VALOn omalla nimellään tai tavaramerkillään ja tarjoaa jatkuvaa ylläpitoa sen pitkän aikavälin toimintakelpoisuuden varmistamiseksi, jotta ohjelmisto voidaan integroida muiden yritysten digitaalisia elementtejä sisältäviin tuotteisiin. Yritys A ei veloita sen käytöstä, ei käsittele digitaalisia elementtejä sisältävän tuotteen kautta keräämiään henkilötietoja eikä myy VALOn julkaisemiseen liittyviä tukipalveluja.

Yritys B tuottaa koodia ja antaa kehittäjien aikaa VALOn ylläpitoon mutta ei jaa sitä kaupallisesti. Yritys B tarjoaa teknisiä tukipalveluja, joita ei ole kytketty VALOn jakeluun. Yritys A katsotaan VALOn ohjelmistovastaavaksi, kun taas yrityksellä B ei ole kyberkestävyyssäädöksen nojalla velvoitteita kyseisen VALOn suhteen.

Esimerkki 32: Voittoa tavoittelematon toimija, jonka perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen, julkaisee VALO-komponentin. Toimija tarjoaa pitkäjänteistä tukea hankkeen pitkän aikavälin toimintakelpoisuuden varmistamiseksi. Ylläpitoa rahoitetaan julkisella rahoituksella, kuten tutkimusavustuksilla. Lisäkehitystyötä, kuten uusia ominaisuuksia, rahoitetaan lahjoituksilla ja erityishankkeilla, jotka toteutetaan yhteistyössä sellaisten valmistajien kanssa, jotka integroivat kyseisen VALOn digitaalisia elementtejä sisältäviin tuotteisiinsa. Nämä ominaisuudet sisällytetään VALOn koodipohjaan.

Voittoa tavoittelematon toimija, joka julkaisee VALOn, katsotaan kyseisen VALO-komponentin ohjelmistovastaavaksi. Valmistajasta, joka on osallistunut tiettyjen ominaisuuksien kehittämiseen, ei tule kyseisen VALO-komponentin valmistajaa. Jos valmistaja integroi kyseisen VALO-komponentin omaan digitaalisia elementtejä sisältävään tuotteeseensa, sen on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti.

Esimerkki 33: Voittoa tavoittelematon yhteisö, jonka perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen, julkaisee VALO-ohjelmistokehityspaketin (SDK) ja huolehtii sen jatkuvasta ylläpidosta. SDK on avoimesti jaettu ja vapaasti kaikkien käytettävissä, muunneltavissa ja jaettavissa uudelleen. Rahoitus toteutetaan voittoa tavoittelemattomalle toimijalle maksettavien jäsenmaksujen muodossa, ja jäsenorganisaatioiden palveluksessa olevat kehittäjät tuottavat SDK:n kehittämiseksi koodia ja muita resursseja. Valmistajat käyttävät SDK:ta komponenttina muiden digitaalisia elementtejä sisältävien tuotteiden rakentamiseksi.

Voittoa tavoittelematon toimija, joka julkaisee SDK:n, on sen ohjelmistovastaava. Säätiön jäsenet eivät ole vastuussa SDK:n kyberkestävyyssäädöksen mukaisuudesta. Jos valmistajat käyttävät SDK:ta rakentaakseen oman digitaalisia elementtejä sisältävän tuotteensa, niiden on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti.

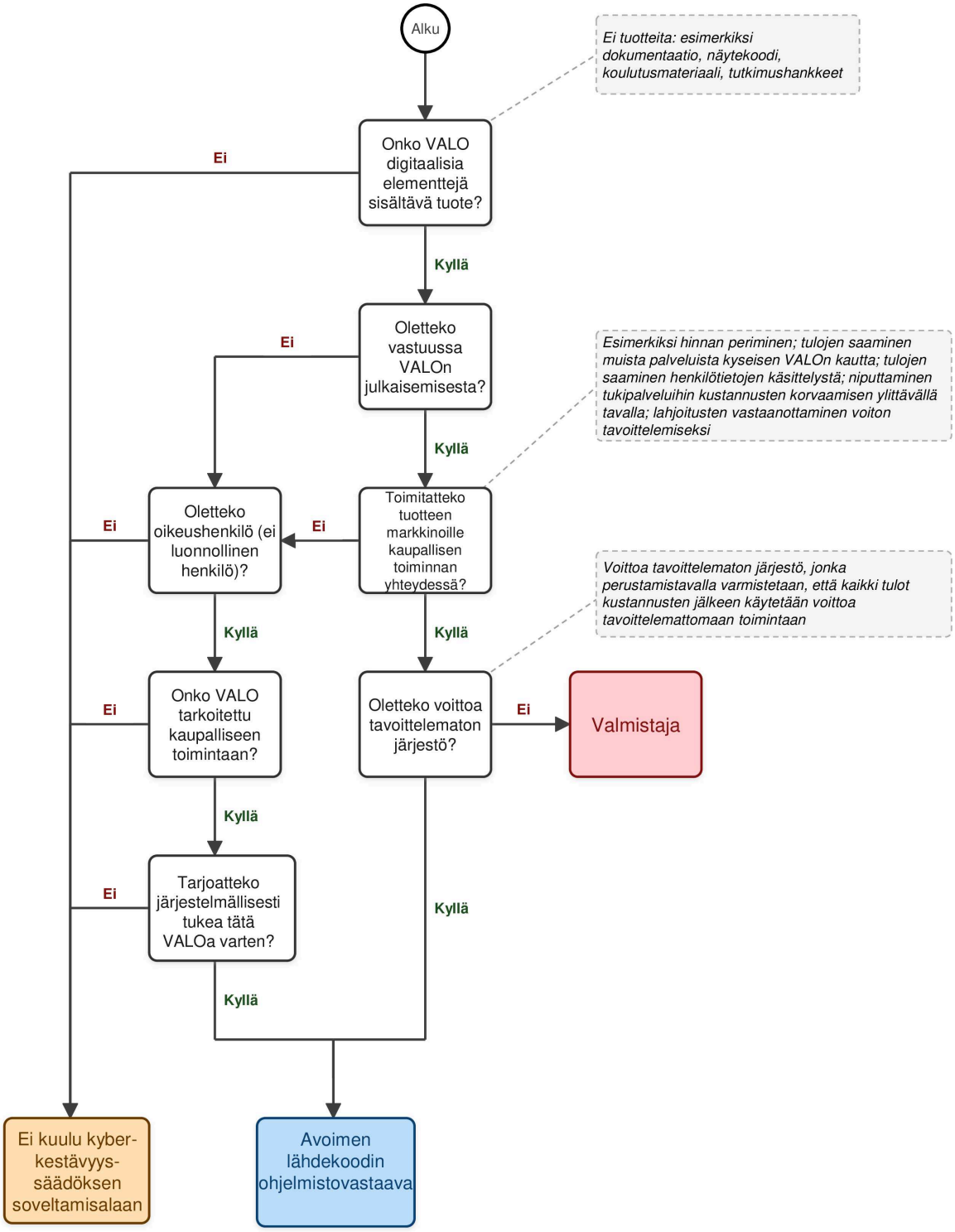
Esimerkki 34: Yksittäinen kehittäjä julkaisee VALO-kirjaston tietyn ohjelmointikielen julkisessa pakettivarastossa ja ylläpitää sitä aktiivisesti. Kehittäjä lisää paketin dokumentaatioon linkin lahjoitusten keräämiseksi. Valmistaja lataa kyseisen kirjaston varastosta maksutta ja integroi sen omaan digitaalisia elementtejä sisältävään tuotteeseensa.

Yksittäisellä kehittäjällä ja pakettivarastolla ei ole kyberkestävyyssäädökseen liittyviä velvoitteita. Kirjaston integroivan valmistajan on noudatettava asianmukaista huolellisuutta 13 artiklan 5 kohdan mukaisesti.

([15]) Jos yritys A on voittoa tavoittelematon toimija, jonka perustamistavalla varmistetaan, että kaikki tulot kustannusten jälkeen käytetään voittoa tavoittelemattomaan toimintaan liittyvien tavoitteiden saavuttamiseen, se katsotaan kuitenkin VALOn ohjelmistovastaavaksi.

Kaavio 1

Tyylitelty vuokaavio kyberkestävyyssäädöksen soveltamisalasta vapaiden ja avoimen lähdekoodin ohjelmistojen suhteen



4. MERKITTÄVÄT MUUTOKSET JA VARAOSAT

90. Kyberkestävyyssäädöksen 3 artiklan 30 kohdassa ”merkittävä muutos” määritellään digitaalisia elementtejä sisältävään tuotteeseen sen markkinoille saattamisen jälkeen tehdyksi muutokseksi, joka i) vaikuttaa siihen, täyttääkö digitaalisia elementtejä sisältävä tuote liitteessä I olevassa I osassa vahvistetut olennaiset vaatimukset tai ii) muuttaa käyttötarkoitusta, jota varten digitaalisia elementtejä sisältävä tuote on arvioitu.

91. Merkittävän muutoksen käsite on merkityksellinen määritettäessä kyberkestävyyssäädöksen mukaisia velvoitteita useissa tapauksissa, kuten seuraavissa:

a) 21 artiklan mukaisesti maahantuojaa tai jakelijaa pidetään valmistajana, kun kyseinen maahantuoja tai jakelija tekee merkittävän muutoksen markkinoille jo saatettuun digitaalisia elementtejä sisältävään tuotteeseen,

b) 22 artiklan mukaisesti ketä tahansa luonnollista henkilöä tai mitä tahansa oikeushenkilöä, joka tekee digitaalisia elementtejä sisältävään tuotteeseen merkittävän muutoksen ja asettaa kyseisen tuotteen saataville markkinoilla, pidetään kyseisen tuotteen valmistajana,

c) 69 artiklan 2 kohdan mukaisesti ketä tahansa luonnollista henkilöä tai mitä tahansa oikeushenkilöä, joka tekee ennen 11:ttä joulukuuta 2027 markkinoille saatettuihin digitaalisia elementtejä sisältäviin tuotteisiin 11. joulukuuta 2027 alkaen merkittävän muutoksen ja asettaa kyseisen tuotteen saataville markkinoilla, pidetään kyseisen tuotteen valmistajana,

d) jotta voidaan määrittää 11. joulukuuta 2027 alkaen markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden valmistajien osalta, onko digitaalisia elementtejä sisältävälle tuotteelle tehtävä uusi vaatimustenmukaisuuden arviointi kyseisen päivämäärän jälkeen tehtyjen muutosten johdosta erityisesti ohjelmistokehityksen iteratiivisen luonteen vuoksi.

92. Siksi on tärkeää antaa ohjeita, jotta talouden toimijat ymmärtävät, milloin laitteisto- tai ohjelmistomuutokset katsotaan merkittäviksi muutoksiksi.

4.1 **Fyysiset korjaukset**

93. Kuten kyberkestävyyssäädöksen johdanto-osan 42 kappaleessa todetaan, ”digitaalisia elementtejä sisältävän tuotteen kunnostaminen, kunnossapito ja korjaaminen Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/1781 2 artiklan 18, 19 ja 20 alakohdassa määritellyllä tavalla ei välttämättä johda tuotteen merkittävään muutokseen esimerkiksi, jos käyttötarkoitus ja toiminnot eivät muutu ja riskitaso säilyy ennallaan. Valmistajan suorittama digitaalisia elementtejä sisältävän tuotteen parannus voi kuitenkin johtaa muutoksiin kyseisen tuotteen suunnittelussa ja kehittämisessä ja näin ollen vaikuttaa sen käyttötarkoitukseen ja siihen, onko kyseinen tuote tässä asetuksessa vahvistettujen vaatimusten mukainen.” Tämä vastaa sinisen oppaan 2.1 kohtaa, jossa mainitaan, että ”tuotetta, johon on käyttöönoton jälkeen tehty merkittäviä muutoksia tai korjauksia, on pidettävä uutena tuotteena, jos i) sen alkuperäinen suorituskyky, käyttötarkoitus tai tyyppi muuttuu ilman, että tämä olisi otettu huomioon alkuperäisessä riskinarvioinnissa, ii) vaaran luonne on muuttunut tai riskin taso on kasvanut suhteessa asiaa koskevaan unionin yhdenmukaistamislainsäädäntöön ja iii) tuote asetetaan saataville (tai otetaan käyttöön, jos sovellettava lainsäädäntö kattaa myös käyttöönoton). Tätä on tarkasteltava tapauskohtaisesti ja etenkin ottamalla huomioon lainsäädännön tavoitteet ja kyseisen lainsäädännön soveltamisalaan kuuluvien tuotteiden tyyppi.”

94. Kunnostamis-, kunnossapito- ja korjaamistoimet, joista on seurauksena jo markkinoille saatettujen digitaalisia elementtejä sisältävien tuotteiden fyysisiä muutoksia, eivät välttämättä muodosta merkittävää muutosta. Näin ollen olisi tehtävä tapauskohtainen arviointi, jotta voidaan määrittää, vaikuttavatko tämänkaltaiset fyysiset muutokset siihen, täyttääkö digitaalisia elementtejä sisältävä tuote liitteessä I olevassa osassa I vahvistetut olennaiset vaatimukset, tai muuttuuko muutosten seurauksena tuotteen käyttötarkoitus tavalla, joka sisältyy kyberturvallisuusriskien arvioinnin piiriin.

95. Viallisten tai kuluneiden osien vaihtaminen suorituskyvyltään parempiin osiin (esimerkiksi teknisen edistyksen vuoksi tai koska vanhaa osaa ei enää valmisteta) ei itsessään saa aikaan merkittävää muutosta korjattuun digitaalisia elementtejä sisältävään tuotteeseen. Näin käy vain siinä tapauksessa, että suorituskyvyn muutos tai se, miten korjattu digitaalisia elementtejä sisältävä tuote toimii, i) vaikuttaa siihen, täyttääkö tuote olennaiset vaatimukset, tai ii) muuttaa käyttötarkoitusta tavalla, joka ei sisältynyt riskinarvioinnin piiriin.

Esimerkki 35: Tietokonepalvelimen valmistaja tekee korjauksen, jossa viallinen RAM-muisti vaihdetaan uuteen, suorituskyvyltään parempaan. Vaihdolla ei ole vaikutusta siihen, täyttääkö palvelin olennaiset vaatimukset. Palvelin toimii paremmin, mutta sen uusi suorituskyky on edelleen palvelimen käyttötarkoituksen mukainen siten kuin kyberturvallisuusriskien arvioinnissa huomioitiin. Tietokonepalvelinta ei pidetä merkittävästi muutettuna.

4.2 **Varaosat**

96. Kyberkestävyyssäädöksen 2 artiklan 6 kohdassa todetaan, että kyberkestävyyssäädöstä ei sovelleta varaosiin, joilla korvataan samanlaisia komponentteja ja jotka valmistetaan samojen eritelmien mukaisesti kuin komponentit, jotka niillä on tarkoitus korvata. Johdanto-osan 29 kappaleessa todetaan lisäksi, että tämä poikkeus koskee sekä ennen tämän asetuksen soveltamispäivää saataville asetettujen digitaalisia elementtejä sisältävien tuotteiden varaosia että varaosia, joille on jo tehty tämän asetuksen mukainen vaatimustenmukaisuuden arviointimenettely.

97. Kyberkestävyyssäädöksen 2 artiklan 6 kohdassa esitetyn poikkeuksen olisi ymmärrettävä koskevan vain tapauksia, joissa varaosa toimitetaan nimenomaisesti markkinoille jo (ennen 11:ttä joulukuuta 2027 tai sen jälkeen) saatetun digitaalisia elementtejä sisältävän tuotteen korjaamiseksi tai tuotteen käyttöiän pidentämiseksi. Jos digitaalisia elementtejä sisältävä tuote toimitetaan erillisenä tuotteena ilman, että sillä on mitään yhteyttä olemassa olevan digitaalisia elementtejä sisältävän tuotteen kunnossapitoon tai korjaamiseen, se saatetaan markkinoille kyberkestävyyssäädöksessä tarkoitetulla tavalla, eikä sitä olisi pidettävä 2 artiklan 6 kohdan soveltamisalaan kuuluvana varaosana. Kunnossapito- tai korjaustarkoituksen pitäisi käydä ilmi markkinoille toimittamisen asiayhteydestä, esimerkiksi digitaalisia elementtejä sisältävän tuotteen tai tuoteperheen yksilöivistä tiedoista tilauksessa tai kaupallisessa tarjouksessa tai toimittamisesta myynnin jälkeisten kanavien tai huoltokanavien kautta. Lisäksi markkinavalvontaviranomaisten saatavilla olisi pidettävä tätä tukevaa näyttöä. Se, että digitaalisia elementtejä sisältävällä tuotteella voitaisiin teknisesti korvata komponentti, ei itsessään riitä saattamaan tuotetta poikkeuksen soveltamisalaan, jos tällaisia elementtejä ei ole.

98. Vastaavasti jos varaosa on identtinen digitaalisia elementtejä sisältävään tuotteeseen jo sisältyvän komponentin kanssa, kun tuote on joko saatettu markkinoille ennen kyberkestävyyssäädöksen soveltamispäivää tai saatettu markkinoille kyberkestävyyssäädöksen mukaisesti, kyseinen varaosa ei kuulu kyberkestävyyssäädöksen soveltamisalaan.

99. Arvioitaessa, olisiko varaosan katsottava olevan identtinen komponentin kanssa, olisi keskityttävä sen toiminnalliseen rooliin digitaalisia elementtejä sisältävässä tuotteessa sekä kyberturvallisuuden kannalta mahdollisesti merkityksellisiin ominaisuuksiin. Vaikka tapauskohtainen arviointi on aina tarpeen, erot, jotka eivät vaikuta komponentin turvallisuusominaisuuksiin tai kyberturvallisuusriskiprofiiliin, eivät sinänsä estä sitä, että kyseinen varaosa voisi kuulua kyberkestävyyssäädöksen 2 artiklan 6 kohdan soveltamisalaan.

100. Sen sijaan erot komponentin kyberturvallisuuden kannalta merkityksellisissä ominaisuuksissa, kuten algoritmeissa, protokollissa, salausmekanismeissa, pääsynvalvontaominaisuuksissa tai muissa turvallisuuden kannalta merkityksellisissä ominaisuuksissa, voivat tarkoittaa, että uutta osaa ei voida pitää identtisenä korvattavan komponentin kanssa.

101. Jos varaosa ei ole identtinen alkuperäisen komponentin kanssa, kyseinen varaosa muodostaa itsessään digitaalisia elementtejä sisältävän tuotteen, ja siksi kyberkestävyyssäädöstä sovelletaan siihen. Tällaisissa tapauksissa olennaisten vaatimusten täyttyminen on arvioitava korvaavan komponentin käyttötarkoituksen perusteella. Erityisen merkityksellinen on korvaavan komponentin tehtävä varmistaa yhteensopivuus tai yhteentoimivuus olemassa olevan digitaalisia elementtejä sisältävän tuotteen kanssa. Näin on myös silloin, kun kyseinen tuote on digitaalisia elementtejä sisältävä tuote, joka on saatettu markkinoille ennen kuin kyberkestävyyssäädöstä alettiin soveltaa. Jos tiettyjä olennaisia vaatimuksia ei voida kohtuudella täyttää kyseisen käyttötarkoituksen tai teknisten rajoitusten vuoksi, valmistajan on otettava tämä huomioon kyberturvallisuusriskien arvioinnissa ja toteutettava asianmukaisia vaihtoehtoisia tai korvaavia riskinvähentämistoimenpiteitä, jotta digitaalisia elementtejä sisältävän tuotteen turvallisuus ei heikkene. Kuten myös jaksossa *2.6 Kompleksiset järjestelmät* todetaan, sekä tekniset asiakirjat että käyttäjälle annettavat tiedot ja ohjeet ovat yksi avaintekijä, jotta voidaan kuvata läpinäkyvästi tunnistetut rajoitteet, niihin liittyvät kyberturvallisuusriskit ja toteutetut riskinhallintatoimenpiteet. Kuten jaksossa *4.1 Fyysiset korjaukset* selitetään, viallisten tai kuluneiden osien vaihtaminen suorituskyvyltään parempiin osiin ei itsessään saa aikaan merkittävää muutosta korjattuun digitaalisia elementtejä sisältävään tuotteeseen.

Esimerkki 36: Valmistaja on saattanut EU:n markkinoille yhdistettyjä ohjaimia. Yhdessä tapauksessa ohjain saatettiin markkinoille vuonna 2026 ennen kyberkestävyyssäädöksen soveltamispäivää. Toisessa tapauksessa ohjain saatettiin markkinoille vuonna 2028 kyberkestävyyssäädöksen mukaisesti. Vuonna 2028 molemmissa ohjaintyypeissä oleva digitaalinen tietoliikennemoduuli lakkaa toimimasta. Valmistaja toimittaa varaosana korvaavan moduulin, joka on identtinen alkuperäisen kanssa ja valmistettu samojen määritysten mukaisesti.

Molemmissa tapauksissa korvaava moduuli kuuluu 2 artiklan 6 kohdassa mainitun poikkeuksen soveltamisalaan. Vaikka varaosa on digitaalisia elementtejä sisältävä tuote, itse varaosaan ei sovelleta kyberkestävyyssäädöstä, koska varaosa korvaa identtisen komponentin digitaalisia elementtejä sisältävässä tuotteessa. Korjaus ei merkitse merkittävää muutosta digitaalisia elementtejä sisältävään tuotteeseen.

Esimerkki 37: Valmistaja saattoi EU:n markkinoille yhdistettävän teollisuusohjaimen vuonna 2026 ennen kyberkestävyyssäädöksen soveltamispäivää. Vuonna 2028 kyseisen ohjaimen tietoliikennesiru lakkaa toimimasta. Koska valmistaja ei enää valmista kyseistä sirua, se toimittaa yhteensopivuuden säilyttämiseksi ja käytön jatkamisen mahdollistamiseksi varaosana uudemman, toiminnoiltaan vastaavan sirun, jossa on kuitenkin erilainen salauksen toteutus ja päivitetty suojatun käynnistyksen mekanismi.

Tässä tapauksessa korvaavaa sirua ei voida pitää identtisenä, koska salauksen toteutuksen ja suojatun käynnistyksen mekanismin erot vaikuttavat sirun kyberturvallisuusominaisuuksiin. Sen vuoksi siihen ei sovelleta 2 artiklan 6 kohdassa mainittua poikkeusta, ja se on kyberkestävyyssäädöksen soveltamisalaan kuuluva digitaalisia elementtejä sisältävä tuote. Korvaavan osan vaatimustenmukaisuus on arvioitava ottaen huomioon sen käyttötarkoitus, mukaan lukien sen rooli ennen kyberkestävyyssäädöksen soveltamista markkinoille saatetun digitaalisia elementtejä sisältävän tuotteen yhteentoimivuuden varmistamisessa.

Esimerkki 38: Valmistaja saattaa markkinoille älytalo-ohjaimen vuonna 2028 kyberkestävyyssäädöksen mukaisesti. Vuonna 2029 kyseisen ohjaimen langaton moduuli lakkaa toimimasta. Koska valmistaja ei enää valmista kyseistä moduulia, se toimittaa varaosana uuden moduulin, jolla on sama tehtävä ja jossa hyödynnetään samoja viestintäprotokollia ja turvamekanismeja, mutta joka perustuu eri piirisarjaan ja sisältää päivitetyn laiteohjelmiston, joka ei muuta kyberturvallisuuden kannalta merkityksellisiä ominaisuuksia.

Tässä tapauksessa korvaavaa moduulia voidaan pitää identtisenä. Näin ollen moduuliin sovelletaan 2 artiklan 6 kohdassa mainittua poikkeusta, eikä siihen sovelleta kyberkestävyyssäädöstä.

102. Varaosia koskevaa poikkeusta sovelletaan riippumatta siitä, korvaako varaosa digitaalisia elementtejä sisältävään tuotteeseen sisältyvän komponentin vai korvaako se kokonaisen digitaalisia elementtejä sisältävän tuotteen, joka puolestaan on osa suurempaa tuotetta, myös silloin, kun kyseinen suurempi digitaalisia elementtejä sisältävä tuote koostuu useista integroiduista komponenteista, edellyttäen, että korvaava osa toimitetaan nimenomaisesti varaosana, kuten edellisissä kohdissa on selitetty.

Esimerkki 39: Vuonna 2027 valmistaja saattaa markkinoille teollisen automaatiojärjestelmän, jonka yhtenä komponenttina on ohjelmoitava logiikkaohjain (PLC). Vuonna 2031 PLC:n keskusyksikkö lakkaa toimimasta. Valmistaja tarjoaa kaksi korjausvaihtoehtoa: i) korvaavan, alun perin asennettuun keskusyksikköön nähden identtisenä pidettävän keskusyksikön toimittaminen tai ii) kokonaisen, alun perin asennettuun PLC:hen nähden identtisenä pidettävän korvaavan PLC:n toimittaminen. Kummassakin tapauksessa korvaava tuote toimitetaan valmistajan toimituksen jälkeisen palvelukanavan kautta, ja teollisuusautomaatiojärjestelmä, johon korvaava tuote on tarkoitettu, on selkeästi yksilöity. Molemmissa tapauksissa korvaava tuote kuuluu 2 artiklan 6 kohdassa mainitun poikkeuksen soveltamisalaan riippumatta siitä, onko korvaava tuote PLC:hen sisältyvä komponentti vai koko PLC.

4.3 **Ohjelmistopäivitykset merkittävänä muutoksena**

103. Ohjelmiston kehitys on luonteeltaan iteratiivista, ja markkinoille jo saatettuja digitaalisia elementtejä sisältäviä ohjelmistotuotteita päivitetään säännöllisesti ja jatkuvasti. Tässä yhteydessä on hyödyllistä antaa enemmän ohjeita sen selvittämiseksi, milloin ohjelmistoa on pidettävä merkittävästi muutettuna. Tällaisten ohjeiden tarkoituksena on erityisesti auttaa omiin digitaalisia elementtejä sisältäviin ohjelmistotuotteisiinsa muutoksia tekeviä valmistajia määrittämään, tarkoittavatko tehdyt muutokset merkittävää muutosta.

104. Johdanto-osan 39 kappaleessa todetaan, että digitaalisia elementtejä sisältävää tuotetta muutetaan merkittävästi, jos muutos muuttaa kyberturvallisuusriskitasoa ja jos valmistaja ei ole ottanut tällaista muuttunutta tai uutta riskiä huomioon riskinarvioinnissaan ja näin ollen olennaisten vaatimusten noudattamisessaan. Valmistajan olisi sen vuoksi arvioitava tapauskohtaisesti, aiheuttaako ohjelmistopäivitys uusia tai lisääntyneitä kyberturvallisuusriskejä ja onko tällaisia riskejä jo käsitelty valmistajan riskinarvioinnissa.

105. Jos valmistaja ottaa käyttöön digitaalisia elementtejä sisältävään tuotteeseen uusia toimintoja, joiden seurauksena tuotteen käyttötarkoitus kokonaisuudessaan muuttuu, on todennäköistä, että valmistaja ei ottanut tällaisia muutoksia huomioon riskinarvioinnissaan. Tällaisissa olosuhteissa muutos katsotaan yleensä merkittäväksi muutokseksi.

Esimerkki 40: Valmistaja saattaa markkinoille kojetaulun, joka kerää tietoja koneista ja näyttää suuntauksia ja hälytyksiä, mutta sillä ei pysty hallinnoimaan kyseisiä koneita. Tämän jälkeen valmistaja kehittää kojetaulusta uuden version ja ottaa käyttöön toimintoja, joiden avulla kojetaululla voi hallinnoida koneita muun muassa säätämällä käyttöparametreja ja käynnistämällä koneet uudelleen vikatilanteiden jälkeen. Näiden muutosten seurauksena kojetaulun käyttötarkoitus on muuttunut riskinarvioinnissa kaavaillusta, ja tuote on muuttunut tilannetietoisuuteen liittyvästä välineestä digitaalisia elementtejä sisältäväksi tuotteeksi, jolla on tarkoitus hallinnoida muiden laitteiden toimintaa. Näin ollen kojetaulua on muutettu merkittävästi.

Esimerkki 41: Valmistaja saattaa markkinoille kuluttajille suunnatun ohjelmistosovelluksen, jolla on tarkoitus järjestää ja esittää henkilötietoja, kuten sähköposteja, viestejä tai asiakirjoja, sekä mahdollistaa perustason haku- ja suodatustoiminnot. Tämän jälkeen valmistaja tuo sovellukseen päivityksen, jonka avulla sovellus voi automaattisesti analysoida käyttäjän sisältöä ja luoda käyttäytymisprofiileja ja tehdä automaattisia päätöksiä, jotka vaikuttavat sisällön priorisointiin, estämiseen tai suositteluun ilman käyttäjän toimia. Muutoksen seurauksena ohjelmiston käyttötarkoitus muuttuu käyttäjän hallinnoimasta tiedonhallintatyökalusta automatisoiduksi päätöksentekojärjestelmäksi, mitä ei huomioitu riskienarvioinnissa. Näin ollen sovellusta on muutettu merkittävästi.

106. Samalla on kuitenkin mahdollista, että valmistaja ottaa asteittain käyttöön uusia toimintoja, jotka on jo sisällytetty riskinarviointiin tai jotka eivät sinänsä muuta digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskiprofiilia. Näin voi olla esimerkiksi silloin, kun valmistaja on ennakoinut kyseisten toimintojen kehittämisen, jo kuvaillut ja arvioinut niihin liittyvät riskit ja toteuttanut asianmukaisia lieventäviä toimenpiteitä, joilla varmistetaan jatkuva olennaisten vaatimusten noudattaminen. Näin voi olla myös silloin, kun uudet toiminnot eivät saa aikaan muutoksia, jotka aiheuttavat uusia tai lisääntyneitä riskejä. Tämänkaltaisia päivityksiä ei siksi pitäisi pitää merkittävinä muutoksina, koska ne eivät lisää kyberturvallisuusriskiä eivätkä näin ollen muuta olennaisten vaatimusten noudattamista.

Esimerkki 42: Valmistaja julkaisee viestintäsovelluksen, jonka toiminnot rajoittuvat aluksi kahdenväliseen viestintään. Valmistajan riskinarvioinnissa on otettu huomioon, että myöhemmin voidaan ottaa käyttöön ryhmäviestit ja esimerkiksi se, että viestien reititys voi monimutkaistua. Myöhemmässä päivityksessä valmistaja lisää ryhmäkeskustelutoiminnon sekä ylläpitäjän valvontaominaisuuksia ja moderointityökaluja, jotka oli jo ennakoitu ja arvioitu alkuperäisessä suunnitelmassa. Päivityksellä toteutetaan toimintoja, jotka kuuluvat alkuperäisen käyttötarkoituksen ja riskinarvioinnin piiriin. Näin ollen viestisovellusta ei ole muutettu merkittävästi.

Esimerkki 43: Markkinoille on saatettu tuotannonvalvontajärjestelmä, jossa on käytössä vain luku -ominaisuuden sisältävät koontinäytöt. Järjestelmäarkkitehtuurissa on automaattisia säätötoimintoja, mutta ne pysyvät poissa käytöstä. Valmistajan riskinarviointi kattaa nimenomaisesti automaattisten säätöpiirien tulevan aktivoinnin, mukaan lukien säätöön liittyvät kyberturvallisuusriskit, sekä suojatoimet, kuten käyttäjän ohitusmekanismit ja vikasietotilat. Myöhemmässä päivityksessä valmistaja ottaa automaattiset säätötoiminnot käyttöön ja aktivoi suojatoimet alkuperäisen arvioinnin mukaisesti. Näin ollen tuotannonvalvontajärjestelmää ei ole muutettu merkittävästi.

107. Sitä vastoin rajallisetkin tai näennäisesti vähäisetkin uudet toiminnot voivat aiheuttaa merkittäviä kyberturvallisuusriskejä, jotka vaikuttavat olennaisten vaatimusten täyttymiseen. Merkittävän muutoksen arvioinnin ei siksi pitäisi perustua muutoksen laajuuteen tai monimutkaisuuteen vaan sen mahdolliseen haittavaikutukseen, joka kohdistuu digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskiprofiiliin ja näin ollen olennaisten vaatimusten täyttymiseen.

Esimerkki 44: Valmistaja lisää ohjelmistosovellukseen päivityksen, joka lisää ”muista minut” -toiminnon eli pysyvän kirjautumisen, joka tallentaa tunnistusvälineitä paikallisesti käyttäjän käyttömukavuuden parantamiseksi. Vaikka toiminto on rajallinen, se tuo mukanaan uusia riskejä, jotka liittyvät tunnistusvälinevarkauksiin, luvattomaan käyttöön ja istuntojen kaappaukseen ja joita ei otettu huomioon riskinarvioinnissa. Näin ollen päivitys vaikuttaa olennaisten vaatimusten täyttymiseen. Ohjelmistosovellusta on muutettu merkittävästi.

Esimerkki 45: Valmistaja lisää olemassa olevaan digitaalisia elementtejä sisältävään ohjelmistotuotteeseen uuden loki- ja diagnostiikkaominaisuuden, jonka ansiosta yksityiskohtaisia järjestelmälokeja voidaan viedä sovelluksesta vianmääritystä varten. Vaikka toiminto vaikuttaa vähäiseltä, se johtaa arkaluonteisten operatiivisten tietojen keräämiseen ja tallentamiseen salaamattomassa muodossa, mikä aiheuttaa tietojen paljastumisen riskejä, joita ei aiemmin arvioitu tai lievennetty. Muutoksella voi näin ollen olla merkittävä vaikutus digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskiprofiiliin. Digitaalisia elementtejä sisältävää ohjelmistotuotetta on muutettu merkittävästi.

108. Kyberkestävyyssäädöksen johdanto-osan 39 kappaleen mukaisesti tietoturvapäivityksiä ei yleensä katsota merkittäviksi muutoksiksi, koska niiden ensisijaisena tarkoituksena on alentaa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskin tasoa. Tietoturvapäivitystä, joka ei muuta kyseisen tuotteen käyttötarkoitusta eikä aiheuta uusia kyberturvallisuusriskejä, ei sen vuoksi pitäisi pitää merkittävänä muutoksena, vaikka kyseinen päivitys voi aiheuttaa merkittäviä teknisiä muutoksia. Tämä koskee myös tapauksia, joissa tiettyjä toimintoja muutetaan tai rajoitetaan yksinomaan havaittujen haavoittuvuuksien lieventämiseksi ja olennaisten vaatimusten jatkuvan noudattamisen varmistamiseksi.

Esimerkki 46: Valmistaja ottaa käyttöön tietoturvapäivityksen korjatakseen haavoittuvuuden digitaalisia elementtejä sisältävän tuotteen koodikannassa korjaamalla syötteen validoinnin virheen, joka saattaa johtaa puskurin ylivuotoon, tai korjaamalla logiikkavirheen, joka mahdollistaa todennuksen ohittamisen väärällä istuntotunnuksen validoinnilla. Päivitys muuttaa ohjelmiston sisäistä toteutusta vaikuttamatta tuotteen käyttötarkoitukseen tai aiheuttamatta uusia haavoittuvuuksia. Tällainen päivitys on tarkoitettu yksinomaan kyberturvallisuusriskin pienentämiseen. Tietoturvapäivitystä ei pitäisi pitää merkittävänä muutoksena.

Esimerkki 47: Valmistaja lisää tietoturvapäivityksen, joka vahvistaa olemassa olevia suojausmäärityksiä ja sisältää esimerkiksi palomuurisääntöjen tiukentamisen, käyttämättömien verkkoporttien käytöstä poistamisen, järjestelmänvalvojan oletussalasana-käytäntöjen muuttamisen tai kaksivaiheisen todennuksen muuttamisen pakolliseksi, kun kyseinen ominaisuus oli jo käytettävissä tai suunniteltu. Vaikka päivitys voi vaikuttaa siihen, miten käyttäjät konfiguroivat digitaalisia elementtejä sisältävän tuotteen tai käyttävät sitä, se ei muuta tuotteen käyttötarkoitusta, vaan ainoastaan parantaa sen tietoturvaa. Tietoturvapäivitystä ei pitäisi pitää merkittävänä muutoksena.

Esimerkki 48: Valmistaja saattaa markkinoille digitaalisia elementtejä sisältävän ohjelmistotuotteen, joka suojaa tietoliikennettä käyttämällä konfiguroitavaa, useita salausalgoritmeja ja avainkokoja tukevaa salauskehystä, kuten tuotteen teknisissä asiakirjoissa ja riskinarvioinnissa on kuvattu. Riskinarviointi kattaa kaikki digitaalisia elementtejä sisältävässä tuotteessa käytettävissä olevat salausvaihtoehdot ja ennakoi tiettyjen algoritmien tulevaa käytöstä poistoa. Riskinarviointi sisältää myös lieventäviä toimenpiteitä, kuten kryptoketteryyden, sisäisen avaintenhallinnan sekä yhteensopivuusanalyysin. Vastauksena uusiin kryptografisiin ohjeisiin valmistaja ottaa käyttöön tietoturvapäivityksen, jolla poistetaan käytöstä vanhentunut algoritmi ja otetaan käyttöön vahvempi, jo tuettu vaihtoehto ilman, että päivitys tuo mukanaan uusia ulkoisia riippuvuuksia tai muuttaa tietovirtoja. Koska päivityksellä pannaan täytäntöön turvallisuustoimenpide, joka oli ennakoitu ja arvioitu osana alkuperäistä suunnitelmaa, eikä se aiheuta uusia kyberturvallisuusriskejä, tietoturvapäivitystä ei pitäisi pitää merkittävänä muutoksena.

109. Sen sijaan tietoturvapäivitystä voidaan pitää merkittävänä muutoksena, jos sen turvallisuustavoitteesta huolimatta päivitys johtaa digitaalisia elementtejä sisältävän tuotteen käyttötarkoituksen muuttumiseen alun perin ennakoidusta tai jos päivitys aiheuttaa uusia tai suurempia kyberturvallisuusriskejä. Näin voi olla esimerkiksi silloin, kun päivitys muuttaa kyseisen tuotteen rajoja tai riippuvuusrakennetta olennaisesti tavalla, jota ei ole ennakoitu riskinarvioinnissa, esimerkiksi muuttamalla olennaisesti tietovirtoja tai lisäämällä uusia ulkoisesti saavutettavissa olevia rajapintoja.

Esimerkki 49: Valmistaja saattaa markkinoille digitaalisia elementtejä sisältävän ohjelmistotuotteen, jonka tarkoituksena on mahdollistaa käyttäjän laitteeseen tallennettujen tiedostojen paikallinen salaus, jotta käyttäjät voivat salata ja purkaa tiedostojen salauksen pyynnöstä. Kun salauksen työnkulussa havaittiin haavoittuvuus, valmistaja tekee tietoturvapäivityksen, jolla paikallinen salaustoiminto poistetaan käytöstä, minkä jälkeen kaikki tiedostot on sen sijaan ladattava, tallennettava ja käsiteltävä valmistajan ylläpitämässä etäsalauspalvelussa. Muutoksen seurauksena digitaalisia elementtejä sisältävällä tuotteella ei enää salata tiedostoja paikallisesti alkuperäisen käyttötarkoituksen mukaisesti, vaan se toimii etäsalaus- ja tietojenkäsittelypalveluna. Vaikka päivitys otetaan käyttöön tietoturvasyistä, se muuttaa kyseisen tuotteen käyttötarkoitusta olennaisesti tavalla, jota ei ole ennakoitu riskinarvioinnissa, joten päivitystä voidaan pitää merkittävänä muutoksena.

Esimerkki 50: Valmistaja saattaa markkinoille digitaalisia elementtejä sisältävän ohjelmistotuotteen, joka perustuu vakiintuneeseen salausprotokollaan ja sisäisesti hallittuun avainten elinkaareen digitaalisia elementtejä sisältävän tuotteen komponenttien välisen viestinnän suojaamiseksi. Vastauksena äskettäin havaittuihin salauksen heikkouksiin valmistaja ottaa käyttöön tietoturvapäivityksen, joka korvaa olemassa olevan salausmekanismin toisella protokollalla, joka edellyttää kolmannen osapuolen hallinnoiman ulkoisen avaintenhallintapalvelun käyttöä. Muutoksen seurauksena digitaalisia elementtejä sisältävän tuotteen riippuvuudet ja tietovirrat muuttuvat olennaisesti, sillä käyttöön otetaan uusia ulkoisia rajapintoja ja kolmannen osapuolen palveluja, joita ei ole otettu huomioon riskiarvioinnissa. Vaikka päivitys on tietoturva-lähtöinen, se aiheuttaa uusia kyberturvallisuusriskejä, joten se katsotaan merkittäväksi muutokseksi.

110. Kuten edellä olevassa kohdassa 104 todetaan, se, muodostaako ohjelmistopäivitys merkittävän muutoksen, olisi arvioitava tapauskohtaisesti. Tätä arviointia tehdessään valmistajat voivat ottaa huomioon (luettelo ei ole tyhjentävä), onko ohjelmistopäivitys sellainen, että se

a) tuo mukanaan uusia uhkavektoreita, kuten ylimääräisiä rajapintoja, viestintäkanavia, toteuttamisympäristöjä tai ulkoisia riippuvuuksia, joiden kautta uhat voivat toteutua;

b) mahdollistaa uusia hyökkäysskenaarioita, mukaan lukien esimerkiksi uusia tapoja, joilla digitaalisia elementtejä sisältävän tuotteen tai siinä käsiteltävän datan luvaton käyttö, manipulointi, häirintä tai väärinkäyttö saattaisi olla uskottavasti mahdollista;

c) muuttaa aiemmin havaittujen hyökkäysskenaarioiden todennäköisyyttä esimerkiksi vähentämällä niiden hyödyntämiseen tarvittavaa vaivannäköä tai asiantuntemusta, lisäämällä altistumista epäluotettaville toimijoille tai heikentämällä olemassa olevia suojatoimia;

d) muuttaa aiemmin havaittujen hyökkäysskenaarioiden mahdollisia vaikutuksia, kuten kohteena olevan datan tai toimintojen laajuutta, toimintoihin, turvallisuuteen tai talouteen kohdistuvien seurausten vakavuutta tai kykyä havaita ja hillitä häiriöitä tai toipua niistä.

111. Joissakin tapauksissa ohjelmistopäivitys ei aiheuta uusia uhkavektoreita eikä mahdollista uusia hyökkäysskenaarioita eikä muuta olennaisesti aiemmin havaittujen hyökkäysskenaarioiden todennäköisyyttä tai vaikutusta. Tämä voi viitata siihen, että päivitys ei aiheuta uusia tai lisääntyneitä kyberturvallisuusriskejä, kunhan riskinarvioinnissa käytetyt oletukset ja lieventävät toimenpiteet ovat edelleen päteviä ja tehokkaita. Näin ollen on todennäköistä, että päivitystä ei pidetä merkittävänä muutoksena.

112. Ohjelmistopäivitys voi sitä vastoin saada aikaan uusia uhkavektoreita, mahdollistaa uusia hyökkäysskenaarioita tai muuttaa olemassa olevien hyökkäysskenaarioiden todennäköisyyttä tai vaikutusta olennaisesti. Tällaisissa tapauksissa valmistajan olisi arvioitava digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusriskit uudelleen ja määritettävä, täyttyvätkö olennaiset vaatimukset edelleen, mukaan lukien se, aiheuttaako päivitys uusia tai lisääntyneitä riskejä, joita ei ole ennakoitu riskinarvioinnissa.

113. Sillä, tulkitaanko ohjelmistopäivitys merkittäväksi muutokseksi, on merkitystä määritettäessä, sovelletaanko tiettyjä kyberkestävyyssäädöksen velvoitteita kohdassa 91 esitetyllä tavalla. Tästä tulkinnasta riippumatta valmistajat ovat kuitenkin edelleen vastuussa ohjelmistopäivitysten ja digitaalisia elementtejä sisältävän tuotteen turvallisuuden varmistamisesta sen tukikauden aikana kyberkestävyyssäädöksen liitteen I olevassa II osassa vahvistettujen haavoittuvuuksien käsittelyä koskevien vaatimusten mukaisesti. Lisäksi valmistajien on 13 artiklan 7 kohdan ja 31 artiklan 2 kohdan mukaisesti pidettävä riskinarviointi ja tekniset asiakirjat paikkansapitävinä, puutteettomina ja jatkuvasti ajan tasalla riippumatta siitä, katsotaanko ohjelmistopäivitykset merkittäviksi muutoksiksi.

4.4 **Merkittävän muutoksen seuraukset**

114. Muun toimijan kuin alkuperäisen valmistajan toteuttaman merkittävän muutoksen seurauksia markkinoille jo saatetulle digitaalisia elementtejä sisältävälle tuotteelle käsitellään kyberkestävyyssäädöksen 21 ja 22 artiklassa. Säädöksen 21 artikla koskee maahantuojia ja jakelijoita, kun taas 22 artikla koskee kaikkia muita luonnollisia henkilöitä tai oikeushenkilöitä kuin valmistajaa, maahantuojaa tai jakelijaa.

115. Jos merkittävän muutoksen tekee digitaalisia elementtejä sisältävän tuotteen alkuperäinen valmistaja, seuraukset johtuvat kyberkestävyyssäädöksen johdanto-osan 41 kappaleessa tarkoitetusta merkittävän muutoksen yleisesti vahvistetusta käsitteestä, ja niitä käsitellään tarkemmin sinisen oppaan 2.1 kohdassa. Kyseisessä kohdassa todetaan, että tuotetta, johon on markkinoille saattamisen jälkeen tehty merkittäviä muutoksia tai korjauksia, on pidettävä uutena tuotteena, jos sen alkuperäinen suorituskyky, käyttötarkoitus tai tyyppi muuttuu, vaaran luonne on muuttunut tai riskin taso on kasvanut ja digitaalisia elementtejä sisältävä tuote asetetaan saataville markkinoilla.

116. Näin ollen yleisesti vahvistettu seuraus on, että jos digitaalisia elementtejä sisältävän tuotteen muutos katsotaan merkittäväksi muutokseksi ja muutettu digitaalisia elementtejä sisältävä tuote asetetaan saataville markkinoilla, sitä on käsiteltävä uutena digitaalisia elementtejä sisältävänä tuotteena kyberkestävyyssäädöksessä tarkoitetulla tavalla. Näin ollen se, että merkittävästi muutettu tuote asetetaan saataville markkinoilla, muodostaa uuden markkinoille saattamisen. Tätä sovelletaan riippumatta siitä, tekeekö merkittävän muutoksen alkuperäinen valmistaja vai muu henkilö. Jotta kyberkestävyyssäädöstä sovelletaan yhdenmukaisesti ja oikeasuhteisesti eri toimijaryhmissä, jotka voivat tehdä merkittäviä muutoksia, seuraavissa alajaksoissa käsitellään merkittäviä muutoksia toteuttavan henkilön velvollisuuksia, kun merkittävästi muutettu digitaalisia elementtejä sisältävä tuote saatetaan markkinoille. Digitaalisia elementtejä sisältävän tuotteen tukiaikaan kohdistuvia seurauksia käsitellään jaksossa *5 Tukiaika*.

4.4.1 *Muun kuin alkuperäisen valmistajan tekemät merkittävät muutokset*

117. Säädöksen 21 ja 22 artiklassa säädetään, että jos markkinoille jo saatetun digitaalisia elementtejä sisältävän tuotteen merkittävän muutoksen tekee muu luonnollinen henkilö tai oikeushenkilö kuin digitaalisia elementtejä sisältävän tuotteen valmistaja, henkilöä, joka tekee kyseisen merkittävän muutoksen ja asettaa kyseisen muutetun tuotteen saataville markkinoilla, pidetään muutetun digitaalisia elementtejä sisältävän tuotteen valmistajana riippumatta siitä, oliko kyseinen henkilö osallisena kyseisen tuotteen alkuperäisessä suunnittelussa tai markkinoille saattamisessa.

118. Lisäksi 22 artiklassa selvennetään, että muutoksen tekevään henkilöön sovelletaan 13 ja 14 artiklassa säädettyjä velvoitteita ainoastaan digitaalisia elementtejä sisältävän tuotteen sen osan osalta, johon merkittävä muutos vaikuttaa, jos kyseinen muutos ei vaikuta digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen koko tuotteen osalta.

119. Jos merkittävä muutos vaikuttaa olennaisten vaatimusten noudattamiseen mutta ei vaikuta kielteisesti digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen koko tuotteen osalta, muutoksen tekevään henkilöön sovelletaan 13 artiklaa (mukaan lukien velvoite varmistaa olennaisten vaatimusten noudattaminen ja suorittaa vaatimustenmukaisuuden arviointimenettely) ja 14 artiklaa (raportointivelvoitteet) vain digitaalisia elementtejä sisältävän tuotteen merkittävästi muutetun osan osalta ([16]). Lisäksi kyberkestävyyssäädöksen mukaisia alkuperäisen valmistajan velvoitteita sovelletaan edelleen alkuperäiseen markkinoille saatettuun digitaalisia elementtejä sisältävään tuotteeseen, millä varmistetaan haavoittuvuuksien käsittelyn jatkuvuus ja vaatimustenmukaisuus muuttumattomien osien osalta.

120. Merkittävää muutosta ei pitäisi sekoittaa integrointitapauksiin, joissa henkilö kokoaa komponentteja (mukaan lukien tarvittaessa muuttamalla niitä) uudeksi digitaalisia elementtejä sisältäväksi tuotteeksi, jonka henkilö itse saattaa markkinoille. Tällaisissa tapauksissa integroinnin suorittaja ei muuta digitaalisia elementtejä sisältävää tuotetta, jonka toinen valmistaja on jo saattanut markkinoille, vaan integroinnin suorittaja saattaa markkinoille uuden digitaalisia elementtejä sisältävän tuotteensa. Integroinnin suorittaja on kyseisen digitaalisia elementtejä sisältävän uuden tuotteen valmistaja kyberkestävyyssäädöksessä tarkoitetulla tavalla, ja integroinnin suorittajan on noudatettava koko asetusta digitaalisia elementtejä sisältävän koko tuotteen osalta. Jos valmistaja integroi komponentteja, joihin kyberkestävyyssäädöstä sovelletaan, valmistaja voi helpottaa omaa kyberkestävyyssäädöksen noudattamistaan hyödyntämällä komponenttien valmistajien vaatimustenmukaisuustoimia.

Esimerkki 51: Yritys ostaa valmiita mikro-ohjainmoduuleja ja liitettävyyskomponentteja ulkopuolisilta toimittajilta, kehittää oman laiteohjelmiston ja anturipaketin ja kokoaa ne yhdistetyksi digitaalisia elementtejä sisältäväksi maataloudenseurantatuotteeksi, jonka se saattaa markkinoille omalla nimellään. Vaikka yritys on muuttanut taustalla olevia mikro-ohjainmoduuleja ja yhdistänyt niitä muihin komponentteihin, yritys ei muuta markkinoille jo saatettua digitaalisia elementtejä sisältävää tuotetta merkittävästi, vaan se saattaa markkinoille uuden digitaalisia elementtejä sisältävän tuotteen. Yritys on kyberkestävyyssäädöksessä tarkoitetulla tavalla maataloudenseurantatuotteen valmistaja, ja sen on noudatettava asetusta koko maataloudenseurantatuotteen osalta.

([16]) Sinisen oppaan 2.1 kohdan mukaisesti ”ei ole tarpeen toistaa testejä ja laatia uusia asiakirjoja sellaisista seikoista, joihin muutos ei vaikuta. Tuotteeseen muutokset suorittavan tai muutokset teettävän luonnollisen tai oikeushenkilön tehtävänä on osoittaa, ettei teknisen aineiston kaikkia osia ole tarpeen päivittää. Tuotteeseen muutokset suorittava tai muutokset teettävä luonnollinen tai oikeushenkilö vastaa muutetun tuotteen vaatimustenmukaisuudesta ja laatii vaatimustenmukaisuusvakuutuksen, vaikka käyttäisi olemassa olevia testejä ja teknisiä asiakirjoja.”

121. Jos muun henkilön kuin alkuperäisen valmistajan tekemä merkittävä muutos vaikuttaa kielteisesti digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen koko tuotteen osalta esimerkiksi siksi, että muutos ei enää kohdistu tai rajoitu tiettyyn komponenttiin tai osajärjestelmään, muutettua digitaalisia elementtejä sisältävää tuotetta, joka asetetaan saataville markkinoilla, olisi käsiteltävä uutena digitaalisia elementtejä sisältävänä tuotteena, joka kuuluu kokonaisuudessaan kyberkestävyyssäädöksen piiriin. Tällaisissa tapauksissa kyseisen tuotteen yleinen kyberturvallisuuden riskiprofiili on muuttunut, eikä muutosta voida arvioida ottamatta huomioon digitaalisia elementtejä sisältävää tuotetta kokonaisuutena. Muutoksen toteuttavaan henkilöön sovelletaan 13 ja 14 artiklassa säädettyjä valmistajan velvoitteita, jotka koskevat muutettua digitaalisia elementtejä sisältävää tuotetta kokonaisuudessaan.

4.4.2 *Alkuperäisen valmistajan tekemät merkittävät muutokset*

122. Jos merkittävän muutoksen tekee alkuperäinen valmistaja, myös digitaalisia elementtejä sisältävien ohjelmistotuotteiden iteratiivisen kehittämisen yhteydessä, kyseinen valmistaja pysyy valmistajana kyberkestävyyssäädöksessä tarkoitetulla tavalla. Merkittävästi muutettua digitaalisia elementtejä sisältävää tuotetta on kuitenkin pidettävä uutena markkinoille saatettuna tuotteena.

123. Sinisen oppaan 2.1 kohdan mukaisesti alkuperäinen valmistaja, joka saattaa markkinoille merkittävästi muutetun digitaalisia elementtejä sisältävän tuotteen, voi käyttää olemassa olevia teknisiä asiakirjoja ja testejä uudelleen sellaisten digitaalisia elementtejä sisältävän tuotteen näkökohtien osalta, joihin merkittävä muutos ei vaikuta. Erityisesti silloin, kun valmistaja saattaa markkinoille saman digitaalisia elementtejä sisältävän tuotteen merkittävästi muutettuja versioita, vaatimustenmukaisuuden arvioinnissa olisi keskityttävä digitaalisia elementtejä sisältävän tuotteen merkittävästi muutettuihin osiin. Vastaavasti silloin, kun kolmas osapuoli suorittaa vaatimustenmukaisuuden arvioinnin, vaatimustenmukaisuuden arviointilaitoksen olisi keskityttävä arvioinnissaan merkittävästi muutettuihin osiin. Digitaalisia elementtejä sisältävän tuotteen muuttumattomien osien osalta arviointilaitos voi käyttää olemassa olevia teknisiä asiakirjoja ja testituloksia uudelleen.

124. Edellisessä alajaksossa esitettyjä suhteellisuusnäkökohtia sovelletaan myös merkittäviin muutoksiin, jotka digitaalisia elementtejä sisältävän tuotteen alkuperäinen valmistaja on tehnyt tuotteeseen, joka on saatettu markkinoille ennen 11:ttä joulukuuta 2027. Alkuperäisen valmistajan tekemä merkittävä muutos ei sinänsä edellytä, että valmistaja saattaa ennen kyseistä päivämäärää markkinoille saatetun digitaalisia elementtejä sisältävän kokonaisen tuotteen täysin kyberkestävyyssäädöksen vaatimusten mukaiseksi, ellei muutos vaikuta kielteisesti digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen koko tuotteen osalta. Jos muutos ei vaikuta digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuteen koko tuotteen osalta, alkuperäisen valmistajan velvoitteet muutoksen osalta olisi rajoitettava koskemaan vain merkittävästi muutettuja osia.

5. **TUKIAIKA**

125. Kyberkestävyyssäädöksen 13 artiklan 8 kohdan mukaan valmistajien on määritettävä tukiaika, jonka aikana digitaalisia elementtejä sisältävän tuotteen ja sen komponenttien haavoittuvuudet käsitellään tehokkaasti ja liitteessä I olevassa II osassa vahvistettujen olennaisten vaatimusten mukaisesti. Tukiaika vastaa ajanjaksoa, jona digitaalisia elementtejä sisältävän tuotteen odotetaan olevan käytössä (odotettu käyttöaika). Sen määrittämisessä on otettava huomioon 13 artiklan 8 kohdassa säädetyt kriteerit, erityisesti käyttäjien kohtuulliset odotukset, digitaalisia elementtejä sisältävän tuotteen luonne, mukaan lukien sen käyttötarkoitus, sekä asiaa koskeva unionin oikeus, jossa määritetään aika, jonka digitaalisia elementtejä sisältävien tuotteiden odotetaan olevan käytössä ([17]). Kriteerejä olisi kaiken kaikkiaan sovellettava tavalla, jolla varmistetaan oikeasuhtaisuus tukiajan määrittämisessä.

([17]) Muita kriteereitä, joita valmistaja voi 13 artiklan 8 kohdan mukaisesti ottaa huomioon, ovat muiden valmistajien markkinoille saattamien samankaltaisen toiminnon tarjoavien digitaalisia elementtejä sisältävien tuotteiden tukiajat, toimintaympäristön saatavuuden, ydintoimintoja tarjoavien ja kolmansilta osapuolilta peräisin olevien integroitujen komponenttien tukiajat sekä kyberkestävyyssäädöstä käsittelevän hallinnollisen yhteistyöryhmän ja komission antamat asiaa koskevat ohjeet.

126. Lisäksi 13 artiklan 8 kohdassa edellytetään, että tukiajan on oltava vähintään viisi vuotta, paitsi jos digitaalisia elementtejä sisältävää tuotetta odotetaan käytettävän alle viisi vuotta, jolloin tukiajan on vastattava tuotteen odotettua käyttöaikaa. Tukiajan vähimmäiskesto on näin ollen tarkoitettu vain suojatoimenpiteeksi: sillä varmistetaan, että haavoittuvuuksia käsitellään riittävän pitkään, ja annetaan valmistajille toisaalta mahdollisuus ottaa huomioon digitaalisia elementtejä sisältävät tuotteet, joiden odotettu käyttöaika on aidosti lyhyempi. Johdanto-osan 60 kappaleessa annetaan tältä osin tarkempia ohjeita ja selvennetään, että jos digitaalisia elementtejä sisältävää tuotetta voidaan kohtuudella odottaa käytettävän yli viisi vuotta, sen tukiajan olisi vastaavasti oltava pidempi. Viiden vuoden tukiaikaa ei siis voida pitää oletuksena kaikille digitaalisia elementtejä sisältäville tuotteille. Sen sijaan valmistajien olisi määritettävä asianmukainen tukiaika 13 artiklan 8 kohdassa tarkoitettujen kriteerien perusteella.

127. Kyberkestävyyssäädöksen 13 artiklan 19 kohdassa edellytetään, että valmistajat ilmoittavat tukiajan päättymispäivän (ainakin kuukauden ja vuoden) selkeästi ja ymmärrettävästi tuotteen hankinta-ajankohtana. Lisäksi valmistajien on annettava käyttäjille ilmoitus tukiajan päättymisestä, jos se on teknisesti toteutettavissa digitaalisia elementtejä sisältävän tuotteen luonteen vuoksi. Tämän velvoitteen tarkoituksena on lisätä avoimuutta sen suhteen, kuinka pitkään käyttäjä voi odottaa saavansa tietoturvatukea.

128. Digitaalisia elementtejä sisältäviä ohjelmistotuotteita kehitetään ja julkaistaan usein iteratiivisesti, ja niistä voidaan ajan mittaan saattaa markkinoille merkittävästi muutettuja versioita. Tukiaika olisi tällöin ymmärrettävä tämän kehitysmallin valossa. Jokaiselle markkinoille saatetulle digitaalisia elementtejä sisältävän ohjelmistotuotteen versiolle, jota on muutettu merkittävästi, on ilmoitettava 13 artiklan 8 kohdan mukainen tukiaika. Niitä koskee myös tukiajan viiden vuoden vähimmäiskesto, jollei kyseisen version odotettu käyttöaika ole selvästi lyhyempi, kuten myös johdanto-osan 60 kappaleessa täsmennetään. Lisäksi jaksossa *5.1 Merkittävät muutokset ja tukiaika* selvennetään, että jos merkittävä muutos ei johda muutoksiin tekijöissä, joiden perusteella alun perin määritettiin digitaalisia elementtejä sisältävän tuotteen odotettu käyttöaika, alkuperäinen tukiaika säilyy muuttumattomana (myös silloin, kun jäljellä oleva tukiaika on alle viisi vuotta).

129. Kyberkestävyyssäädöksen 13 artiklan 10 kohdassa säädetään digitaalisia elementtejä sisältäviä ohjelmistotuotteita koskevasta joustomahdollisuudesta, jonka nojalla valmistajat voivat tietyin edellytyksin varmistaa liitteessä I olevan II osan 2 kohdassa vahvistetun haavoittuvuuksien käsittelyä koskevan vaatimuksen (haavoittuvuuksiin puuttuminen ja niiden korjaaminen) noudattamisen vain viimeksi markkinoille saattamansa digitaalisia elementtejä sisältävän ohjelmistotuotteen version osalta. Tämä sallitaan vain, jos aiemmin markkinoille saatettujen versioiden käyttäjät voivat käyttää viimeksi markkinoille saatettua versiota maksutta eikä käyttäjille aiheudu lisäkustannuksia sen laitteisto- ja ohjelmistoympäristön mukauttamisesta, jossa he käyttävät kyseisen tuotteen alkuperäistä versiota.

130. Sovellettaessa 13 artiklan 10 kohtaa lisäkustannusten käsitettä olisi tulkittava käytännöllisesti ja oikeasuhteisesti siten, että huomioon otetaan tavanomaiset ja odotettavissa olevat ohjelmistojen ylläpitoon ja käyttöön liittyvät käytännöt. Lisäkustannuksilla ei tarkoiteta kohtuullista operatiivista työtä, joka kuuluu luonnostaan ohjelmistopäivitysten asentamiseen tai turvallisen käyttöympäristön ylläpitoon. Tämä tarkoittaa esimerkiksi henkilöstön työaikaa, rutiininomaista testausta, konfiguraatiomuutoksia tai taustalla olevien ohjelmistoriippuvuuksien päivittämistä, jos päivitys on tarpeen elinkaarensa päässä olevien komponenttien tai tunnettujen tietoturvahaavoittuvuuksien vuoksi. Lisäkustannuksiksi katsottavat rasitteet ylittävät ohjelmistopäivitysten yhteydessä tavanomaisesti odotettavissa olevat kustannukset. Niitä ovat esimerkiksi pakollinen uuden laitteiston hankinta, infrastruktuurin korvaaminen tai perustavanlaatuiset muutokset toimintaympäristöön.

131. Jatkuvasti kehittyvien digitaalisia elementtejä sisältävien ohjelmistotuotteiden valmistajat voivat saattaa markkinoille perättäisiä merkittävästi muutettuja versioita suhteellisen lyhyin väliajoin, jolloin käyttäjien odotetaan päivittävän tuotetta säännöllisesti. Tällaisissa tapauksissa kunkin merkittävästi muutetun version ilmoitetun tukiajan on sen markkinoille saattamisen ajankohtana oltava 13 artiklan 8 kohdan mukainen. Valmistajan on toisin sanottuna ilmoitettava uusi tukiaika, joka koskee kyseistä merkittävästi muutettua versiota. Valmistajat voivat kuitenkin 13 artiklan 10 kohdan nojalla lopettaa aiempien versioiden haavoittuvuuksiin puuttumisen ja niiden korjaamisen, jos käyttäjät voivat päivittää uuteen versioon maksutta eikä heille aiheudu edellä tarkoitettuja lisäkustannuksia.

Tämä on mahdollista myös, vaikka se lyhentäisi aiempien versioiden tosiasiallista tukiaikaa ([18]). Valmistajaan sovelletaan edelleen muita liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyä koskevia vaatimuksia sekä 14 artiklassa säädettyjä raportointivelvoitteita. Kuten myös johdanto-osan 40 kappaleessa selitetään, näitä ovat muun muassa seuraavat vaatimukset, jotka koskevat kaikkia markkinoille saatettuja merkittävästi muutettuja myöhempiä versioita digitaalisia elementtejä sisältävästä ohjelmistotuotteesta: i) koordinoitua haavoittuvuuksien julkistamista koskevien periaatteiden noudattaminen ja ii) toimenpiteet, joilla helpotetaan tietojen jakamista mahdollisista haavoittuvuuksista ([19]).

Esimerkki 52: Valmistaja saattaa EU:n markkinoille älypuhelinmallin ja ilmoittaa markkinoille saattamisen päivämäärästä alkavan X vuoden tukiajan, jonka aikana se tarjoaa tietoturvapäivityksiä haavoittuvuuksien käsittelemiseksi. Tänä aikana valmistaja julkaisee säännöllisesti ohjelmistopäivityksiä ja käyttöjärjestelmän merkittävästi muutettuja versioita, jotka käyttäjät voivat asentaa maksutta ja jotka eivät edellytä uuden laitteen hankkimista.

Valmistaja voi 13 artiklan 10 kohdan mukaisesti puuttua kyseisen älypuhelinmallin käyttöjärjestelmän uusimman version haavoittuvuuksiin ja korjata ne, jos aiemmat versiot voidaan päivittää maksutta eikä käyttäjille aiheudu niistä lisäkustannuksia. Tukiaikana valmistajaan sovelletaan muita haavoittuvuuksien käsittelyä koskevia vaatimuksia, muun muassa koordinoituun haavoittuvuuksien julkistamiseen ja tietojen jakamista koskeviin toimenpiteisiin liittyviä vaatimuksia.

Esimerkki 53: Valmistaja saattaa markkinoille yrityksille suunnatun digitaalisia elementtejä sisältävän ohjelmistotuotteen. Se julkaisee muutaman kuukauden välein merkittävästi muutettuja versioita, joilla tehdään tietoturvaan liittyviä parannuksia, lisätään uusia ominaisuuksia ja huomioidaan yhteensopivuus päivitettyjen käyttöjärjestelmien ja alustojen kanssa. Kullekin markkinoille saatetulle versiolle ilmoitetaan 13 artiklan 8 kohdan mukainen tukiaika. Valmistaja odottaa käyttäjien tekevän päivityksiä säännöllisesti osana tavanomaista käyttöä ja asettaa tuotteen uusimman version heidän saatavilleen maksutta. Päivittämiseen voi liittyä kohtuullista operatiivista työtä, kuten testausta tai konfiguraatiomuutoksia, mutta se ei edellytä lisäkustannuksia, kuten uuden laitteiston hankintaa tai perustavanlaatuisia muutoksia infrastruktuuriin. Tässä tapauksessa valmistaja voi 13 artiklan 10 kohdan nojalla lopettaa aiempien versioiden haavoittuvuuksiin puuttumisen ja niiden korjaamisen siitä lähtien, kun käyttäjillä on mahdollisuus päivittää uusimpaan versioon. Valmistajan on edelleen noudatettava muita haavoittuvuuksien käsittelyä koskevia vaatimuksia kaikkien merkittävästi muutettujen myöhempien versioiden osalta.

5.1 **Merkittävät muutokset ja tukiaika**

132. Kuten jaksossa *4.4 Merkittävän muutoksen seuraukset* esitetään, jos digitaalisia elementtejä sisältävän tuotteen muuttamisessa on kyse merkittävästä muutoksesta ja muutettu digitaalisia elementtejä sisältävä tuote asetetaan saataville markkinoilla, se katsotaan kyberkestävyyssäädöstä sovellettaessa uudeksi tuotteeksi. Tällaisen merkittävästi muutetun digitaalisia elementtejä sisältävän tuotteen asettaminen saataville markkinoilla on siis uusi markkinoille saattaminen. Näin ollen on hyvä selventää, miten uusi markkinoille saattaminen vaikuttaa merkittävästi muutetun digitaalisia elementtejä sisältävän tuotteen tukiajan pituuteen.

133. Merkittävästi muutetun digitaalisia elementtejä sisältävän tuotteen tukiaika määritetään tuotteen odotettuun käyttöaikaan nähden ottaen huomioon kyberkestävyyssäädöksen 13 artiklan 8 kohdassa vahvistetut kriteerit. Merkittävä muutos edellyttää tästä syystä uudelleenarviointia kyseisten kriteerien valossa, mutta se ei automaattisesti johda tukiajan alkamiseen alusta tai edes pidennä sitä. Olennaista on, vaikuttaako merkittävä muutos tekijöihin, joiden perusteella alun perin määritettiin kyseisen tuotteen odotettu käyttöaika ja siten alkuperäinen tukiaika.

([18]) Valmistajan on kuitenkin 13 artiklan 19 kohdan mukaan annettava käyttäjille ilmoitus siitä, että heidän digitaalisia elementtejä sisältävän tuotteensa tukiaika on päättynyt, jos se on teknisesti toteutettavissa digitaalisia elementtejä sisältävän tuotteen luonteen vuoksi. Jos valmistaja lakkaa puuttumasta aiempien versioiden haavoittuvuuksiin ja korjaamasta niitä, sen odotetaan näin ollen ilmoittavan asiasta niille käyttäjille, jotka eivät ole päivittäneet uusimpaan versioon, mikäli tällainen ilmoitus on teknisesti toteutettavissa.

([19]) On huomattava, että vaikka käyttäjät voisivat päivittää ohjelmiston uusimpaan versioon ilman, että heille aiheutuu lisäkustannuksia, valmistajat voivat halutessaan jatkaa ohjelmiston aiempien versioiden haavoittuvuuksiin puuttumista ja niiden korjaamista, myös maksua vastaan tai muilla kaupallisilla järjestelyillä. Kyberkestävyyssäädöksessä ei edellytä, että valmistajat tarjoaisivat tällaisessa tapauksessa maksuttomia tietoturvapäivityksiä aiemmille versioille.

134. Jos merkittävä muutos ei vaikuta näihin tekijöihin, alun perin määritetty odotettu käyttöaika pysyy 13 artiklan 8 kohdan kriteerien perusteella samana ja digitaalisia elementtejä sisältävän tuotteen tukiaika vastaa alun perin markkinoille saatetun tuotteen jäljellä olevaa odotettua käyttöaikaa. Näin on yleensä silloin, kun odotettu käyttöaika määräytyy pääasiassa sellaisten tekijöiden perusteella, jotka pysyvät muutoksessa ennallaan (esimerkiksi laitteistokomponenttien fyysinen kestävyys), tai kun merkittävä muutos koskee ainoastaan ohjelmistotoiminnallisuutta tai taustapalveluja.

Esimerkki 54: Valmistaja saattaa markkinoille robottipölynimurin, jonka odotettu käyttöaika on X vuotta. Käyttöaika perustuu digitaalisia elementtejä sisältävän tuotteen luonteeseen, muun muassa laitteistokomponenttien fyysiseen kestävyyteen ja kulumisominaisuuksiin, ja sen määrittämisessä on otettu huomioon käyttäjien kohtuulliset odotukset tuotteen käyttöiästä. Valmistaja määrittää tukiajaksi X vuotta. Y vuoden jälkeen valmistaja julkaisee ohjelmistopäivityksen, jolla otetaan käyttöön uusia siivoustoimintoja ja navigointiominaisuuksia ja joka katsotaan merkittäväksi muutokseksi. Ohjelmistopäivitys ei vaikuta laitteen fyysiseen kestävyyteen eikä muuta käyttäjien kohtuullisia odotuksia kyseisen tuotteen käyttöiästä. Odotettu käyttöaika pysyy näin ollen 13 artiklan 8 kohdan kriteerien perusteella samana. Muutetun digitaalisia elementtejä sisältävän tuotteen tukiaika vastaa jäljellä olevaa alun perin määritettyä odotettua käyttöaikaa.

Esimerkki 55: Valmistaja saattaa markkinoille monimutkaisen teollisuuskäyttöön tarkoitetun digitaalisia elementtejä sisältävän konetuotteen, johon kuuluu datan etäkäsittelyratkaisuna pilvipalvelun taustajärjestelmä. Tuotteen odotettu käyttöaika on X vuotta. Se on määritetty käyttäjien kohtuullisten odotusten ja digitaalisia elementtejä sisältävän tuotteen luonteen perusteella, muun muassa koneiston fyysinen kestävyys ja odotettavissa oleva kuluminen huomioon ottaen. Tukiajaksi määritetään odotettua käyttöaikaa vastaava X vuotta. Y vuoden jälkeen valmistaja uudistaa pilvipalvelun taustajärjestelmän (datan etäkäsittelyratkaisun) ja ottaa käyttöön uusia sovellusrajapintoja ja tietovirtoja tavalla, joka voidaan katsoa merkittäväksi muutokseksi digitaalisia elementtejä sisältävään tuotteeseen mutta joka ei muuta tuotteen luonnetta tai vaikuta käyttäjän odotuksiin. Odotettu käyttöaika pysyy näin ollen 13 artiklan 8 kohdan kriteerien perusteella samana. Muutetun digitaalisia elementtejä sisältävän tuotteen tukiaika vastaa jäljellä olevaa alun perin määritettyä odotettua käyttöaikaa.

135. Jos merkittävä muutos vaikuttaa tekijöihin, joiden perusteella digitaalisia elementtejä sisältävän tuotteen odotettu käyttöaika alun perin määritettiin, valmistajan on laskettava tukiaika uudelleen siten, että se vastaa uutta odotettua käyttöaikaa, soveltamalla vastaavasti 13 artiklan 8 kohdan kriteereitä. Näin voi olla esimerkiksi, jos tuotteen käyttöikä pitenee laitteistoa uudistavien muutosten vuoksi, tai jos laitteen odotettu käyttöaika muuttuu olennaisesti perusohjelmiston merkittävän uudelleenohjelmoinnin tai uudelleenkirjoittamisen myötä ([20]).

Esimerkki 56: Valmistaja saattaa markkinoille ohjelmoitavan logiikan (PLC), jonka odotettu käyttöaika on X vuotta. Käyttöaika on määritetty pääasiassa digitaalisia elementtejä sisältävän tuotteen luonteen ja taustalla olevan laitteiston kestävyyden perusteella. Tukiaika määritetään vastaamaan odotettua käyttöaikaa. Useita vuosia alkuperäisen markkinoille saattamisen jälkeen valmistaja muuttaa tuotetta merkittävästi. Ohjelmoitavan logiikan sisäinen laskenta-alusta, mukaan lukien prosessori, muisti ja ajoympäristö, korvataan uuden sukupolven komponenteilla, jotka mahdollistavat huomattavasti pidemmän käyttöiän. Tämän vuoksi käyttäjien kohtuulliset odotukset ja digitaalisia elementtejä sisältävän tuotteen luonne muuttuvat: ohjelmoitavan logiikan käyttäjä voi nyt kohtuudella odottaa, että uuden laskenta-alustan ansiosta tuote pysyy tuottavassa käytössä alun perin ilmoitetun käyttöajan jälkeenkin. Näin ollen odotettu käyttöaika on 13 artiklan 8 kohdan kriteereiden perusteella pidempi, ja valmistaja laskee kyseisen ohjelmoitavan logiikan tukiajan uudelleen vastaavasti.

6. **DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVÄT TÄRKEÄT JA KRIITTISET TUOTTEET**

136. Kyberkestävyyssäädöksen 7 artiklan 1 kohdan mukaan digitaalisia elementtejä sisältävät tuotteet, joilla on liitteessä III vahvistetun tuoteryhmän ydintoiminto, katsotaan ”digitaalisia elementtejä sisältäviksi tärkeiksi tuotteiksi”. Digitaalisia elementtejä sisältävät tärkeät tuotteet jaotellaan liitteessä III edelleen luokkiin I ja II. Vastaavasti 8 artiklan 1 kohdassa säädetään, että digitaalisia elementtejä sisältäviä tuotteita, joilla on kyberkestävyyssäädöksen liitteessä IV vahvistetun tuoteryhmän ydintoiminto, pidetään ”digitaalisia elementtejä sisältävinä kriittisinä tuotteina” ([21]).

([20]) Tuotteen kunnostaminen, kunnossapito ja korjaaminen eivät kuitenkaan yleensä johda merkittävään muutokseen, kuten jaksossa *4.1 Fyysiset korjaukset* todetaan.

([21]) Tärkeiden ja kriittisten tuotteiden ryhmien tekninen kuvaus esitetään komission täytäntöönpanoasetuksessa (EU) 2025/2392.

137. Digitaalisia elementtejä sisältävien tuotteiden luokittelulla tärkeiksi tai kriittisiksi – tai niin sanottuun oletusluokkaan eli makroluokkaan ([22]) kuuluviksi – on merkitystä määritettäessä, millainen vaatimustenmukaisuuden arviointimenettely valmistajan on suoritettava 32 artiklan mukaisesti ennen kuin digitaalisia elementtejä sisältävä tuote voidaan saattaa markkinoille. Makroluokkaan kuuluvien digitaalisia elementtejä sisältävien tuotteiden osalta voidaan noudattaa moduuliin A perustuvaa sisäisen valvonnan menettelyä (itsearviointi) ([23]). Luokkiin I ja II kuuluviin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin sovelletaan tiukempia vaatimustenmukaisuuden arviointimenettelyjä. Tämä ei koske luokkaan I tai II kuuluvia digitaalisia elementtejä sisältäviä tärkeitä tuotteita, jotka on luokiteltu vapaiksi ja avoimen lähdekoodin ohjelmistoiksi. Saattaessaan markkinoille tällaisia tuotteita valmistajat voivat noudattaa oletusluokan menettelyjä 32 artiklan 5 kohdan nojalla.

138. Ydintoiminnon käsite on näin ollen olennainen tekijä valmistajan määrittäessä, minkä järjestelmän puitteissa vaatimustenmukaisuus arvioidaan. ”Ydintoimintoa” ei kuitenkaan ole nimenomaisesti määritelty kyberkestävyyssäädöksessä. Digitaalisia elementtejä sisältävät tuotteet voivat suorittaa monenlaisia toimintoja. Osa niistä voi olla tuotteen ydintoiminnon oheistoimintoja, jotka eivät vaikuta siihen, luokitellaanko tuote oletusluokkaan, tärkeiden tuotteiden luokkaan I tai II taikka kriittiseksi tuotteeksi. Tämän vuoksi on hyvä antaa lisäohjeistusta, jonka avulla valmistajat voivat valita asiaankuuluvan vaatimustenmukaisuuden arviointimenettelyn ja suorittaa sen asianmukaisesti. Ohjeistuksella tuetaan myös markkinavalvontaviranomaisia ja edesautetaan kyberkestävyyssäädöksen täytäntöönpanon yhdenmukaista valvontaa kaikkialla EU:ssa.

6.1 **Ydintoiminnot**

139. Digitaalisia elementtejä sisältävän tuotteen ydintoiminnolla tarkoitetaan tuotteen pääominaisuuksia ja teknisiä valmiuksia, joita ilman tuote ei täyttäisi käyttötarkoitustaan. Käyttötarkoitusta voidaan arvioida kyseisen tuotteen erityisen käyttöyhteyden ja erityisten käyttöolosuhteiden perusteella ottaen huomioon muun muassa tiedot, jotka valmistaja on antanut käyttöohjeissa, markkinointi- tai myyntimateriaaleissa ja -ilmoituksissa sekä teknisissä asiakirjoissa.

Esimerkki 57: Digitaalisia elementtejä sisältävä ohjelmistotuote muodostaa taustalla olevan laitteiston päällisen abstraktiokerroksen ja hallinnoi ohjelmistokomponenttien suorittamista. Sen pääominaisuuksia ovat laitteiston ja oheislaitteiden alustaminen, prosessien ja muistin hallinta, syötön ja tulostuksen ohjaus, ajoituksen hallinta, resurssien jakaminen sekä sellaisten järjestelmäpalvelujen ja sovellusrajapintojen tarjoaminen, joiden kautta sovellukset voivat olla vuorovaikutuksessa laitteen laitteisto- ja ohjelmistoresurssien kanssa. Teknisten asiakirjojen mukaan digitaalisia elementtejä sisältävä tuote koordinoi laskentaresursseja, valvoo järjestelmäkokoonpanoja ja tarjoaa yhdenmukaiset rajapinnat ohjelmistomoduuleille ja liitetyille oheislaitteille. Valmistaja korostaa näitä ominaisuuksia, joiden ansiosta alusta toimii keskeisenä ohjelmistoympäristönä, jossa sovellukset voivat toimia luotettavasti. Digitaalisia elementtejä sisältävällä tuotteella on täytäntöönpanoasetuksen (EU) 2025/2392 liitteessä I olevassa 11 kohdassa tarkoitettu käyttöjärjestelmien ydintoiminto.

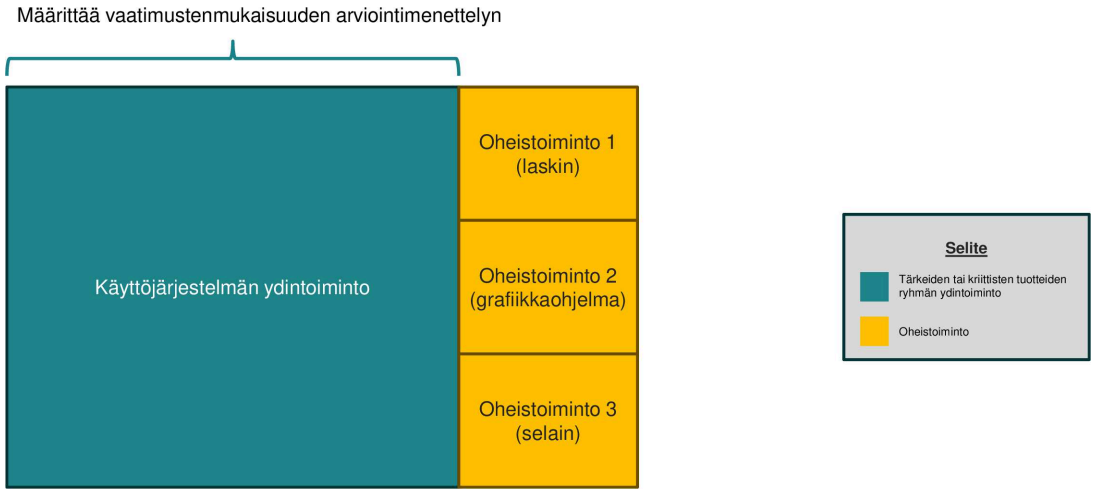
140. Digitaalisia elementtejä sisältävän tuotteen toiminnot rajoittuvat harvoin pelkästään sen ydintoimintoon, koska tällaiset tuotteet suorittavat tyypillisesti – elleivät jopa aina – myös muita toimintoja, jotka eivät suoraan edistä ydintoimintoa. Tämä voi tarkoittaa myös sitä, että tuotteeseen on sisällytetty komponentteja, joilla on itsessään jonkin muun digitaalisia elementtejä sisältävän tärkeän tai kriittisen tuotteen toiminto. Se, että digitaalisia elementtejä sisältävä tuote suorittaa muita kuin digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden teknisissä kuvauksissa esitettyjä toimintoja tai niiden lisäksi myös muita toimintoja, ei itsessään merkitse sitä, ettei tuotteella olisi jotakin tällaista ydintoimintoa.

([22]) Ilmaisua ”oletusluokka” tai ”makroluokka” ei määritellä kyberkestävyyssäädöksessä. Tässä asiakirjassa sillä viitataan digitaalisia elementtejä sisältäviin tuotteisiin, joilla ei ole asetuksen liitteessä III tai IV vahvistettuja tuoteryhmän ydintoimintoja, ja joihin sen vuoksi sovelletaan vaatimustenmukaisuuden arviointimenettelyjä 32 artiklan 1 kohdan mukaisesti.

([23]) Valmistaja voi kuitenkin aina päättää soveltaa tiukempaa vaatimustenmukaisuuden arviointimenettelyä 32 artiklan 1 kohdan mukaisesti.

Kaavio 2

Sovellettava vaatimustenmukaisuuden arviointimenettely määrittyy ydintoiminnon, ei oheistoimintojen, perusteella.



141. Digitaalisia elementtejä sisältävä tuote saattaa pystyä suorittamaan tärkeiden tai kriittisten tuotteiden toimintoja, mutta sen ydintoiminto voi erota tällaisen tuoteryhmän ydintoiminnosta. Tällaisessa tapauksessa kyseistä digitaalisia elementtejä sisältävää tuotetta ei katsota digitaalisia elementtejä sisältäväksi tärkeäksi tai kriittiseksi tuotteeksi. Kuten kyberkestävyyssäädöksen 7 artiklan 1 kohdassa nimenomaisesti todetaan digitaalisia elementtejä sisältävien tärkeiden tuotteiden osalta (ja soveltaen samaa logiikkaa digitaalisia elementtejä sisältäviin kriittisiin tuotteisiin), pelkkä digitaalisia elementtejä sisältävän tärkeän tai kriittisen tuotteen integrointi toiseen tuotteeseen ei itsessään johda siihen, että tämä tuote katsottaisiin digitaalisia elementtejä sisältäväksi tärkeäksi tai kriittiseksi tuotteeksi.

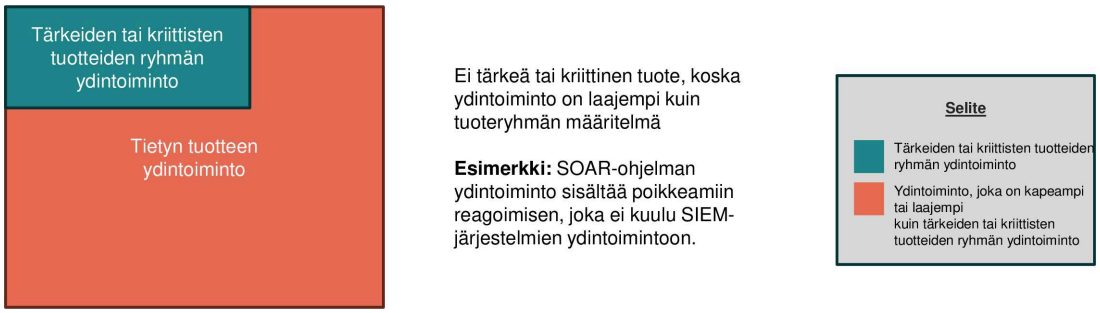
Esimerkki 58: Älypuhelimeen integroidaan käyttöjärjestelmä, jolla on täytäntöönpanoasetuksen (EU) 2025/2392 liitteessä I olevassa 11 kohdassa kuvatut toiminnot. Käyttöjärjestelmä mahdollistaa laitteistoresurssien hallinnan ja ohjelmistosovellusten suorittamisen, mutta älypuhelimella on kokonaisuutena eri ydintoiminto (viestinnän sekä tiedon ja palvelujen saannin mahdollistaminen). Pelkkä käyttöjärjestelmän integrointi ei tarkoita, että älypuhelimella olisi käyttöjärjestelmän ydintoiminto.

142. Tietyt digitaalisia elementtejä sisältävät tuotteet voivat muistuttaa tärkeitä tai kriittisiä tuotteita tai kuulua niiden kanssa samaan yleiseen tuoteperheeseen, mutta niiden ydintoiminto voi olla merkittävästi laajempi tai kapeampi kuin kyseisten tuoteryhmien ydintoiminto. Näin ei ole silloin, kun digitaalisia elementtejä sisältävässä tuotteessa on muita toimintoja, jotka ainoastaan täydentävät tai tehostavat sen ydintoimintoa, joka itsessään vastaa jotakin tärkeiden tai kriittisten tuotteiden ryhmän toimintoa. Tällaisessa tapauksessa digitaalisia elementtejä sisältävällä tuotteella on edelleen kyseisen ryhmän ydintoiminto, ja se luokitellaan vastaavasti. Tätä koskevan arvioinnin olisi perustuttava kyseisen tuotteen pääominaisuuksiin ja teknisiin valmiuksiin, joita tarkastellaan objektiivisesti tuotteen käyttötarkoituksen kannalta. Arvioinnin ei siis tule perustua siihen, kuinka digitaalisia elementtejä sisältävää tuotetta kuvataan tai markkinoidaan, jos tämä kuvaus ei vastaa tuotteen todellisia teknisiä ominaisuuksia.

Esimerkki 59: SOAR-ohjelma (tietoturvan orkestrointi, automatisointi ja tietoturvahäiriöön vastaaminen) pystyy usein suorittamaan ryhmään ”tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)” kuuluvien digitaalisia elementtejä sisältävien tuotteiden toiminnot eli keräämään dataa useista lähteistä, analysoimaan ja vertailemaan tätä dataa ja esittämään sen käyttökelpoisena tietona turvallisuuteen liittyviä tarkoituksia varten. Ohjelman ydintoiminto on kuitenkin merkittävästi laajempi kuin SIEM-järjestelmien, koska keskeinen osa sen teknisiä valmiuksia ovat myös poikkeamiin reagoimisen kaltaiset palvelut. Tämän vuoksi SOAR-ohjelmalla ei yleensä katsota olevan SIEM-järjestelmien ydintoimintoa.

Kaavio 3

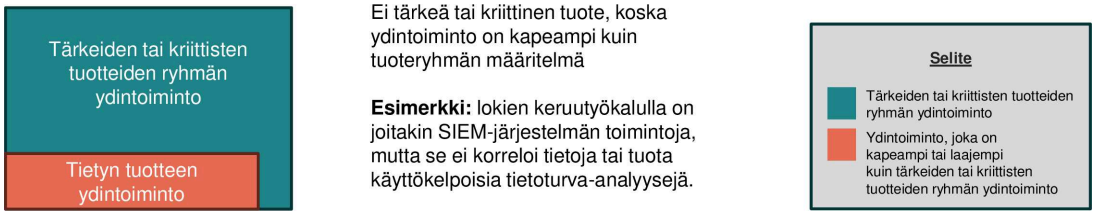
Digitaalisia elementtejä sisältävän tuotteen ydintoiminto voi olla merkittävästi laajempi kuin tärkeiden tai kriittisten tuotteiden ryhmän määritelmä.



Esimerkki 60: Jotkin lokien keruu- ja visualisointityökalut pystyvät käsittelemään lokitietoja ja esittämään järjestelmätapahtumia yksinkertaisilla koontinäytöillä. Vaikka tällaiset työkalut voivat tukea tietoturvan seurantaa, niiden ydintoiminto on kapeampi kuin SIEM-järjestelmillä, koska ne eivät suorita tietojen korrelointia tai tarjoa käyttökelpoisia tietoturva-analyysejä. Tämän vuoksi näillä työkaluilla ei yleensä katsota olevan SIEM-järjestelmien ydintoimintoa.

Kaavio 4

Digitaalisia elementtejä sisältävän tuotteen ydintoiminto voi olla merkittävästi kapeampi kuin tärkeiden tai kriittisten tuotteiden ryhmän määritelmä.

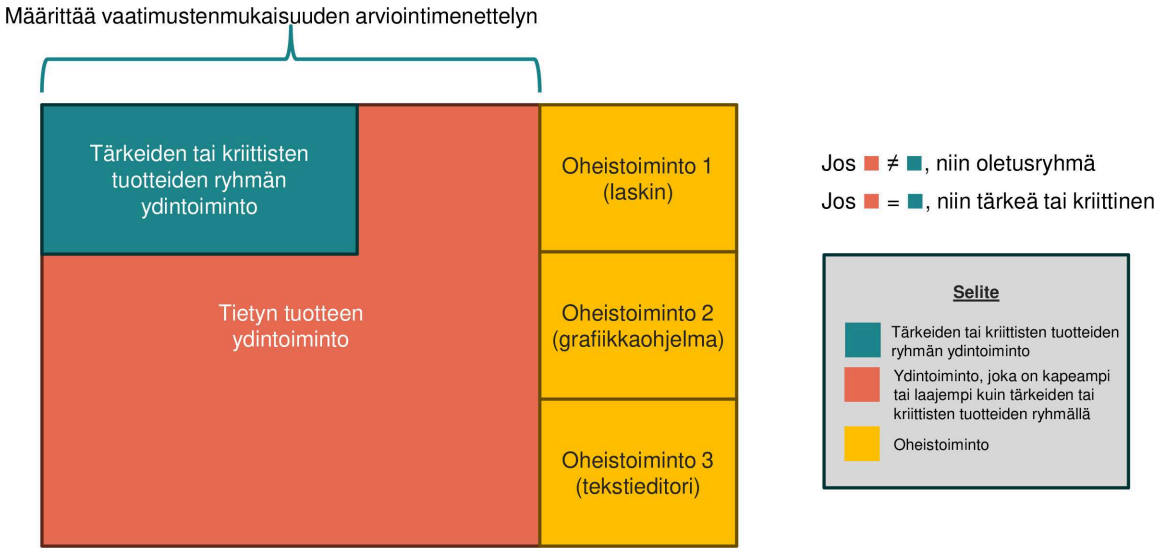


143. Valmistaja ei saa esittää digitaalisia elementtejä sisältävän tuotteensa ydintoimintoa harhaanjohtavalla tavalla tarkoituksenaan välttää digitaalisia elementtejä sisältävien tärkeiden tai kriittisten tuotteiden vaatimustenmukaisuuden arvioinnin piiriin kuuluminen. Harhaanjohtavana pidetään esimerkiksi jonkin toiminnon merkityksen korostamista tai häivyttämistä siten, että tuotteen toiminnot vaikuttavat tiettyä ydintoimintoa merkittävästi laajemmilta tai kapeammilta. Tällaisessa tapauksessa myyntimateriaalit, käyttöohjeet ja tekniset asiakirjat ovat selvästi ristiriidassa keskenään.

144. Digitaalisia elementtejä sisältävällä tuotteella voi olla enintään yksi ydintoiminto, jonka perusteella sovellettava vaatimustenmukaisuuden arviointimenettely määritetään. Valmistajan on kuvattava digitaalisia elementtejä sisältävän tuotteensa käyttötarkoitus ja noudattamansa vaatimustenmukaisuuden arviointimenettely tuotteen teknisissä asiakirjoissa kyberkestävyyssäädöksen liitteen VII mukaisesti. Tuotteen ydintoiminto on näin ollen yksilöitävä selkeästi. Sen ansiosta vaatimustenmukaisuuden arviointimenettely voidaan määrittää oikein ja markkinavalvontaviranomaiset voivat valvoa ja tarkistaa, että kyberkestävyyssäädöstä sovelletaan asianmukaisesti.

Kaavio 5

Miten digitaalisia elementtejä sisältävän tuotteen ydintoiminnon perusteella määritetään tuoteryhmä ja sitä kautta sovellettava vaatimustenmukaisuuden arviointimenettely.



145. Digitaalisia elementtejä sisältävä tuote voidaan toisinaan saattaa markkinoille yksittäisenä digitaalisia elementtejä sisältävänä tuotteena, joka kuitenkin koostuu erillisistä moduuleista, joista kullakin on oma toimintonsa. Jos valmistaja asettaa tällaisia moduuleja myös erikseen saataville markkinoilla, esimerkiksi erillään ostettaviksi, lisensoitaviksi tai tilattaviksi, kyseiset moduulit ovat itsenäisiä digitaalisia elementtejä sisältäviä tuotteita. Ne siis luokitellaan oman ydintoimintonsa perusteella (ja niihin sovelletaan asianmukaista vaatimustenmukaisuuden arviointimenettelyä, joka määritetään kunkin moduulin ydintoiminnon perusteella). Tämä ei koske moduuleja, joita tarjotaan ainoastaan integroidun digitaalisia elementtejä sisältävän tuotteen komponentteina eikä aseteta saataville erikseen. Näissä tapauksissa ydintoiminto määritetään digitaalisia elementtejä sisältävän integroidun tuotteen tasolla.

Esimerkki 61: Valmistaja saattaa markkinoille yhtenäisen tietoturvapaketin. Pakettiin kuuluu useita moduuleja, muun muassa SIEM-järjestelmä, tunkeutumisen havaitsemisjärjestelmä ja analytiikkamoduuli. Valmistaja tarjoaa mahdollisuuden tilata kyseisiä moduuleja myös erikseen. Tässä tapauksessa kukin moduuli on erillinen digitaalisia elementtejä sisältävä tuote, joka luokitellaan oman ydintoimintonsa perusteella. SIEM-moduuliin sovelletaan luokkaan I kuuluvien digitaalisia elementtejä sisältävien tärkeiden tuotteiden vaatimustenmukaisuuden arviointia, koska sen ydintoiminto on ”tietoturvatietojen ja tapahtumien hallintajärjestelmät (SIEM)”. Tunkeutumisen havaitsemisjärjestelmään sovelletaan luokkaan II kuuluvien digitaalisia elementtejä sisältävien tärkeiden tuotteiden vaatimustenmukaisuuden arviointia, koska sen ydintoiminto on ”palomuurit ja tunkeutumisen havaitsemis- ja estojärjestelmät”. Analytiikkamoduuliin sovelletaan digitaalisia elementtejä sisältävien oletusluokkaan kuuluvien tuotteiden vaatimustenmukaisuuden arviointia, koska sen ydintoiminto ei kuulu mihinkään tärkeiden tai kriittisten tuotteiden ryhmään.

146. Kyberkestävyyssäädöksen 32 artiklassa säädettyjen velvoitteiden noudattamatta jättäminen voi johtaa 64 artiklan 3 kohdan mukaisiin hallinnollisiin sakkoihin.

6.2 Digitaalisia elementtejä sisältävien tärkeiden ja kriittisten tuotteiden vaatimustenmukaisuuden arviointi

147. Kun valmistaja on määrittänyt digitaalisia elementtejä sisältävän tuotteensa ydintoiminnon, sen on suoritettava jokin sovellettavista vaatimustenmukaisuuden arviointimenettelyistä. Valmistajan on varmistettava, että digitaalisia elementtejä sisältävä tuote täyttää kokonaisuudessaan olennaiset vaatimukset ottaen huomioon tuotteeseen mahdollisesti integroitujen komponenttien tai toimintojen turvallisuus.

148. Luokaan II kuuluville digitaalisia elementtejä sisältäville tärkeille tuotteille (lukuun ottamatta vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavia tuotteita 32 artiklan 5 kohdan nojalla) sekä digitaalisia elementtejä sisältäville kriittisille tuotteille on tehtävä pakollinen vaatimustenmukaisuuden arviointi, johon osallistuu kolmas osapuoli (perustuen moduuliin B ja C, moduuliin H tai kyberturvallisuuden sertifiointijärjestelmään) ([24]). Sitä vastoin luokkaan I kuuluvien digitaalisia elementtejä sisältävien tärkeiden tuotteiden (lukuun ottamatta vapaiksi ja avoimen lähdekoodin ohjelmistoiksi luokiteltavia tuotteita 32 artiklan 5 kohdan nojalla) vaatimustenmukaisuuden arviointimenettelyn on oltava kolmannen osapuolen suorittama ainoastaan, jos valmistaja ei ole käyttänyt tai on käyttänyt vain osittain yhdenmukaistettuja standardeja, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*, jäljempänä 'yhdenmukaistetut standardit', yhteisiä eritelmiä tai eurooppalaisia kyberturvallisuuden sertifiointijärjestelmiä varmuustasolla "korotettu" ([25]).

149. Jotta luokkaan I kuuluva digitaalisia elementtejä sisältävä tärkeä tuote voidaan arvioida sisäisen valvonnan menettelyllä, i) on sovellettava kaikkia asiaankuuluvan yhdenmukaistetun standardin sovellettavia vaatimuksia ja ii) standardin soveltamisalan on katettava vähintään kaikki kyseisen tuotteen ydintoimintoon liittyvät kyberturvallisuusriskit.

150. Digitaalisia elementtejä sisältävä tuote voi olla toiminnoiltaan laajempi kuin mitä asiaankuuluvan yhdenmukaistetun standardin soveltamisalassa on ennakoitu, ja sen lisätoimintoihin voi liittyä erilaisia tai uusia kyberturvallisuusriskejä. Valmistajan on aina tehtävä 13 artiklan 2 kohdan mukainen riskinarviointi ja sen myötä tarkistettava, kattaako yhdenmukaistetun standardin soveltaminen kaikki digitaalisia elementtejä sisältävään tuotteeseen liittyvät riskit. Jos standardin soveltamisella ei kateta kaikkia riskejä, valmistajan olisi varmistettava muilla tavoin, että digitaalisia elementtejä sisältävä tuote on olennaisten vaatimusten mukainen.

151. Jos luokkaan I kuuluvan digitaalisia elementtejä sisältävän tärkeän tuotteen valmistaja on soveltanut asiaankuuluvaa yhdenmukaistettua standardia, joka kattaa tuotteen ydintoimintoon liittyvät riskit, se voi päättää osoittaa tuotteen vaatimustenmukaisuuden käyttämällä sisäisen valvonnan menettelyä. Osana vaatimustenmukaisuuden arviointitoimiaan valmistajan on edelleen osoitettava, että kaikki kyseiseen digitaalisia elementtejä sisältävään tuotteeseen liittyvät riskit on otettu huomioon. Jos yhdenmukaistetun standardin soveltamisala ei vastaa digitaalisia elementtejä sisältävää tuotetta kokonaisuudessaan, valmistajan on lisäksi dokumentoitava, mitä lisätoimenpiteitä se on toteuttanut kyseisten riskien käsittelemiseksi.

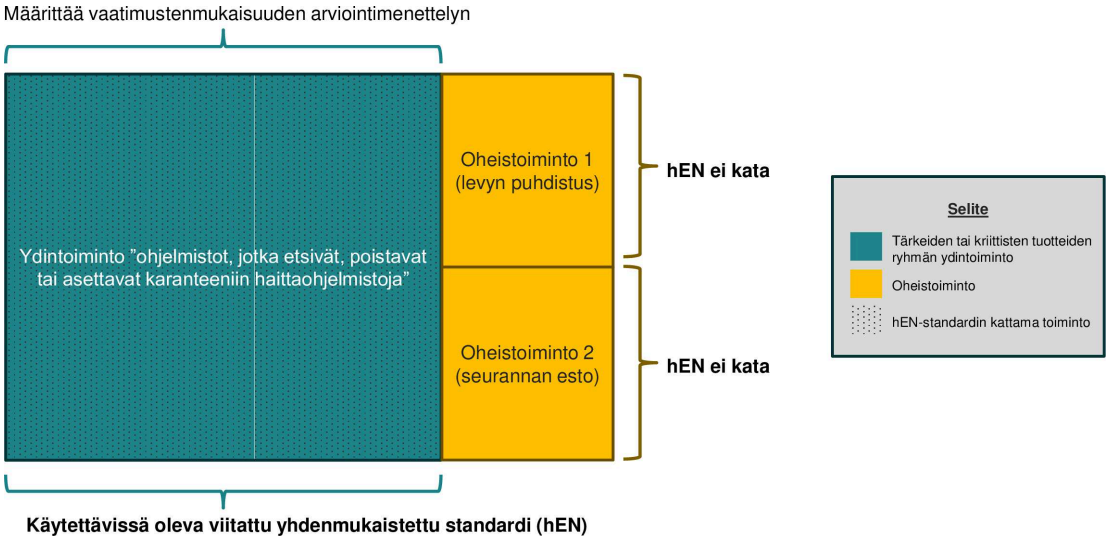
Esimerkki 62: Virustorjuntaohjelmistolla on täytäntöönpanoasetuksen (EU) 2025/2392 liitteessä I olevassa 4 kohdassa on kuvattu ydintoiminto "ohjelmistot, jotka etsivät, poistavat tai siirtävät karanteeniin haittaohjelmistoja". Kyseisellä digitaalisia elementtejä sisältävällä tuotteella on myös muita toimintoja, joita ovat levyn puhdistus ja seurannan esto, jolla suojataan käyttäjää tämän selatessa verkkoa. Valmistaja tekee riskinarvioinnin, joka kattaa digitaalisia elementtejä sisältävän tuotteen kokonaisuudessaan, toisin sanottuna virustentorjuntaohjelmiston ydintoiminnon sekä levyn puhdistuksen ja seurannan eston toiminnot. Valmistaja soveltaa yhdenmukaistettua standardia, joka kattaa virustentorjuntaohjelmiston ydintoimintoon liittyvät riskit, ja toteuttaa lisätoimenpiteitä muiden toimintojen aiheuttamien riskien hallitsemiseksi. Valmistaja saa käyttää vaatimustenmukaisuuden arvioinnissa sisäisen valvonnan menettelyä, joka kattaa digitaalisia elementtejä sisältävän tuotteen kokonaisuudessaan, levyn puhdistus ja seurannan eston toiminnot mukaan lukien.

([24]) Tämä koskee myös tapauksia, joissa käytetään eurooppalaista kyberturvallisuuden sertifiointijärjestelmää varmuustasolla, joka on vähintään "korotettu", ja näin ollen edellytetään kolmatta osapuolta edustavan sertifiointielimen osallistumista.

([25]) Tiiviyden vuoksi tässä kohdassa viitataan jatkossa ainoastaan yhdenmukaistettuihin standardeihin, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*. Samaa ohjeistusta sovelletaan kuitenkin myös 27 artiklan 2 kohdan mukaisesti hyväksyttyihin yhteisiin eritelmiin sekä eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin, jos komissio on yksilöinyt sellaisia 27 artiklan 9 kohdan mukaisesti annetuissa delegoiduissa säädöksissä.

Kaavio 6

Sovellettava vaatimustenmukaisuuden arviointimenettely määritetään sellaisen viitatun yhdenmukaistetun standardin käytön perusteella, joka kattaa vain ydintoiminnon.



152. Edellä mainittu pätee myös silloin, kun digitaalisia elementtejä sisältävään tuotteeseen on integroitu lisätoiminto, joka itsessään on jonkin digitaalisia elementtejä sisältävän tärkeän tai kriittisen tuotteen toiminto. Onkin huomattava, että digitaalisia elementtejä sisältävän tuotteen ydintoiminto kokonaisuutena – eivät yksittäisten integroitujen osien toiminnot erillään tarkasteltuina – määrittää, kuuluuko digitaalisia elementtejä sisältävä tuote johonkin tärkeiden tai kriittisten tuotteiden ryhmään (ja siten sellaiseen sovellettavan vaatimustenmukaisuuden arviointimenettelyn piiriin). Esimerkiksi jos digitaalisia elementtejä sisältävällä tuotteella on luokkaan I kuuluvan digitaalisia elementtejä sisältävän tärkeän tuotteen ydintoiminto, koko tuotteeseen sovelletaan luokkaan I kuuluviin digitaalisia elementtejä sisältäviin tärkeisiin tuotteisiin sovellettavaa vaatimustenmukaisuuden arviointia myös silloin, jos tuotteeseen on integroitu komponentti, joka itsessään on digitaalisia elementtejä sisältävä kriittinen tuote. Jos valmistaja tällaisessa tapauksessa käyttää kyseisen tuotteen ydintoimintoon liittyvät riskit kattavaa yhdenmukaistettua standardia, se saa käyttää sisäisen valvonnan menettelyä.

Esimerkki 63: Digitaalisia elementtejä sisältävällä laitteistotuotteella on täytäntöönpanoasetuksen (EU) 2025/2392 liitteessä I olevassa 12 kohdassa kuvattu reitittimen ydintoiminto. Kyseisellä digitaalisia elementtejä sisältävällä tuotteella on myös muita toimintoja. Se voi esimerkiksi toimia palomuurina, koska siihen on integroitu palomuurikomponentti. Valmistaja tekee riskinarvioinnin, jossa otetaan huomioon digitaalisia elementtejä sisältävä tuote kokonaisuudessaan, reitittimen ydintoiminto ja palomuuritoiminto mukaan lukien. Valmistaja soveltaa yhdenmukaistettua standardia, joka kattaa reitittimen ydintoimintoon liittyvät riskit, ja toteuttaa lisätoimenpiteitä muiden toimintojen aiheuttamien riskien hallitsemiseksi. Valmistaja voi esimerkiksi soveltaa palomuurin osalta yhdenmukaistettua standardia, joka kattaa palomuurin toimintaan liittyvät riskit. Valmistaja saa käyttää sisäisen valvonnan menettelyä vaatimustenmukaisuuden arvioinnissa, koska arviointi kattaa digitaalisia elementtejä sisältävän tuotteen kokonaisuudessaan palomuuritoiminto mukaan luettuna.

6.3 Vaikutukset vaatimustenmukaisuusolettamaan

153. Kyberkestävyyssäädöksen 27 artiklan 1 kohdassa säädetään, että digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, jotka ovat sellaisten yhdenmukaistettujen standardien tai niiden osien mukaisia, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä* (EUVL), on pidettävä niiden kyberkestävyyssäädöksen olennaisten vaatimusten mukaisina, jotka kyseiset standardit tai niiden osat kattavat ([26]). Tämä

([26]) Sinisen oppaan 4.1.2.2 kohdassa todetaan yksiselitteisesti, että ”vaaroja koskevassa yhdenmukaistamislainsäädännössä [...] valmistajat vastaavat aina – myös sovellettaessa yhdenmukaistettuja standardeja, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*:ssä – kaikilta osin tuotteeseensa liittyvien vaarojen arvioinnista määrittääkseen, mitkä olennaiset (tai muut) vaatimukset ovat asiaankuuluvia. Arvioinnin jälkeen valmistaja voi valita, soveltaako se yhdenmukaistetuissa standardeissa esitettyjä teknisiä eritelmiä toteuttaakseen riskien vähentämistoimenpiteet, jotka on määritelty yhdenmukaistetuissa standardeissa, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*:ssä”.

vaatimustenmukaisuusolettama laajennetaan 27 artiklan 5 kohdassa koskemaan digitaalisia elementtejä sisältäviä tuotteita ja valmistajan käyttöön ottamia prosesseja, jotka ovat komission täytäntöönpanosäädöksillä hyväksymien yhteisten eritelmien mukaisia. Asetuksen 27 artiklan 8 kohdassa vahvistetaan vaatimustenmukaisuusolettama digitaalisia elementtejä sisältäville tuotteille ja valmistajan käyttöön ottamille prosesseille, joille on annettu asetuksen (EU) 2019/881 nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukainen EU-vaatimustenmukaisuusilmoitus tai sertifikaatti, jos tästä on säädetty 27 artiklan 9 kohdan mukaisesti annetuissa delegoiduissa säädöksissä ([27]).

154. Näin ollen valmistaja, joka on soveltanut yhdenmukaistettua standardia, jonka viitetiedot on julkaistu EUVL:ssä, hyötyy vaatimustenmukaisuusolettamasta kyseisen standardin kattamien riskien osalta. Tästä voi olla kyse esimerkiksi silloin, kun viitattu yhdenmukaistettu standardi kattaa kaikki riskit, jotka liittyvät digitaalisia elementtejä sisältävän tuotteen ydintoimintoon, eikä tuotteella ole muita toimintoja, joista voisi aiheutua kyberturvallisuusriskejä. Esimerkiksi reitittimiä koskevan yhdenmukaistetun standardin odotetaan kattavan vähintään riskit, jotka liittyvät tällaisten digitaalisia elementtejä sisältävien tuotteiden ydintoimintoon. Jos kyseisellä tuotteella ei ole muita toimintoja tai jos standardi kattaa sen muihin toimintoihin liittyvät riskit, digitaalisia elementtejä sisältävään tuotteeseen voidaan soveltaa vaatimustenmukaisuusolettamaa.

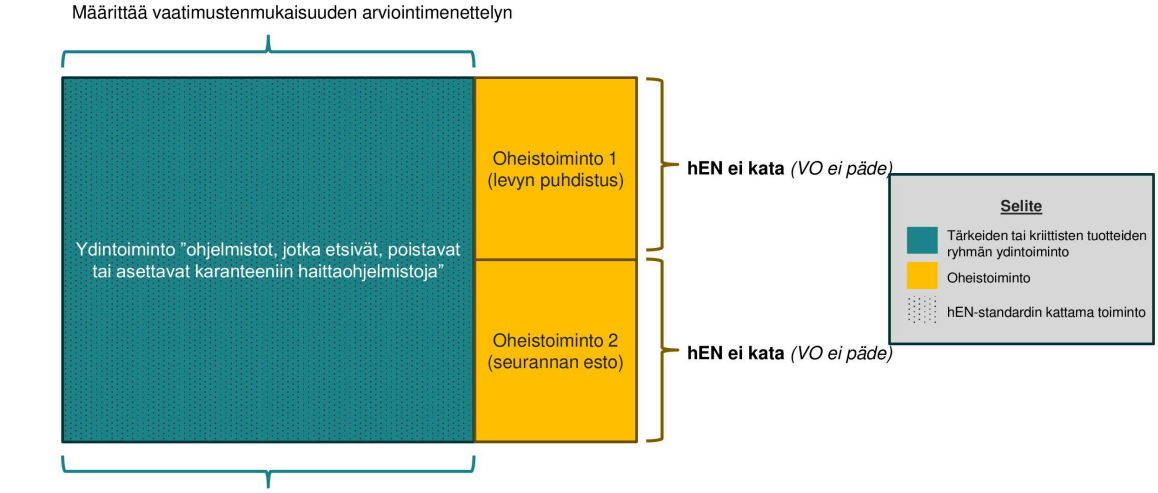
155. Edellä esitetyissä 151 ja 152 kohdan esimerkkitapauksissa valmistaja saa käyttää sisäisen valvonnan menettelyä, koska yhdenmukaistettu standardi kattaa digitaalisia elementtejä sisältävän tuotteen ydintoimintoon liittyvät riskit. Näiden esimerkkien digitaalisia elementtejä sisältävät tuotteet voivat kuitenkin olla yhdenmukaistettujen standardien soveltamisalaa laajempia, ja niiden muut toiminnot voivat aiheuttaa kyberturvallisuusriskejä, joita kyseisellä yhdenmukaistetulla standardilla ei oteta huomioon. Tällaisiin digitaalisia elementtejä sisältäviin tuotteisiin ei voida soveltaa vaatimustenmukaisuusolettamaa kyberturvallisuusriskejä aiheuttavien muiden toimintojen osalta.

Esimerkki 64: Virustorjuntaohjelmistolla on ydintoiminto ”ohjelmistot, jotka etsivät, poistavat tai siirtävät karanteeniin haittaohjelmistoja”, ja yhdenmukaistettu standardi kattaa tähän ydintoimintoon liittyvät riskit. Kyseisellä digitaalisia elementtejä sisältävällä tuotteella on myös muita toimintoja, joita ovat levyn puhdistus ja seurannan esto, jolla suojataan käyttäjää tämän selatessa verkkoa. Yhdenmukaistettu standardi ei kata näihin toimintoihin liittyviä riskejä. Jos valmistaja soveltaa yhdenmukaistettua standardia, se saa käyttää vaatimustenmukaisuuden arvioinnissa sisäisen valvonnan menettelyä. Se hyötyy vaatimustenmukaisuusolettamasta tuotteen ydintoimintoon liittyvien riskien osalta, mutta ei muihin toimintoihin liittyvien riskien osalta.

([27]) Kuten edellä, tässä kohdassa viitataan tiiviyden vuoksi jatkossa ainoastaan yhdenmukaistettuihin standardeihin, joiden viitetiedot on julkaistu *Euroopan unionin virallisessa lehdessä*:ssä. Samaa ohjeistusta sovelletaan kuitenkin myös yhteisiin eritelmiin ja eurooppalaisiin kyberturvallisuuden sertifiointijärjestelmiin.

Kaavio 7

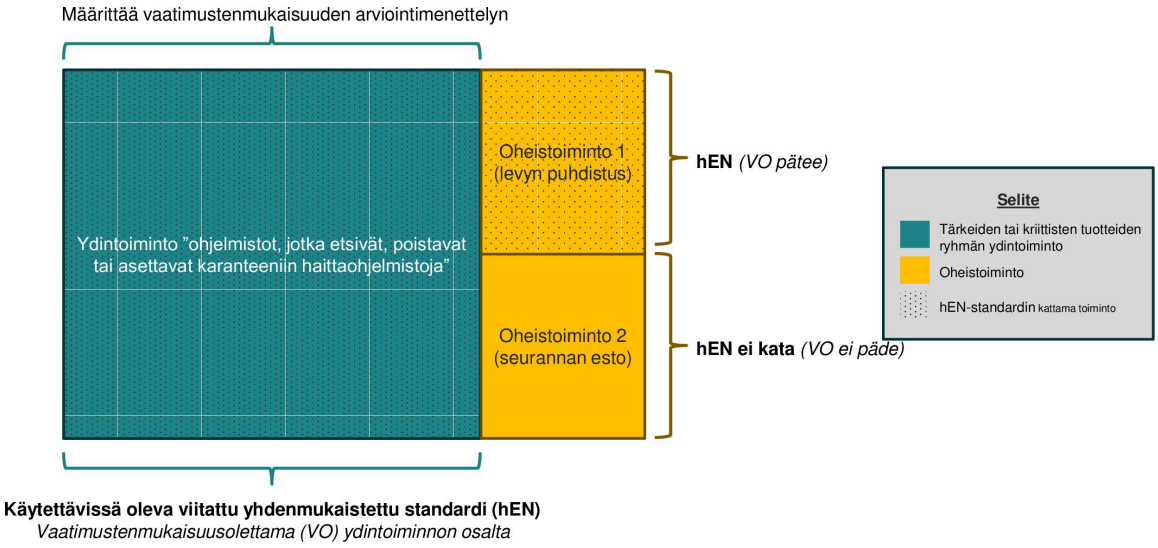
Yhdenmukaistettu standardi luo vaatimustenmukaisuusolettaman ydintoiminnon osalta, koska se kattaa kaikki kyseiseen ydintoimintoon liittyvät riskit. Vaatimustenmukaisuusolettama ei päde oheistoimintoihin.



Esimerkki 65: Edellisen esimerkin mukaisessa tilanteessa yhdenmukaistettu standardi saatetaan ajan tasalle siten, että se kattaa myös riskit, jotka liittyvät yhteen lisätoiminnoista eli levyn puhdistukseen, mutta eivät toiseen eli seurannan estoon. Jos valmistaja soveltaa yhdenmukaistettua standardia, se saa käyttää vaatimustenmukaisuuden arvioinnissa sisäisen valvonnan menettelyä. Se hyötyy vaatimustenmukaisuusolettamasta tuotteen ydintoimintoon ja levyn puhdistuksen toimintoon liittyvien riskien osalta, mutta ei seurannan estoon liittyvien riskien osalta.

Kaavio 8

Yhdenmukaistettu standardi luo vaatimustenmukaisuusolettaman ydintoiminnon ja oheistoiminnon 1 osalta, koska se kattaa kaikki näihin toimintoihin liittyvät riskit. Vaatimustenmukaisuusolettama ei päde oheistoimintoon 2.



7. KYBERTURVALLISUUSRISKIEN ARVIOINTI JA DIGITAALISIA ELEMENTTEJÄ SISÄLTÄVIEN TUOTTEIDEN JA KOMPONENTTIEN INTEGROINTI

7.1 Kyberturvallisuusriskien arviointi ja käsittely

156. Kyberkestävyyssäädöksen 13 artiklan 2 kohdassa säädetty kyberturvallisuusriskien arviointi edellyttää, että valmistajat tunnistavat asiaankuuluvat riskit ja arvioivat niiden mahdolliset vaikutukset digitaalisia elementtejä sisältävään tuotteeseen. Valmistajien on lisäksi toteutettava asianmukaiset toimenpiteet näihin riskeihin puuttumiseksi liitteessä I vahvistettujen olennaisten vaatimusten mukaisesti.

157. Organisaation riskinhallinnassa riskejä arvioidaan yleensä organisaation sisäisistä tavoitteista tai riskinottohalusta johdettujen hyväksymiskriteerien perusteella. Sen sijaan kyberkestävyyssäädöksen mukaan jäännöskyberturvallisuusriskiä olisi arvioitava sen vaatimuksen valossa, jonka mukaan markkinoille saatettavan digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuden tason on oltava oikeassa suhteessa riskeihin, ottaen huomioon tuotteen käyttötarkoitus ja kohtuudella ennakoitavissa oleva käyttö.

158. Näin ollen valmistajan sisäisellä riskinsietokyvyllä, kaupallisella strategialla tai pelkillä kustannusnäkökohdilla ei ole merkitystä määritettäessä, onko riskeihin puututtu. Sovellettaessa 13 artiklan 2 ja 3 kohtaa valmistajien on pystyttävä määrittämään, onko tunnistettuihin kyberturvallisuusriskeihin puututtu riittävästi panemalla täytäntöön liitteessä I olevan I osan olennaiset vaatimukset, ottaen huomioon käyttötarkoitus, kohtuudella ennakoitavissa oleva käyttö ja käyttöolosuhteet, mukaan lukien tarvittaessa toimintaympäristö (esimerkiksi digitaalisia elementtejä sisältävän tuotteen aiotut käyttäjät) ja suojattava omaisuus, sekä aika, jonka digitaalisia elementtejä sisältävän tuotteen odotetaan olevan käytössä.

159. Jäännöskyberturvallisuusriski on riskien arvioinnin ja riskien käsittelyn luontainen seuraus. On tunnustettua, että kyberturvallisuusriskejä ei voida käytännössä poistaa kokonaan. Jäännösriskin olemassaolo ei kuitenkaan merkitse sitä, että valmistaja voisi harkintansa mukaan hyväksyä minkä tahansa riskin. Digitaalisia elementtejä sisältävä tuote voidaan saattaa markkinoille vain, jos jäännösriskeihin on asianmukaisten toimenpiteiden toteuttamisen jälkeen puututtu riittävästi panemalla täytäntöön olennaiset vaatimukset, ottaen huomioon digitaalisia elementtejä sisältävän tuotteen käyttötarkoitus ja kohtuudella ennakoitavissa oleva käyttö.

160. Kyberkestävyyssäädöksen 13 artiklan 3 kohdan mukaisesti valmistajien on puututtava tunnistettuihin kyberturvallisuusriskeihin asianmukaisin toimenpitein, myös tuotetasolla. Olosuhteista riippuen tämä voi tarkoittaa esimerkiksi hyökkäyspinta-alan pienentämistä, teknisten suojatoimien toteuttamista, toimintojen rajoittamista tai mukauttamista taikka digitaalisia elementtejä sisältävän tuotteen käyttötarkoituksen määrittelemistä täsmällisemmin. Valmistajat voivat myös ryhtyä toimiin vaikuttaakseen digitaalisia elementtejä sisältävän tuotteen kohtuudella ennakoitavissa olevaan käyttöön esimerkiksi riskiviestinnän, käyttäjäohjeistuksen tai käyttöliittymän suunnittelun avulla, jotta käyttäjien toimintaa voidaan ohjata turvallisiin käyttötapoihin.

161. Kyberkestävyyssäädöksessä ei säädetä kyberturvallisuusriskien tai niitä koskevan vastuun siirtämisestä käyttäjille tai kolmansille osapuolille tuotesuunnittelun puutteiden kompensoimiseksi tai sen perustelemiseksi, että kyberturvallisuusriskeihin jätetään puuttumatta. Valmistajalla säilyy velvollisuus saattaa markkinoille turvallinen digitaalisia elementtejä sisältävä tuote ja osoittaa, että tuote on olennaisten vaatimusten mukainen.

162. Käyttäjille annettavia tietoja ja ohjeita voidaan käyttää digitaalisia elementtejä sisältävän tuotteen turvallisen käyttöönoton ja käytön tukemiseen, myös silloin, kun valmistaja on päättänyt rajata kyseisen tuotteen käyttötarkoituksen luotettaviin ympäristöihin. Näillä tiedoilla ja ohjeilla voidaan myös tiedottaa käyttäjille jäännösriskeistä tavalla, joka on asianmukainen digitaalisia elementtejä sisältävän tuotteen luonne ja sen aiotut käyttäjät huomioon ottaen.

Esimerkki 66: Valmistaja kehittää teollisuusanturin käytettäväksi luotettavissa ympäristöissä. Jotta anturi toimisi oikein, valmistaja ei toteuta toimenpiteitä anturin itsensä suojaamiseksi fyysisiltä hyökkäyksiltä. Riskien arvioinnissa tunnistettujen tähän liittyvien riskien lieventämiseksi valmistaja rajaa anturin käyttötarkoituksen ainoastaan käyttöön luotettavissa ympäristöissä, joissa estetään luvaton fyysinen pääsy digitaalisia elementtejä sisältävään tuotteeseen. Käyttäjille annettavissa tiedoissa ja ohjeissa annetaan selkeät tiedot näistä anturin käyttöä koskevista rajoituksista tavalla, joka on asianmukainen digitaalisia elementtejä sisältävän tuotteen luonne ja sen aiotut käyttäjät huomioon ottaen.

Esimerkki 67: Valmistaja kehittää ammattikäyttöön tarkoitetun ohjelmistosovelluksen käytettäväksi hallinnoiduilla pöytäkoneilla ja mobiililaitteilla. Sovellus käsittelee paikallisesti tallennettuja arkaluonteisia tietoja ja käyttäjien tuottamaa sisältöä. Riskien arvioinnin yhteydessä valmistaja tunnistaa riskin, että tällaisiin tietoihin päästään luvattomasti, jos ne tallennetaan laitteelle selväkielitekstinä. Sen sijaan, että valmistaja suunnittelisi ja toteuttaisi sovelluksessa oman salausmekanismin, se päättää hyödyntää sovelluksen ajamiseen tarkoitetun käyttöjärjestelmän omia salaus- ja avaintenhallintatoimintoja, sillä käyttöjärjestelmän sisäänrakennetut kryptografiset palvelut ovat kehittyneitä ja niitä ylläpidetään säännöllisesti.

163. Jos kyberturvallisuusriskien arvioinnissa tunnistetaan riskejä, joihin ei voida asianmukaisin toimenpitein puuttua riittävästi, kyberkestävyyssäädöksen noudattaminen voi edellyttää muutoksia digitaalisia elementtejä sisältävän tuotteen suunnitteluun, toimintoihin tai käyttötarkoitukseen. Pelkästään kustannuksiin tai kaupalliseen toteutettavuuteen liittyvät näkökohdat eivät ole riittävä peruste jättää tällaisia riskejä käsittelemättä, jos tämä estäisi digitaalisia elementtejä sisältävää tuotetta täyttämästä olennaisia vaatimuksia.

7.2 Digitaalisia elementtejä sisältävien tuotteiden suunnittelu, kehittäminen ja tuottaminen siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin

164. Kyberkestävyyssäädöksen liitteessä I olevan I osan 1 kohdassa tarkoitetun olennaisen kyberturvallisuusvaatimuksen mukaan digitaalisia elementtejä sisältävät tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin.

165. Tämän olennaisen vaatimuksen tarkoituksena on puuttua kaikkiin kyberturvallisuusriskeihin, jotka on tunnistettu osana kyberturvallisuusriskien arviointia. Tähän kuuluvat erityisesti kyberturvallisuusriskit, joihin ei muutoin puututa riittävästi pantaessa täytäntöön liitteessä I olevan I osan muita olennaisia vaatimuksia kuin 1 kohdassa olevaa vaatimusta. Tämä olennainen vaatimus eroaa oikeudellisesta velvoitteesta suorittaa kyberturvallisuusriskien arviointi, joka on suoritettava 13 artiklan 2 kohdan mukaisesti.

166. Jos kaikki digitaalisia elementtejä sisältävään tuotteeseen liittyvät asiaankuuluvat kyberturvallisuusriskit käsitellään toteuttamalla asianmukaiset toimenpiteet muiden sovellettavien olennaisten vaatimusten kuin 1 kohdassa tarkoitetun vaatimuksen noudattamiseksi, liitteessä I olevan I osan 1 kohdassa tarkoitetun olennaisen vaatimuksen katsotaan täyttyvän. Sitä vastoin, jos kyberturvallisuusriskien arvioinnissa tunnistetaan muita riskejä, joihin tällaisilla toimenpiteillä ei ole puututtu kaikilta osin, valmistajien on toteutettava digitaalisia elementtejä sisältävään tuotteeseen kohdistuvia asianmukaisia toimenpiteitä näihin riskeihin puuttumiseksi, jotta liitteessä I olevan I osan 1 kohdassa tarkoitettua olennaista vaatimusta noudatetaan. Käytännössä muiden olennaisten vaatimusten noudattamisen odotetaan useimmissa tapauksissa johtavan myös tämän vaatimuksen noudattamiseen.

7.3 Riskien arviointi ja asianmukainen huolellisuus ulkoisten riippuvuuksien ja integroitujen komponenttien osalta

167. Kyberkestävyyssäädöksessä asetetaan valmistajille kyberturvallisuusriskien hallinnan osalta kaksi erillistä mutta toisiaan täydentävää velvoitetta. Ensinnäkin 13 artiklan 2 kohdassa edellytetään, että valmistajat suorittavat itse digitaalisia elementtejä sisältävää tuotetta koskevan kyberturvallisuusriskien arvioinnin. Toiseksi 13 artiklan 5 kohdassa asetetaan velvoite noudattaa asianmukaista huolellisuutta integroitujen komponenttien osalta. Yhdessä näillä kahdella velvoitteella pyritään varmistamaan, että digitaalisia elementtejä sisältävä tuote säilyy turvallisena myös silloin, kun se on riippuvainen datan etäkäsittelyratkaisuista, etäpalveluista tai kolmansien osapuolten ohjelmisto- tai laitteistokomponenteista.

168. Kyberturvallisuusriskien arviointi koskee sellaisten asiaankuuluvien riskien tunnistamista ja hallintaa, jotka voivat vaikuttaa digitaalisia elementtejä sisältävään tuotteeseen, mukaan lukien riskit, jotka ovat peräisin itse tuotteen ulkopuolelta, kuten ulkoisista verkoista, ympäristötekijöistä tai muista ulkoisista seikoista, jotka voivat vaikuttaa digitaalisia elementtejä sisältävään tuotteeseen tai joista tuote on riippuvainen. Tällaisten ulkoisten riskien osalta kyberkestävyyssäädöksessä ei edellytetä, että valmistajat valvovat tai hallitsevat ulkoista ympäristöä. Sen sijaan valmistajien on tunnistettava tällaiset riskit ja lievennettävä niitä itse digitaalisia elementtejä sisältävän tuotteen suunnittelun ja kehittämisen avulla. Tämä edellyttää liitteessä I olevassa I osassa vahvistettujen asianmukaisten olennaisten vaatimusten täytäntöönpanoa ja tarvittaessa sitä, että käyttäjille annetaan tietoja ja ohjeita integrointiin tai käyttöönottoon liittyvistä riskeistä.

169. Valmistaja voi esimerkiksi tunnistaa riskin siitä, että asiattomat henkilöt voivat digitaalisia elementtejä sisältävän tuotteen ollessa käytössä päästä sellaisiin taustajärjestelmiin, jotka eivät ole osa itse tuotetta, ja yrittää lähettää digitaalisia elementtejä sisältävälle tuotteelle haitallisia komentoja. Tällaiset taustajärjestelmät eivät ole datan etäkäsittelyratkaisuja, jos niitä ei ole suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla taikka jos ne eivät tue jotakin digitaalisia elementtejä sisältävän tuotteen toimintoa, eivätkä ne näin ollen kuulu kyberkestävyyssäädöksessä tarkoitetun digitaalisia elementtejä sisältävän tuotteen piiriin. Kyberkestävyyssäädöksessä edellytetään kuitenkin, että valmistaja puuttuu niiden mahdollisesti aiheuttamaan riskiin tuotetasolla toteutettavilla toimenpiteillä, kuten edellyttämällä etäkomentojen kryptografista todentamista, varmistamalla konfiguraatiomuutosten eheyden tai tuottamalla turvallisuuden kannalta merkityksellisiä lokitietoja tai hälytyksiä, kun havaitaan poikkeavaa toimintaa. Vastaavasti, jos valmistaja tunnistaa riskin, joka aiheutuu siitä, että tällainen ulkoinen palvelu ei ole saatavilla esimerkiksi sähkökatkosten tai infrastruktuurin toimintahäiriöiden vuoksi, kyberkestävyyssäädös voi edellyttää tuotetasolla toteutettavia toimenpiteitä tällaisten kyberturvallisuusriskien lieventämiseksi, esimerkiksi sen varmistamista, ettei käyttökatkos saa digitaalisia elementtejä sisältävää tuotetta siirtymään turvattomaan tilaan. Tällaisissa tapauksissa kyberkestävyyssäädöksessä säännellään sitä, miten digitaalisia elementtejä sisältävä tuote reagoi tällaisiin ulkoisiin riskeihin. Siinä ei aseteta velvoitteita sen suhteen, miten taustainfrastruktuuri on järjestetty, miten sen henkilöstö on järjestetty tai miten sitä käytetään, eikä kyseistä infrastruktuuria katsota osaksi digitaalisia elementtejä sisältävää tuotetta.

170. Asianmukainen huolellisuus liittyy osiin, jotka kuuluvat digitaalisia elementtejä sisältävään tuotteeseen itseensä. Erityisesti tämä koskee kolmannen osapuolen toimittamia integroituja ohjelmisto- tai laitteistokomponentteja. Valmistajien on toteutettava asianmukaiset toimenpiteet sen varmistamiseksi, etteivät tällaiset komponentit vaaranna olennaisten vaatimusten täyttymistä digitaalisia elementtejä sisältävässä tuotteessa. Tämä voidaan saavuttaa vain määrittämällä, mitä digitaalisia elementtejä sisältävä tuote edellyttää komponenteiltaan kyberturvallisuustavoitteidensa saavuttamiseksi, ja varmistamalla riskiperusteisesti, että kyseiset komponentit vastaavat tuotteen tarpeita, kuten myös johdanto-osan 34 kappaleessa todetaan.

171. Kyberturvallisuusriskien arviointinsa mukaisesti valmistajan on määritettävä vaatimukset, jotka integroidun komponentin olisi täytettävä. Jos digitaalisia elementtejä sisältävä tuote on esimerkiksi riippuvainen komponentin tarjoamista kryptografisista toiminnoista, päivitysmekanismeista tai suojatusta viestinnästä, valmistajan on asianmukaista huolellisuutta noudattaessaan tunnistettava nämä tarpeet ja varmistettava, että komponentti vastaa niitä. Tätä tarkoitusta varten näyttönä voidaan käyttää komponentin valmistajalta saatuja asiakirjoja, kuten teknisiä eritelmiä, turvallisuusasiakirjoja tai asiaankuuluvia vaatimustenmukaisuusasiakirjoja tai varmennusdokumentaatiota. Valmistaja voi tarvittaessa myös tehdä testejä varmistaakseen, että kyseiset komponentit toteuttavat asiaankuuluvat toiminnot asianmukaisesti. Vaikka asianmukainen huolellisuus on erillinen oikeudellinen velvoite, se tukee ja vahvistaa valmistajan kykyä osoittaa, että digitaalisia elementtejä sisältävä tuote on kokonaisuutena olennaisten vaatimusten mukainen.

172. Arvioitaessa digitaalisia elementtejä sisältävään tuotteeseen kokonaisuutena kohdistuvia riskejä kyberturvallisuusriskien arvioinnissa on otettava huomioon tuotteen ulkopuoliset elementit, kuten ympäristöön liittyvät elementit, ulkoinen infrastruktuuri, muut järjestelmät tai verkot, ja niihin on tarvittaessa puututtava tuotetasolla toteutettavilla toimenpiteillä sen varmistamiseksi, että digitaalisia elementtejä sisältävä tuote on olennaisten vaatimusten mukainen. Digitaalisia elementtejä sisältävään tuotteeseen fyysisesti tai loogisesti integroidut mutta kolmannelta osapuolelta hankitut komponentit on myös otettava huomioon riskien arvioinnissa. Vaatimustenmukaisuuden kannalta valmistajan olisi kuitenkin pidettävä niitä ulkopuolelta toimitettuina komponentteina, joiden ominaisuudet varmistetaan integroinnin yhteydessä asianmukaista huolellisuutta noudattaen, koska valmistaja ei välttämättä ole suunnitellut tai kehittänyt niitä uudelleen.

173. Samaa logiikkaa sovelletaan komponenttien kehittämiseen ja integrointiin. Jos valmistaja kehittää toimintoja itse, sen on pantava olennaiset vaatimukset suoraan täytäntöön. Jos valmistaja integroi muiden kehittämiä komponentteja, sen on asianmukaista huolellisuutta noudattaen varmistettava, että kyseisiä komponentteja voidaan käyttää tavalla, joka mahdollistaa sen, että digitaalisia elementtejä sisältävä tuote on kokonaisuutena vaatimusten mukainen. Molemmissa tapauksissa tavoitteena on, että digitaalisia elementtejä sisältävä tuote saavuttaa markkinoille saatettuna kyberkestävyyssäädöksessä edellytetyn asianmukaisen kyberturvallisuuden tason ottaen huomioon kyberturvallisuusriskien arvioinnissa tunnistetut riskit.

7.4 **Riskien arviointien ja vaatimustenmukaisuusasiakirjojen uudelleenkäyttö digitaalisia elementtejä sisältävien tuoteperheiden osalta**

174. Valmistajat voivat saattaa markkinoille toisiaan muistuttavia digitaalisia elementtejä sisältäviä tuotteita, esimerkiksi saman tuoteperheen eri variantteja, malleja tai kokoonpanoja. Jos tällaisilla digitaalisia elementtejä sisältävillä tuotteilla on sama arkkitehtuuri, turvallisuuden kannalta merkityksellinen suunnittelu ja käyttötarkoitus ja niihin kohdistuvat samat kyberturvallisuusriskit, kyberkestävyyssäädöksessä ei edellytetä, että valmistajat pitävät kutakin varianttia täysin erillisenä digitaalisia elementtejä sisältävänä tuotteena riskien arviointia ja vaatimustenmukaisuuden arviointia varten.

175. Tällaisissa tapauksissa valmistajat voivat, edellyttäen että kaikki kyseiset variantit on otettu asianmukaisesti huomioon asiaankuuluvien riskien ja olennaisten vaatimusten osalta, tukeutua i) yhteen kyberturvallisuusriskien arviointiin, joka on suoritettu kyberkestävyyssäädöksen 13 artiklan 2 kohdan mukaisesti, ii) yhteen teknisten asiakirjojen kokonaisuuteen ja iii) yhteen vaatimustenmukaisuuden arviointimenettelyyn. Tämä mahdollistaa myös yhden EU-vaatimustenmukaisuusvakuutuksen antamisen digitaalisia elementtejä sisältävien tuotteiden ryhmälle, kunhan vakuutuksessa yksilöidään selkeästi ne tuotevariantit, joihin sitä sovelletaan.

176. Ratkaisevaa on se, ovatko varianttien väliset erot merkityksellisiä kyberturvallisuuden kannalta. Sellaiset erot, jotka eivät vaikuta digitaalisia elementtejä sisältävän tuotteen kyberturvallisuusominaisuuksiin, kuten erot värissä, muototekijässä, muistin koossa tai muissa turvallisuuden kannalta merkityksettömissä ominaisuuksissa, eivät edellytä erillisiä riskien arviointeja tai vaatimustenmukaisuuden arviointeja. Sitä vastoin variantit voivat joissakin tapauksissa poiketa toisistaan tavoilla, jotka vaikuttavat olennaisten vaatimusten täytäntöönpanoon, esimerkiksi erilaisten viestintärajapintojen, ohjelmistopinojen, päivitysmekanismien tai etäyhteyksien vuoksi. Tällaisissa tapauksissa nämä erot on otettava huomioon riskien arvioinnissa ja tarvittaessa vaatimustenmukaisuuden arvioinnissa ja teknisissä asiakirjoissa.

177. Valmistajat vastaavat edelleen sen varmistamisesta, että riskien arviointi ja siihen liittyvät asiakirjat kuvaavat täsmällisesti niitä digitaalisia elementtejä sisältäviä tuotteita, jotka on saatettu markkinoille. Jos uusi variantti aiheuttaa uusia kyberturvallisuusriskejä tai muuttaa tapaa, jolla olennaiset vaatimukset pannaan täytäntöön, olemassa oleva riskien arviointi ja olemassa olevat vaatimustenmukaisuusasiakirjat on päivitettävä vastaavasti. Yhteen vaatimustenmukaisuuden arviointiin voidaan tukeutua vain siltä osin kuin digitaalisia elementtejä sisältävien tuotteiden kyberturvallisuusominaisuuksissa ei ole eroja.

8. **DATAN ETÄKÄSITTELY**

178. Kyberkestävyyssäädöksen 3 artiklan 1 alakohdassa määritellään, että digitaalisia elementtejä sisältävällä tuotteella tarkoitetaan ”ohjelmisto- tai laitteistotuotetta ja sen ratkaisuja datan etäkäsittelystä, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit”. Tämän perusteella valmistajan on tarkasteltava digitaalisia elementtejä sisältävää tuotetta kokonaisuutena, mukaan lukien sen datan etäkäsittelyratkaisut. Esimerkiksi osoitettaessa, että digitaalisia elementtejä sisältävä tuote on liitteessä I vahvistettujen olennaisten vaatimusten mukainen, datan etäkäsittelyratkaisut on otettava huomioon jo riskien arvioinnista lähtien (13 artiklan 2 kohta). Sama pätee elinkaaren aikaisiin velvoitteisiin, kuten aktiivisesti hyödynnetyistä haavoittuvuuksista ja vakavista poikkeamista ilmoittamiseen (14 artikla).

179. Näiden ohjeiden tarkoituksena on antaa valmistajille lisätukea sen selvittämisessä, sisältyykö niiden digitaalisia elementtejä sisältävään tuotteeseen kyberkestävyyssäädöksessä määriteltyjä datan etäkäsittelyratkaisuja ja miten niiden on täytettävä vaatimustenmukaisuutta koskevat velvoitteensa tältä osin. Kyberkestävyyssäädöksessä vahvistettujen määritelmien ja johdanto-osan kappaleiden alustavan analyysin jälkeen näissä ohjeissa esitetään kysymyksiä, joiden avulla valmistajat voivat selvittää, sisältyykö niiden digitaalisia elementtejä sisältävään tuotteeseen datan etäkäsittelyratkaisuja (ks. jakso *8.1 Mitä pidetään digitaalisia elementtejä sisältävän tuotteen datan etäkäsittelyratkaisuna?*). Tämän jälkeen ohjeissa käsitellään yksityiskohtaisemmin datan etäkäsittelyratkaisujen teknisiä vaikutuksia ja sitä, miten kyberkestävyyssäädöksen noudattamista arvioidaan (ks. jakso *8.2 Datan etäkäsittelyratkaisujen ja kolmannen osapuolen ratkaisuihin tukeutumisen käytännön vaikutukset ja tekniset vaikutukset*).

180. Kyberkestävyyssäädöksen 3 artiklan 2 alakohdassa määritellään, että datan etäkäsittelyllä tarkoitetaan ”etäältä tapahtuvaa datan käsittelyä, jota varten on suunniteltu ja kehitetty ohjelmisto valmistajan toimesta tai valmistajan vastuulla ja jota ilman digitaalisia elementtejä sisältävä tuote ei kykenisi suorittamaan jotakin toimintoaan”. Datan etäkäsittelyratkaisuilla tarkoitetaan näin ollen etäältä tapahtuvan datan käsittelyn ohjelmistoelementtejä. Ohjelmistolla tarkoitetaan 3 artiklan 4 alakohdan mukaan ”sitä sähköisen tietojärjestelmän osaa, joka koostuu tietokonekoodista”. Datan etäkäsittelyratkaisuja koskevalla määritelmällä ei kuitenkaan ole tarkoitus lukea osaksi digitaalisia elementtejä sisältävää tuotetta laitteistoa, johon datan etäkäsittely voi tukeutua.

181. Johdanto-osan 11 ja 12 kappaleissa selitetään tarkemmin, miten tätä käsitettä olisi tulkittava. Johdanto-osan 11 kappaleessa selvennetään, että datan etäkäsittelyratkaisujen sisällyttämisellä soveltamisalaan pyritään siihen, että ”valmistajat suojaavat tällaiset tuotteet asianmukaisesti kokonaisuudessaan riippumatta siitä, suoritetaanko tietojen käsittely ja tallentaminen paikallisesti käyttäjän laitteella vai suorittaako valmistaja sen etäältä” Siinä todetaan myös seuraavaa: ”Tämän asetuksen soveltamisalaan kuuluvia datan etäkäsittelyratkaisuja koskevat vaatimukset eivät sen vuoksi edellytä teknisiä, operatiivisia tai organisatorisia toimenpiteitä, joiden tarkoituksena on hallinnoida valmistajan koko verkko- ja tietojärjestelmien tietoturvaan kohdistuvia riskejä.”

182. Näin ollen johdanto-osan 11 kappaleesta käy ilmi, ettei kyberkestävyyssäädöksen vaatimuksia ole tarkoitus soveltaa organisaation koko tietotekniseen infrastruktuuriin vaan ainoastaan ohjelmistokomponentteihin, jotka mahdollistavat datankäsittelyratkaisun suorittamisen. Esimerkiksi valmistajan omiin henkilöstöhallintoon, palkanlaskentaan, asiakkuudenhallintaan, jatkuvaluonteisen integroinnin ja toimituksen (continuous integration/continuous delivery, CI/CD) putkiin tai tietoturvapäivitysten reunapalvelimiin jakeluun liittyviä sisäisiä järjestelmiä ei pitäisi katsoa datan etäkäsittelyratkaisuiksi. Samoin auditointi- ja testaustoimintaan, kuten tunkeutumistestaukseen, uhkien etsintään ja red teaming -testaukseen, liittyvät järjestelmät eivät kuulu kyberkestävyyssäädöksessä tarkoitetun digitaalisia elementtejä sisältävän tuotteen piiriin. On tärkeää huomata, että vaikka digitaalisia elementtejä sisältävän tuotteen tietoturvaan liittyvien tehokkaiden testien ja arviointien tekeminen säännöllisesti on kyberkestävyyssäädöksen liitteessä I olevan II osan 3 kohdassa vahvistettu olennainen vaatimus, tämä ei tarkoita, että tällaisia toimia olisi pidettävä datan etäkäsittelyratkaisuina digitaalisia elementtejä sisältävälle tuotteelle.

183. Johdanto-osan 12 kappaleessa keskitytään pilvipalveluihin ja selvennetään, millaisissa olosuhteissa pilvipalveluja voidaan pitää datan etäkäsittelyratkaisuina. Kappaleen lopuksi muistutetaan, että pilvipalvelut ja pilvipalvelumallit kuuluvat direktiivin (EU) 2022/2555 (NIS 2 -direktiivi) ([28]) soveltamisalaan. Kyseisessä direktiivissä vahvistetaan kyberturvallisuusriskien hallintaa koskevat vaatimukset pilvipalvelujen tarjoajille. Näitä vaatimuksia täsmennetään tarkemmin komission täytäntöönpanoasetuksessa (EU) 2024/2690 ([29]).

8.1 **Mitä pidetään digitaalisia elementtejä sisältävän tuotteen datan etäkäsittelyratkaisuna?**

184. Näin ollen 3 artiklan 2 alakohdassa vahvistettu datan etäkäsittelyn määritelmä perustuu kolmeen seikkaan: i) tapahtuuko datan käsittely ”etäältä”, ii) estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan ja iii) onko ohjelmisto suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla. Seuraavissa kolmessa alajaksossa käsitellään kutakin näistä seikoista yksityiskohtaisemmin.

([28]) Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS 2 -direktiivi) (EUVL L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Komission täytäntöönpanoasetus (EU) 2024/2690, annettu 17 päivänä lokakuuta 2024, direktiivin (EU) 2022/2555 soveltamista koskevista säännöistä DNS-palveluntarjoajia, aluetunnusrekistereitä, pilvipalvelujen tarjoajia, datakeskuspalvelujen tarjoajia, sisällönjakeluverkkojen tarjoajia, hallintapalvelun tarjoajia, tietoturvapalveluntarjoajia, verkossa toimivien markkinapaikkojen tarjoajia, verkossa toimivien hakukoneiden tarjoajia, verkkoyhteisöalustojen tarjoajia ja luottamuspalvelun tarjoajia varten siltä osin kuin on kyse kyberturvallisuusriskien hallintatoimenpiteiden teknisistä ja menetelmiin liittyvistä vaatimuksista ja sellaisten tapausten täsmentämisestä, joissa poikkeama katsotaan merkittäväksi (EUVL L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1 *Ilmaus ”etäältä”*

185. Kyberkestävyyssäädöksen 3 artiklan 2 alakohdassa tarkoitettu ilmaus ”etäältä” on merkityksellinen, mutta se ei yksin riitä sen määrittämiseen, sisältyykö digitaalisia elementtejä sisältävään tuotteeseen datan etäkäsittelyratkaisuja. Lisäksi tähän käsitteeseen mahdollisesti kuuluvien ratkaisujen moninaisuuden vuoksi ilmaukselle ”etäältä” ei ole mahdollista antaa tyhjentävää määritelmää. Valmistajan on tehtävä tapauskohtainen arviointi.

186. Kyberkestävyyssäädöksen johdanto-osan 11 kappaleessa mainitaan valmistajan etäältä suorittama tietojen käsittely ja tallentaminen erotuksena tietojen käsittelystä ja tallentamisesta paikallisesti käyttäjän laitteella. Datan etäkäsittely tapahtuu tyypillisesti digitaalisia elementtejä sisältävän tuotteen käyttäjäympäristön ulkopuolella tai ammattikäyttäjän tapauksessa organisaation toimintaympäristön ulkopuolella. Tämä ei kuitenkaan estä sitä, että käsittely voi tapahtua myös lähellä laitetta (”verkon reunalla”). Datan siirto voi tapahtua langallisesti (esimerkiksi Ethernet-kaapelin välityksellä) tai langattomasti (esimerkiksi Wi-Fi- tai Bluetooth-yhteydellä). Pilvilaskenta, reunalaskenta mukaan lukien, on tyypillinen esimerkki ”etäältä” tapahtuvasta datan käsittelystä. Esimerkiksi kun käyttäjä käyttää mobiilisovelluksen kautta pilvipohjaista toimintoa, osa datan käsittelystä tapahtuu pilvessä käyttäjäympäristön ulkopuolella.

187. On tärkeää huomata, että datan etäkäsittelyratkaisuja ei välttämättä käytetä kolmannen osapuolen pilvi-infrastruktuurissa. Myös valmistajan tiloissa sijaitsevilla paikallisilla palvelimilla ajettava datan etäkäsittely voi olla datan etäkäsittelyratkaisu. Toisin sanoen valmistajan omissa tiloissa ja yksityisessä pilvessä ajettava ratkaisu voi yhtä lailla olla datan etäkäsittelyratkaisu kuin julkisessa pilvessä ja valmistajan tilojen ulkopuolella ajettava ratkaisu.

188. Jäljempänä jaksoissa *8.1.2* ja *8.2* esitetään kaksi ratkaisevaa ja kumulatiivista kysymystä, joiden perusteella määritetään, kuuluuko datan käsittely kyberkestävyyssäädöksen soveltamisalaan datan etäkäsittelyratkaisuna. Jos molempiin kysymyksiin vastataan myöntävästi, datan etäkäsittelyä pidetään datan etäkäsittelyratkaisuna.

8.1.2 *Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan?*

189. Kuten 3 artiklan 2 alakohdassa vahvistetussa datan etäkäsittelyn määritelmässä todetaan, jotta etäältä tapahtuvaa datan käsittelyä voidaan pitää datan etäkäsittelyratkaisuna, sen puuttumisen olisi estettävä digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan. Tässä määritelmässä käytetty toiminnon käsite ei rajoitu digitaalisia elementtejä sisältävän tuotteen ”ydintoimintoon” tai ”käyttötarkoitukseen”, sillä kyberkestävyyssäädöksessä ei aseteta tällaista rajoitusta. Kyberkestävyyssäädöksen soveltamisalaan kuuluvat sekä toiminnot, jotka käyttäjien näkökulmasta toteuttavat suoraan digitaalisia elementtejä sisältävän tuotteen käyttötarkoitusta, että toiminnot, jotka tukevat tuotteen yleistä suorituskykyä.

190. Esimerkkejä toiminnoista, joissa datan käsittely voi tapahtua etäältä ja joissa tällaisen datan käsittelyn puuttuminen estäisi digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan, ovat i) komentojen lähettäminen laitteelle, ii) tiedostojen synkronointi, iii) käyttösuhteen aloittaminen, iv) konfigurointi (digitaalisia elementtejä sisältävän tuotteen personointi), v) päivitysten automaattinen jakelu, mukaan lukien ominaisuuspäivitykset ja turvallisuuspuutteiden paikkaus ja vi) identiteetin- ja pääsynhallinta.

191. Joissakin tapauksissa käyttäjä voi käyttää toimintoa sekä etänä että manuaalisesti (esimerkiksi kytkeä lampun päälle tai pois sovelluksella tai manuaalisesti). Tällaisen vaihtoehdon olemassaolo ei sulje pois sitä, että toiminnon suorittamiseen etänä liittyvää datan käsittelyä voitaisiin pitää datan etäkäsittelyratkaisuna. Tällaisen toiminnon suorittamista etänä pidetään myös osana digitaalisia elementtejä sisältävän tuotteen tarjoamia toimintoja.

192. Sitä vastoin, jos tietyn datan käsittelyn puuttuminen ei estä digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan, tällaista käsittelyä ei pidetä kyberkestävyyssäädöksessä tarkoitettuna datan etäkäsittelyratkaisuna. Tähän kuuluu esimerkiksi yksinomaan tilastollisiin tarkoituksiin tai tulevaa tuotekehitystä varten kerättyjen kaukomittaustietojen etäanalyysi.

193. Vaikka datan käsittely ei tukisi digitaalisia elementtejä sisältävän tuotteen toimintoa, valmistajien voi kuitenkin olla tarpeen arvioida osana kyberturvallisuusriskien arviointia, aiheuttavatko kyseiset etäkomponentit riskejä digitaalisia elementtejä sisältävälle tuotteelle (esimerkiksi tuotteen toimintaympäristön perusteella), ja lieventää tällaisia riskejä vastaavasti (esimerkiksi tuotetasolla toteutettavilla lieventämistoimenpiteillä).

194. Verkkosivustot ovat erityistapaus, jota on syytä selventää tarkemmin. Tätä selitetään myös jaksossa *2.1 Markkinoille saattaminen*. Verkkosivustot eivät kuulu datan etäkäsittelyratkaisujen piiriin, jos ne eivät tue digitaalisia elementtejä sisältävän tuotteen toimintoa, kuten kyberkestävyyssäädöksen johdanto-osan 11 kappaleessa selitetään. Pelkästään se, että verkkosivustolla on tietoja digitaalisia elementtejä sisältävästä tuotteesta, ei riitä siihen, että verkkosivuston katsottaisiin kuuluvan datan etäkäsittelyratkaisujen piiriin, vaikka tuote ohjaisi tällaiselle verkkosivustolle. Esimerkiksi käyttäjien ohjaaminen ulkoiselle verkkosivulle, jolla annetaan käyttäjille tietoja ja ohjeita, ei ole datan etäkäsittelyratkaisu. Sen sijaan verkkosivusto voi kuulua datan etäkäsittelyratkaisujen piiriin, jos se mahdollistaa digitaalisia elementtejä sisältävän tuotteen toiminnon tai tukee sitä. Esimerkiksi todennusportaalia, joka myöntää digitaalisia elementtejä sisältävän tuotteen toiminnan edellyttämiä pääsytunnuksia tai tunnistusvälineitä, pidettäisiin datan etäkäsittelyratkaisuna (edellyttäen, että myös muut määritelmän kriteerit täyttyvät).

8.1.3 *Onko ohjelmisto suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla?*

195. Kyberkestävyyssäädöksen 3 artiklan 2 alakohdassa olevassa datan etäkäsittelyn määritelmässä täsmennetään lisäksi, että tällaista etäältä tapahtuvaa datan käsittelyä varten tarkoitetun ohjelmiston on oltava suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla. Kokonaan valmistajan sisäisesti suunnittelemaa ja kehittämää datan etäkäsittelyä pidettäisiin luonnollisesti datan etäkäsittelyratkaisuna. Sama pätee, jos valmistaja käyttää ulkoista palveluntarjoajaa ratkaisun suunnitteluun ja kehittämiseen (eli ”valmistajan vastuulla”). Ilmaisulla ”valmistajan vastuulla” viitataan valmistajalle räätälöityihin datan etäkäsittelyratkaisuihin. Kyse on tapauksista, joissa valmistaja ei pelkästään lisensoi olemassa olevaa digitaalisia elementtejä sisältävää tuotetta tai palvelua, jota palveluntarjoaja tarjoaa asiakkailleen, tai tällaisen tuotteen tai palvelun hieman muunneltuja versioita. Ilmaisu ”valmistajan vastuulla” merkitsee, että ohjelmisto rakennetaan yksinomaan valmistajan toimesta tai sen puolesta valmistajan toimittamien suunnitelmien ja eritelmien perusteella.

196. Datan etäkäsittelyratkaisujen käsitteen tulkinnassa se, kuka huolehtii ratkaisun toiminnasta, ei ole ratkaiseva tekijä, sillä kyberkestävyyssäädöksen määritelmässä viitataan ainoastaan datan etäkäsittelyratkaisun suunnitteluun ja kehittämiseen. Tämä vastaa kyberkestävyyssäädöksen lähestymistapaa, jonka mukaan vaatimukset ja velvoitteet kohdistuvat valmistajiin eivätkä digitaalisia elementtejä sisältävän tuotteen toimintaan. Jos valmistajat suunnittelevat ja kehittävät ratkaisuja, joiden toiminnasta huolehtii tämän jälkeen kolmas osapuoli, valmistajat vastaavat edelleen siitä, että niiden markkinoille saattama digitaalisia elementtejä sisältävä tuote on kyberkestävyyssäädöksen olennaisten vaatimusten mukainen.

197. On tarpeen erottaa toisistaan tapaukset, joissa ratkaisu suunnitellaan ja kehitetään valmistajan toimesta (tai valmistajan vastuulla), ja tapaukset, joissa tukeudutaan kolmannen osapuolen ratkaisuihin, joita ei ole suunniteltu eikä kehitetty valmistajan toimesta (tai valmistajan vastuulla). Esimerkkinä on hyödyllistä tarkastella yleisimpiä pilvipalvelumalleja, joissa käyttäjän hallintamahdollisuudet ovat eriasteiset ja jotka mainitaan myös kyberkestävyyssäädöksen johdanto-osan 12 kappaleessa, eli ohjelmistopalveluja (SaaS), alustapalveluja (PaaS) ja infrastruktuuripalveluja (IaaS).

198. Kolmannen osapuolen IaaS-ratkaisussa valmistaja ei hallinnoi tai valvo sen taustalla olevia fyysisiä ja virtuaalisia resursseja (kuten taustalla olevaa laitteistoa ja pilvipalveluntarjoajan virtualisointialustaa), mutta se voi tällaisia resursseja käyttäen ottaa käyttöön ja ajaa mitä tahansa ohjelmistoja, kuten käyttöjärjestelmiä ja sovelluksia. Tällainen ohjelmisto suunnitellaan ja kehitetään valmistajan toimesta tai valmistajan vastuulla, ja sitä voidaan näin ollen pitää datan etäkäsittelyratkaisuna (jos se täyttää määritelmän muut osatekijät).

199. Kolmannen osapuolen PaaS-ratkaisussa valmistaja ottaa käyttöön oman (itse kehittämänsä tai hankkimansa) sovelluksen käyttäen pilvipalveluntarjoajan tarjoamia ohjelmointikieliä ja toteuttamisympäristöjä ja integroi sovelluksen digitaalisia elementtejä sisältävään tuotteeseensa. Valmistaja hallitsee sovellusta ja mahdollisesti myös toteuttamisympäristön konfiguraatioasetuksia. Näin ollen sovellus suunnitellaan ja kehitetään valmistajan toimesta tai valmistajan vastuulla, ja sitä voidaan näin ollen pitää datan etäkäsittelyratkaisuna (jos se täyttää määritelmän muut osatekijät).

200. Kolmannen osapuolen SaaS-ratkaisussa SaaS-palveluntarjoaja tarjoaa valmistajalle täysin kehitetyn sovelluksen integroitavaksi valmistajan digitaalisia elementtejä sisältävään tuotteeseen. Valmistajalla on vain rajalliset mahdollisuudet hallita sovelluksen käyttäjäkohtaisia konfiguraatioasetuksia. Sovellusta ei näin ollen ole suunniteltu eikä kehitetty valmistajan toimesta tai valmistajan vastuulla.

201. Vaikka tietyt elementit eivät täyttäisi datan etäkäsittelyratkaisun määritelmää (esimerkiksi virtualisointialusta kolmannen osapuolen IaaS-infrastruktuurin tapauksessa, käyttöjärjestelmä kolmannen osapuolen PaaS-ratkaisun tapauksessa tai kolmannen osapuolen SaaS-sovellus), mutta ne integroidaan digitaalisia elementtejä sisältävään tuotteeseen tavalla, joka vaikuttaa sen turvallisuuteen, tällaisia ratkaisuja olisi pidettävä kolmannen osapuolen komponenttien kaltaisina. Valmistajan on tunnistettava ja arvioitava näiden elementtien integrointiin liittyvät riskit ja puututtava niihin panemalla olennaiset vaatimukset täytäntöön itse digitaalisia elementtejä sisältävässä tuotteessa. Tätä voidaan tarvittaessa tukea pilvipalveluntarjoajan jaetun vastuun mallinsa puitteissa saataville asettamilla turvatoiminnoilla, jos valmistaja käyttää tai konfiguroi näitä toimintoja tunnistettuihin riskeihin puuttumiseksi. Valmistajan odotetaan lisäksi noudattavan näiden komponenttien turvallisuuden osalta velvoitetta, joka vastaa 13 artiklan 5 kohdassa tarkoitettua asianmukaisen huolellisuuden noudattamista koskevaa velvoitetta. Tätä velvoitetta olisi noudatettava tavalla, joka on oikeassa suhteessa siihen riskiin, jonka etäratkaisu aiheuttaa digitaalisia elementtejä sisältävän tuotteen turvallisuudelle.

202. Näin ollen voidaan tiivistää seuraavasti:

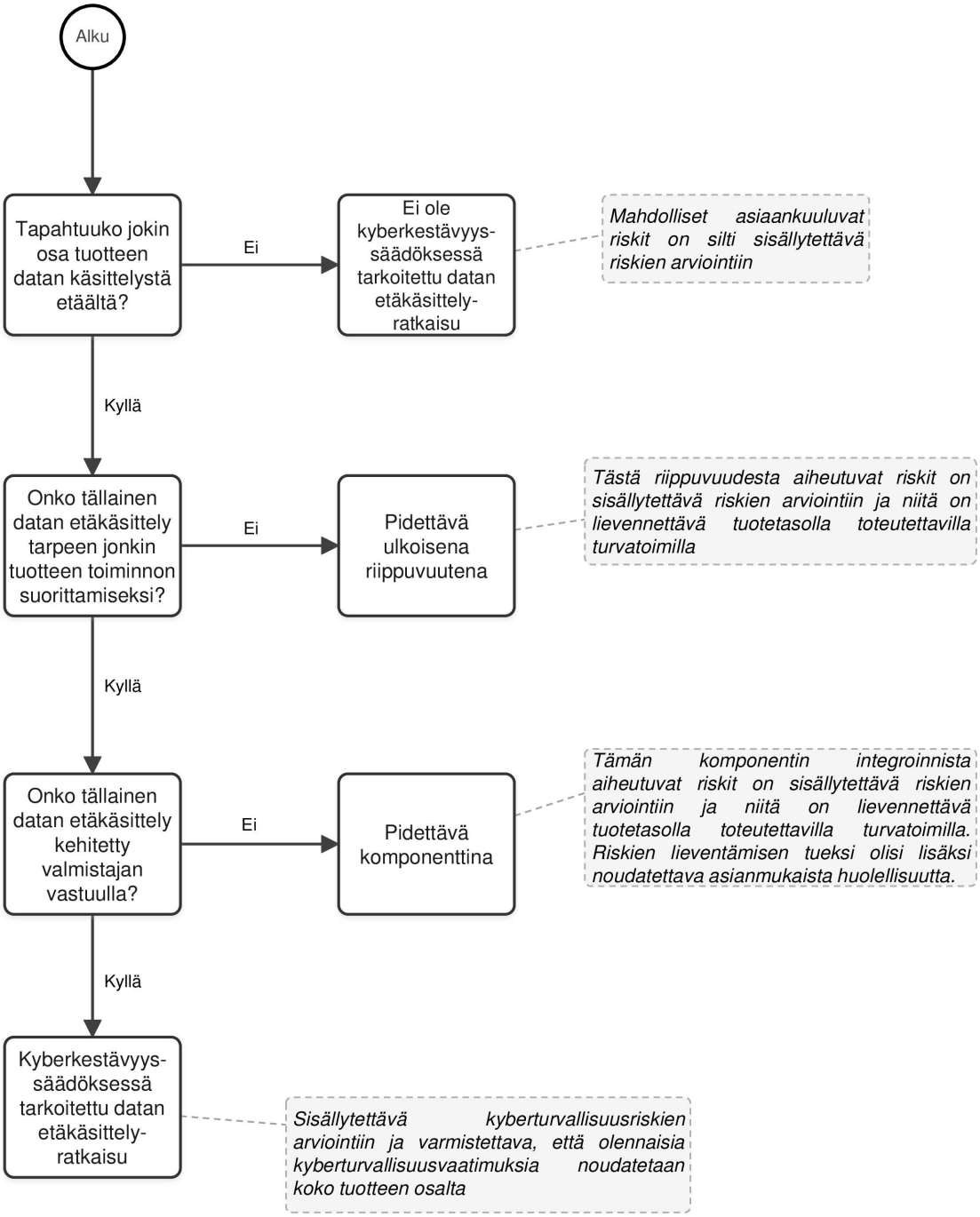
a) Jotta datan käsittelyä voidaan pitää datan etäkäsittelyratkaisuna, sekä jaksossa *8.1.2 Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan?* että jaksossa *8.1.3 Onko ohjelmisto suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla?* esitettyyn kysymykseen on vastattava myöntävästi.

b) Jos jaksossa *8.1.2 Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan?* esitettyyn kysymykseen vastataan kieltävästi, valmistajien olisi arvioitava tällaisen datan käsittelyn olemassaolosta aiheutuvat riskit osana riskien arviointia.

c) Jos jaksossa *8.1.2 Estäisikö tällaisen datan käsittelyn puuttuminen digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toimintoaan?* esitettyyn kysymykseen vastataan myöntävästi mutta jaksossa *8.1.3 Onko ohjelmisto suunniteltu ja kehitetty valmistajan toimesta tai valmistajan vastuulla?* esitettyyn kysymykseen kieltävästi, valmistajien olisi pidettävä kolmannen osapuolen ratkaisua komponenttina. Osana riskien arviointia valmistajien olisi arvioitava tällaisen ratkaisun integroinnista aiheutuvat riskit ja lievennettävä niitä vastaavasti. Lisäksi valmistajien olisi noudatettava asianmukaista huolellisuutta.

Kaavio 9

Tyylitelty vuokaavio sen määrittämiseksi, sisältääkö digitaalisia elementtejä sisältävä tuote datan etäkäsittelyratkaisuja



8.2 Datan etäkäsittelyratkaisujen ja kolmannen osapuolen ratkaisuihin tukeutumisen käytännön vaikutukset ja tekniset vaikutukset

203. Kyberkestävyyssäädöksessä noudatetaan riskiperusteista lähestymistapaa, joka vahvistetaan 13 artiklan 2 ja 3 kohdassa sekä liitteessä I olevan I osan ensimmäisessä olennaisessa vaatimuksessa, jonka mukaan ”digitaalisia elementtejä sisältävät tuotteet on suunniteltava, kehitettävä ja tuotettava siten, että niiden kyberturvallisuuden taso on oikeassa suhteessa riskeihin”. Näin ollen olisi harkittava riskiperusteisen lähestymistavan soveltamista sovellettaessa kyberkestävyyssäädöksen vaatimuksia datan etäkäsittelyratkaisuihin ja käsiteltäessä riskejä, jotka aiheutuvat digitaalisia elementtejä sisältävään tuotteeseen integroiduista kolmannen osapuolen palveluista.

204. Ensinnäkin valmistajien olisi i) ilmoitettava teknisissä asiakirjoissa, että niiden digitaalisia elementtejä sisältävä tuote sisältää datan etäkäsittelyratkaisuja tai tukeutuu kolmannen osapuolen etäratkaisuihin, ja ii) kuvattava tällaiset ratkaisut. Jos sama datan etäkäsittelyratkaisu tukee useita digitaalisia elementtejä sisältäviä tuotteita, se on ilmoitettava kunkin tuotteen teknisissä asiakirjoissa. Useita digitaalisia elementtejä sisältäviä tuotteita palvelevia datan etäkäsittelyratkaisuja koskevia asiakirjoja voidaan käyttää uudelleen tuotteen yhdestä vaatimustenmukaisuuden arvioinnista toiseen.

205. Kuten johdanto-osan 11 kappaleessa todetaan, tuotteen vaatimustenmukaisuuden arvioinnin piiriin kuuluvat datan etäkäsittelyratkaisut eli ne, jotka ovat osa digitaalisia elementtejä sisältävää tuotetta, olisi rajattava niihin ohjelmistomoduuleihin, jotka vastaavat digitaalisia elementtejä sisältävän tuotteen toiminnoista, sekä rajapintoihin, joita kyseiset moduulit käyttävät ulkoisten palvelujen kanssa. Muita taustajärjestelmiä, joissa suoritetaan jatkokäsittelyä ja joiden kanssa digitaalisia elementtejä sisältävä tuote ei ole suorassa vuorovaikutuksessa, ei pidetä datan etäkäsittelyratkaisuina.

206. Tällaiset taustajärjestelmät ovat kuitenkin edelleen ulkoisia riippuvuuksia, jotka on arvioitava osana kyberturvallisuusriskien arviointia ja joihin liittyviä riskejä on lievennettävä tuotetasolla toteutettavilla toimenpiteillä. Valmistajan suorittamassa riskien arvioinnissa olisi otettava huomioon i) datan etäkäsittelyratkaisuihin liittyvät riskit; ii) kolmannen osapuolen etäratkaisuihin, joita pidetään kolmannen osapuolen komponenttien kaltaisina, tukeutumiseen liittyvät riskit; ja iii) tuotteen ympäristöön (esimerkiksi taustalla oleva laitteisto) liittyvät riskit. Valmistajien olisi toteutettava itse digitaalisia elementtejä sisältävässä tuotteessa turvatoimia näiden riskien lieventämiseksi.

207. Lisäksi valmistajan arvioinnin tueksi voidaan vaatimustenmukaisuuden arvioinnin ja/tai kolmansien osapuolten etäpalveluihin liittyvien asianmukaista huolellisuutta koskevien velvoitteiden täyttämisen yhteydessä käyttää uudelleen muun muassa seuraavia varmennusaineistoja:

a) näyttö komission täytäntöönpanoasetuksen (EU) 2024/2690 mukaisten velvoitteiden täyttämisestä

b) näyttö asetuksen (EU) 2022/2554 (DORA-asetus) mukaisten velvoitteiden täyttämisestä

c) eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän nojalla saatu vaatimustenmukaisuusilmoitus tai sertifikaatti (järjestelmä on hyväksytty asetuksen (EU) 2019/881 eli kyberturvallisuusasetuksen nojalla)

d) näyttö standardin ISO/IEC 27017:2015 tai ISO/IEC 27001:2022 mukaisuudesta.

208. Ollessaan vuorovaikutuksessa etäpalvelujen tarjoajina olevien kolmansien osapuolten kanssa valmistajien on toteutettava riskien arviointinsa perusteella asianmukaisimmat turvatoimet (tarvittaessa palveluntarjoajan jaetun vastuun mallin tukemina). Näihin lieventämistoimenpiteisiin olisi sisällyttävä digitaalisia elementtejä sisältäviä tuotteita koskevia turvatoimia sekä palveluntarjoajina olevien kolmansien osapuolten itsensä tarjoamien turvatoimien varmistaminen (asianmukainen huolellisuus). Yksi keino tällaisten riskien lieventämiseen voi olla turvallisuutta koskevien takeiden sisällyttäminen palveluntarjoajina olevien kolmansien osapuolten kanssa tehtäviin palvelutasosopimuksiin, mukaan lukien takeet siitä, että palveluntarjoajat käsittelevät haavoittuvuuksia asianmukaisesti. Etäpalvelujen tarjoajina olevien kolmansien osapuolten tarjoamiin ratkaisuihin tehtävää huomattavaa muutosta ei pitäisi pitää digitaalisia elementtejä sisältävän tuotteen merkittävänä muutoksena, koska kyseiset elementit eivät ole valmistajan vastuulla. Osana asianmukaista huolellisuutta koskevia velvoitteitaan ja lieventääkseen asianmukaisesti palveluntarjoajina olevien kolmansien osapuolten käytöstä aiheutuvia riskejä valmistajia kannustetaan varmistamaan, että niiden käyttämät pilvipalvelujen tarjoajina olevat kolmannet osapuolet pitävät ne asianmukaisesti ajan tasalla ratkaisuihinsa tekemistään muutoksista. Tällaisten tietojen perusteella valmistajien voi olla tarpeen tarkistaa riskien arviointiaan. Päivitetyssä riskien arvioinnissa olisi otettava huomioon, tarjoavatko palveluntarjoajina olevat kolmannet osapuolet edelleen riittävät takeet kyberturvallisuuden osalta ja ovatko tuotetasolla toteutettavat turvatoimet edelleen asianmukaisia. Joissakin tapauksissa valmistajien voi olla tarpeen muuttaa tällaisia turvatoimia tai vaihtaa palveluntarjoajina olevia kolmansia osapuolia.

8.3 **Datan etäkäsittelyratkaisujen käyttötapaukset**

Jotta valmistajille voidaan antaa käytännön lisäohjeita, tässä jaksossa esitetään joukko kuvitteellisia käyttötapauksia, joissa kuvataan tyypillisiä datan etäkäsittelyyn tukeutuvia digitaalisia elementtejä sisältäviä tuotteita ja havainnollistetaan, voidaanko tällaista käsittelyä pitää kyberkestävyyssäädöksessä tarkoitettuna datan etäkäsittelyratkaisuna.

8.3.1 *Mobiilipankkisovellus*

Finanssialan yhteisö tuo markkinoille mobiilipankkisovelluksen. Sovelluksen taustajärjestelmät tukevat muun muassa todennusta, valtuutusta, tilinhallintaa ja maksuja. Finanssialan yhteisö toteuttaa sovelluksen toiminnot hybridistrategialla, joka perustuu sen omaan sisäiseen infrastruktuuriin sekä kolmannen osapuolen etäratkaisuihin. Näihin kuuluvat seuraavat:

Finanssialan yhteisön kehittämä itseisännöity infrastruktuuri:

— Asiakas avaa mobiilipankkisovelluksen, ja hänet todennetaan pankkitoiminnan rajapinnan kautta. Se on finanssialan yhteisön kehittämä itseisännöity ratkaisu, joka vastaanottaa sovelluksen pyynnöt ja lähettää takaisin tarvittavat vastaukset. Pankkitoiminnan rajapinta varmistaa asiakkaan henkilöllisyyden tekemällä kyselyn tilinhallintajärjestelmään ja myöntää sovellukselle pääsyn.

— Asiakas käynnistää siirron sovelluksessa. Sovellus välittää ohjeen pankkitoiminnan rajapintaan, joka lähettää vastaavan pyynnön tilikirjajärjestelmään.

— Tapahtuma kirjautuu tilinhallintajärjestelmään ja tilikirjajärjestelmään, jotka ovat molemmat itseisännöityjä mutta loogisesti eroteltuja pankkitoiminnan rajapinnasta.

— Tilikirjajärjestelmä palauttaa tapahtuman tilan pankkitoiminnan rajapintaan, joka esittää tuloksen asiakkaalle.

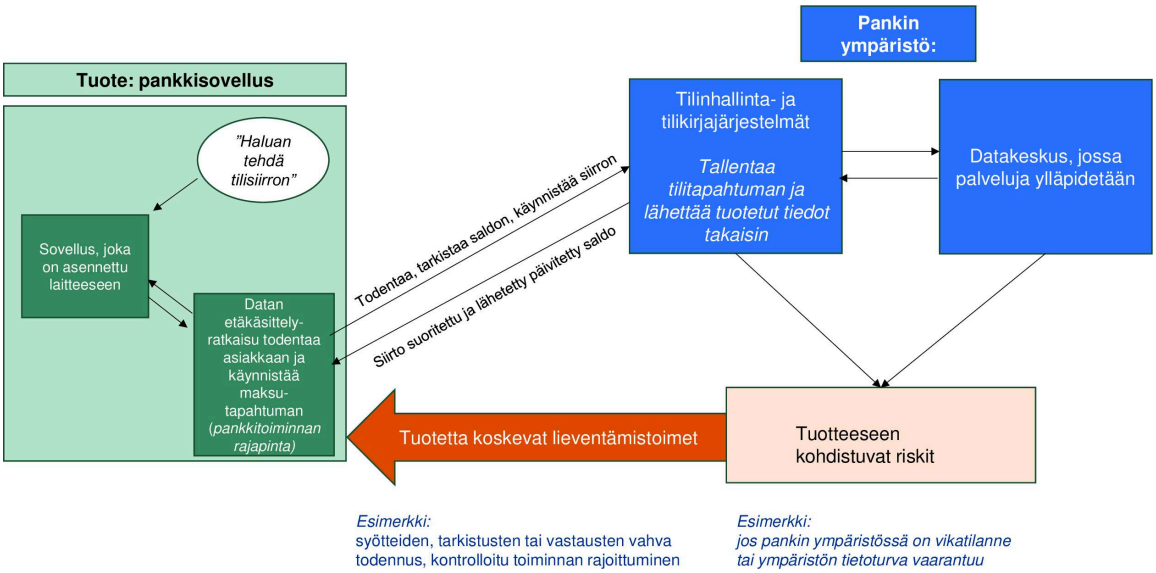
Vaikutukset datan etäkäsittelyratkaisun kannalta:

— Pankkitoiminnan rajapinta on välttämätön sovelluksen toiminnalle eli asiakkaan todentamiselle, asiakkaan ohjeiden lähettämiselle, maksu- ja rahansiirto-ohjeet mukaan lukien, ja tuloksena olevan tilan palauttamiselle. Pankkitoiminnan rajapinta on suunniteltu ja kehitetty valmistajan vastuulla. Koska vastaus molempiin aiemmissa jaksoissa esitettyihin kysymyksiin on myönteinen, pankkitoiminnan rajapintaa on pidettävä datan etäkäsittelyratkaisuna. Se on siis sisällytettävä kyberturvallisuusriskien arviointiin ja digitaalisia elementtejä sisältäviä tuotteita koskevien olennaisten vaatimusten täytäntöönpanoon kokonaisuudessaan. Lähetetyn ohjeen myöhempi käsittely, varsinkin tapahtuman kirjaaminen tilinhallinta- ja tilikirjajärjestelmiin sekä maksu ja selvitys, suoritetaan järjestelmissä, joiden kanssa sovellus ei ole suoraan vuorovaikutuksessa eikä sillä perusteella muodosta datan etäkäsittelyratkaisua.

— Tilinhallintajärjestelmä ja tilikirjajärjestelmä eivät muodosta datan etäkäsittelyratkaisua mobiilipankkisovellukselle. Sovellus ei ole suoraan vuorovaikutuksessa niiden kanssa (vaan pankkitoiminnan rajapinnan kanssa, jonka toiminta puolestaan tukeutuu kyseisiin järjestelmiin). Vaikka järjestelmien saatavuus voi olla tarpeen toiminnon suorittamiseksi, kyberkestävyyssäädös kattaa vain ne järjestelmän osat, jotka ovat suoraan vuorovaikutuksessa digitaalisia elementtejä sisältävän tuotteen kanssa. Näin ollen ne eivät täytä datan etäkäsittelyratkaisun määritelmää kyberkestävyyssäädöksen puitteissa. Nämä järjestelmät ovat kuitenkin edelleen ulkoisia riippuvuuksia, jotka voivat aiheuttaa merkittäviä kyberturvallisuusriskejä digitaalisia elementtejä sisältävälle tuotteelle. Esimerkiksi tilikirjajärjestelmän turvallisuuden vaarantuminen voi johtaa siihen, että hyökkääjä pääsee vaikuttamaan tapahtuman tuloksiin, jotka näkyvät vuorostaan sovelluksessa. Valmistajan on siksi kartoitettava ja arvioitava nämä riskit osana kyberturvallisuusriskien arviointia ja pyrittävä vähentämään niitä tuotekohtaisilla toimenpiteillä, kuten taustajärjestelmien rajapintojen vahvalla todentamisella, tapahtumatietojen eheyden suojaamisella, suojatuilla viestintäkanavilla ja sovelluksen vastaanottamien vastausten todentamisella.

Kaavio 10

Tyylitelty esitys datan etäkäsittelyratkaisuun perustuvasta pankkisovelluksesta



Kolmannen osapuolen ohjelmistopalvelu asiakastukea varten:

— Finanssialan yhteisö integroi sovellukseensa kolmannen osapuolen kehittämän ja ylläpitämän chat-asiakastuen. Kolmannen osapuolen palveluntarjoaja on kirjoittanut palvelinkoodin chat-toimintoa varten, rakentanut käyttöliittymän ja hallinnoi infrastruktuuria, jossa chat-palvelu otetaan käyttöön (eli kyseessä on SaaS-malli).

— Kun asiakas tekee tukipyynnön, sovellus yhdistää asiakkaan kolmannen osapuolen palveluun, jossa chat-istunto järjestetään ja viestivirta käsitellään, eikä tarjoa kolmannelle osapuolelle pääsyä itse pankkijärjestelmiin.

Vaikutukset datan etäkäsittelyratkaisun kannalta:

— Chat-asiakastukiratkaisu on välttämätön, jotta digitaalisia elementtejä sisältävä tuote voi suorittaa yhden toiminnoistaan, mutta se ei ole finanssialan yhteisön suunnittelema tai kehittämä eikä sen vastuulla; näin ollen se ei ole datan etäkäsittelyratkaisu. Sitä olisi kuitenkin kohdeltava kolmannen osapuolen komponenttina. Tähän kolmannen osapuolen palveluun tukeutuminen voi aiheuttaa pankkisovellukselle kyberturvallisuusriskejä, esimerkiksi jos hyökkääjä käyttää chat-kanavaa tekeytyäkseen pankiksi tai toimittaakseen käyttäjille haitallista sisältöä. Finanssialan yhteisön on otettava nämä riskit huomioon kyberturvallisuusriskien arvioinnissa ja vähennettävä niitä tuotetason toimenpiteillä, kuten eristämällä chat-toiminto itse pankkitoiminnoista, valvomalla tietovirtoja ja validoimalla sisältöä. Ohjelmistopalvelun osalta olisi myös noudatettava asianmukaista huolellisuutta.

8.3.2 *Älytermostaatti*

Älytermostaatin avulla käyttäjä voi säätää kodin huonelämpötilaa mobiilisovelluksesta. Mobiilisovellus ja älytermostaatti hyödyntävät datan etäkäsittelyä tietojen vaihtamiseen (esimerkiksi lämpötilan nostamista koskeva pyyntö) ja tietojen tallentamiseen (esimerkiksi käyttäjän asetukset). Nämä toiminnot on kehitetty ja suunniteltu valmistajan vastuulla, mutta ne toimivat kolmannen osapuolen tarjoamassa fyysisessä ja virtuaalisessa infrastruktuurissa (eli infrastruktuuripalvelussa).

Koska älytermostaatti ei pystyisi suorittamaan älytoimintojaan ilman tätä datan etäkäsittelyä, sen puuttuminen estäisi digitaalisia elementtejä sisältävää tuotetta suorittamasta yhtä tai useampaa toimintoaan. Lisäksi ohjelmisto on kehitetty ja suunniteltu älytermostaatin valmistajan vastuulla. Näin ollen tämä datan etäkäsittely katsotaan kyberkestävyyssäädöksessä määritellyksi datan etäkäsittelyratkaisuksi.

Kyberkestävyyssäädöksen noudattamiseksi älytermostaatin valmistajan on dokumentoitava digitaalisia elementtejä sisältävän tuotteen teknisiin asiakirjoihin datan etäkäsittelyratkaisu sekä tukeutuminen kolmannen osapuolen infrastruktuuripalveluun, mukaan lukien sopimuksen alaisen palvelun yksityiskohdat. Valmistajan on otettava nämä tekijät huomioon riskinarvioinnissa, joka kattaa digitaalisia elementtejä sisältävän tuotteen käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön. Valmistaja panee täytäntöön kyberkestävyyssäädöksen olennaiset vaatimukset datan etäkäsittelyratkaisuun liittyvien riskien perusteella. Kolmannen osapuolen infrastruktuuripalvelun osalta valmistajan on varmistettava, että kolmannen osapuolen tarjoamat turvallisuustoimenpiteet ovat asianmukaisia ja/tai toteutettava infrastruktuuriin liittyviä asianmukaisia toimia. Ensiksi mainitun osalta valmistaja voisi esimerkiksi pyytää näyttöä siitä, että NIS 2 -direktiivin velvoitteet on täytetty.

8.3.3 *Sähköinen lukulaite*

Sähköisen lukulaitteen ohjelmiston valmistaja käyttää kolmannen osapuolen SaaS-tallennuspalvelua (software as a service, etäsovelluspalvelu), johon asiakkaiden ostamat e-kirjat tallennetaan ja jossa ne ovat heidän käytettävissään. Tämän tallennuspalvelun puuttuminen estäisi digitaalisia elementtejä sisältävää tuotetta suorittamasta yhtä toiminnoistaan, mutta kolmannen osapuolen SaaS-tallennuspalvelu ei ole valmistajan kehittämä eikä sitä ole kehitetty valmistajan vastuulla SaaS-tallennuspalvelun tarjoaja toimittaa sen asiakkaan saataville kaikissa käyttötapauksissa.

SaaS-tallennuspalvelu ei täytä datan etäkäyttöratkaisun määritelmää. Sähköisen lukulaitteen valmistaja käyttää kuitenkin kyseistä ulkoista palvelua digitaalisia elementtejä sisältävän tuotteensa toiminnassa, ja siksi sen on otettava siihen liittyvät riskit huomioon kyberturvallisuusriskien arvioinnissa. Sähköisen lukulaitteen valmistajan tulee kohdella SaaS-palvelua komponenttina. Valmistajan on toteutettava asianmukaiset tuotetason turvallisuustoimenpiteet, kuten suojattu todennus, salaus ja tallennuspalvelun kanssa tapahtuvan tietoliikenteen eheyden suojaaminen. Asianmukainen huolellisuus SaaS-palveluntarjoajan valinnassa ja integroinnissa tukee myös valmistajan velvoitteita, jotta digitaalisia elementtejä sisältävä tuote kokonaisuutena täyttäisi olennaiset vaatimukset.

8.3.4 *Teollisuusrobotti*

Teollisuusrobotin tehtävänä on noutaa osia. Robotti lähettää kameroiden kautta kerättyä tietoa valmistajan suunnittelemaan ja kehittämään etäpalveluun. Tämä palvelu toimii kolmannen osapuolen palveluntarjoajan tarjoamassa fyysisessä ja virtuaalisessa infrastruktuurissa (kolmannen osapuolen infrastruktuuripalvelussa). Pilvipalvelu laskee osan sijainnin kameran syötteiden perusteella ja lähettää robotille komennon noutaa osa.

Jos tätä datankäsittelyä ei tapahtuisi, teollisuusrobotti ei vois poimia osia eli suorittaa yhtä toiminnoistaan. Lisäksi infrastruktuurin päällä toimiva ohjelmisto on valmistajan suunnittelema ja kehittämä. Valmistajan suunnittelema ja kehittämä ohjelmisto vastaa datan etäkäsittelyratkaisun määritelmää.

Teollisuusrobotin valmistajan on dokumentoitava digitaalisia elementtejä sisältävän tuotteen teknisiin asiakirjoihin datan etäkäsittelyratkaisu sekä tukeutuminen kolmannen osapuolen infrastruktuuripalveluun, mukaan lukien sopimuksen alaisen palvelun yksityiskohdat. Valmistajan on myös otettava nämä tekijät huomioon riskinarvioinnissa, joka kattaa digitaalisia elementtejä sisältävän tuotteen käyttötarkoituksen ja kohtuudella ennakoitavissa olevan käytön. Valmistaja panee täytäntöön kyberkestävyyssäädöksen olennaiset vaatimukset riskien perusteella digitaalisia elementtejä sisältävän tuotteen ja myös sen datan etäkäsittelyratkaisun osalta. Asianmukainen huolellisuus infrastruktuuripalvelun tarjoajan valinnassa tukee myös valmistajan velvoitteita. Valmistaja voisi esimerkiksi pyytää näyttöä siitä, että NIS 2 -direktiivin velvoitteet on täytetty.

8.3.5 *Matkaviestinverkko*

Älypuhelin käyttää 5G-verkkoa mobiiliyhteyden eli internetyhteyden, puheluiden ja viestien tarjoamiseen käyttäjilleen. Matkaviestinverkon kehittämisestä ja suunnittelusta vastaavat teleoperaattorit. Tällainen matkaviestinverkko koostuu mikrosoluista ja tukiasemamastoista sekä muista verkkolaitteista.

Digitaalisia elementtejä sisältävän tuotteen olisi kyettävä muodostamaan yhteys verkkoon ongelmitta, sillä se on yksi sen toiminnoista. Sillä, onko kyseinen verkko toiminnassa, ei kuitenkaan ole merkitystä sen varmistamisessa, toimiiko digitaalisia elementtejä sisältävä tuote oikein. Verkko on vain viestintäkanava, eikä se ole välttämätön, jotta digitaalisia elementtejä sisältävä tuote voisi suorittaa toimintonsa eli muodostaa yhteyden verkkoon. Myöskään Ethernet-kaapelia, reititintä tai Wi-Fi-signaalia ei pidetä datankäsittelynä, jonka puuttuminen estäisi digitaalisia elementtejä sisältävää tuotetta suorittamasta jotakin toiminnoistaan, vaan ennemmin tiedonsiirron ja yhteyksien mahdollistajana.

Näin ollen matkaviestinverkko ei täytä datan etäkäsittelyratkaisun määritelmää. Verkkoa ei pitäisi pitää kolmannen osapuolen komponenttina, koska digitaalisia elementtejä sisältävän tuotteeseen ei ole integroitu ohjelmistoa, vaan tuote vain käyttää tätä verkkoa. Valmistajan ei näin ollen tarvitse noudattaa huolellisuusvelvoitteita verkon tarjoajaa kohtaan.

9. **MUUT ELEMENTIT**

9.1 **Raportointivelvoitteet**

209. Kyberkestävyyssäädöksen 14 artiklan 1 ja 3 kohdan mukaan valmistajan on samanaikaisesti ilmoitettava koordinaattoriksi nimetylle CSIRT-yksikölle ja ENISAlle i) kaikista sen digitaalisia elementtejä sisältävään tuotteeseen sisältyvistä aktiivisesti hyödynnetyistä haavoittuvuuksista, joista se on tullut tietoiseksi, ja ii) kaikista digitaalisista elementtejä sisältävän tuotteen tietoturvaan vaikuttavista vakavista poikkeamista, joista se on tullut tietoiseksi.

210. Asetuksen 69 artiklan 3 kohdan ja 71 artiklan 2 kohdan toisen virkkeen mukaisesti velvoitetta noudattaa 14 artiklaa sovelletaan 11. syyskuuta 2026 alkaen kaikkiin kyberkestävyysasetuksen soveltamisalaan kuuluviin digitaalisia elementtejä sisältäviin tuotteisiin, mukaan lukien digitaalisia elementtejä sisältävät tuotteet, jotka on saatettu markkinoille ennen 11:ttä joulukuuta 2027. Lisäksi toisin kuin haavoittuvuuksien käsittelyä koskevat velvoitteet, jotka ovat voimassa vain tuotteen tukiajan ajan, raportointivelvoitteita sovelletaan senkin jälkeen, kun digitaalisia elementtejä sisältävää tuotetta ei enää tueta. Jos digitaalisia elementtejä sisältävä tuote on saatettu markkinoille ennen 11:ttä joulukuuta 2027 tai jos sen tukiaika on päättynyt, valmistajan ei tarvitse noudattaa liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyä koskevia velvoitteita.

211. On muistettava, että valmistajan velvollisuutta ilmoittaa tällaisista tapahtumista sovelletaan, kun valmistaja on saanut tietoonsa, että haavoittuvuutta hyödynnetään aktiivisesti tai että on tapahtunut vakava poikkeama, joka on johtanut digitaalisia elementtejä sisältävän tuotteen tietoturvan vaarantumiseen. Sen vuoksi ohjeiden siitä, milloin valmistajan katsotaan tulleen tietoiseksi tapahtumasta, olisi autettava valmistajia määrittämään ajankohta, josta sovellettava ilmoitusvelvollisuus alkaa.

212. Valmistajiin voidaan soveltaa EU:n eri säädösten mukaisia vertailukelpoisia raportointivelvoitteita. Sen varmistamiseksi, että valmistajan ”tuleminen tietoiseksi” tulkitaan johdonmukaisesti ja että valmistajien on helpompi noudattaa näitä velvoitteita, nämä ohjeet ovat yhdenmukaisia komission täytäntöönpanoasetuksen (EU) 2024/2690 johdanto-osan 31 kappaleen ja yleisen tietosuoja-asetuksen mukaisista henkilötietojen tietoturvaloukkauksia koskevista ilmoituksista annettujen suuntaviivojen 9/2022 II kohdan A alakohdan kanssa.

213. Joissakin tapauksissa valmistaja havaitsee epäilyttävän tapahtuman, tai kolmas osapuoli, kuten yksityishenkilö, asiakas, yhteisö, viranomainen, mediaorganisaatio tai muu lähde, tuo valmistajan tietoon mahdollisen poikkeaman tai haavoittuvuuden. Tällaisissa tapauksissa valmistajan olisi arvioitava epäilyttävä tapahtuma välittömästi sen määrittämiseksi, onko kyseessä aktiivisesti hyödynnetty haavoittuvuus tai digitaalisia elementtejä sisältävän tuotteen tietoturvaan vaikuttava vakava poikkeama. Valmistajan katsotaan näin ollen tulleen tietoiseksi tapahtumasta, kun sillä on tällaisen alustavan arvion jälkeen kohtuullinen varmuus siitä, että i) sen digitalisia elementtejä sisältävään tuotteeseen sisältyvää haavoittuvuutta hyödynnetään aktiivisesti, tai ii) on tapahtunut vakava poikkeama, joka aiheuttanut digitaalisia elementtejä sisältävän tuotteen tietoturvan vaarantumisen.

214. Näin ollen ajankohta, jolloin valmistajan voidaan katsoa tulleen tietoiseksi tapahtumasta, riippuu kyseisen aktiivisesti hyödynnetyn haavoittuvuuden tai vakavan poikkeaman olosuhteista. Joissakin tapauksissa on alusta alkaen suhteellisen selvää, että haavoittuvuutta hyödynnetään aktiivisesti tai että vakava poikkeama vaikuttaa digitaalisia elementtejä sisältävän tuotteen tietoturvaan. Toisissa tapauksissa saattaa kestää jonkin aikaa selvittää, vaikuttaako haavoittuvuus digitaalisia elementtejä sisältävään tuotteeseen ja hyödyntääkö pahantahtoinen toimija tätä haavoittuvuutta tai vaikuttaako poikkeama digitaalisia elementtejä sisältävän tuotteen tietoturvaan. Tärkeintä olisi kuitenkin suorittaa alustava arvio viipymättä, jotta voidaan määrittää, täyttyvätkö tällaiset edellytykset, erityisesti jos haavoittuvuus voi aiheuttaa merkittävän riskin, ja jos näin on, ryhtyä korjaaviin toimiin ja ilmoittaa asiasta kyberkestävyyssäädöksen mukaisesti.

215. Lisäksi raportointivelvoitteiden rakenne edellyttää, että valmistaja päivittää ilmoitustaan asteittain, kun sen sisäiset tutkimukset etenevät ja tiedot aktiivisesti hyödynnetystä haavoittuvuudesta tai poikkeamasta tarkentuvat. Valmistajan on erityisesti annettava rajalliset tiedot sisältävä ennakkovaroitusilmoitus ilman aiheetonta viivytystä ja joka tapauksessa 24 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi asiasta. Lisätietoja on tämän jälkeen toimitettava osana ilmoitusta, joka on annettava ilman aiheetonta viivytystä ja joka tapauksessa 72 tunnin kuluessa siitä, kun valmistaja on tullut tietoiseksi asiasta, jäljempänä ’72 tunnin kuluessa annettava ilmoitus’. Valmistajan on annettava kattava loppuraportti 14 päivän kuluessa siitä, kun aktiivisesti hyödynnettyä haavoittuvuutta korjaava tai lieventävä toimenpide on käytettävissä, tai kuukauden kuluessa vakavia poikkeamia koskevasta 72 tunnin kuluessa annettavasta ilmoituksesta.

216. Kuten myös jaksossa *3.3.1 Pitkäjänteinen tuki ja VALOn toimintakelpoisuuden varmistaminen* muistutetaan, avoimen lähdekoodin ohjelmistovastaavien on myös ilmoitettava aktiivisesti hyödynnetyistä haavoittuvuuksista 24 artiklan 3 kohdan mukaisesti ([30]). Tätä velvoitetta sovelletaan, kun ohjelmistovastaava on tullut tietoiseksi aktiivisesti hyödynnetystä haavoittuvuudesta. Se ei siis koske vain niitä tilanteita, joissa haavoittuvuus on sellaisen VALOn koodissa, jonka ohjelmistovastaava kyseinen yhteisö on. Koska VALO-komponentit on yleensä integroitu digitaalisia elementtejä sisältäviin tuotteisiin ketjun loppupäässä, ohjelmistovastaava tulee todennäköisesti tietoiseksi haavoittuvuuden aktiivisesta hyödyntämisestä käytännössä saatuaan kolmansilta osapuolilta ilmoituksen, jossa ilmoitetaan VALO-komponenttien haavoittuvuuksien hyödyntämisestä osana digitaalisia elementtejä sisältäviä muita tuotteita. Näin voi tapahtua esimerkiksi silloin, kun digitaalisia elementtejä sisältävän tuotteen valmistaja havaitsee, että sen omaan tuotteeseen integroidun VALO-komponentin haavoittuvuutta hyödynnetään aktiivisesti, ja ilmoittaa siitä kyseisen komponentin ohjelmistovastaavalle, tai kun käyttäjä tai tietoturvatutkija havaitsee näyttöä digitaalisia elementtejä sisältävään tuotteeseen integroidun VALO-komponentin haavoittuvuuden hyödyntämisestä ja ilmoittaa tästä aktiivisesta hyödyntämisestä komponentin ohjelmistovastaavalle.

217. Olisi myös selvennettävä, että koska velvoitetta ilmoittaa aktiivisesti hyödynnetyistä haavoittuvuuksista sovelletaan, kun valmistaja tulee tietoiseksi aktiivisesta hyödyntämisestä, valmistajan ei tarvitse ilmoittaa haavoittuvuuksista, joiden aktiivisesta hyödyntämisestä se on tullut tietoiseksi jo ennen 11:ttä syyskuuta 2026 (päivämäärä, josta alkaen raportointivelvoitetta sovelletaan). Kyberkestävyyssäädös ei näin ollen edellytä tällaisten haavoittuvuuksien takautuvaa raportointia. Velvoitetta sovelletaan sitä vastoin silloin, kun valmistaja on tiennyt haavoittuvuudesta ennen 11:ttä syyskuuta 2026, mutta ei tuolloin ole ollut tietoinen haavoittuvuuden aktiivisesta hyödyntämisestä (joko siksi, että hyödyntämistä ei ollut vielä tapahtunut tai siksi, että valmistaja ei ollut tietoinen siitä). Jos haavoittuvuutta hyödynnetään aktiivisesti tai valmistaja tulee tietoiseksi aktiivisesta hyödyntämisestä 11. syyskuuta 2026 alkaen, haavoittuvuus katsotaan aktiivisesti hyödynnetyksi ja siihen sovelletaan raportointivelvoitetta.

218. Vastaavasti valmistajan on raportoitava vain digitaalisia elementtejä sisältävän tuotteen sisältämistä aktiivisesti hyödynnetyistä haavoittuvuuksista. Jos digitaalisia elementtejä sisältävä tuote sisältää kolmannen osapuolen komponentista johtuvan aktiivisesti hyödynnetyn haavoittuvuuden, digitaalisia elementtejä sisältävän tuotteen valmistajan on ilmoitettava kyseisestä aktiivisesti hyödynnetystä haavoittuvuudesta. Kuitenkin tilanteessa, jossa valmistaja tietää, että kolmannen osapuolen komponentti sisältää haavoittuvuuden, mutta kyseistä haavoittuvuutta joko i) ei voida hyödyntää digitaalisia elementtejä sisältävässä tuotteessa (esimerkiksi siksi, että haavoittuvaan koodiin ei pääse käsiksi) tai ii) ei ole hyödynnetty digitaalisia elementtejä sisältävässä tuotteessa, kyseistä haavoittuvuutta ei pidetä valmistajan digitaalisia elementtejä sisältävän tuotteen aktiivisesti hyödynnettynä haavoittuvuutena, minkä vuoksi siihen ei sovelleta pakollista raportointia kyseisen valmistajan osalta. Kyseinen valmistaja voi silti ilmoittaa kyseisestä haavoittuvuudesta vapaaehtoisesti kyberkestävyyssäädöksen 15 artiklan mukaisesti. Sen on myös noudatettava kyberkestävyyssäädöksen liitteessä I olevassa II osassa vahvistettuja haavoittuvuuksien käsittelyä koskevia vaatimuksia sekä ilmoitettava haavoittuvuudesta komponenttia valmistavalle tai ylläpitävälle henkilölle tai yhteisölle 13 artiklan 6 kohdan mukaisesti ja kuten jaksossa *9.2.1 Raportointi ketjun alkupäähän ja tietoturvakorjausten jakaminen* selitetään tarkemmin.

([30]) Siltä osin kuin ohjelmistovastaavat osallistuvat digitaalisia elementtejä sisältävien tuotteiden kehittämiseen.

219. Kun valmistaja on tullut tietoiseksi aktiivisesti hyödynnetystä haavoittuvuudesta tai vakavasta poikkeamasta, sen on 14 artiklan 8 kohdan mukaisesti tiedotettava asiasta käyttäjille, joihin vaikutukset kohdistuvat, ja tarvittaessa kaikille käyttäjille. Jos valmistaja ei tiedota asiasta käyttäjille oikea-aikaisesti, ilmoituksen vastaanottaneet CSIRT-yksiköt voivat antaa näitä tietoja käyttäjille, kun se katsotaan oikeasuhtaiseksi ja tarpeelliseksi haavoittuvuuden tai poikkeaman vaikutusten ehkäisemiseksi tai lieventämiseksi.

220. Kyberkestävyyssäädöksen riskiperusteisen lähestymistavan mukaisesti 14 artiklan 8 kohdassa säädettyä velvoitetta ilmoittaa käyttäjille on sovellettava riskiperusteisesti ja oikeasuhteisesti. Tiedottaminen aktiivisesti hyödynnetystä haavoittuvuudesta tai vakavasta poikkeamasta ei etenkään tarkoita, että tällaiset tiedot olisi tuotava esiin yleisölle tai julkistettava valikoimattomasti. Kun otetaan huomioon digitaalisia elementtejä sisältävän tuotteen luonne, käyttäjät, joihin vaikutukset kohdistuvat, sekä haavoittuvuuden tai poikkeaman mahdollinen vaikutus, valmistajat voivat tarvittaessa rajoittaa yksityiskohtaisten tietojen julkistamisen vain asianomaisiin käyttäjiin tai asiakkaisiin. Tämä koskee erityisesti digitaalisia elementtejä sisältäviä tuotteita, joita käytetään arkaluonteisissa tai kriittisissä toimintaympäristöissä, jolloin teknisten yksityiskohtien julkistaminen yleisölle voisi itsessään lisätä kyberturvallisuusriskejä tai helpottaa haavoittuvuuksien hyödyntämistä entisestään.

221. Laajempi tietojen julkistaminen voi olla asianmukaista sitten, kun haavoittuvuutta on saatu korjattua tai lievennettyä riittävästi. Tämä koskee esimerkiksi tilanteita, joissa julkistaminen auttaisi lisäämään yleistä tietoisuutta tai antaisi käyttäjille mahdollisuuden tarkistaa, että haavoittuvuus ei enää vaikuta heidän digitaalisia elementtejä sisältäviin tuotteisiinsa. Tällaisissa tapauksissa laajemmassa tietojen julkistamisessa olisi pyrittävä yksityiskohtien tason ja ajoituksen oikeasuhteisuuteen ja otettava huomioon jäljelle jäävät riskit haavoittuvuuden hyödyntämiseen, digitaalisia elementtejä sisältävän tuotteen luonne ja asianomaisten käyttäjien edut. Lisäksi liitteessä I olevan II osan 4 kohdassa edellytetään, että valmistajat julkistavat tiedot korjatuista haavoittuvuuksista, kun tietoturvapäivitys asetettu saataville.

9.2 **Haavoittuvuuksien käsittely**

9.2.1 *Raportointi ketjun alkupäähän ja tietoturvakorjausten jakaminen*

222. Kyberkestävyyssäädöksen 13 artiklan 6 kohdassa edellytetään, että valmistajat ilmoittavat integroitujen komponenttien haavoittuvuuksista kyseistä komponenttia valmistavalle tai ylläpitävälle henkilölle tai yhteisölle, jäljempänä ’raportointi ketjun alkupäähän’.

223. Valmistajien on raportoitava ketjun alkupäähän vain komponentin sen version osalta, joka on integroitu niiden tuotteeseen. Jos komponenttia valmistavalla tai ylläpitävällä henkilöllä tai yhteisöllä on vakiintuneita tietoturvapolitiikkoja, koordinoitua haavoittuvuuksien julkistamista koskevia prosesseja tai nimettyjä kanavia haavoittuvuuksien raportointia varten, valmistajien olisi raportoitava niiden mukaisesti. Näin olisi toimittava erityisesti silloin, kun paikkaamattomien haavoittuvuuksien ennenaikainen ilmoittaminen voisi lisätä kyberturvallisuusriskejä. Tuotantoketjun alkupään ylläpitäjiin erityisesti avoimen lähdekoodin hankkeissa kohdistuvan rasitteen vähentämiseksi valmistajien ei myöskään tarvitse raportoida ketjun alkupäähän, jos ne voivat vahvistaa, että komponenttia valmistava tai ylläpitävä henkilö tai yhteisö on tietoinen haavoittuvuudesta. Valmistajia kannustetaan toteuttamaan kohtuullisia toimia välttääkseen päällekkäisten raporttien lähettämisen, esimerkiksi tarkistamalla julkisesti saatavilla olevat haavoittuvuustietokannat, hankekohtaiset turvallisuusohjeet tai vakiintuneet ongelmien seurantajärjestelmät ennen raportoimista ketjun alkupäähän.

224. Valmistajien on raportoitava ketjun alkupäähän ainoastaan sellaiset haavoittuvuudet, jotka ovat itse integroidussa komponentissa. Sellaisia haavoittuvuuksia, jotka johtuvat komponentin ja valmistajan luoman muun koodin yhdistämisestä tai muiden komponenttien integroinnista, ei tarvitse raportoida. Joissakin tilanteissa komponentin integrointi tiettyyn digitaalisia elementtejä sisältävään tuotteeseen voi kuitenkin paljastaa tiettyjä kyseisen komponentin toiminta- tai vuorovaikutusmalleja tai turvallisuuden kannalta merkityksellisiä ominaisuuksia, jotka eivät olleet erillisessä komponentissa ilmeisiä tai helposti tunnistettavissa. Tällaisissa tapauksissa valmistajia kannustetaan välittämään nämä tiedot komponenttia valmistavalle tai ylläpitävälle henkilölle tai yhteisölle, jotta voidaan edistää haavoittuvuuksien käsittelyä koskevia hyviä käytäntöjä, joilla pyritään helpottamaan haavoittuvuuksien tehokasta korjaamista ja parantamaan komponenttien ekosysteemin yleistä turvallisuutta.

225. Valmistajien ei myöskään tarvitse ilmoittaa haavoittuvuudesta ketjun alkupäähän, jos komponentilla ei enää ole ylläpitäjää tai jos valmistaja ei enää tarvitse uusia versioita tai tietoturvakorjauksia alkuperäiseltä ylläpitäjältä. Tällaisissa tapauksissa valmistajaa kannustetaan kuitenkin tiedottamaan kyseisestä komponentista käyttäjille kohtuullisilla vaihtoehtoisilla toimilla, kuten käyttämällä olemassa olevia yhteisöllisiä mekanismeja (esimerkiksi postituslistoja tai tikettejä) tai julkisia haavoittuvuustietokantoja.

226. Lisäksi 13 artiklan 6 kohdan mukaan valmistajien, jotka ovat kehittäneet ohjelmiston muutoksen, jolla puututaan integroidun komponentin haavoittuvuuteen, on jaettava kyseinen ohjelmistomuutos, jäljempänä 'tietoturvakorjaus', komponenttia valmistavan tai ylläpitävän henkilön tai yhteisön kanssa, jäljempänä 'jakaminen ketjun alkupäähän'.

227. Jos valmistajien edellytetään 13 artiklan 6 kohdan nojalla jakavan tietoturvakorjauksen, se olisi tarvittaessa toimitettava koneellisesti luettavassa muodossa, helposti todennettavissa olevalla tavalla ja tarvittaessa komponenttia valmistavan tai ylläpitävän henkilön tai yhteisön integroimana. Jos komponentti on vapaa ja avoimen lähdekoodin ohjelmistokomponentti, tietoturvakorjaus olisi jaettava kyseisen komponentin lisenssin kanssa yhteensopivalla tavalla, esimerkiksi jakamalla se saman lisenssin nojalla tai sellaisella lisenssillä, jonka avulla ylläpitäjä voi jakaa korjauksen omalla lisenssillään. Jos kyseisen komponentin ylläpitäjällä on ohjeita siitä, miten tietoturvakorjaukset olisi jaettava, valmistajan olisi noudatettava näitä ohjeita.

228. Kyberkestävyyssäädöksessä ei kuitenkaan vaadita valmistajia varmistamaan, että komponenttia valmistava tai ylläpitävä henkilö tai yhteisö hyväksyisi niiden tietoturvakorjaukset. Niiden ei myöskään tarvitse varmistaa, että kyseiset korjaukset sisällytettäisiin välttämättä komponentin koodivarastoon esimerkiksi silloin, jos ylläpitäjä suosii toista vaihtoehtoa ongelman korjaamiseksi. Valmistajien ei myöskään tarvitse hyväksyä komponentin ylläpitäjän kehittämää korjausehdotusta, vaan ne saattavat mieluummin lieventää ongelmaa muilla sopivilla tavoilla.

229. Joissakin tapauksissa komponenttia valmistava tai ylläpitävä henkilö tai yhteisö on jo saattanut tarjota tietoturvakorjauksen haavoittuvuutta varten, mutta valmistaja soveltaa erilaista lieventämisstrategiaa (esimerkiksi muuttamalla toista kokoonpanoa). Tällaisissa tapauksissa kyberkestävyyssäädös ei edellytä, että valmistaja jakaisi järjestelmän toiseen osaan tehtyä muutosta tuotantoketjun alkupäähän. Valmistajaa kannustetaan kuitenkin tekemään niin, jos siten voidaan tukea komponenttia ylläpitävää henkilöä tai yhteisöä.

9.2.2 *Tiedossa olevat hyödynnettävissä olevat haavoittuvuudet*

230. Yksi kyberkestävyyssäädöksen liitteessä I olevassa I osassa määritelty vaatimus on, että digitaalisia elementtejä sisältävien tuotteiden on 13 artiklan 2 kohdassa tarkoitetun kyberturvallisuusriskien arvioinnin perusteella ja soveltuvin osin täytettävä seuraava vaatimus: ne on asetettava saataville markkinoilla ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia.

231. Direktiivin 3 artiklan 41 kohdassa "hyödynnettävissä olevalla haavoittuvuudella" tarkoitetaan "haavoittuvuutta, jota vastapuoli voi käyttää tehokkaasti käytännön toimintaolosuhteissa". Kaikkia haavoittuvuuksia ei voida hyödyntää käytännön toimintaolosuhteissa, ja joitakin haavoittuvuuksia voidaan hyödyntää vain teoreettisissa olosuhteissa (esimerkiksi laboratoriossa tai simulaatiossa) ja/tai muissa kuin sellaisissa olosuhteissa, jotka toteutuisivat digitaalisia elementtejä sisältävän tuotteen toimintaympäristössä.

232. Kyberkestävyyssäädöksessä edellytetään, että valmistajilla on asianmukaiset toimintatavat ja menettelyt, joilla käsitellään ja korjataan sisäisten tai ulkoisten lähteiden raportoimat mahdolliset haavoittuvuudet (13 artiklan 8 kohta). Siinä ei kuitenkaan nimenomaisesti täsmennetä, milloin hyödynnettävissä olevan haavoittuvuuden olisi katsottava olevan valmistajan tiedossa, mikä aiheuttaa velvoitteen noudattaa tätä olennaista vaatimusta markkinoille saattamisen ajankohtana.

233. Haavoittuvuutta olisi pidettävä tiedossa olevana, kun se on lueteltu asiaankuuluvissa julkisesti saatavilla olevissa haavoittuvuustietokannoissa, kuten direktiivin (EU) 2022/2555 12 artiklan 2 kohdan nojalla perustetussa eurooppalaisessa haavoittuvuustietokannassa tai muissa merkittävissä haavoittuvuustietokannoissa.

234. Haavoittuvuus voi olla tiedossa oleva myös silloin, kun valmistaja on tullut siitä tietoiseksi ei-julkisen tiedon kautta, esimerkiksi turvallisuustutkijan toteuttaman koordinoidun julkistamisen kautta tai valmistajan oman sisäisen testauksen ja analyysin kautta, esimerkiksi tekoälyyn perustuvia palveluja käytettäessä. Samoin haavoittuvuus voi olla tiedossa oleva, kun siitä on raportoitu julkisesti ja näkyvästi luotettavissa medialähteissä, mukaan lukien kyberturvallisuuteen erikoistuneet julkaisut tai yleiset joukkotiedotusvälineet.

235. Pelkkä haavoittuvuudesta ilmoittaminen tai sen havaitseminen ei kuitenkaan sinänsä tarkoita, että haavoittuvuutta voitaisiin hyödyntää käytännössä tai että se koskisi tiettyä kyseistä digitaalisia elementtejä sisältävää tuotetta. Valmistajan on tutkittava haavoittuvuus ja vahvistettava tällaisten tietojen todenperäisyys ja sovellettavuus omaan digitaalisia elementtejä sisältävään tuotteeseensa. Näin ollen ensimmäisen haavoittuvuutta koskevan ilmoituksen ja haavoittuvuuden vahvistamisen välillä voi kulua rajallinen aika. Kuten jaksossa *9.1 Raportointivelvoitteet* todetaan, painopisteen tulisi olla nopeissa toimissa haavoittuvuuden tutkimiseksi ja siihen reagoimiseksi.

236. Lisäksi valmistajien velvollisuutta noudattaa liitteessä I olevassa I osassa vahvistettuja olennaisia vaatimuksia sovelletaan markkinoille saattamisen ajankohtana 13 artiklan 1 kohdan mukaisesti. Käytännössä digitaalisia elementtejä sisältävän tuotteen tuotekehityksen elinkaaren loppuvaiheessa saattaa ilmetä uusia mahdollisesti hyödynnettävissä olevia haavoittuvuuksia, myös vähän ennen tuotteen tuomista jakeluketjuun (ja saattamista markkinoille).

237. Koska velvoite saattaa markkinoille digitaalisia elementtejä sisältäviä tuotteita ilman tiedossa olevia hyödynnettävissä olevia haavoittuvuuksia on riskiperusteinen velvoite, valmistajan on määritettävä kyberturvallisuusriskien arvioinnin perusteella, voidaanko digitaalisia elementtejä sisältävä tuote saattaa turvallisesti markkinoille kyberkestävyyssäädöksen mukaisesti. Vaihtoehtoisesti valmistaja voi määrittää, että mahdollisesti tietoon tullut uusi haavoittuvuus on korjattava, ennen kuin digitaalisia elementtejä sisältävä tuote voidaan saattaa markkinoille. Tätä määrittäessään valmistajien olisi otettava huomioon haavoittuvuuden vakavuus, hyödynnettävyys ja mahdolliset vaikutukset sekä riskit, joita digitaalisia elementtejä sisältävälle tuotteelle aiheutuu käytön jälkeen. Ne voivat myös ottaa huomioon riskit, jotka liittyvät tuotteen julkaisun lykkäämiseen, kunnes haavoittuvuus korjataan, esimerkiksi siksi, että uudessa versiossa on korjattu myös muita hyödynnettävissä olevia haavoittuvuuksia, tai siksi, että uusi versio on tarpeen kriittisten järjestelmien keskeytymättömän toiminnan kannalta. Kun digitaalisia elementtejä sisältävä tuote on saatettu markkinoille, valmistajalla on joka tapauksessa edelleen velvollisuus käsitellä haavoittuvuuksia tehokkaasti ja liitteessä I olevassa II osassa vahvistettujen haavoittuvuuksien käsittelyä koskevien vaatimusten mukaisesti.

9.2.3 *Tehokkaat ja säännölliset testit ja arvioinnit*

238. Liitteessä I olevan II osan 3 kohdassa edellytetään, että valmistajat tekevät digitaalisia elementtejä sisältävälle tuotteelle tehokkaita ja säännöllisiä testejä ja arviointeja koko tuotteen tukiajan ajan. Säännöllisten testien tekeminen ei edellytä testauksen mekaanista toistamista tietyin väliajoin ilman muutoksia. Se tarkoittaa, että tarkistetaan säännöllisesti, edellyttävätkö uudet syöttötiedot esimerkiksi vasta tunnistetuista uhista tai uusista havaituista haavoittuvuuksista nykyisten testien päivittämistä, ja suoritetaan testit sen mukaisesti.

239. Tarkistusten aikavälin, perusteellisuuden ja sisällön olisi oltava oikeassa suhteessa digitaalisia elementtejä sisältävän tuotteen kyberturvallisuuden riskiprofiiliin, sen kehitykseen ajan mittaan ja uhkaympäristön tilaan. Jos tarkistuksessa havaitaan merkityksellisiä uusia syöttötietoja, jotka vaikuttavat testisarjaan, tuotteelle olisi suunniteltava ja suoritettava uusia tai muutettuja testejä sen varmistamiseksi, että kaikkiin haavoittuvuuksiin puututaan. Tämä voi tarkoittaa myös olemassa olevien testien suorittamista uudelleen, jos digitaalisia elementtejä sisältävän tuotteen muuttaminen tekee tällaisesta testauksesta tarkoituksenmukaista, kuten regressiotestauksen tapauksessa.

240. Jos tarkistuksessa ei havaita tällaisia syöttötietoja, lisätestejä ei tarvitse laatia. Samalla sovelletaan edelleen rinnakkain muita haavoittuvuuksien käsittelyä koskevia velvoitteita, mukaan lukien haavoittuvuuksiin puuttuminen ja niiden korjaaminen tuotteisiin kohdistuvien riskien yhteydessä.

9.3 **Vuorovaikutus muun lainsäädännön kanssa**

9.3.1 *Asetus (EU) 2019/2144 ja asetus (EU) N:o 168/2013*

241. Kyberkestävyyssäädöksen 2 artiklan 2 kohdan c alakohdassa säädetään, että asetusta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, joihin sovelletaan asetusta (EU) 2019/2144. Asetusta (EU) 2019/2144 sovelletaan ”asetuksen (EU) 2018/858 4 artiklassa määriteltyihin luokkien M, N ja O ajoneuvoihin sekä niitä varten suunniteltuihin ja rakennettuihin järjestelmiin, komponentteihin ja erillisiin teknisiin yksiköihin”.

242. Vastaavasti digitaalisia elementtejä sisältävät tuotteet, jotka kuuluvat asetuksen (EU) N:o 168/2013 soveltamisalaan, on suljettu kyberkestävyyssäädöksen soveltamisalan ulkopuolelle komission delegoidulla asetuksella (EU) 2025/1535. Asetusta (EU) N:o 168/2013 sovelletaan L-luokan ajoneuvoihin ja ”tällaisia ajoneuvoja varten suunniteltuihin ja valmistettuihin järjestelmiin, komponentteihin ja erillisiin teknisiin yksiköihin sekä osiin ja varusteisiin” (2 artiklan 1 kohta).

243. Ajoneuvoihin, joihin kyseisiä asetuksia sovelletaan, ei sovelleta kyberkestävyyssäädöstä. Lisäksi tarvitaan lisäselvennyksiä poikkeuksen soveltamisalasta sellaisten järjestelmien, komponenttien, erillisten teknisten yksiköiden, osien ja varusteiden osalta, tässä jaksossa jäljempänä ’komponentit’, jotka on suunniteltu ja rakennettu tällaisia ajoneuvoja varten ja joiden katsotaan olevan kyberkestävyyssäädöksessä tarkoitettuja digitaalisia elementtejä sisältäviä tuotteita.

244. Tällaisten komponenttien ei katsota kuuluvan kyberkestävyyssäädöksen soveltamisalaan edellyttäen, että ne on suunniteltu ja rakennettu yksinomaan integroitaviksi asetusten (EU) 2019/2144 ja (EU) N:o 168/2013 soveltamisalaan kuuluviin ajoneuvoihin. Tähän ei vaikuta se, myykö kyseisen komponentin valmistaja sen suoraan ajoneuvon valmistajalle vai toiselle talouden toimijalle autoteollisuuden toimitusketjussa, kunhan komponentti on selvästi tarkoitettu ja soveltuu ainoastaan lopulliseen integrointiin kyseisiin ajoneuvoihin.

245. Sen sijaan kyberkestävyyssäädöstä sovelletaan, jos valmistaja myy yleisiä komponentteja, jotka ovat digitaalisia elementtejä sisältäviä tuotteita ja jotka voidaan integroida erityyppisiin tuotteisiin eikä yksinomaan kyseisten asetusten soveltamisalaan kuuluviin ajoneuvoihin.

246. Arvioinnin siitä, saatetaanko jokin komponentti markkinoille kyberkestävyyssäädöksessä tarkoitetulla tavalla, on perustuttava objektiivisiin edellytyksiin, joiden mukaisesti se asetetaan saataville. Jos valmistaja tarjoaa komponentin, joka soveltuu muuhunkin kuin yksinomaan lopulliseen integrointiin kyseisiin ajoneuvoihin, sellaisten jakelukanavien kautta, jotka ovat avoinna autoteollisuuden toimitusketjun ulkopuolisille asiakkaille, kuten kuluttaja-asiakkaiden tilauksia hyväksyville tavanomaisille vähittäismyymälöille tai verkkomyyntikanaville, kyseinen komponentti kuuluu kyberkestävyyssäädöksen soveltamisalaan riippumatta mahdollisista sen aiottua käyttötarkoitusta koskevista väittämiä. Tällaisissa olosuhteissa komponentin ei voida katsoa olevan suunniteltu ja rakennettu yksinomaan asetusten (EU) 2019/2144 ja (EU) N:o 168/2013 soveltamisalaan kuuluviin ajoneuvoihin integrointia varten, joten valmistajan on noudatettava kyberkestävyyssäädöstä. Sitä vastoin rajoitettujen, yritysten välisten, autoteollisuuden toimitusketjuun rajoittuvien jakelukanavien käyttö voi osoittaa, että komponentti on suunniteltu ja rakennettu yksinomaan tällaista integrointia varten.

9.3.2 *EU-tyyppitarkastustodistusten voimassaolo (69 artiklan 1 kohta)*

247. Kyberkestävyyssäädöksen 69 artiklan 1 kohdassa todetaan, että ”EU-tyyppitarkastustodistukset ja hyväksymispäätökset, jotka on annettu digitaalisia elementtejä sisältävien tuotteiden, joihin sovelletaan muuta unionin yhdenmukaistamislainsäädäntöä kuin tätä asetusta, kyberturvallisuusvaatimuksista, pysyvät voimassa 11 päivään kesäkuuta 2028 saakka, paitsi jos niiden voimassaolo päättyy ennen kyseistä ajankohtaa tai jos tällaisessa muussa unionin yhdenmukaistamislainsäädännössä toisin säädetään, jolloin ne pysyvät voimassa kyseisessä lainsäädännössä tarkoitetulla tavalla”.

248. Tällaisten todistusten ja hyväksymispäätösten voimassaolon jatkamisen olisi katsottava rajoittuvan kyberturvallisuusriskeihin ja vastaaviin vaatimuksiin, jotka kuuluvat unionin sen yhdenmukaistamislainsäädännön soveltamisalaan, jonka perusteella ne on annettu. Näiden riskien osalta valmistajien ei tarvitse arvioida uudelleen tai osoittaa uudelleen vaatimustenmukaisuutta ainoastaan kyberkestävyyssäädöksen tarkoituksia varten 69 artiklan 1 kohdassa tarkoitettuna voimassaoloaikana sellaisten digitaalisia elementtejä sisältävien tuotteiden osalta, joita ne aikovat saattaa markkinoille 11. joulukuuta 2027 tai sen jälkeen ja 11:nteen kesäkuuta 2028 saakka ([31]). Tämä koskee todistuksia ja hyväksymispäätöksiä, jotka on annettu, jos sovellettavassa unionin yhdenmukaistamislainsäädännössä vaaditaan valmistajaa suorittamaan vaatimustenmukaisuusmenettely ilmoitetun laitoksen välityksellä tai jos valmistaja on vapaaehtoisesti päättänyt tehdä niin.

249. Näin ollen muun unionin yhdenmukaistamislainsäädännön mukainen voimassa oleva todistus tai hyväksymispäätös ei vapauta valmistajia velvoitteesta suorittaa kattava kyberturvallisuusriskien arviointi kyberkestävyyssäädöksen mukaisesti (tai muista säädöksen mukaisista velvoitteista). Sen sijaan valmistajat voivat osoittaa olemassa olevilla todistuksilla vaatimustenmukaisuusmenettelyjen noudattamisen siltä osin kuin niissä on käsitelty vastaavia kyberturvallisuusriskejä. Vaikka todistus tai hyväksymispäätös olisi muun unionin yhdenmukaistamislainsäädännön nojalla voimassa vielä 11. kesäkuuta 2028 jälkeen, valmistaja voi turvautua tällaiseen todistukseen tai päätökseen kyberkestävyyssäädöksen velvoitteita varten ainoastaan 11. kesäkuuta 2028 saakka.

250. Jos 13 artiklan 2 kohdan mukaisesti tehdyssä kyberturvallisuusriskien arvioinnissa havaitaan lisäriskejä, joita olemassa olevan todistuksen tai hyväksymispäätöksen perustana olevat kyberturvallisuusvaatimukset eivät kata, valmistajat ovat edelleen vastuussa kyseisiin riskeihin puuttumisesta kyberkestävyyssäädöksen mukaisesti. Tällaisissa tapauksissa vaatimustenmukaisuus edellyttää, että havaitut puutteet arvioidaan ja niitä paikataan riippumatta voimassa olevan todistuksen tai hyväksymispäätöksen voimassaolon jatkumisesta.

251. Tätä voidaan havainnollistaa tarkastelemalla tapausta, jossa digitaalisia elementtejä sisältävään tuotteeseen sovelletaan direktiivin 2014/53/EU täydentämisestä annetussa komission delegoidussa asetuksessa (EU) 2022/30 (radiolaitedirektiiviä koskeva delegoitu säädös) säädettyjä kyberturvallisuusvaatimuksia ja jossa näiden vaatimusten perusteella on annettu EU-tyyppitarkastustodistus tai hyväksymispäätös. Tällöin todistus tai päätös on edelleen voimassa 69 artiklan 1 kohdan mukaisesti niiden kyberturvallisuusriskien osalta, jotka kyseinen todistus kattaa ja jotka liittyvät direktiivin 2014/53/EU (radiolaitedirektiivi) olennaisiin kyberturvallisuusvaatimuksiin.

252. Tällaisissa tapauksissa valmistajien ei tarvitse kyberkestävyyssäädöksen tarkoituksia varten arvioida uudelleen tai osoittaa uudelleen vaatimustenmukaisuutta kyseisissä todistuksissa jo käsiteltyjen riskien osalta niin kauan kuin kyseinen todistus tai hyväksymispäätös on voimassa ja joka tapauksessa enintään 11:nteen kesäkuuta 2028 asti. Tähän sisältyvät esimerkiksi verkon suojaamiseen, henkilötietojen ja yksityisyyden suojaan tai petosten ehkäisemiseen liittyvät kyberturvallisuusriskit (siltä osin kuin kyseinen todistus kattaa nämä riskit), jotka liittyvät radiolaitedirektiivin kyberturvallisuusvaatimuksiin ja jotka otetaan huomioon vaatimustenmukaisuuden arvioinnissa.

253. Jos kyberkestävyyssäädöksen 13 artiklan 2 kohdan mukaisesti suoritetussa kyberturvallisuusriskien arvioinnissa kuitenkin havaitaan muita kyberturvallisuusriskejä, joita kyseiset todistukset eivät kata, valmistajat ovat edelleen vastuussa kyseisiin riskeihin puuttumisesta kyberkestävyyssäädöksen mukaisesti. Näitä riskit voivat liittyä esimerkiksi haavoittuvuuksien käsittelyprosesseihin, tietojen minimointiin ja hyökkäyspinta-alan pienentämiseen tai muihin tuotekohtaisiin kyberturvallisuusnäkökohtiin, joita kyseiset todistukset eivät kata tai jotka eivät toisaalta kuulu radiolaitedirektiivin olennaisten kyberturvallisuusvaatimusten soveltamisalaan.

254. Näin ollen radiolaitedirektiivin mukainen voimassa oleva EU-tyyppitarkastustodistus tai hyväksymispäätös ei sinänsä osoita sen olennaisten kyberturvallisuusvaatimusten osalta kyberkestävyyssäädöksen vaatimusten täyttä noudattamista. Sen sijaan valmistajat voivat käyttää kyseistä todistusta tai päätöstä todisteena vastaavia riskejä koskevien vaatimusten noudattamisesta, mutta niiden on samalla varmistettava, että kaikki jäljellä olevat tai uudet havaitut riskit arvioidaan ja niitä lievennetään kyberkestävyyssäädöksen mukaisesti.

([31]) Ennen 11:ttä joulukuuta 2027 markkinoille saatettuihin digitaalisia elementtejä sisältäviin tuotteisiin sovelletaan niiden markkinoille saattamisen aikaan sovellettavaa unionin lainsäädäntöä, ja jos ne ovat vaatimusten mukaisia, niitä voidaan myydä ja ottaa käyttöön, jollei niihin tehdä merkittäviä muutoksia 11. joulukuuta 2027 tai sen jälkeen. Käsitteiden ”markkinoille saattaminen” ja ”asettaminen saataville markkinoilla” osalta ks. myös tämän asiakirjan jakso *2.1 Markkinoille saattaminen* sekä sinisen oppaan luku 2.

255. Vastaavasti jos digitaalisia elementtejä sisältävään tuotteeseen sovelletaan asetuksessa (EU) 2023/1230 (koneasetus) säädettyjä kyberturvallisuuteen liittyviä olennaisia terveys- ja turvallisuusvaatimuksia, joita sovelletaan kokonaisuudessaan 20. tammikuuta 2027 alkaen, ja jos EU-tyyppitarkastustodistus tai hyväksymispäätös on annettu näiden vaatimusten perusteella, kyseinen todistus tai hyväksymispäätös on edelleen voimassa kyberkestävyyssäädöksen 69 artiklan 1 kohdan mukaisesti koneasetuksen kattamien kyberturvallisuusriskien osalta.

256. Tämä koskee erityisesti tietojen turmeltumiselta suojautumiseen sekä ohjausjärjestelmien turvallisuuteen ja toimintavarmuuteen liittyviä kyberturvallisuusnäkökohtia koneasetuksen liitteessä III olevien 1.1.9 ja 1.2.1 kohdan mukaisesti. Näiden riskien osalta valmistajien ei tarvitse kyberkestävyyssäädöksen tarkoituksia varten arvioida uudelleen tai osoittaa uudelleen vaatimustenmukaisuutta niin kauan kuin kyseinen todistus tai hyväksymispäätös on voimassa ja joka tapauksessa enintään 11:nteen kesäkuuta 2028 asti. Tätä sovelletaan siltä osin kuin kyseisiä riskejä on käsitelty osana koneasetuksen mukaista vaatimustenmukaisuuden arviointia.

257. Edellä mainittujen radiolaitedirektiivin olennaisten kyberturvallisuusvaatimusten tavoin silloin, kun kyberkestävyyssäädöksen 13 artiklan 2 kohdan mukaisesti suoritetussa kyberturvallisuusriskien arvioinnissa havaitaan muita kyberturvallisuusriskejä, joita koneasetuksen nojalla myönnetty asiaankuuluva todistus ei kata ja jotka liittyvät kyseisen asetuksen kyberturvallisuusvaatimuksiin, valmistajat ovat edelleen vastuussa näihin riskeihin puuttumisesta kyberkestävyyssäädöksen mukaisesti.