C/2026/6013

17.11.2026

KOMISJONI TEATIS

Komisjoni suunised määruse (EL) 2024/2847 (küberkerksuse määrus) kohaldamise kohta

(C/2026/6013)

Sisukord

Lehekülg

1. SISSEJUHATUS 3
   - 1.1. Küberkerksuse määrus 3
   - 1.2. Käesolevate suuniste otstarve 3
2. KOHALDAMISALA 4
   - 2.1. Turule laskmine 4
   - 2.2. Tarkvara kui digielemente sisaldav toode 5
   - 2.3. Arvutikood 6
   - 2.4. Digielemente sisaldava riist- ja tarkvaratoote kombinatsioon 7
   - 2.5. Andmesideühendus 8
   - 2.6. Komplekssed süsteemid 8
   - 2.7. Enne küberkerksuse määruse kohaldamise algust projekteeritud digielemente sisaldavad tooted 9
3. VABA JA AVATUD LÄHTEKOODIGA TARKVARA 11
   - 3.1. Kindakstegemine, kas vaba ja avatud lähtekoodiga tarkvara kuulub isiku vastutusalasse 12
   - 3.2. Kindlakstegemine, kas vaba ja avatud lähtekoodiga tarkvara lastakse ELi turule 13
     - 3.2.1. Tasu küsimine 13
     - 3.2.2. Muude teenuste eest tasu saamine või isikuandmete töötlemise vajadus 13
     - 3.2.3. Tugiteenused 14
     - 3.2.4. Annetused 15
     - 3.2.5. Vaba ja avatud lähtekoodiga tarkvara rahastamine 15
     - 3.2.6. Mittetulunduslikud üksused, mis on loodud mittetulunduslike eesmärkide saavutamiseks 16
     - 3.2.7. Teiste tootjate poolne integreerimine 16
   - 3.3. Avatud lähtekoodiga tarkvara korraldajad 16
     - 3.3.1. Vaba ja avatud lähtekoodiga tarkvara pidev toetus ning elujõulisuse tagamine 17
   - 3.4. Edasiarendajad ja järgneva etapi kasutusviisid 18
   - 3.5. Näitlikustavad stsenaariumid 19
4. OLULISED MUUDATUSED JA VARUOSAD 21
   - 4.1. Füüsiline parandamine 22
   - 4.2. Varuosad 23
   - 4.3. Tarkvarauuendused kui olulised muudatused 24

4.4. Olulise muudatuse tagajärjed 27
4.4.1. Muu isiku kui algse tootja tehtud oluline muudatus 28
4.4.2. Algse tootja tehtud oluline muudatus 29
5. TOE KESTUS 29
5.1. Olulised muudatused ja toe kestus 31
6. DIGIELEMENTE SISALDAVAD OLULISED JA KRIITILISE TÄHTSUSEGA TOOTED 32
6.1. Põhifunktsioon 33
6.2. Digielemente sisaldavate oluliste ja kriitilise tähtsusega toodete vastavushindamine 36
6.3. Nõuetele vastavuse eeldamise mõju 38
7. KÜBERRISKIDE HINDAMINE NING DIGIELEMENTE SISALDAVATE TOODETE JA KOMPONENTIDE INTEGREERIMINE 41
7.1. Küberriskide hindamine ja nende maandamine 41
7.2. Digielemente sisaldavate toodete projekteerimine, arendamine ja tootmine sellisel viisil, et need tagaksid riskidest lähtuvalt asjakohase küberturvalisuse taseme 42
7.3. Riskihindamine ja hoolsuskohustus välise sõltuvuse ning integreeritud komponentide puhul 42
7.4. Riskihindamiste ja vastavusdokumentatsiooni taaskasutamine digielemente sisaldavate tooterühmade puhul 44
8. ANDMETE KAUGTÖÖTLUS 44
8.1. Mida käsitatakse digielemente sisaldava toote andmete kaugtöötluslahendusena? 45
8.1.1. Mõiste „distantsilt“ määratlus 46
8.1.2. Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni? 46
8.1.3. Kas tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel? 47
8.2. Andmete kaugtöötluslahenduste ja kolmandate isikute lahendustele tuginemise praktiline ja tehniline mõju 49
8.3. Andmete kaugtöötluslahenduste kasutusmallid 50
8.3.1. Mobiilpanganduse rakendus 51
8.3.2. Nutitermostaat 52
8.3.3. E-luger 53
8.3.4. Tööstusrobot 53
8.3.5. Mobiilivõrk 53
9. LISAELEMENDID 54
9.1. Teatamiskohustus 54
9.2. Nõrkuste käsitlemine 56
9.2.1. Algse projektiga seotud isikute teavitamine ja turvaparanduste jagamine 56
9.2.2. Teadaolevad ärakasutatavad nõrkused 57
9.2.3. Mõjusad ja korrapärased testid ja läbivaatamised 58
9.3. Koosmõju muude õigusaktidega 59
9.3.1. Määrus (EL) 2019/2144 ja määrus (EL) nr 168/2013 59
9.3.2. ELi tüübihindamissertifikaatide kehtivus (artikli 69 lõige 1) 59

1. **SISSEJUHATUS**

1.1. **Küberkerksuse määrus**

1. Euroopa Parlamendi ja nõukogu 23. oktoobri 2024. aasta määrus (EL) 2024/2847, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrusi (EL) nr 168/2013 ja (EL) 2019/1020 ning direktiivi (EL) 2020/1828 (küberkerksuse määrus) ([1]), jõustus 10. detsembril 2024. Määruse eesmärk on tugevdada ELi lähenemisviisi küberturvalisusele, tegeleda küberkerksuse küsimusega ELi tasandil ning parandada siseturu toimimist, kehtestades selleks ühtse õigusraamistiku, mis käsitleb digielemente sisaldavate toodete liidu turule laskmise jaoks olulisi küberturvalisuse nõudeid ning samuti olulisi küberturvalisuse nõudeid digielemente sisaldavate toodete elutsükli vältel.

2. Küberkerksuse määrus tugineb ELi uuele õigusraamistikule, mis on sätestatud Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määruses (EÜ) nr 765/2008, millega sätestatakse akrediteerimise nõuded ja tunnistatakse kehtetuks määrus (EMÜ) nr 339/93, ning Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta otsuses nr 768/2008/EÜ toodete turustamise ühise raamistiku kohta ja millega tunnistatakse kehtetuks nõukogu otsus 93/465/EMÜ ([2]).

3. Turujärelevalvet ja nõuete täitmise tagamist rakendavad riiklikud turujärelevalveasutused. Küberkerksuse määruse kohaldamisalasse kuuluvaid digielemente sisaldavaid tooteid käsitletakse Euroopa Parlamendi ja nõukogu 20. juuni 2019. aasta määruses (EL) 2019/1020 turujärelevalve ja toodete vastavuse kohta ning millega muudetakse direktiivi 2004/42/EÜ ja määruseid (EÜ) nr 765/2008 ja (EL) nr 305/2011. Komisjon ja Euroopa Liidu Küberturvalisuse Amet (edaspidi „ENISA“) toetavad ettevõtjaid ja liikmesriike küberkerksuse määruse kohaldamisel.

1.2. **Käesolevate suuniste otstarve**

4. Küberkerksuse määruse artikli 26 lõikes 1 nõutakse, et komisjon avaldaks suunised, et aidata ettevõtjatel kõnealust määrust kohaldada, pöörates erilist tähelepanu nõuete täitmise lihtsustamisele mikro- ning väikeste ja keskmise suurusega ettevõtjate jaoks. Artikli 26 lõikes 2 on sätestatud miinimumaspektid, mida tuleks suunistes käsitleda. Need on järgmised: i) küberkerksuse määruse kohaldamisala (eelkõige andmete kaugtöötluslahendused ning vaba ja avatud lähtekoodiga tarkvara), ii) toe kestuse mõiste, iii) küberkerksuse määruse ja muude ELi õigusaktide koostoime ning iv) olulise muudatuse mõiste.

5. 3. detsembril 2025 avaldas komisjon korduma kippuvate küsimuste (edaspidi „KKK“) kogumi, mille eesmärk on aidata ettevõtjatel valmistuda küberkerksuse määruse rakendamiseks ([3]).

6. Käesolevate suuniste eesmärk on aidata ettevõtjatel järgida küberkerksuse määrust ning toetada turujärelevalveasutuste, teavitavate asutuste ja teada antud asutuste tegevust, et tagada küberkerksuse määruse nõuete ühtlustatud täitmine liidus. Käesolevate suuniste eesmärk ei ole hõlmata küberkerksuse määruse kogu kohaldamisala, vaid pigem anda selgitusi teatavate peamiste sätete põhjenduse ning selle kohta, kuidas neid oleks võimalik tegelikkuses rakendada. Käesolevad suunised käsitlevad küberkerksuse määrust ja neid ei kohaldata muude ELi õigusaktide suhtes.

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

([2]) Komisjoni 2026. aasta tööprogrammiga nähakse ette Euroopa tootemääruse esitlemine, millega ajakohastatakse uut õigusraamistikku ning turujärelevalve ja standardimise norme: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52025DC0870.

([3]) KKK saab laadida alla komisjoni küberkerksuse määruse rakendamise veebisaidi sihtotstarbeliselt KKK veebilehelt.

7. Käesolevate suuniste koostamise ajal konsulteeriti ulatuslikult sidusrühmadega, sh digielemente sisaldavate toodete küberturvalisuse eksperdirühmaga ([4]), ning korraldati 3. märtsist kuni 13. aprillini 2026 toimunud avalik konsultatsioon ([5]).

8. Käesolevad suunised ei ole siduvad ettevõtjatele ega muudele osalejatele, kelle suhtes kohaldatakse küberkerksuse määrust. Küberkerksuse määruse autoriteetse tõlgenduse võib anda ainult Euroopa Liidu Kohus. Sellest hoolimata on käesolevates suunistes esitatud komisjoni tõlgendus küberkerksuse määruse kohta, et aidata kaasa nõuete täitmisele ja panustada määruse tulemuslikku rakendamisse. Lisaks sellele sisaldavad suunised mitut iseloomustavat näidet konkreetsete sätete kohaldamise kohta. Kuid nende näidete eesmärk ei ole asendada juhtumipõhist hindamist, mis on alati vajalik iga konkreetse juhtumi eripärade arvesse võtmiseks.

9. Kooskõlas küberkerksuse määruse artikliga 26 võib komisjon kaaluda täiendavate suuniste väljastamist, sh suunised, mis on mõeldud tootjatele, kelle suhtes kohaldatakse küberkerksuse määrust ja muid liidu ühtlustamisõigusakte või muid seonduvaid liidu õigusakte. Kõnealused suunised võivad näiteks käsitleda küsimusi küberkerksuse määruse ning määruse (EL) 2024/1689 (millega nähakse ette tehisintellekti käsitlevad ühtlustatud õigusnormid, edaspidi „tehisintellektimäärus“) ja määruse (EL) 2022/2554 (mis käsitleb finantssektori digitaalset tegevuskerksust, edaspidi „DORA“) omavahelise mõju kohta.

2. **KOHALDAMISALA**

2.1. **Turule laskmine**

10. Küberkerksuse määrust kohaldatakse digielemente sisaldavate toodete suhtes, mis tehakse ELi turul kättesaadavaks. Turul kättesaadavaks tegemise mõiste on määratletud küberkerksuse määruse artikli 3 punktis 22 kui „kaubandustegevuse käigus digielemente sisaldava toote tasu eest või tasuta tarnimine liidu turule kas turustamiseks või kasutamiseks“. Kooskõlas artikli 3 punktiga 21 lastakse digielemente sisaldav toode ELi turule, kui see tehakse esmakordselt kättesaadavaks.

11. ELi toote-eeskirjade rakendamist käsitleva sinise raamatu 2022. aastal avaldatud viimases väljaandes (edaspidi „sinine raamat“) ([6]) on esitatud suunised, mis aitavad mõista ELi toote-eeskirju ja nende ühtset kohaldamist eri sektoripõhistes õigusraamistikes, mis on viidud vastavusse uue õigusraamistikuga, näiteks küberkerksuse määrusega. Sinise raamatu kohaselt käivad turule laskmise ja kättesaadavaks tegemise mõisted „iga üksiku toote, mitte tootetüübi kohta, olenemata sellest, kas see toodeti üksikuna või seeriatoodanguna“ (punkt 2.3).

12. Uue õigusraamistikuga hõlmatud digielemente sisaldavate nn tavapärasemate toodete puhul, nagu riistvara digielemente sisaldavate masinate või raadioseadmete kujul, on turule laskmise kontseptsioon hästi välja kujunenud ja sinine raamat annab täiendavaid suuniseid, et selgitada, millal käsitatakse kõnealuseid tooteid turule lastuna. Sinise raamatu punktis 2.12 esitatud kokkuvõtlikud näited pakuvad täiendavaid näiteid turule laskmise mõiste kohta.

13. Kuid võttes arvesse immateriaalsete digielemente sisaldavate toodete, näiteks eraldiseisva tarkvara olemust, on vaja täiendavaid suuniseid selle kohta, millal käsitatakse kõnealuseid digielemente sisaldavaid tooteid turule lastuna. Kui tarkvara tootmisetapp on lõppenud ja digielemente sisaldavat toodet pakutakse võimalikele kasutajatele ELi turul, võib selle tootjat käsitada kui ettevõtjat, kes on tootnud digielemente sisaldavast samast tarkvaratootest mitu eksemplari ja tarninud neid turustamiseks või kasutamiseks. Tegelikkuses ei kohaldata erinevalt materiaalsetest digielemente sisaldavatest toodetest erialdiseisva tarkvara suhtes füüsilise tootmise või varude piiranguid: iga

([4]) Digielemente sisaldavate toodete küberturvalisuse eksperdirühm komisjoni eksperdirühmade ja teiste sarnaste üksuste registris.
([5]) Avalik konsultatsioon küberkerksuse määrust käsitlevate komisjoni suuniste eelnõu üle.
([6]) Komisjoni teatis „Sinine raamat ELi toote-eeskirjade rakendamise kohta (2022)“ 2022/C 247/01 (ELT C 247, 29.6.2022, lk 1).

tarkvara allalaadimise või jaotamise otstarbel kättesaadavaks tegemise toimingu tulemusena luuakse kasutaja jaoks uus identne eksemplar. Kuni seda tarkvara versiooni ei muudeta küberkerksuse määrusele vastavust mõjutaval viisil, käsitatakse ELi turule laskmist toimunuks hetkel, kui seda esimest korda turustamiseks või kasutamiseks pakutakse. Võimalust seda digielemente sisaldava tarkvaratoote versiooni seejärel alla laadida või turustada tuleb seega käsitada olukorrana, kus kõnealune digielemente sisaldav tarkvaratoode tehakse kättesaadavaks ([7]).

14. Seega tuleks digielemente sisaldavat eraldiseisvat tarkvaratoodet käsitada turule lastuna, kui selle tootmisetapp on lõppenud ja tarkvara tarnitakse esimest korda turustamiseks või kasutamiseks ELi turul äritegevuse käigus. Tuleks võtta seisukoht, et tootjad on lasknud samal ajal turule digielemente sisaldava sama tarkvaratoote mitu eksemplari. Seega, kuigi sama tarkvara mitu eksemplari jäävad digielemente sisaldavateks individuaalseteks toodeteks, käsitatakse neid samal ajal turule lastuna olenemata sellest, millal iga individuaalse eksemplari valdamine või kasutamine antakse üle teisele füüsilisele või juriidilisele isikule. Samas, kui tootja teeb tarkvara kättesaadavaks erinevate variantidena, milles sisalduvad komponendid, mille konfiguratsioon või võimaldatud funktsioonid (näiteks tugineb erinevatele operatsioonisüsteemidele või erinevaid omadusi sisaldavatele komplektidele) on erinevad, siis ei saa neid variante käsitada digielemente sisaldava sama tarkvaratoote mitme eksemplarina. Seega tuleks neid käsitada turule laskmise otstarbel kui digielemente sisaldavaid eraldiseisvaid tooteid.

Näide 1: 1. jaanuaril 2028 tarnib ettevõte A oma veebisaidi kaudu esimest korda turustamiseks oma tarkvara X versiooni 1.0.0. Samal päeval ostab klient 1 tarkvara X versiooni 1.0.0. 15. jaanuaril 2028 ostab klient 2 tarkvara X versiooni 1.0.0 eksemplari. Mõlemad tarkvara X versiooni 1.0.0 eksemplarid on turule lastud 1. jaanuaril 2028.

15. Võttes arvesse tarkvara arendamise järkjärgulist olemust, tuleks täpsemalt selgitada, et digielemente sisaldava tarkvaratoote edasisi versioone käsitatakse uute turule lastud toodetena, kui kõnealuste versioonide puhul on tegemist juba turule lastud digielemente sisaldava tarkvaratoote „olulise muutmisega“, nagu on märgitud küberkerksuse määruse põhjenduses 41. Versioonide puhul, mis ei hõlma olulist muudatust, ei nõuta tootjalt uue vastavushindamismenetluse korraldamist ning seega ei muuda need kõnealuse tarkvara turule laskmise kuupäeva. Olulise muudatuse kontseptsiooni kohta enamate suuniste saamiseks vt punkt *4 Olulised muudatused*.

Näide 2: 1. jaanuaril 2028 tarnib ettevõte A oma veebisaidi kaudu esimest korda turustamiseks tarkvara X versiooni 1.0.0. Samal päeval ostab klient 1 tarkvara X versiooni 1.0.0. 15. jaanuaril 2028 väljastab ettevõte A tarkvara X ajakohastatud versiooni 1.0.1, mida ei ole oluliselt muudetud. 30. jaanuaril 2028 ostab klient 2 tarkvara X versiooni 1.0.1 eksemplari. Tarkvara X versioonide 1.0.0 ja 1.0.1 mõlemaid eksemplare käsitatakse 1. jaanuaril 2028 turule lastuna.

16. Punktides 13, 14 ja 15 esitatud suuniseid kohaldatakse ainult juhul, kui digielemente sisaldav toode on eraldiseisev tarkvara. See ei ole nii näiteks juhul, kui tarkvara on kombineeritud riistvaraga, nagu on käsitletud punktis *2.4 Digielemente sisaldava riist- ja tarkvaratoote kombinatsioon*.

2.2. **Tarkvara kui digielemente sisaldav toode**

17. Küberkerksuse määruse artikli 3 punktis 1 on digielemente sisaldav toode määratletud kui „tarkvara- või riistvaratoode ja selle andmete kaugtöötluslahendused, kaasa arvatud tarkvara- ja riistvarakomponendid, mis lastakse turule eraldi“. Kõnealused digielemente sisaldavad tooted kuuluvad küberkerksuse määruse kohaldamisalasse, kui nende sihtotstarve või mõistlikult prognoositav kasutamine hõlmab otsest või kaudset loogilist või füüsilist ühendust seadme või võrguga andmeside eesmärgil.

([7]) Kooskõlas artikli 13 lõikega 11 võib tootja pidada avalikke tarkvaraarhiive, et kasutajatel oleks parem juurdepääs varasematele versioonidele. Sellistel juhtudel teavitatakse kasutajaid selgelt ja kergesti kättesaadaval viisil riskidest, mis kaasnevad sellise tarkvara kasutamisega, millele tuge ei pakuta.

18. Küberkerksuse määrus võib seega hõlmata mitmesuguseid digielemente sisaldavaid tooteid, sh: i) eraldiseisev tarkvara, näiteks rakendused ja arvutiprogrammid, mida turustatakse digitaalselt või füüsiliselt, ii) sissehitatud tarkvaraga riistvara (nt esemevõrgu seadmed, süle- ja tahvelarvutid), iii) eraldiseisev riistvara (nt integraallülitused, emaplaadid), ning iv) eraldi tarnitud, aga koos kasutamiseks mõeldud riistvara ja tarkvara mis tahes kombinatsioon.

19. Eraldiseisev tarkvara kuulub seega küberkerksuse määruse kohaldamisalasse, kui see lastakse turule digielemente sisaldava tootena. On kasulik eristada digielemente sisaldavaid tarkvaratooteid, mille suhtes kohaldatakse küberkerksuse määrust, ning kaugteenuste osutamist, mis ei kuulu küberkerksuse määruse kohaldamisalasse.

20. Selleks et tarkvara kuuluks küberkerksuse määruse kohaldamisalasse, peab digielemente sisaldav tarkvaratoode olema kasutajale kättesaadavaks tehtud, kasutaja peab olema selle vastu võtnud ja seda tuleb käitada kasutajapoolses elektroonilises infosüsteemis või selle osana. Tarkvara, mis laaditakse alla, installitakse või tarnitakse muul viisil kasutajale ja mis käivitub kasutaja elektroonilises infosüsteemis, vastab nendele kriteeriumidele, sh näiteks juhul, kui selle puhul on tegemist veebibrauseri laiendi või rakendusega, mis on arendatud veebitehnoloogiat kasutades, aga tarnitakse kohapeal käivitamiseks.

21. Samas tarkvara, mis käivitatakse kaugühenduse teel ja millele kasutaja saab üksnes juurdepääsu, ei ole ainult seda arvesse võttes digielemente sisaldav toode. Küberkerksuse määruse põhjendustes 11 ja 12 on tehtud see eristus, selgitades et kaugtöötlemise või -salvestamise suhtes kohaldatakse küberkerksuse määrust ainult niivõrd, kuivõrd see on vajalik digielemente sisaldava toote funktsioonide täitmiseks (s.o vastavalt artikli 3 punktis 2 määratletud andmete kaugtöötluse mõistele) ja mitte iseenesest digielemente sisaldava tootena. See on üldjuhul nii veebirakenduste, sh pseudoäppide puhul, kui neile saadakse juurdepääs ainult veebibrauseri kaudu. Sama kehtib veebisaitide puhul: kuigi veebisaite võidakse piiratud ulatuses tehniliselt käitada ja käivitada kasutaja seadmes, tuleneb küberkerksuse määruse põhjendusest 12, et veebisaite endid ei käsitata digielemente sisaldavate toodetena ning need kuuluvad küberkerksuse määruse kohaldamisalasse ainult juhul, kui need toetavad digielemente sisaldava toote funktsiooni, s.o ulatuses, milles nende puhul on tegemist andmete kaugtöötlusega (nagu on täpsemalt selgitatud punktis *8* ja eelkõige punktis *8.1.2 Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni?*).

Näide 3: rakenduste poest kasutaja alla laaditud ja oma nutitelefoni installitud mobiilirakendus tarnitakse kasutajale ja see käivitatakse kasutaja seadmes ning see on seega digielemente sisaldav toode. Kui see lastakse turule äritegevuse käigus, siis võib see kuuluda küberkerksuse määruse kohaldamisalasse.

Näide 4: veebitehnoloogia abil loodud, aga kohapealseks installimiseks pakendatud töölauarakendus tarnitakse kasutajale ja see käivitatakse kasutaja seadmes ning see on seega digielemente sisaldav toode. Kui see lastakse turule äritegevuse käigus, siis võib see kuuluda küberkerksuse määruse kohaldamisalasse.

Näide 5: veebirakendus, millele kasutaja saab juurdepääsu ainult veebibrauseri abil, ei ole digielemente sisaldav toode. Kui see ei toeta digielemente sisaldava toote funktsiooni, siis ei kuulu see küberkerksuse määruse kohaldamisalasse. Samas on rakendus, mis tarnitakse kasutajale kohapeal installimiseks, mida käitatakse kasutaja seadmes, digielemente sisaldav toode. Kui see lastakse turule äritegevuse käigus, siis võib see kuuluda küberkerksuse määruse kohaldamisalasse.

Kui see klient tugineb ühe või enama oma funktsiooni täitmiseks andmete distantsilt töötlemisele, mis vastab andmete kaugtöötluse määratlusele, siis on kõnealune andmete distantsilt töötlemine samuti digielemente sisaldava toote osa.

Näide 6: veebisait, mis lihtsalt esitab külastajatele teabe ja ei toeta digielemente sisaldava toote funktsiooni, ei ole ise digielemente sisaldav toode. Seega ei kuulu see küberkerksuse määruse kohaldamisalasse.

2.3. **Arvutikood**

22. Samuti on kasulik selgitada, kas lähtekoodi puhul saab tegemist olla digielemente sisaldava tarkvaratootega. Küberkerksuse määruses on tarkvara määratletud kui „elektroonilise infosüsteemi osa, mis koosneb arvutikoodist“ (artikli 3 punkt 4). Arvutikood võib olla i) masinakood, mille puhul on tegemist arvuti protsessori otseselt täidetavate juhiste komplektiga, mis on kirjutatud kahendvormingus, või ii) lähtekood, sh programmeerimiskeeles kirjutatud juhiste ja lausete komplekt, mis tuleb arvutis käivitamiseks kompileerida või mida tuleb selleks tõlgendada. Küberkerksuse määruses esitatud tarkvara määratlus hõlmab mõlemat.

23. Omaette küsimus on see, kas konkreetse arvutikoodi tarnimise puhul on tegemist digielemente sisaldava toote laskmisega ELi turule, mille eelduseks on äritegevuse käigus toimuv tarnimine. See ei pruugi lähtekoodi puhul sageli nii olla. Näiteks füüsilist või juriidilist isikut, kes jagab vaba ja avatud lähtekoodiga arvutikoodi üldsusele kättesaadavas hoidlas, ei käsitata üldjuhul selle koodi ELi turule laskjana küberkerksuse määruse tähenduses (nagu on täpsemalt käsitletud punktis *3 Vaba ja avatud lähtekoodiga tarkvara*). Digielemente sisaldava toote projekteerimise ja arendamise etapis (näiteks testimise või läbivaatamise eesmärgil) jagatud osalist koodi ei käsitata samuti küberkerksuse määruse tähenduses turule lastuna, kuna selle tootmisetapp ei ole lõppenud. Samal moel ei käsitata õpikute või õppematerjali osana esitatud näidis- või demokoodi küberkerksuse määruse tähenduses turule lastuna ([8]).

24. Teisest küljest, kui tootja pakub oma klientidele arvutikoodi digielemente sisaldava tootena, siis käsitatakse koodi turule lastuna olenemata sellest, kas see on masinakood või lähtekood ([9]).

Näide 7: ettevõte A annab ettevõttele B litsentsi lähtekoodi kohandatava asutusesisese platvormi jaoks ja edastab selle lähtekoodi tekstifailina. Isegi kui kõnealune lähtekood nõuab ettevõttelt B enne kasutamist täiendavat kohandamist ja kompileerimist, laseb ettevõte A selle lähtekoodi turule ning seega kohaldatakse tema suhtes küberkerksuse määrust. Ettevõte A ei vastuta selle eest, kas ettevõte B tehtud koodi edasised kohandused ja kompileerimised vastavad küberkerksuse määrusele.

2.4. **Digielemente sisaldava riist- ja tarkvaratoote kombinatsioon**

25. See, kas tarkvara on digielemente sisaldava toote osa, tuleks teha kindlaks mitte lähtuvalt sellest, kuidas või millal kõnealune tarkvara kasutajale kohale toimetatakse, vaid lähtuvalt sellest, kas toote sihtotstarvet ja mõistlikult prognoositavat kasutamist arvesse võttes on tarkvara vajalik, et digielemente sisaldav toode täidaks selle jaoks kavandatud funktsioone. Kui digielemente sisaldav riistvaratoode on projekteeritud toimima koos sama tootja pakutava konkreetse tarkvaraga oma funktsioonide täitmiseks, siis moodustavad kõnealune riistvara ja tarkvara koos digielemente sisaldava toote. Tarkvara, mis on vajalik digielemente sisaldava toote käitamiseks, seadistamiseks, juhtimiseks või kasutamiseks kooskõlas selle sihtotstarbega, on seega digielemente sisaldava toote osa, isegi kui see saadakse muu kanali kaudu (nt rakenduste pood, allalaadimise link või muu digikanal pärast digielemente sisaldava riistvaratoote turule laskmist). Seega toimub selle turuleviimine samal ajal, kui viiakse turule digielemente sisaldavad riistvaratooted.

Näide 8: võrguprinter lastakse turule digielemente sisaldava riistvaratootena, samas kui prinditööde saatmiseks, seadme konfigureerimiseks ja selle käitamise haldamiseks vajalikud tarkvaradraiverid tehakse allalaadimiseks kättesaadavaks tootja veebisaidil. Kuigi printer ja draiverid tarnitakse eri kanalite kaudu, moodustavad nad koos ühe digielemente sisaldava toote, kuna printer ei saa täita oma sihtotstarvet ilma draiveriteta.

Näide 9: kantav tervisespordi seade lastakse turule, et mõõta kasutaja südame löögikiirust ja südametegevust, ning tootja pakutav nutitelefoni rakendus on vajalik, et kuvada mõõtmistulemusi, näidata ajalugu ja võimaldada seadme konfigureerimist. Kuigi rakendus laaditakse alla eraldi äpipoe kaudu, moodustavad kantav seade koos rakendusega ühe digielemente sisaldava toote, kuna need on projekteeritud ja mõeldud koos toimima, et tagada digielemente sisaldava toote funktsioon.

([8]) Tuleks pidada meeles, et artikli 4 lõige 3 võimaldab tootjatel teha turul kättesaadavaks pooleliolevat tarkvara, mis ei vasta määruse nõuetele, näiteks alfa-, beeta- või kandidaatversioone, tingimusel et lõpetamata tarkvara tehakse kättesaadavaks üksnes selle testimiseks ja tagasiside kogumiseks vajaliku aja jooksul.

([9]) Samas tuleks tähele panna, et tootevastutuse õiguse kohaldamisel ei ole arvutikood iseenesest toode ja seega ei saa tootjaid, kes kõnealust koodi turule lasevad, võtta vastutusele direktiivi (EL) 2024/2853 (edaspidi „tootevastutuse direktiiv“) alusel. Kõnealuse direktiivi põhjenduses 13 on märgitud, et „[t]eavet ei käsitata tootena, mistõttu ei tohiks tootevastutuse norme kohaldada digifailide, näiteks meediafailide või e-raamatute sisu või pelgalt tarkvara lähtekoodi suhtes“. See ei välista võimalust, et tootjaid võidakse võtta vastutusele riigisiseste lepinguvälist vastutust käsitlevate õigusnormide alusel.

2.5. **Andmesideühendus**

26. Küberkerksuse määruse artikli 2 lõikes 1 on märgitud, et seda määrust „kohaldatakse turul kättesaadavaks tehtud digielemente sisaldavate toodete suhtes, mille sihtotstarve või mõistlikult prognoositav kasutamine hõlmab otsest või kaudset loogilist või füüsilist ühendust seadme või võrguga andmeside eesmärgil“. Küberkerksuse määruse kohaldamisala ei tugine seega ainult elektroonika olemasolule, vaid digielemente sisaldava toote võimele vahetada digitaalset teavet.

27. Kuigi mõisted „loogiline ühendus“ ja „füüsiline ühendus“ on määratletud artiklis 3, ei ole küberkerksuse määruses määratletud mõisteid „andmesideühendus“ ja „digiandmed“. Seega on kasulik esitada andmesideühenduse olemuse tõlgendus, et selgitada küberkerksuse määruse kohaldamisala piiri. Kõnealune piir on eriti oluline, et eristada digielemente sisaldavaid tooteid, mis lihtsalt kasutavad elektrisignaali, toodetest, mis osalevad digitaalses kommunikatsioonis ja puutuvad seega kokku küberriskidega.

28. Kõige lihtsamal tasandil hõlmab andmesideühendus teabe edastamist binaarvormis, s.o nullide ja ühtede jadana. Lihtsalt väljundi sisse- ja väljalülitamine (s.o 0/1) ei kujuta endast iseenesest andmesideühendust, kui nende seisundite eesmärk ei ole väljendada andmeid või neid ei loeta digisisendi kaudu. Andmesideühenduse olemasoluks peavad kahendolekud olema lähtekohas tahtlikult kodeeritud teabena ja neid peab olema võimalik sihtkohas teabena dekodeerida. Teisisõnu peab olemas olema saatja, mis tahtlikult genereerib digitaalsed sümbolid kindlaks määratud süsteemi alusel, ning vastuvõtja, mis suudab neid sümboleid andmetena tõlgendada. Kui elektrilisi või elektroonilisi signaale kasutatakse ainult funktsiooni käivitamiseks või toiteks, edastamata digitaalselt kodeeritud teavet, siis küberkerksuse määruse tähenduses andmesideühendust ei toimu ning seega ei kuulu digielemente sisaldav toode artikli 2 lõike 1 kohaldamisalasse.

2.6. **Komplekssed süsteemid**

29. Küberkerksuse määruse kohaldamisalasse kuuluvad digielemente sisaldavad tooted ei pruugi koosneda ainult ühest seadmest või tarkvarakomponendist, vaid ka komplekssetest süsteemidest, sh süsteemidest, mis koosnevad mitmest riist- ja tarkvaraelemendist, mis toimivad koos teatava funktsiooni täitmiseks. Kui kõnealune süsteem lastakse turule ühe digielemente sisaldava tootena, siis on selle puhul tegemist digielemente sisaldava tootega küberkerksuse määruse tähenduses.

30. Selliseid komplekssseid süsteeme iseloomustavad sageli pikad projekteerimis- ja arendustsüklid, lepingud, mis võivad olla allkirjastatud enne küberkerksuse määruse kohaldamise alguskuupäeva, pikendatud operatiivsed kasutusajad ning suur tehniline ja korralduslik keerukus. Kõnealused süsteemid, mis lastakse turule pärast küberkerksuse määruse kohaldamise algust, võivad tugineda enne küberkerksuse määruse kohaldamise algust turule lastud komponentidele, väljakujunenud arhitektuurile või laialdaselt kasutatud koostalitlusvõime standarditele, sh standarditele, millele on osutatud muudes ELi õigusaktides või sektoripõhistes raamistikes. Seega võib kõnealuste süsteemide teatavate tehniliste omaduste muutmine, ilma et see mõjutaks nende sihtotstarvet, ohutust, usaldusväärsust või koostalitlusvõimet olemasoleva taristuga, olla keerukas või nõuda ebaproportsionaalselt palju vaeva.

31. Kõnealused omadused ei arva iseenesest komplekssseid süsteeme välja küberkerksuse määruse kohaldamisalast. Selle asemel näitlikustavad need küberkerksuse määruse riskipõhise lähenemisviisi kohaldamist, mis võimaldab tõendada nõuetele vastavust erineval viisil, olenevalt digielemente sisaldava toote omadustest ja piirangutest, kooskõlas küberkerksuse määruse artikli 13 lõikega 3. Kõnealused omadused on selle sihtotstarbe ja kasutamise konteksti osa ning seega asjakohased, kui hinnatakse vastavust olulistele küberturvalisuse nõuetele (edaspidi „olulised nõuded“). Eelkõige on põhjenduses 55 otseselt kinnitatud, et teatavad olulised nõuded ei pruugi olla täielikult kooskõlas digielemente sisaldava toote olemusega. See võib nii olla näiteks juhul, kui nõuetele vastavus õõnestaks süsteemi nõuetekohase toimimise kohustuslikke koostalitlusvõime nõudeid.

32. Seetõttu peavad tootjad maandama küberriske lähtuvalt artikli 13 lõikes 2 osutatud küberriskide hindamisest. Nagu on selgitatud ka põhjenduses 55, ei ole konkreetsed olulised nõuded vahel kohaldatavad või neid ei saa täita tehnika tasemele vastavate turvameetmete rakendamise abil, näiteks süsteemi kavandatud sihtotstarbe tõttu, mis nõuab

digielemente sisaldava toote koostoimimist olemasolevate sõltuvustega või teatavate koostalitlusnõuete täitmist. Sellistel juhtudel peaksid tootjad tegema kindlaks kõnealused konkreetsed piirangud ja neid dokumenteerima, hindama nendega seotud riske ning rakendama sobilikud alternatiivsed või kompenseerivad riskimaandamise meetmed, et mitte õõnestada digielemente sisaldava toote turvalisust. Neil otstarvetel on nii artiklis 31 osutatud tehnilisel dokumentatsioonil kui ka II lisas osutatud kasutajatele mõeldud teabel ja juhistel oluline roll, et kirjeldada läbipaistval viisil kindlaks tehtud piiranguid, nendega seotud küberturvalisuse riske ja rakendatud riskimaandamise meetmeid. Kooskõlas kohustusega hoida riskihindamist toe kestuse vältel ajakohastatuna peaksid tootjad samuti korrapäraselt uuesti hindama, kas kõnealused piirangud on jätkuvalt olemas. Kui kõnealuseid piiranguid saab aja jooksul kõrvaldada või vähendada, siis peaksid tootjad ajakohastama digielemente sisaldavat toodet vastavalt, et see saaks jõuda lähemale sobilikule küberturvalisuse tasemele ([10]).

Näide 10: tootja laseb turule digielemente sisaldava toote, mis peab võrguprotokolli kaudu sidet väliste süsteemidega. Oluliste nõuete kohaldamise osana teeb tootja küberriskide hindamise alusel kindlaks, et digielemente sisaldava toote vahetatavate andmete konfidentsiaalsuse ja tervikluse tagamiseks tuleb kasutada turvalist sideprotokolli.

Kuid selle sihtotstarve hõlmab koostalitlusvõimet olemasolevate süsteemidega, mis toetavad ainult vanemat ja vähem turvalist protokolli. Neil juhtudel võib tootja kasutada seda protokolli, kui see on vajalik koostalitlusvõime saavutamiseks, tingimusel et sellega seotud küberturvalisuse riskid tehakse kindlaks ning neid maandatakse muul moel.

Kui digielemente sisaldava toote puhul on tehniliselt võimalik kasutada nii turvalist kui ka vähem turvalist protokolli, siis eeldatakse, et tootja rakendab turvalise protokolli ja määrab vaikimisi selle kasutamise. Vähem turvalise protokolli kasutamist lubataks ainult juhul, kui see on koostalitlusvõime jaoks vajalik.

Näide 11: tööstusautomaatika süsteemi tootja ostab enne küberkerksuse määruse kohaldamise algust mõned mikrokontrollerid. Tootja korraldab küberriskide hindamise oma tööstusautomaatika süsteemi puhul, mis lastakse turule pärast küberkerksuse määruse kohaldamise algust. Kõnealuse küberriskide hindamise kohaselt ei tee tootja kindlaks konkreetseid küberriske, mis on seotud nende mikrokontrollerite kasutamisega. Tootja integreerib mikrokontrolleri oma tööstusautomaatika süsteemi ja tagab, et digielemente sisaldav toode tervikuna (s.o tööstusautomaatika süsteem) vastab olulistele nõuetele.

2.7. **Enne küberkerksuse määruse kohaldamise algust projekteeritud digielemente sisaldavad tooted**

33. Mõnel juhul laseb tootja pärast küberkerksuse määruse kohaldamise algust 11. detsembril 2027 turule digielemente sisaldavad tooted, mis on valmistatud vastavalt tüübile või mudelile, mis projekteeriti ja töötati välja enne kõnealuse määruse kohaldamise algust. Neil juhtudel ei nõua selle määruse järgimine ilmtingimata, et kõnealuseid digielemente sisaldavad tooteühikud ümber projekteeritaks. Tootja peab korraldama küberriskide hindamise kooskõlas küberkerksuse määruse artikli 13 lõikega 2, et teha digielemente sisaldava toote sihtotstarbe ja mõistlikult prognoositava kasutamise alusel kindlaks, millised I lisa I osa olulised nõuded on kõnealuse digielemente sisaldava toote suhtes kohaldatavad ja kuidas neid nõudeid täidetakse.

34. Kui kõnealuse riskihindamise tulemusena on näha, et digielemente sisaldav toode juba hõlmab sobilikke ja tulemuslikke turvameetmeid, mis maandavad asjakohaseid riske, siis võib tootja tugineda kõnealustele olemasolevatele meetmetele, et tõendada vastavust küberkerksuse määrusele. Küberkerksuse määrusega ei kehtestata iseenesest kohustust võtta kasutusele uusi turvaomadusi või digielemente sisaldav toode ümber projekteerida, kui see ei ole vajalik kindlaks tehtud riskide maandamiseks.

([10]) Tuleks märkida, et käesolevas punktis esitatud kaalutlused võivad olla kohaldatavad, nagu on asjakohane, kõigi küberkerksuse määruse kohaldamisalasse kuuluvate digielemente sisaldavate toodete ja mitte ainult komplekssüsteemide suhtes.

35. Sellest hoolimata kohaldatakse tootja suhtes jätkuvalt küberkerksuse määruses kehtestatud kohustusi. Need hõlmavad enne digielemente sisaldava toote turule laskmist veendumist, et kohaldatav vastavushindamismenetlus on tehtud, ELi vastavusdeklaratsioon on koostatud ja CE-märgis on lisatud. Nende nõuete täitmine ei olene sellest, kas digielemente sisaldava toote projekteerimist oli vaja riskihindamise tulemusena muuta. Enne küberkerksuse määruse kohaldamise alguskuupäeva projekteeritud digielemente sisaldavate toodete puhul, mis lastakse turule pärast kõnealust kuupäeva, tuleks juhul, kui tootjal ei ole võimalik tõendada, kuidas riskihindamist on digielemente sisaldava toote projekteerimise ja arendamise etapis arvesse võetud, mõista artikli 13 lõikes 2 sätestatud kohustust selliselt, et sellega nõutakse tootjatelt küberriskide hindamist ja selle alusel tõendamist, et digielemente sisaldav toode sisaldab piisavaid turvameetmeid, et minimeerida küberriske, ennetada intsidente ja minimeerida nende mõju, sealhulgas seoses kasutajate tervise ja ohutusega.

36. Seega võidakse enne küberkerksuse määruse kohaldamise alguskuupäeva projekteeritud digielemente sisaldavad tooted lasta turule küberkerksuse määruse alusel ilma ümber projekteerimata, kui tootja suudab küberriskide hindamise ja tehnilise dokumentatsiooni alusel tõendada, et digielemente sisaldava toote puhul saavutatakse sobilik küberturvalisuse tase, võttes arvesse selle sihtotstarvet ja mõistlikult prognoositavat kasutamist, ning see vastab olulistele küberturvalisuse nõuetele.

37. Samuti on kasulik selgitada vastavushindamise kohustuste kohaldamist pärast küberkerksuse määruse kohaldamise alguskuupäeva turule lastud digielemente sisaldavate toodete tootjate suhtes, kui need tooted on toodetud enne kõnealust kuupäeva projekteeritud ja arendatud tüübi või mudeli alusel. Artikli 13 lõike 12 kohaselt peab tootja tõendama asjakohase vastavushindamismenetluse alusel, et digielemente sisaldav toode vastab kohaldatavatele olulistele nõuetele, ning lisama seda käsitlevad tõendid toote tehnilisse dokumentatsiooni (VII lisa punkt 6).

38. Kuid nende nõuete kohaldamist tuleb tõlgendada, võttes arvesse digielemente sisaldava toote küberriskide hindamist ja küberriski profiili. Eelkõige enne küberkerksuse määruse kohaldamise alguskuupäeva projekteeritud (kuid pärast kõnealust kuupäeva turule lastud) digielemente sisaldavate toodete puhul, mis on läbinud artikli 32 lõike 1 kohased vastavushindamismenetlused, ei tohiks juhul, kui kõnealune riskihindamine näitab, et digielemente sisaldav toode juba sisaldab kohaseid ja tulemuslikke turvameetmeid, mis maandavad toote riske, mõista vastavushindamismenetluse raames tõendite esitamise kohustust selliselt, et sellega nõutakse tootjalt testitulemuste esitamist, mis hõlmavad kõnealuste digielemente sisaldavate toodete algset projekteerimise ja arendamise etappi. See ei oleks vajalik, kuna see ei suurendaks digielemente sisaldava toote enda turvalisust. Kui testid võivad sellest hoolimata vajalikud olla, ei nõuta tootjatelt tõendeid kõigi tootevariantide testimise kohta, vaid nad saavad rühmitada kõnealused testid digielemente sisaldavate tooterühmade kaupa, nagu on täpsemalt käsitletud punktis *7.4 Riskihindamiste ja vastavusdokumentatsiooni taaskasutamine digielemente sisaldavate tooterühmade puhul*.

39. Sellest hoolimata peaks tootja esitama tõendid selle kohta, kuidas ta järgib I lisa II osas sätestatud nõrkuste käsitlemise protsesse; ta peaks hoidma oma riskihindamist ajakohastatuna kooskõlas artikli 13 lõikega 3 ning täitma kõiki muid küberkerksuse määruses sätestatud kohustusi, sh esitades kasutajatele teabe ja juhised kooskõlas artikli 13 lõikega 18.

Näide 12: tootja laseb turule mikrokontrolleri, mis projekteeriti ja arendati enne küberkerksuse määruse kohaldamise alguskuupäeva. Mikrokontroller on kavas integreerida mitmesugustesse digielemente sisaldavatesse elektroonikatoodetesse, sh ühenduvusfunktsiooniga digielemente sisaldavatesse toodetesse.

Enne seda, kui tootja laseb pärast küberkerksuse määruse kohaldamise alguskuupäeva turule uued mikrokontrollerite eksemplarid, teeb ta küberriskide hindamise kooskõlas artikli 13 lõikega 2. Mikrokontrolleri sihtotstarbe ja mõistlikult prognoositava kasutamise alusel teeb tootja kindlaks asjakohased küberriskid, näiteks loata juurdepääs, tarkvara või andmetega manipuleerimine ning kättesaadavate liideste väärkasutamine.

Riskihindamise tulemus näitab, et mikrokontroller juba sisaldab algselt projekteeritud kujul kohaseid ja tulemuslikke turvameetmeid kindlaks tehtud riskide maandamiseks. Tootja järeldab seega, et digielemente sisaldav toode vastab I lisa I osas märgitud asjakohastele olulistele nõuetele ning et ümberprojekteerimine ega täiendavate turvafunktsioonide kasutusele võtmine ei ole vajalik.

Kui ei ole võimalik tõendada, kuidas küberriskide hindamist algse projekteerimis- ja arendusetapi ajal arvesse võeti, siis dokumenteerib tootja praeguse küberriskide hindamise ja selgitab, kuidas olemasolev lahendus ja kehtivad meetmed maandavad kindlaks tehtud riske. Tootja ei pea taastama varasemat projekteerimis- või testimisdokumentatsiooni, kuna see ei aitaks suurendada digielemente sisaldava toote küberturvalisust. Kui mikrokontrolleri mitu varianti põhinevad samal lahendusel ja neil on sama küberturvalisuse riskiprofiil, siis võib tootja tugineda ka asjakohast tooteperekonda hõlmavatele esindavatele tõenditele.

Tootja peab samuti tagama vastavuse I lisa II osas sätestatud nõrkuste käsitlemise nõuetele, sh hoides kasutuses protsesse nõrkuste arvesse võtmiseks ja kõrvaldamiseks ning vaadates küberriskide hindamise korrapäraselt läbi kooskõlas artikli 13 lõikega 3.

Sellistel asjaoludel võib enne küberkerksuse määruse kohaldamise alguskuupäeva projekteeritud mikrokontroller lasta turule küberkerksuse määruse alusel ilma ümber projekteerimata, kui tootja suudab küberriskide hindamise ja tehnilise dokumentatsiooni alusel tõendada, et mikrokontrolleri puhul saavutatakse sobilik küberturvalisuse tase, võttes arvesse selle sihtotstarvet ja mõistlikult prognoositavat kasutamist, ning see vastab olulistele küberturvalisuse nõuetele.

3. **VABA JA AVATUD LÄHTEKOODIGA TARKVARA**

40. Nagu on märgitud punktis *2.1 Turule laskmine*, kohaldatakse küberkerksuse määrust digielemente sisaldavate toodete suhtes, mis tehakse ELi turul äritegevuse käigus esmakordselt kättesaadavaks (s.o „lastakse turule“) ning mis tahes edasiste juhtumite suhtes, mille puhul on tegemist sama digielemente sisaldava toote turul kättesaadavaks tegemisega. Sinises raamatus (punkt 2.2) selgitatakse, et äritegevus on kaupade pakkumine ärilises kontekstis tasu eest või tasuta, mida saab hinnata ainult juhtumipõhiselt, võttes arvesse tarnimise korrapärasust, toote omadusi, tarnija kavatsusi jne.

41. Äritegevuse käigus toimuvat tarnimist iseloomustavad mitmesugused asjaolud, mis on põhjalikult dokumenteeritud sinises raamatus ja käsitletud küberkerksuse määruse põhjenduses 15. Need võivad hõlmata otsest hinna küsimist, ning samuti „tehniliste tugiteenuste eest hinna [---] [küsimist], kui see ei täida ainult tegelike kulude katmise eesmärki, kui selle eest on kavatsus tulu teenida näiteks tarkvaraplatvormi pakkumisega, mille kaudu tootja teenib tulu muude teenuste eest, nõudes kasutamise eeltingimusena isikuandmete töötlemist muul otstarbel kui üksnes tarkvara turvalisuse, ühilduvuse või koostalitlusvõime parandamiseks, või võttes vastu annetusi, mis ületavad digielemente sisaldava toote projekteerimise, väljatöötamise ja pakkumisega seotud kulusid“ (põhjendus 15) ([11]).

42. Küberkerksuse määruses võetakse siiski arvesse vaba ja avatud lähtekoodiga tarkvara arendamise ja avaldamise eri meetodite eripärasid ning antakse teatavaid suuniseid, et aidata teha kindlaks, millal vaba ja avatud lähtekoodiga tarkvara on (äritegevuse käigus) turule lastud digielemente sisaldav toode küberkerksuse määruse tähenduses. Nagu on märgitud põhjenduses 18, „ei tohiks selle kindlaksmääramisel, kas niisuguse tegevuse olemus on äriline või mitte, võtta arvesse üksnes asjaolusid, mille korral digielemente sisaldavat toodet on arendatud, või seda, kuidas arendamist on rahastatud“. Täpsemalt „ei tohiks [---] käsitada äritegevusena selliste digielemente sisaldavate toodete pakkumist, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana, millega tootjad ei teeni tulu, et tagada arendus- ja tarneetappide selge eristamine“.

([11]) Samuti tuleb silmas pidada, et kuigi digielemente sisaldavate toodete eest teenitakse sageli tulu (samuti) isikuandmete töötlemise teel, on isikuandmete kaitse põhiõigus ja seega ei saa isikuandmeid käsitada kaubana, nagu on märgitud Euroopa Parlamendi ja nõukogu 20. mai 2019. aasta direktiivi (EL) 2019/770 (digisisu üleandmise ja digiteenuste osutamise lepingute teatavate aspektide kohta (*ELT L 136, 22.5.2019, lk 1*, ELI: http://data.europa.eu/eli/dir/2019/770/oj) põhjenduses 24.

43. Seetõttu on kasulik i) selgitada, mis on vaba ja avatud lähtekoodiga tarkvara, ii) millal peetakse seda füüsilise või juriidilise isiku vastutuse alla kuuluvaks ning iii) esitada näiteid, mis aitavad sidusrühmadel mõista, millal on vaba ja avatud lähtekoodiga tarkvara turustamise puhul tegemist turule laskmisega. Kui vaba ja avatud lähtekoodiga tarkvara turule ei lasta, siis jääb see küberkerksuse määruse kohaldamisalast välja, v.a juhul, kui selle avaldanud üksus on juriidiline isik, kes vastab artikli 3 punktis 14 esitatud „avatud lähtekoodiga tarkvara korraldaja“ (edaspidi „korraldaja“) mõistele. Sellisel juhul kohaldatakse tema suhtes ainult artiklis 24 sätestatud kohustusi.

44. Artikli 3 punktis 48 on vaba ja avatud lähtekoodiga tarkvara määratletud kui „tarkvara, mille lähtekoodi jagatakse avalikult ja mis tehakse kättesaadavaks vaba ja avatud lähtekoodi litsentsi alusel, mis annab kõik õigused teha see vabalt kättesaadavaks, kasutatavaks, muudetavaks ja turustatavaks“. Kuigi käesolevates suunistes ei määrata kindlaks konkreetset vaba ja avatud lähtekoodi litsentsi, mis on kooskõlas artikli 3 punktis 48 esitatud määratlusega, tuleneb kõnealuse sätte sõnastusest, et küberkerksuse määruse tähenduses on vaba ja avatud lähtekoodiga tarkvara ainult tarkvara, mis vastab mõlemale järgmisele tingimusele: i) tarkvara tuleb teha kättesaadavaks vaba ja avatud lähtekoodi litsentsi alusel, millega antakse kõik artikli 3 punktis 48 osutatud õigused, ning ii) selle lähtekoodi tuleb avalikult jagada.

45. Nõue, et tarkvara litsents oleks vabalt kättesaadav, kasutatav, muudetav ja turustatav, kajastab tavapärast arusaama vabast ja avatud lähtekoodiga tarkvarast, mille kohaselt peab olema kasutajatel juurdepääs lähtekoodile, nad peavad saama seda põhjendamatute piiranguteta kasutada, seda muuta ja edasi levitada selle orginaalversiooni või muudetud versioone. Juurdepääs lähtekoodile on seega vajalik eeltingimus muude õiguste kasutamiseks: ilma lähtekoodile juurdepääsuta on praktiliselt võimatu tarkvara muuta või seda tähenduslikult korduskasutada.

46. Kuid artikli 3 lõige 48 läheb kaugemale ainult litsentsi tingimustele osutamisest, kuna sellega nõutakse otseselt, et lähtekoodi jagataks avalikult. Avalikult jagamise mõiste osutab sellele, et lähtekood peab olema üldsusele kättesaadav (kas algses või järgnevas etapis) ning seda ei tohi pakkuda ainult piiratud olukorras või tingimuste alusel. Seega ei peeta artikli 3 lõike 48 tähenduses vaba ja avatud lähtekoodiga tarkvaraks tarkvara, mida jaotatakse vaba ja avatud lähtekoodi litsentsi alusel, aga mille lähtekoodi jagatakse (või jagamist lubatakse) ainult maksvatele klientidele või kasutajate piiratud rühmale. Seega tuleks küberkerksuse määruse kohaldamisel käsitada vaba ja avatud lähtekoodiga tarkvarana ainult tarkvara, mille lähtekood on üldsusele kättesaadav ja mis on litsentsitud vaba ja avatud lähtekoodi litsentsi alusel, mis annab kõik artikli 3 punktis 48 osutatud õigused.

3.1. **Kindakstegemine, kas vaba ja avatud lähtekoodiga tarkvara kuulub isiku vastutusalasse**

47. Küberkerksuse määrusega pannakse olulised kohustused ettevõtjatele, kes tarnivad digielemente sisaldavaid tooteid ELi turul. Selles on määratletud tootja füüsilise või juriidilise isikuna, kes tarnib digielemente sisaldavat toodet oma nime või kaubamärgi all ja teeb seda äritegevuse käigus (lastes seeläbi selle turule). Samal moel on importija ELis asutatud füüsiline või juriidiline isik, kes tarnib väljaspool ELi asutatud isiku digielemente sisaldavat toodet ja teeb seda äritegevuse käigus (lastes seeläbi selle turule). Korraldajate kohustused kehtivad juriidilise isiku suhtes, kes tarnib äritegevuseks mõeldud vaba ja avatud lähtekoodiga tarkvara ([12]), kuid ei lase seda turule küberkerksuse määruse tähenduses.

48. Seega, selleks et teha kindlaks, kas füüsiline või juriidiline isik laseb vaba ja avatud lähtekoodiga tarkvara ELi turule, tuleb kõigepealt välja selgitada, kas füüsiline või juriidiline isik tegelikult tarnib vaba ja avatud lähtekoodiga tarkvara. Küberkerksuse määruse alusel kohaldatavate kohustuste nõuetekohaseks kindlaksmääramiseks on hädavajalik teha kindlaks, kas füüsiline või juriidiline isik teostab tõepoolest vaba ja avatud lähtekoodiga tarkvara tarnimist. Nagu on märgitud põhjenduses 18, ei kohaldata küberkerksuse määrust füüsiliste või juriidiliste isikute suhtes, kes panustavad lähtekoodiga sellistesse digielemente sisaldavatesse toodetesse, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ja mis ei kuulu nende vastutusalasse.

([12]) See on vajalik, aga mitte piisav tingimus, et juriidiline isik kvalifitseeruks avatud lähtekoodiga tarkvara korraldajaks, kuna artikli 3 punktis 14 esitatud määratlusega kehtestatakse juriidilisele isikule korraldajana käsitamiseks täiendavad tingimused.

49. Võttes arvesse vaba ja avatud lähtekoodiga tarkvara arendamise eripärasid, mis hõlmab sageli mitut edasiarendajat, detsentraliseeritud koostöömudeleid ning panustavate ja otsuseid tegevate isikute eristamist, on kasulik selgitada, et vaba ja avatud lähtekoodiga tarkvara käsitatakse selle füüsilise või juriidilise isiku vastutusalasse kuuluvana, kes selle avaldab ja kellel on peamine kontroll selle arendamise, väljaandmise ja levitamise otsuste üle (kellele osutatakse sageli nimetusega „hooldaja“) Isikuid, kes panustavad lähtekoodi, aga ei mõjuta väljalaskeid, tegevuskavasid ega juhtimisotsuseid, käsitatakse „edasiarendajatena“ ning neil juhtudel ei kuulu vaba ja avatud lähtekoodiga tarkvara nende vastutusalasse, kuigi nad panustasid sellesse lähtekoodi. Pelgalt tehniliste õiguste – näiteks muudatuste sisseviimise õiguse – olemasolu ei ole piisav selle kindlaks tegemiseks, et vaba ja avatud lähtekoodiga tarkvara kuulub kõnealuse isiku vastutusalasse, vastutus lasub neil, kes tarkvara avaldavad ja kontrollivad.

Näide 13: üksikarendaja või ettevõtte töötaja esitab koodi ühendamise või mestimise taotluse, mis sisaldab vaba ja avatud lähtekoodiga tarkvara projekti turbepaika või uut funktsiooni. Projekti haldajad vaatavad koodi läbi, kiidavad selle heaks ja lõimivad põhihoidlasse ning seejärel uude versiooni. Selles stsenaariumis on muutmistaotluse esitanud isik „edasiarendaja“ ja tema suhtes ei kohaldata küberkerksuse määrust. Kuigi see isik panustas lähtekoodi, ei ole tema käes esmast kontrolli arenduse, versioonide väljalaskmise või levitamisotsuste üle.

3.2. **Kindlakstegemine, kas vaba ja avatud lähtekoodiga tarkvara lastakse ELi turule**

50. Kui tehakse kindlaks, et vaba ja avatud lähtekoodiga tarkvara kuulub füüsilise või juriidilise isiku vastutusalasse, siis tuleb teha kindlaks, kas kõnealune isik tarnib seda äritegevuse käigus, mille puhul on tegemist turule laskmisega.

3.2.1. *Tasu küsimine*

51. Kui füüsiline või juriidiline isik, kes tarnib vaba ja avatud lähtekoodiga tarkvara, küsib tarkvara enda eest tasu (näiteks eelkompileeritud kahendkoodi eest), siis laseb kõnealune isik turule digielemente sisaldava toote. Kõnealune vaba ja avatud lähtekoodiga tarkvara turule laskev isik on seega tootja küberkerksuse määruse tähenduses.

52. Vaba ja avatud lähtekoodiga tarkvara tootjad tarnivad sageli tasuta tarkvara versioone (sageli nimetatakse neid kogukonnaversioonideks), mille koodibaas on (peaaegu) identne tasulise versiooniga. Need digielemente sisaldavad tooted on siiski erinevad tooted: tasulise versiooni eest teenitakse mingil viisil tulu (näiteks küsides tasu või muul käesolevas punktis käsitletud viisil) ja seega käsitatakse seda turule lastuna, millest tulenevad tootja kohustused. Tasuta pakutav versioon (ehk kogukonna versioon) ei teeni tulu ja seega ei käsitata seda küberkerksuse määruse kohaldamisel turule lastuna. See on samuti nii juhul, kui tasuline versioon on nn täiustatud kaubanduslik versioon, mis laiendab tasuta pakutava versiooni koodibaasi või lõimib selle versiooni laiemasse digielemente sisaldavasse tootesse (nt *open-core* mudeli puhul (avatud tuuma mudel)).

53. Kui kogukonna versiooni tarniv isik on juriidiline isik, kohaldatakse kõnealuse juriidilise isiku suhtes korraldajate kohustusi ka tema tasuta tarnitava versiooni (kogukonnaversiooni) puhul. Kui tegemist on füüsilise isikuga, siis ei kuulu tasuta tarnitav versioon (kogukonnaversioon) küberkerksuse määruse kohaldamisalasse.

3.2.2. *Muude teenuste eest tasu saamine või isikuandmete töötlemise vajadus*

54. Füüsiline või juriidiline isik, kes avaldab vaba ja avatud lähtekoodiga tarkvara, võib samuti lasta seda turule (s.o tarnida seda äritegevuse käigus), kui ta pakub tarkvara, mille kaudu ta teenib tulu oma muudelt digielemente sisaldavatelt toodetelt või teenustelt, või kui ta nõuab kasutamise tingimusena isikuandmete töötlemist muul põhjusel kui ainult tarkvara turvalisuse, ühilduvuse või koostalitlusvõime parandamine.

Näide 14: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga kauplemiskoha rakenduse. Rakendus on saadaval tasuta ja see võimaldab kasutajatel osta selle kaudu kaupa või teenuseid. Rakendus võimaldab selle avaldajal saada tasu selle kaudu pakutavate muude digielemente sisaldavate toodete ja teenuste eest (nt reklaami, komisjonitasude või tellimustasude kaudu). Seega käsitatakse rakendust äritegevuse käigus turule lastuna.

Näide 15: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga virtuaalse privaatvõrgu (edaspidi VPN). Rakendus on tasuta kättesaadav, kuid võimaldab kasutajatel maksta täiendavatele serveritele või püsivatele IP-aadressidele juurdepääsu eest See rakendus võimaldab isikul saada tasu selle kaudu pakutavate muude teenuste eest ja seega käsitatakse seda äritegevuse käigus turule lastuna.

Näide 16: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga treeningu jälgimise rakenduse. Rakendus on tasuta kättesaadav, aga selle kasutamine on seotud kasutajate isikuandmete töötlemisega sellistel eesmärkidel nagu isikustatud reklaam või analüütika, mis ei ole seotud tarkvara turvalisuse, ühilduvuse ega koostalitlusvõimega. Kuna sellist andmete töötlemist nõutakse kasutamise eeltingimusena, käsitatakse rakendust seega äritegevuse käigus turule lastuna.

3.2.3. *Tugiteenused*

55. Lihtsalt fakt, et vaba ja avatud lähtekoodiga tarkvara avaldav füüsiline või juriidiline isik pakub sellega seoses ka tasulisi tugiteenuseid, ei tähenda iseenesest, et digielemente sisaldavat toodet tarnitakse äritegevuse käigus. Tugiteenused võivad hõlmata sellist tegevust nagu nõustamine, koolitus või erialased teenused, mis on seotud tarkvara kliendipoolse kasutamise, konfigureerimise ja kasutuselevõtuga ning tarkvara dokumentatsiooniga.

56. Määrav tegur on see, kas juurdepääs vabale ja avatud lähtekoodiga tarkvarale endale (s.o digielemente sisaldava toote pakkumine), sh selle hooldus, on seotud tasu maksmisega, mitte aga pelgalt professionaalsete teenuste pakkumine seoses vabalt kättesaadava digielemente sisaldava tootega, nagu on märgitud küberkerksuse määruse põhjenduses 18 („ei tohiks [---] käsitada äritegevusena selliste digielemente sisaldavate toodete pakkumist, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana, millega tootjad ei teeni tulu“). Kui vaba ja avatud lähtekoodiga tarkvara saab vabalt alla laadida ja installida ning kasutajad saavad vabalt valida, kas osta eraldi kutsealaseid teenuseid, siis ei käsitata kõnealust vaba ja avatud lähtekoodiga tarkvara turule lastuna.

57. Samas on teatavatel juhtudel juurdepääs digielemente sisaldava toote konkreetsele versioonile, mis hõlmab teatud hüvesid, nagu tehnilisele abile või jõudluse optimeerimisele, seotud tasu maksmisega. Sellisel juhul kujutab see endast digielemente sisaldava toote tasulist pakkumist äritegevuse käigus ning toode loetakse seega turule lastuks See hõlmab juhtumeid, mil tasuline väljaanne või ettevõtetele mõeldud versioon tehakse kättesaadavaks ärilepingu alusel, olenemata sellest, kas funktsionaalselt võrdväärne tarkvara on saadaval ka tasuta vaba ja avatud lähtekoodiga litsentsi alusel.

Näide 17: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga operatsioonisüsteemi, pakkudes kõnealuse operatsioonisüsteemi tasulist versiooni, mis sisaldab tugiteenuseid, näiteks tehniline abi või jõudluse optimeerimine. Operatsioonisüsteemi tasulist versiooni käsitatakse äritegevuse käigus turule lastuna.

Näide 18: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga käsureatööriista. Tööriist on tasuta kättesaadav ning kõik saavad selle alla laadida ja installida. Kõnealune füüsiline või juriidiline isik pakub eraldi erialaseid teenuseid, näiteks valikulisi nõustamisteenuseid kasutajate koolitamiseks ning nende toetamiseks tööriista installimisel ja kasutamisel. Sellist vaba ja avatud lähtekoodiga tarkvara ei käsitata küberkerksuse määruse tähenduses turule lastuna.

58. Eelkõige füüsiliste isikute puhul, kes avaldavad vaba ja avatud lähtekoodiga tarkvara, ei kvalifitseeruks digielemente sisaldava tootega otseselt seotud tehnilise abi pakkumine ikkagi äritegevuseks, kui küsitud tasu katab ainult tegelikult tekkinud kulud, nagu on märgitud küberkerksuse määruse põhjenduses 15. Need tegelikud kulud hõlmavad mitmesuguseid kulusid, mis on seotud selle tarkvara projekteerimise, arendamise ja hooldamisega, sh inimeste mõistlike elamiskuludega. Seega ei käsitata füüsilist isikut, kes avaldab vaba ja avatud lähtekoodiga tarkvara ning pakub tehnilist abi oma kulude katmiseks ja õiglase tasu saamiseks, ainult sellest lähtuvalt tarkvara ELi turule laskvana.

59. Füüsilist või juriidilist isikut, kes pakub tehnilist abi seoses vaba ja avatud lähtekoodiga tarkvaraga, mis ei kuulu tema vastutusalasse, ei käsitata kõnealust tarkvara turule laskvana, v.a juhul, kui see isik muudab abi andmise osana vaba ja avatud lähtekoodiga tarkvara oluliselt kooskõlas artikliga 22.

Näide 19: teenuseosutaja ei avalda vaba ja avatud lähtekoodiga tarkvara, vaid aitab kliendil installida selle kliendi ruumides asuvasse serverisse. Ta teeb seda ilma nimetatud tarkvara oluliselt muutmata. Teenuseosutajat ei käsitata seega kõnealuse vaba ja avatud lähtekoodiga tarkvara turule laskjana.

3.2.4. *Annetused*

60. Vaba ja avatud lähtekoodiga tarkvara projekte avaldavad füüsilised või juriidilised isikud pakuvad kasutajatele regulaarselt võimalust teha vabatahtlikke rahalisi annetusi, et tänada projekti avaldajat (avaldajaid) ning tagada projekti aktiivne edasine hooldus.

61. Nagu on märgitud küberkerksuse määruse põhjenduses 15, ei tohiks „[a]nnetuste vastuvõtmist kasumi saamise kavatsuseta [---] käsitada äritegevusena“. Lihtsalt fakti, et on lisatud link annetusplatvormile või samalaadsele vahendile annetuste kogumiseks, ei tohiks käsitada kasumi saamise kavatsusena, isegi kui annetuste kaudu kogutud summa ületab digielemente sisaldava toote projekteerimise, arendamise ja tagamisega seotud kulud. See hõlmab mõistlikku hüvitist juriidilise isiku palgatud edasiarendajatele ja/või füüsilise isiku mõistlikke elamiskulusid. Annetused kõiguvad oma olemuselt aja jooksul ning seega tuleb rakendada teataval määral paindlikkust, kui hinnatakse, kas ainult annetuste kaudu rahastatud vaba ja avatud lähtekoodiga tarkvara käsitatakse turule lastuna. Seega on ebatõenäoline, et ainult annetuste kaudu toetatud vaba ja avatud lähtekoodiga tarkvara käsitatakse küberkerksuse määruse tähenduses turule lastuna.

Näide 20: füüsiline või juriidiline isik avaldab vaba ja avatud lähtekoodiga tarkvara tööriista avalikus veebihoidlas, võimaldades igaühel seda vaba ja avatud lähtekoodiga litsentsi alusel alla laadida, kasutada, muuta ja edasi levitada. Väljaandja kutsub kasutajaid tegema annetusplatvormi kaudu vabatahtlikke annetusi, et toetada projekti jätkuvat arendamist ja käigus hoidmist. Annetuse tegemine ei ole tarkvarale, selle lähtekoodile ega uuendustele juurdepääsu saamise tingimuseks. Seda vaba ja avatud lähtekoodiga tarkvara ei käsitata äritegevuse käigus tarnituna ega turule lastuna küberkerksuse määruse tähenduses.

62. Selles hoolimata on juhtumeid, kui annetuste kaudu toetatud vaba ja avatud lähtekoodiga tarkvara võib käsitada turule lastuna. See on nii juhul, kui asjaolude üldise hindamise tulemusena on annetused *de facto* võrdväärsed digielemente sisaldavale tootele või selle teatavatele funktsioonidele juurepääsu eest tasu küsimisega. See võib olla nii eelkõige juhul, kui vabale ja avatud lähtekoodiga tarkvarale, selle olulistele funktsioonidele või uuendustele juurdepääsu eeltingimus on tegelikkuses annetuse tegemine või kui annetustega kaasnevad lepingulised hüved või ainuõiguslikud eelised, mis ületavad kogukonnale pakutavaid hüvesid.

Näide 21: füüsiline või juriidiline isik avaldab digielemente sisaldava tarkvaratoote vaba ja avatud lähtekoodi litsentsi alusel, kuid pakub allalaaditavaid versioone ja turvauuendusi ainult annetuse teinud kasutajatele. Kasutajatel, kes ei ole annetust teinud, puudub juurdepääs tarkvara praegusele versioonile.

Sel juhul on annetused de facto tingimus digielemente sisaldavale tootele juurdepääsu saamiseks ja seega võrdväärsed tasu küsimisega. Kõnealust vaba ja avatud lähtekoodiga tarkvara käsitatakse seega küberkerksuse määruse tähenduses turule lastuna.

Näide 22: füüsiline või juriidiline isik teeb vaba ja avatud lähtekoodiga tarkvara avalikult kättesaadavaks, kuid pakub eelnevalt kompileeritud kahendkoodi, korrapäraseid uuendusi ja tagatud turvaparandusi ainult annetajatele. Sel juhul on annetused seotud digielemente sisaldava toote olulistele aspektidele juurdepääsuga ja kujutavad endast tasu toote tarnimise eest. Sellist vaba ja avatud lähtekoodiga tarkvara käsitatakse seega äritegevuse käigus turule lastuna.

3.2.5. *Vaba ja avatud lähtekoodiga tarkvara rahastamine*

63. Lihtsalt fakt, et kolmas isik on vaba ja avatud lähtekoodiga tarkvara arendamise kinni maksnud, seda sponsinud või muul viisil rahastanud, ei määra iseenesest kindlaks, kas vaba ja avatud lähtekoodiga tarkvara on turule lastud. Vaba ja avatud lähtekoodiga tarkvara ökosüsteemis on tavapärane, et individuaalsed arendajad, fondid või kogukonnad saavad rahastamist ettevõtetelt, avaliku sektori asutustelt või muudelt sponsoritelt, et arendada konkreetseid funktsioone, kõrvaldada programmivigu või hooldada kriitilisi komponente. See rahastamine võib toimuda mitmel kujul, sh toetused, puugipreemiad, sponsorlus, teenuslepingud või tasuline arendustöö.

64. Nagu on juba märgitud, selgitatakse küberkerksuse määruse põhjenduses 18, et selle kindlaksmääramisel, kas tegevuse olemus on äriline, ei tohiks võtta arvesse üksnes asjaolusid, mille korral digielemente sisaldavat toodet on arendatud, või seda, kuidas arendamist on rahastatud.

65. Seega, kui vaba ja avatud lähtekoodiga tarkvara jagatakse avalikult ja see tehakse kõigile vabalt kättesaadavaks juurdepääsu saamiseks, kasutamiseks, muutmiseks ja levitamiseks, ei tohiks asjaolu, et ärierttevõtja võib olla projekti eest tasunud, mõjutada selle kindlaks määramist, kas tarkvara on turule lastud. Kui kõnealuselt vaba ja avatud lähtekoodiga tarkvaralt muul viisil tulu ei teenita, siis ei käsitata seda turule lastuna. Kui vaba ja avatud lähtekoodiga tarkvara arendamist rahastanud ettevõte (ning mis tahes muu ettevõte) integreerib selle oma digielemente sisaldavasse tootesse, siis peab kõnealune ettevõte täitma hoolsuskohustust kooskõlas küberkerksuse määruse artikli 13 lõikega 5.

Näide 23: individuaalne arendaja avaldab vaba ja avatud lähtekoodiga tarkvara projekti ja hoiab seda aktiivselt käigus. Tootja A taotleb, et individuaalne arendaja lisaks kõnealusele vabale ja avatud lähtekoodiga tarkvarale konkreetse funktsiooni, ning rahastab seda arendustegevust. Arendaja lisab selle funktsiooni vaba ja avatud lähtekoodiga tarkvara koodibaasi, jagab seda avalikult ja teeb selle kõigile vabalt kättesaadavaks juurdepääsu saamiseks, kasutamiseks, muutmiseks ja edasi levitamiseks. Individuaalset arendajat ei käsitata kõnealuse vaba ja avatud lähtekoodiga tarkvara turule lasknuna. Kui tootja integreerib vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavasse tootesse, siis peab ta täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5.

3.2.6. *Mittetulunduslikud üksused, mis on loodud mittetulunduslike eesmärkide saavutamiseks*

66. Kui vaba ja avatud lähtekoodiga tarkvara avaldanud juriidiline isik on mittetulundusühendus, mis „on loodud viisil, mis tagab, et kogu tulu, millest on maha arvestatud kulud, kasutatakse mittetulunduslike eesmärkide saavutamiseks“ (küberkerksuse määruse põhjendus 18), siis ei käsitata tema avaldatud vaba ja avatud lähtekoodiga tarkvara turule lastuna. Kui kõnealune juriidiline isik vastab korraldaja määratlusele, siis peab ta täitma vastavaid kohustusi (küberkerksuse määruse artikkel 24).

Näide 24: juriidiline isik avaldab vaba ja avatud lähtekoodiga veebibrauseri, millelt teenitakse tulu otseselt otsingumootoritega sõlmitud partnerluste kaudu, kuid kogu tulu pärast kulude katmist kasutatakse mittetulunduslike eesmärkide saavutamiseks. Kõnealust veebibrauserit ei käsitata küberkerksuse määruse tähenduses turule lastuna. Selle avaldanud juriidiline isik peab täitma korraldajate suhtes kohaldatavaid kohustusi.

3.2.7. *Teiste tootjate poolne integreerimine*

67. Teatavatel juhtudel avaldab vaba ja avatud lähtekoodiga tarkvara selgelt kindlaks tehtav füüsiline või juriidiline isik, kuid seda vaba ja avatud lähtekoodiga tarkvara „käsitatakse teiste tootjate poolt nende digielemente sisaldavatesse toodetesse integreerimiseks mõeldud“ tarkvarana. Neil juhtudel ei käsitata sellist vaba ja avatud lähtekoodiga tarkvara ELi turule lastuna, v.a juhul, kui selle avaldaja (st algne tootja) sellest ka tulu teenib, kooskõlas käesolevate suuniste eespool esitatud punktidega.

68. Kui sellist vaba ja avatud lähtekoodiga tarkvara turule ei lasta, siis kohaldatakse selle avaldanud juriidilise isiku suhtes korraldajate kohustusi, kui ta pakub sellele pidevat tuge kooskõlas korraldaja määratlusega.

Näide 25: juriidiline isik avaldab vaba ja avatud lähtekoodiga tarkvarateegi kasutajaliideste loomiseks. Ta ei teeni selle tarkvarateegi tarnimise eest tulu, vaid integreerib selle ühte oma digielemente sisaldavatest toodetest (mis lastakse omakorda turule). Tarkvarateeki ei käsitata küberkerksuse määruse tähenduses turule lastuna, see on mõeldud muudesse digielemente sisaldavatesse toodetesse integreerimiseks. Selle avaldanud juriidiline isik on selle korraldaja.

Näide 26: juriidiline isik laseb turule operatsioonisüsteemi ja avaldab ühtlasi vaba ja avatud lähtekoodiga tarkvarateegid, mis toimivad selle operatsioonisüsteemi kasutajate jaoks näidisrakendustena. Juriidiline isik ei teeni tulu vaba ja avatud lähtekoodiga tarkvarateekidelt, mis on mõeldud integreerimiseks muudesse digielemente sisaldavatesse toodetesse. Need välja andnud juriidiline isik on kõnealuste vaba ja avatud lähtekoodiga tarkvarateekide korraldaja.

3.3. **Avatud lähtekoodiga tarkvara korraldajad**

69. Küberkerksuse määruses on võetud kasutusele avatud lähtekoodiga tarkvara korraldaja uus õiguslik kategooria, „[v] õttes arvesse, kui olulised on paljud sellised digielemente sisaldavad tooted, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ning mida avaldatakse, kuid ei tehta turul kättesaadavaks [---] [küberkerksuse] määruse tähenduses“ (küberkerksuse määruse põhjendus 19).

70. Teatavatel juhtudel avaldab vaba ja avatud lähtekoodiga tarkvara juriidiline isik, kes ei tee seda küberkerksuse määruse tähenduses turul kättesaadavaks „kelle eesmärk on süstemaatiliselt ja püsivalt toetada [vaba ja avatud lähtekoodiga tarkvara] [---] arendamist, mis [---] on ette nähtud kaubandustegevuseks, ning kes tagab nende toodete elujõulisuse“ (küberkerksuse määruse artikli 3 punkt 14). Sellistel juhtudel on kõnealusel juriidilisel isikul korraldaja kohustused.

71. Korraldaja on määratletud kui „juriidiline isik, kes ei ole tootja“, kuna tootja on määratluse kohaselt füüsiline või juriidiline isik, kes laseb turule digielemente sisaldavaid tooteid (s.o turustab neid) oma nime või kaubamärgi alusel. Juriidiline isik võib samuti olla korraldaja ainult digielemente sisaldavatele toodetele, mille puhul on tegemist vaba ja avatud lähtekoodiga tarkvaraga ja mis avaldatakse, aga mida ei tehta küberkerksuse määruse tähenduses turul kättesaadavaks. Korraldaja mõiste kehtib seega vaba ja avatud lähtekoodiga tarkvara konkreetsetele juhtumitele, mis „on lõppkokkuvõttes ette nähtud äritegevuseks, näiteks integreerimiseks äriteenustesse või digielemente sisaldavatesse toodetesse, millega teenitakse tulu“ (küberkerksuse määruse põhjendus 19 ([13])), kuid mida ei tehta küberkerksuse määruse tähenduses turul kättesaadavaks ja millele tagab süstemaatilise toe seda tarkvara avaldav juriidiline isik.

72. Ühe konkreetse vaba ja avatud lähtekoodiga tarkvara korraldajaks olemine ei tähenda, et juriidiline isik on samuti ilmtingimata tema avaldatava muu vaba ja avatud lähtekoodiga tarkvara korraldaja. Samal moel ei tähenda ühe konkreetse vaba ja avatud lähtekoodiga tarkvara tootjaks olemine, et juriidiline isik ei saa olla muu vaba ja avatud lähtekoodiga tarkvara korraldaja. See hõlmab sama vaba ja avatud lähtekoodiga tarkvara nn kogukonnaversioonide pakkumist, nagu on kirjeldatud punktis *3.2.1 Tasu küsimine*.

73. Juriidiline isik võib seega olla samal ajal ühe konkreetse vaba ja avatud lähtekoodiga tarkvara puhul korraldaja (kui korraldaja pakub pidevalt süstemaatiliselt tuge ja tagab tarkvara elujõulisuse) ning teise konkreetse vaba ja avatud lähtekoodiga tarkvara tootja (kui ta laseb selle turule). Teisisõnu võidakse samalt juriidiliselt isikult nõuda eri rollide täitmist erisuguste vaba ja avatud lähtekoodiga tarkvara projektide jaoks.

74. Juriidiline isik peab tegema iga konkreetse tema avaldatava vaba ja avatud lähtekoodiga tarkvara puhul kindlaks, kas seda tarkvara käsitatakse küberkerksuse määruse tähenduses turule lastuna. Kui see on nii, siis on kõnealune juriidiline isik tarkvara tootja. Kui vaba ja avatud lähtekoodiga tarkvara ei käsitata turule lastuna, siis võib juriidiline isik olla selle korraldaja, kui tarkvara on mõeldud äritegevuseks ja juriidiline isik toetab seda kooskõlas korraldaja määratlusega ([14]).

3.3.1. *Vaba ja avatud lähtekoodiga tarkvara pidev toetus ning elujõulisuse tagamine*

75. Põhjenduses 19 on selgitatud, et pidev toetus digielemente sisaldava toote arendamiseks võib hõlmata (kuid mitte ainult) järgmist: i) tarkvaraarenduse koostööplatvormide majutamine ja haldamine, ii) lähtekoodi või tarkvara majutamine, iii) selliste digielemente sisaldavate toodete juhtimine või haldamine, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ning iv) selliste digielemente sisaldavate toodete arendamise suunamine.

76. See võib olla nii näiteks juriidilise isiku puhul, kes arendab vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse integreerimiseks ning avaldab selle seejärel ilma seda turule laskmata. Seda on samuti käsitletud punktis *3.2.7 Teiste tootjate poolne integreerimine*. Sellisel juhul ei ole juriidiline isik tarkvara tootja, aga võib olla selle korraldaja. Lisaks, nagu on selgitatud ka eelnevates jaotistes, peetakse juriidilist isikut, kes avaldab sama vaba ja avatud lähtekoodiga tarkvara tasuta (ehk kogukonna-) versiooni ja tasulise versiooni, tasuta (ehk kogukonna-) versiooni korraldajaks ja tasulise versiooni tootjaks.

77. Samal moel on juriidiline isik, kes teenib vaba ja avatud lähtekoodiga tarkvara pealt tulu, kui tegemist on mittetulundusliku üksusega, kelle tulu pärast kulude mahaarvamist kasutatakse mittetulunduslike eesmärkide saavutamiseks (ning seega ei lasta selle vaba ja avatud lähtekoodiga tarkvara küberkerksuse määruse tähenduses turule, nagu on käsitletud punktis *3.2.6 Mittetulunduslikud üksused*), avaldatava vaba ja avatud lähtekoodiga tarkvara korraldaja.

78. Lisaks sellele pakuvad teatavad fondid mitmesuguste juhtimisvormidega koostööplatvorme, mis võimaldavad tootjatel panustada korrapäraselt vaba ja avatud lähtekoodiga tarkvara arendamisse ja/või mida rahastavad korrapäraselt tootjad. Kõnealuseid fonde käsitatakse korraldajatena konkreetse vaba ja avatud lähtekoodiga tarkvara puhul, mis on mõeldud äritegevuseks ja mille jaoks fond pakub pidevat toetust. Kuid nagu on selgitatud punktis *3.3 Avatud lähtekoodiga tarkvara korraldajad*, ei saa kõnealuse fondi suhtes kohaldada mingeid küberkerksuse määrusest tulenevaid kohustusi muu selle majutatava konkreetse vaba ja avatud lähtekoodiga tarkvara puhul, kui ta ei paku konkreetsele vabale ja avatud lähtekoodiga tarkvarale süstemaatilist toetust, ei taga selle toimivust ja/või see konkreetne tarkvara ei ole mõeldud äritegevuseks.

([13]) See tuleneb ka sõnastusest „ette nähtud kaubandustegevuseks“, mis on lisatud küberkerksuse määruse artikli 3 lõikes 14 esitatud avatud lähtekoodiga tarkvara korraldaja mõiste määratlusse.

([14]) Juriidilise isiku suhtes ei pruugita kohaldada küberkerksuse määrusest tulenevaid kohustusi järgmistel juhtudel: i) konkreetset vaba ja avatud lähtekoodiga tarkvara ei lasta küberkerksuse määruse tähenduses turule ning ii) juriidiline isik ei vasta kõnealuse konkreetse vaba ja avatud lähtekoodiga tarkvara puhul korraldaja määratlusele.

79. Fondide ja samalaadsete organisatsioonide poolt konkreetsetele vaba ja avatud lähtekoodiga tarkvara projektidele antava püsiva toetuse olemus võib olla väga erinev. Näiteks pakuvad teatavad juriidilised isikud ainult mittetehnilist toetust, näiteks haldavad projektide tootemargikujundust, kehtestavad juhtimisnormid, korraldavad kogukonna üritusi või koguvad annetusi. Teised üksused pakuvad ka IT alustaristut, mis on vajalik projekti rakendamiseks, näiteks lähtekoodi hoidlate majutamine, versioonihaldussüsteemide pakkumine või elektroonilise allkirja võtmete genereerimine. Teised lähevad pakutava toe osas kaugemale, panustades projekti aktiivselt insener-tehnilisi ressursse, näiteks palgates arendajaid, koordineerides arendustööd, vaadates läbi või ühendades koodi, hallates versioone või tegeledes turvanõrkustest teavitamisega ja turvapaikadega. Kuigi kõik küberkerksuse määruse alusel korraldajatena käsitatavad juriidilised isikud peavad täitma artikli 24 lõigetes 1 ja 2 sätestatud kohustusi, erineb ulatus, milles artikli 14 lõigetes 1, 3 ja 8 sätestatud kohustusi nende juriidiliste isikute suhtes kohaldatakse, olenevalt nende pakutava toe liigist kooskõlas artikli 24 lõikega 3.

80. Näiteks korraldaja, kes pakub ainult muud kui tehnilist tuge, ei osale määratluse kohaselt digielemente sisaldava toote arendamises ning seega ei nõuta talt aktiivselt ärakasutatavatest nõrkustest teatamist. Samuti ei paku see korraldaja võrgu- ja infosüsteeme kõnealuste digielemente sisaldavate toodete arendamiseks ning seega ei pea ta teatama tõsistest intsidentidest ENISA-le, küberintsidentidele reageerimise üksustele (edaspidi „CSIRT“) ega mõjutatud kasutajatele. Sellest hoolimata, kui korraldaja saab teada aktiivselt ärakasutatavast nõrkusest (nt sellise välise allika kaudu nagu turbeuurijate aruanne), siis peaks ta jagama seda teavet digielemente sisaldava toote hooldajatega kooskõlas oma küberturvalisuse põhimõtetega. Digielemente sisaldavate toodete hooldajad ja/või korraldajad peaksid samuti kaaluma, kas teatada nõrkusest vabatahtlikult kooskõlas artikliga 15.

81. Teisest küljest, kui korraldaja pakub teatavate digielemente sisaldavate toodete jaoks IT alustaristut, siis peab ta teavitama ENISAt ja CSIRTe kooskõlas artikli 14 lõikega 3 kõnealuse taristuga seotud mis tahes tõsistest vahejuhtumitest, mis mõjutavad digielemente sisaldavate toodete turvalisust. Samuti tuleb vajaduse korral teavitada kõiki kasutajaid (nt üldise teadaande teel). Nagu on märgitud eelmises punktis, ei ole korraldajal kohustust aktiivselt teatada talle teatavaks saanud ärakasutatavatest nõrkustest, kuid ta peaks edendama nõrkuste nõuetekohast käsitlemist ja kaaluma vabatahtlikku teavitamist kooskõlas artikliga 15.

82. Kui korraldaja pakub konkreetsetele digielemente sisaldavatele toodetele insener-tehnilisi ressursse, siis ta peab: i) teatama artikli 14 lõike 1 kohaselt aktiivselt ärakasutatavatest nõrkustest, millest ta teada saab, ning ii) kui see on asjakohane, siis teavitama kõiki kasutajaid. Selles ulatuses, milles korraldajal on otsene suhe mõjutatud kasutajatega, peab ta neid samuti otseselt teavitama kooskõlas artikli 14 lõikega 8.

83. Kui üksus ei paku konkreetsele vabale ja avatud lähtekoodiga tarkvarale enam pidevat süsteemset toetust, siis ei pruugi ta enam vastata korraldaja määratlusele ning tal ei pruugi enam olla vastavaid kohustusi. Neil juhtudel kutsutakse kõnealust üksust üles andma selgelt teada oma seisundi muutusest konkreetse vaba ja avatud lähtekoodiga tarkvara puhul.

84. Teatavas olukorras võib üksus, kes oli konkreetse projekti korraldaja, otsustada teenida projekti eest otsest tulu, lastes seeläbi digielemente sisaldava toote turule ja omandades tootja kohustused küberkerksuse määruse alusel. Selles olukorras saab kõnealusest üksusest digielemente sisaldava toote tootja alates kuupäevast, kui ta laseb selle turule (aga mitte varasemate versioonide puhul, kui ta tegutses korraldajana).

3.4. **Edasiarendajad ja järgneva etapi kasutusviisid**

85. Nagu on juba märgitud punktis *3.1 Kindakstegemine, kas vaba ja avatud lähtekoodiga tarkvara kuulub isiku vastutusalasse*, on küberkerksuse määruses selgitatud, et seda ei kohaldata „füüsiliste või juriidiliste isikute suhtes, kes panustavad lähtekoodiga sellistesse digielemente sisaldavatesse toodetesse, mida käsitatakse vaba ja avatud lähtekoodiga tarkvarana ja mis ei kuulu nende vastutusalasse“ (põhjendus 18).

86. Digielemente sisaldavate toodete tootjad, kes integreerivad vaba ja avatud lähtekoodiga tarkvara komponendid oma digielemente sisaldavatesse toodetesse, ei muutu samuti vastutavaks nende komponentide endi vastavuse eest küberkerksuse määrusele, isegi kui kõnealused tootjad panustavad lähtekoodiga nende hooldamisse.

87. Samal moel ei mõjuta lihtsalt fakt, et tootjad integreerivad vaba ja avatud lähtekoodiga tarkvara komponendid enda (tulu teenivatesse) digielemente sisaldavatesse toodetesse, kõnealuse vaba ja avatud lähtekoodiga tarkvara komponendi seisundit küberkerksuse määruse alusel. Nende vaba ja avatud lähtekoodiga tarkvara komponentide hooldajatel, mida turule ei lasta, ei ole kohustusi muude üksuste ees, kes võivad integreerida kõnealused komponendid oma digielemente sisaldavatesse toodetesse. See, kas küberkerksuse määrust kohaldatakse konkreetse vaba ja avatud lähtekoodiga tarkvara komponendi suhtes, oleneb ainult sellest, kas selle välja andnud füüsiline või juriidiline isik laseb selle turule.

88. Sellest hoolimata peavad selliste digielemente sisaldavate toodete tootjad, millesse on integreeritud vaba ja avatud lähtekoodiga tarkvara komponendid, täitma küberkerksuse määruse nõudeid nende endi digielemente sisaldavate toodete puhul. Nad peavad samuti täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5 vaba ja avatud lähtekoodiga tarkvara komponentide puhul, mille nad integreerivad. Lisaks sellele peavad nad teatama integreeritud komponentide nõrkustest ja jagama turvaparandusi kooskõlas artikli 13 lõikega 6. Vt seda teemat käsitlevaid täpsemaid suuniseid punktis *9.2.1 Algse projektiga seotud isikute teavitamine ja turvaparanduste jagamine*.

3.5. **Näitlikustavad stsenaariumid**

89. Järgmised näited on täiesti hüpoteetilised ning esitatud selleks, et näitlikustada eelmistes punktides selgitatud juhtumeid.

Näide 27: individuaalne arendaja A on arendanud vaba ja avatud lähtekoodiga tarkvara. Arendaja A avaldab kõnealuse vaba ja avatud lähtekoodiga tarkvara oma kaubamärgi all, kuid ei küsi selle kasutamise eest tasu. Tarkvara jagatakse avatult ja see on vabalt kättesaadav kõigile juurdepääsu saamiseks, kasutamiseks, muutmiseks ja edasi levitamiseks. Arendaja A lisab samuti lingi platvormile, et koguda vabatahtlikke annetusi.

Ettevõtted B, C ja D integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse. Jätkuva hoolduse toetamiseks teevad ettevõtted B, C ja D arendajale A vabatahtlikud annetused. Need annetused võimaldavad arendajal A hoida projekti aktiivselt käigus.

Seda vaba ja avatud lähtekoodiga tarkvara ei lasta küberkerksuse määruse tähenduses turule. Arendajal A ei ole küberkerksuse määruse alusel kohustusi. Ettevõtted B, C ja D peavad täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5, kui nad integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse.

Näide 28: mittetulunduslik sihtasutus F avaldab vaba ja avatud lähtekoodiga tarkvara komponendi integreerimiseks muudesse digielemente sisaldavatesse kommertstoodetesse. Sihtasutus F võtab kohustuse anda sellele vabale ja avatud lähtekoodiga tarkvarale pidevat toetust, et tagada selle elujõulisus ja kasutuselevõtt. Ettevõtted A, B ja C integreerivad selle vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse. Ettevõtted A ja B panustavad vabatahtlikult osa oma arendajate ajast sihtasutuse F vaba ja avatud lähtekoodiga tarkvara projektide arendamisse ja hooldamisse, sh kõnealuse vaba ja avatud lähtekoodiga tarkvara puhul.

Kuna sihtasutus F on mittetulundusüksus, mis on loodud viisil, et selle tulusid pärast kulude mahaarvamist kasutatakse mittetulunduslike eesmärkide saavutamiseks, ei käsitata seda vaba ja avatud lähtekoodiga tarkvara küberkerksuse määruse tähenduses turule lastuna. Sihtasutus F on kõnealuse vaba ja avatud lähtekoodiga tarkvara korraldaja ja tema suhtes kohaldatakse artiklis 24 märgitud vastavaid kohustusi. Ettevõtted A, B ja C peavad täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5, kui nad integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse.

Näide 29: ettevõte A on töötanud välja vaba ja avatud lähtekoodiga tarkvara komponendi integreerimiseks tema enda digielemente sisaldavatesse toodetesse. Ta avaldab samuti kõnealuse vaba ja avatud lähtekoodiga tarkvara eraldi oma nime või kaubamärgi all ning hooldab seda aktiivselt. Kuid ta ei nõua selle kasutamise eest tasu ega teeni selle pealt muul viisil tulu. Ettevõtted B, C ja D integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse ja panustavad vabatahtlikult osa oma arendajate ajast selle hooldamisse.

Kõnealust vaba ja avatud lähtekoodiga tarkvara ei käsitata küberkerksuse määruse tähenduses turule lastuna. Ettevõte A ei ole tootja, vaid korraldaja. Ettevõtted B, C ja D peavad täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5, kui nad integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse.

Näide 30: ettevõte A avaldab vaba ja avatud lähtekoodiga tarkvara välja oma nime või kaubamärgi all ja pakub seda tasulise versioonina, mis sisaldab teatavaid eeliseid, nagu tehniline abi või jõudluse optimeerimine. Ettevõtete B, C ja D arendajad panustavad vaba ja avatud lähtekoodiga tarkvara hooldamisse, kuid see jääb ettevõtte A kontrolli alla.

Ettevõtet A käsitatakse kõnealuse vaba ja avatud lähtekoodiga tarkvara tootjana ([15]). Ettevõtete B, C ja D suhtes ei kohaldata kõnealuse konkreetse vaba ja avatud lähtekoodiga tarkvara puhul küberkerksuse määrusest tulenevaid kohustusi. Kui nad integreerivad selle vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavasse tootesse, peavad nad täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5.

Näide 31: ettevõte A avaldab vaba ja avatud lähtekoodiga tarkvara oma nime või kaubamärgi all ning tagab jätkuva hoolduse selle pikaajalise elujõulisuse huvides, et kõnealuse tarkvara saaks integreerida muude ettevõtete digielemente sisaldavatesse toodetesse. Ettevõte A ei nõua selle kasutamise eest tasu, ei töötle digielemente sisaldava toote kaudu kogutud isikuandmeid ega müü tugiteenuseid, mis on seotud vaba ja avatud lähtekoodiga tarkvara avaldamisega.

Ettevõte B panustab avatud lähtekoodiga tarkvara hooldusesse koodi ja arendajate tööajaga, kuid ei levita seda ärilisel eesmärgil. Ettevõte B pakub tehnilisi tugiteenuseid vaba ja avatud lähtekoodiga tarkvara levitamisest sõltumatult. Ettevõtet A peetakse kõnealuse vaba ja avatud lähtekoodiga tarkvara korraldajaks ning ettevõttel B puuduvad kõnealuse vaba ja avatud lähtekoodiga tarkvara puhul küberkerksuse määrusest tulenevad kohustused.

Näide 32: vaba ja avatud lähtekoodiga tarkvara komponendi avaldab mittetulundusüksus, mis on loodud sellisel viisil, et selle puhul tagatakse, et kõiki tulusid pärast kulude mahaarvamist kasutatakse mittetulunduslike eesmärkide saavutamiseks. Üksus pakub pidevat toetust, et tagada projekti pikaajaline elujõulisus. Hooldust rahastatakse avaliku sektori vahenditest, näiteks teadusuuringute toetustest. Täiendavat arendustegevust, sh uusi funktsioone, rahastatakse läbi annetuste ja konkreetsete projektide, mis rakendatakse partnerluses tootjatega, kes integreerivad kõnealuse vaba ja avatud lähtekoodiga tarkvara oma digielemente sisaldavatesse toodetesse. Sellised funktsioonid kaasatakse vaba ja avatud lähtekoodiga tarkvara koodibaasi.

Mittetulundusüksust, mis avaldab vaba ja avatud lähtekoodiga tarkvara, käsitatakse kõnealuse vaba ja avatud lähtekoodiga tarkvara komponendi korraldajana. Tootja, kes on panustanud teatavate funktsioonide arendamisse, ei saa kõnealuse vaba ja avatud lähtekoodiga tarkvara komponendi tootjaks. Kui tootja integreerib vaba ja avatud lähtekoodiga tarkvara komponendi oma digielemente sisaldavasse tootesse, siis peab ta täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5.

Näide 33: mittetulundusüksus, mis on loodud sellisel viisil, et selle puhul tagatakse, et kõiki tulusid pärast kulude mahaarvamist kasutatakse mittetulunduslike eesmärkide saavutamiseks, avaldab vaba ja avatud lähtekoodiga tarkvara tarkvaraarenduse komplekti ja tagab selle jätkuva hoolduse. Tarkvaraarenduse komplekti jagatakse avatult ja see on vabalt kättesaadav kõigile juurdepääsu saamiseks, kasutamiseks, muutmiseks ja edasi levitamiseks. Rahastamine tagatakse mittetulundusüksusele tasutavate liikmetasude kaudu ning liikmesorganisatsioonide heaks töötavad arendajad panustavad koodi ja muid ressursse tarkvaraarenduse komplekti arendamiseks. Tootjad kasutavad tarkvaraarenduse komplekti komponendina muude digielemente sisaldavate toodete loomiseks.

Mittetulundusüksust, mis avaldab kõnealuse tarkvaraarenduse komplekti, käsitatakse selle korraldajana. Fondi liikmed ei vastuta tarkvaraarenduse komplekti vastavuse eest küberkerksuse määruse nõuetele. Kui tootja kasutab tarkvaraarenduse komplekti oma digielemente sisaldava toote loomiseks, siis peab ta täitma hoolsuskohustust kooskõlas artikli 13 lõikega 5.

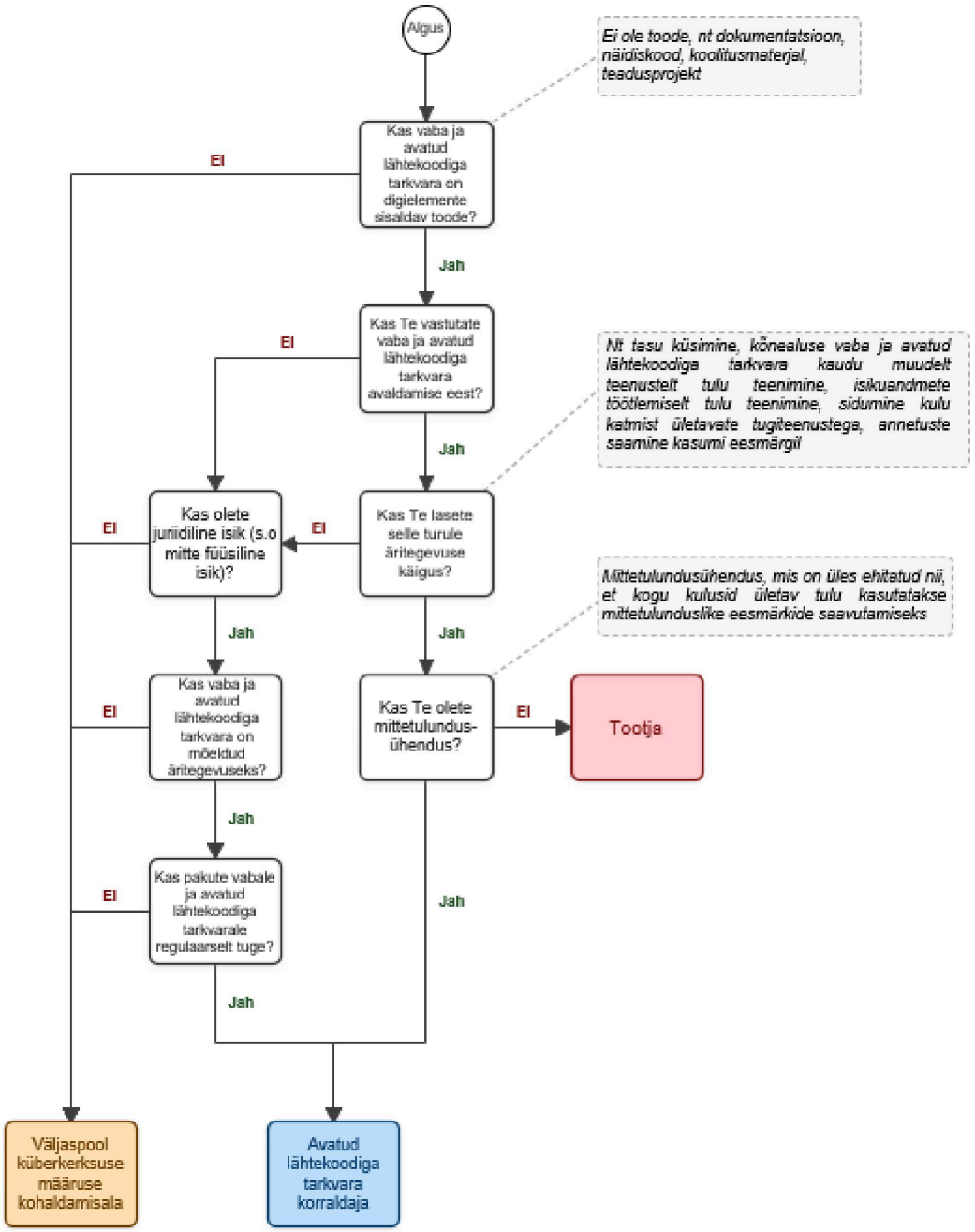
Näide 34: individuaalne arendaja avaldab konkreetse programmeerimiskeele jaoks mõeldud vaba ja avatud lähtekoodiga teegi avalikus paketihoidlas ning hooldab seda aktiivselt. Arendaja lisab paketi dokumentatsiooni lingi annetuste kogumiseks. Tootja laadib kõnealuse tarkvarateegi hoidlast tasuta alla ja integreerib selle oma digielemente sisaldavasse tootesse.

Individuaalsel arendajal ja paketihoidlal ei ole kohustusi küberkerksuse määruse alusel. Tarkvarateegi integreerinud tootja peab täitma hoolsuskohustust artikli 13 lõike 5 kohaselt.

([15]) V.a juhul, kui ettevõte A on mittetulundusüksus, mis on loodud sellisel viisil, et selle puhul tagatakse, et kõiki tulusid pärast kulude mahaarvamist kasutatakse mittetulunduslike eesmärkide saavutamiseks; sellisel juhul oleks see ettevõte kõnealuse vaba ja avatud lähtekoodiga tarkvara korraldaja.

Joonis 1

Kujundlik vooskeem, mis näitlikustab küberkerksuse määruse kohaldamisala seoses vaba ja avatud lähtekoodiga tarkvaraga



4. OLULISED MUUDATUSED JA VARUOSAD

90. Küberkerksuse määruse artikli 3 punktis 30 on „oluline muudatus“ määratletud kui digielemente sisaldavas tootes pärast selle turule laskmist tehtud muudatus, mis i) mõjutab digielemente sisaldava toote vastavust I lisa I osas sätestatud olulistele nõuetele või ii) mille tõttu muutub sihtotstarve, mida silmas pidades on digielemente sisaldavat toodet hinnatud.

91. Olulise muudatuse mõiste on asjakohane küberkerksuse määrusest tulenevate kohustuste kindlakstegemiseks mitmel juhul, sh järgmistel juhtudel:

a) kooskõlas artikliga 21 käsitatakse importijat või turustajat, kes muudab oluliselt juba turule lastud digielemente sisaldavat toodet, selle tootjana;

b) kooskõlas artikliga 22 käsitatakse mis tahes füüsilist või juriidilist isikut, kes muudab oluliselt juba turule lastud digielemente sisaldavat toodet ja teeb selle toote turul kättesaadavaks, selle tootjana;

c) kooskõlas artikli 69 lõikega 2 käsitatakse füüsilist või juriidilist isikut, kes pärast 11. detsembrit 2027 muudab oluliselt enne 11. detsembrit 2027 turule lastud digielemente sisaldavat toodet ning laseb selle turule, selle tootjana;

d) pärast 11. detsembrit 2027 turule lastud digielemente sisaldavate toodete tootjate puhul tuleb teha kindlaks, kas digielemente sisaldav toode peab läbima uue vastavushindamismenetluse pärast kõnealust kuupäeva tehtud muudatuste tõttu, eelkõige võttes arvesse tarkvaraarenduse olemuslikku korduvust.

92. Seetõttu on oluline esitada suunised, et aidata ettevõtjatel aru saada, millal on riistvara- või tarkvaramuudatuste puhul tegemist oluliste muudatustega.

4.1. **Füüsiline parandamine**

93. Nagu on märgitud küberkerksuse määruse põhjenduses 42, ei pruugi „Euroopa Parlamendi ja nõukogu määruse (EL) 2024/1781 artikli 2 punktides 18, 19 ja 20 määratletud digielemente sisaldava toote „taastamine“, „hooldus“ ja „parandamine“ [---] põhjustada toote olulist muutmist, näiteks siis, kui sihtotstarvet ja funktsioone ei muudeta ja riski taset ei mõjutata. Digielemente sisaldava toote uuendamine tootja poolt võib siiski põhjustada muudatusi kõnealuse toote projektis ja arendamises ning võib seega mõjutada selle kavandatud otstarvet ja vastavust käesolevas määruses sätestatud nõuetele.“ See on kooskõlas sinise raamatu punktiga 2.1, milles juhitakse tähelepanu sellele, et „[t]oodet, mida on pärast kasutusele võtmist oluliselt muudetud või täiustatud, tuleb pidada uueks tooteks juhul, kui: i) selle algset toimivust, otstarvet või tüüpi on muudetud viisil, mis ei olnud toote algses riskihindamises ette nähtud; ii) muutunud on ohu iseloom või tõusnud on ohu tase vastavalt asjaomasele liidu ühtlustamisõigusaktile; iii) toode tehakse kättesaadavaks (või võetakse kasutusele, kui kohaldatavate õigusaktide kohaldamisala hõlmab ka kasutusele võtmist). Seda tuleb hinnata igal juhtumil eraldi ning eelkõige arvestades õigusaktide eesmärki ja asjaomaste õigusaktidega hõlmatud toodete liiki.“

94. Taastamine, hooldus või parandamine, mille tulemuseks on juba turule lastud digielemente sisaldava toote füüsiline muutmine, ei kujuta endast ilmtingimata olulist muudatust. Seetõttu tuleks hinnata iga juhtumit eraldi, et teha kindlaks, kas kõnealune füüsiline muutmine mõjutab digielemente sisaldava toote vastavust I lisa I osa olulistele nõuetele või selle tulemuseks on küberriskide hindamisega hõlmatud toote sihtotstarbe muutmine.

95. Defektsete või kulunud detailide asendamist paremini toimivate osadega (nt tehnoloogiliste edusammude tõttu või kuna varasemat osa enam ei toodeta) ei käsitata iseenesest digielemente sisaldava parandatud toote olulise muudatusena. Olulise muudatusega on tegemist ainult juhul, kui digielemente sisaldava parandatud toote toimivuse või toimimisviisi muudatus i) mõjutab selle vastavust olulistele nõuetele või ii) selle tulemusena muutub sihtotstarve viisil, mis ei olnud riskihindamisega hõlmatud.

Näide 35: arvutiserveri tootja teostab remonditööd, asendades defektse muutmälu uue ja suurema jõudlusega mäluga. See ei mõjuta serveri vastavust olulistele nõuetele. Server toimib paremini, aga selle uus jõudlus jääb küberriskide hindamise käigus käsitletud serveri sihtotstarbelise kasutuse piiresse. Arvutiserverit ei käsitata oluliselt muudetuna.

4.2. **Varuosad**

96. Küberkerksuse määruse artikli 2 lõikes 6 on määratud kindlaks, et küberkerksuse määrust ei kohaldata varuosade suhtes, mis on mõeldud identsete komponentide asendamiseks ja mida toodetakse kõnealuste komponentidega samade spetsifikatsioonide kohaselt. Põhjenduses 29 on lisaks sellele märgitud, et erand hõlmab nii enne küberkerksuse määruse kohaldamise alguskuupäeva kättesaadavaks tehtud digielemente sisaldavate toodete varuosi kui ka varuosi, mis on juba läbinud määruses sätestatud vastavushindamismenetluse.

97. Küberkerksuse määruse artikli 2 lõikes 6 märgitud erandit tuleks mõista nii, et seda kohaldatakse ainult juhul, kui varuosa tarnitakse konkreetselt (enne või pärast 11. detsembrit 2027) juba turule lastud digielemente sisaldava toote parandamiseks või selle vastupidavuse pikendamiseks. Kui digielemente sisaldavat toodet tarnitakse eraldiseisva tootena, ilma et see oleks ühelgi moel seotud olemasoleva digielemente sisaldava toote hooldamise või parandamisega, siis lastakse see küberkerksuse määruse tähenduses turule ja seda ei tohiks käsitada artikli 2 lõike 6 kohaldamisalasse kuuluva varuosana. Hooldamise või parandamise otstarve peaks olema ilmne tarnimise kontekstist, näiteks tellimuses või kaubanduslikus pakkumises digielemente sisaldava toote või tooteperekonna identifitseerimise teel või lähtuvalt tarnimisest müügijärgsete või teeninduskanalite kaudu. Seda käsitlevaid tõendeid tuleks samuti säilitada, et turujärelevalveasutused saaksid neid kontrollida. Asjaolu, et digielemente sisaldavat toodet oleks võimalik tehniliselt kasutada komponendi asendamiseks, ei ole iseenesest piisav, et see kuuluks kõnealuste elementide puudumise korral erandi kohaldamisalasse.

98. Seega, kui varuosa on identne komponendiga, mis juba kuulub digielemente sisaldava toote koosseisu, mis on lastud turule kas enne küberkerksuse määruse kohaldamise alguskuupäeva või kooskõlas küberkerksuse määrusega, siis ei kohaldata selle varuosa enda suhtes küberkerksuse määrust.

99. Kui hinnatakse, kas varuosa tuleks käsitada komponendiga identsena, tuleks keskenduda selle funktsionaalsele rollile digielemente sisaldavas tootes ning selle omadustele, mis võivad olla olulised küberturvalisuse puhul. Kuigi iga juhtumit tuleb alati eraldi hinnata, ei takista erinevused, mis ei mõjuta komponendi turvaomadusi või küberriski profiili, iseenesest kõnealuse varuosa kuulumist küberkerksuse määruse artikli 2 lõike 6 kohaldamisalasse.

100. Seevastu võivad erinevused komponendi küberturvalisuse seisukohast asjakohastes omadustes, näiteks algoritmid, protokollid, krüptograafilised mehhanismid, juurdepääsukontrolli funktsioonid või muud turvalisuse seisukohast olulised omadused, tähendada, et uut osa ei saa käsitada identsena komponendiga, mille asendamiseks see on ette nähtud.

101. Kui varuosa ei ole algse komponendiga identne, siis on kõnealuse varuosa puhul tegemist digielemente sisaldava omaette tootega ja selle suhtes kohaldatakse seega küberkerksuse määrust. Sellisel juhul tuleb hinnata vastavust olulistele nõuetele, võttes arvesse asenduskomponendi sihtotstarvet. Eelkõige on oluline asenduskomponendi otstarve tagada ühilduvus või koostalitlusvõime olemasoleva digielemente sisaldava tootega, sh kui kõnealune toode on digielemente sisaldav toode, mis on turule lastud enne küberkerksuse määruse kohaldamise alguskuupäeva. Kui olulisi nõudeid ei ole võimalik mõistlikult täita kõnealuse sihtotstarbe või tehniliste piirangute tõttu, siis peab tootja kajastama seda küberriskide hindamises ja rakendama sobilikud alternatiivsed või kompenseerivad riskimaandamismeetmed, et mitte kahjustada digielemente sisaldava toote turvalisust. Nagu on märgitud ka punktis *2.6 Komplekssed süsteemid*, on nii tehnilisel dokumentatsioonil kui ka kasutajatele mõeldud teabel ja juhistel oluline roll, et kirjeldada läbipaistval viisil kindlaks tehtud piiranguid, nendega seotud küberturvalisuse riske ja rakendatud riski maandamise meetmeid. Nagu on selgitatud punktis *4.1 Füüsiline parandamine*, ei too defektsete või kulunud detailide asendamine paremini toimivate osadega iseenesest kaasa digielemente sisaldava parandatud toote olulist muutmist.

Näide 36: tootja on lasknud ELi turule võrguühendusega kontrollerid. Ühel juhul lasti kontroller turule 2026. aastal enne küberkerksuse määruse kohaldamise alguskuupäeva. Teisel juhul lasti kontroller turule 2028. aastal kooskõlas küberkerksuse määrusega. 2028. aastal tekib mõlemat liiki kontrolleri digitaalse sidemooduli puhul tõrge. Tootja tarnib varuosana asendusmooduli, mis on originaaliga identne ja toodetud sellega samade spetsifikatsioonide kohaselt.

Asendusmoodul kuulub mõlemal juhul artikli 2 lõikes 6 sätestatud erandi kohaldamisalasse. Varuosa enda suhtes ei kohaldata küberkerksuse määrust, kuigi see on digielemente sisaldav toode, kuna sellega asendatakse digielemente sisaldavas tootes identne komponent. Parandamise puhul ei ole tegemist digielemente sisaldava toote olulise muudatusega.

Näide 37: tootja lasi võrguühendusega tööstusliku juhtseadme ELi turule 2026. aastal enne küberkerksuse määruse kohaldamise alguskuupäeva. 2028. aastal tekib kõnealuse juhtseadme sidekiibi tõrge. Kuna tootja ei tooda enam seda kiipi, tarnib ta varuosana võrdväärsete funktsioonidega uuema kiibi, millel on erinev krüptograafiline rakendus ja ajakohastatud turvaline alglaadimise mehhanism, et säilitada ühilduvust ja tagada tegevuse jätkumine.

Sel juhul ei saa käsitada asenduskiipi identsena, kuna krüptograafilise rakendamise ja turvalise alglaadimise mehhanismi erinevused mõjutavad kiibi küberturvalisuse omadusi. Seega ei kehti selle puhul artikli 2 lõikes 6 sätestatud erand ja on tegemist digielemente sisaldava tootega, mille suhtes kohaldatakse küberkerksuse määrust. Asendusosa nõuetele vastavust tuleb hinnata, võttes arvesse selle sihtotstarvet, sh selle rolli koostalitlusvõime tagamisel digielemente sisaldava tootega, mis on turule lastud enne küberkerksuse määruse kohaldamise alguskuupäeva.

Näide 38: tootja laseb 2028. aastal turule nutihoone juhtseadme kooskõlas küberkerksuse määrusega. 2029. aastal ütleb üles selle seadme juhtmevaba moodul. Kuna tootja ei tooda enam seda moodulit, tarnib ta varuosana uue mooduli, mis täidab sama otstarvet samade sideprotokollide ja turvamehhanismide abil, kuid põhineb erineval kiibistikul ja omab ajakohastatud püsivara, mis ei muuda omadusi, mis võivad olla asjakohased küberturvalisuse puhul.

Sel juhul võib käsitada asendusmoodulit identsena. Mooduli puhul kehtib seega artikli 2 lõikes 6 sätestatud erand ja selle suhtes ei kohaldata küberkerksuse määrust.

102. Varuosade erandit kohaldatakse olenemata sellest, kas varuosa asendab komponendi digielemente sisaldavas tootes või kogu digielemente sisaldava toote, mis on ise suurema toote osa, sh kui kõnealune digielemente sisaldav suurem toode koosneb mitmest integreeritud komponendist, tingimusel et asendusosa tarnitakse konkreetselt varuosana, nagu on selgitatud jaotistes eespool.

Näide 39: 2027. aastal laseb tootja turule tööstusautomaatika süsteemi, mille üks komponent on programmeeritav kontroller. 2031. aastal tekib programmeeritava kontrolleri protsessori tõrge. Tootja pakub kaks parandusvarianti: i) tarnida asendusprotsessor, mida võib käsitada identsena algselt paigaldatud protsessoriga, või ii) tarnida terviklik programmeeritav asenduskontroller, mida võib käsitada identsena algselt paigaldatud programmeeritava kontrolleriga. Mõlemal juhul tarnitakse asendusosa tootja müügijärgse teeninduse kanali kaudu varuosana ja tööstusautomaatikasüsteem, mille jaoks see asendusosa on mõeldud, on selgelt identifitseeritud. Mõlemal juhul kehtib asendamise puhul artikli 2 lõikes 6 sätestatud erand olenemata sellest, kas asendatakse programmeeritava kontrolleri komponent või kogu programmeeritav kontroller.

4.3. **Tarkvarauuendused kui olulised muudatused**

103. Tarkvaraarendus on oma olemuselt järkjärguline, kusjuures juba turule lastud digielemente sisaldavaid tarkvaratooteid ajakohastatakse sageli ja pidevalt. Selles kontekstis on kasulik esitada rohkem suuniseid, et teha kindlaks, millal käsitatakse tarkvara oluliselt muudetuna. Nende suuniste eesmärk on eelkõige aidata digielemente sisaldavate tarkvaratoodete tootjatel, kes muudavad oma tooteid, teha kindalaks, kas kõnealuste muudatuste puhul on tegemist oluliste muudatustega.

104. Põhjenduses 39 on märgitud, et digielemente sisaldavat toodet muudetakse oluliselt juhul, kui muutmine mõjutab küberriski taset ja kui tootja ei ole võtnud kõnealust muutunud või täiendavat riski arvesse oma riskihindamises ning seega ka oluliste nõuete rakendamisel. Tootja peaks seega hindama iga juhtumi puhul eraldi, kas tarkvarauuendus põhjustab uue või suurema küberriski ning kas kõnealuseid riske on tema riskihindamise käigus juba arvesse võetud.

105. Kui tootja võtab digielemente sisaldava toote puhul kasutusele uued funktsioonid, mille tulemusena muutub toote kui terviku sihtotstarve, siis on tõenäoline, et tootja ei võtnud neid muudatusi arvesse oma riskihindamises. Selles olukorras käsitatakse muudatust üldjuhul olulise muudatusena.

Näide 40: tootja laseb turule juhtpaneeli, mis kogub masinatelt andmeid ning kuvab suundumusi ja hoiatusi, ilma et suudaks kõnealuseid masinaid juhtida. Tootja töötab seejärel välja kõnealuse juhtpaneeli uue versiooni, mille puhul võetakse kasutusele uued funktsioonid, mis võimaldavad sellel masinaid juhtida, sh kohandades tööparameetreid ning taaskäivitades masinad pärast veatingimuste tekkimist. Nende muudatuste tulemusena on juhtpaneeli sihtotstarve muutunud võrreldes riskihindamises ette nähtuga, minnes üle olukorrateadlikkuse vahendist digielemente sisaldavaks tooteks, mis on mõeldud muude seadmete operatiivseks juhtimiseks. Juhtpaneeli on seega oluliselt muudetud.

Näide 41: tootja laseb turule tarbijatele mõeldud tarkvararakenduse, mille eesmärk on korrastada ja kuvada isikuandmeid, näiteks e-kirju, sõnumeid või dokumente, ning võimaldada baastaseme otsingu ja filtreerimise funktsioone. Tootja annab seejärel välja uuenduse, mis võimaldab rakendusel automaatselt analüüsida kasutajate sisu, et luua käitumisprofiilid ning teha automaatseid otsuseid, mis mõjutavad sisu prioritiseerimist kasutaja sekkumiseta. Selle muudatuse tulemusena on tarkvara sihtotstarve muutunud kasutaja juhitud teabehaldusvahendist automaatseks otsustussüsteemiks, mida ei nähtud riskihindamise käigus ette. Rakendust on seega oluliselt muudetud.

106. Samal ajal on siiski võimalik, et tootja võtab järk-järgult kasutusele uusi funktsioone, mis on juba hõlmatud tema riskihindamisega või mis iseenesest ei muuda digielemente sisaldava toote küberriski profiili. See võib olla nii näiteks juhul, kui tootja on nende funktsioonide arendamist ette näinud, on seonduvaid riske juba kirjeldanud ja hinnanud ning rakendanud sobilikke maandamismeetmeid, et tagada jätkuv vastavus olulistele nõuetele. See võib olla nii ka juhul, kui uute funktsioonide tulemusena ei tehta muudatusi, millest tekivad uued või suuremad riskid. Seda laadi ajakohastusi ei tohiks seega käsitada oluliste muudatustena, kuna need ei suurenda küberriski ega muuda sellest tulenevalt oluliste nõuete rakendamist.

Näide 42: sõnumirakendus antakse algselt välja ainult privaatsõnumeid võimaldavana. Tootja riskihindamine hõlmab hiljem grupisõnumite lisamist, sh näiteks sõnumite keerukamat marsruutimist. Edasises uuenduses lisab tootja grupivestluse funktsiooni koos halduslikku kontrolli ja modereerimise vahenditega, mis nähti ette ja mida hinnati juba algse projekteerimise ajal. Uuendusega rakendatakse funktsioonid, mis on hõlmatud algse sihtotstarbe ja riskihindamisega. Sõnumirakendust ei ole seega oluliselt muudetud.

Näide 43: tootmise seiresüsteem lastakse turule nii, et aktiveeritud on vaid lugemist võimaldavad näidikupaneelid, samas kui automaatjuhtimise funktsioonid on süsteemiarhitektuuris olemas, kuid välja lülitatud. Tootja riskihindamine hõlmab otseselt automaatsete juhtimisahelate tulevast aktiveerimist, sh suletud ahela põhise juhtimisega seotud küberturvalisuse riske ning selliseid kaitsemeetmeid nagu käitaja sekkumismehhanismid ja tõrkekindluse olekud. Hilisema uuenduse käigus aktiveerib tootja automaatjuhtimise funktsioonid ja turvameetmed vastavalt algsele hinnangule. Tootmise seiresüsteemi ei ole seega oluliselt muudetud.

107. Samas võivad isegi piiratud või näiliselt ebaolulised uued funktsioonid põhjustada märkimisväärseid küberriske, mis mõjutavad vastavust olulistele nõuetele. Olulise muudatuse hindamine ei tohiks seega põhineda muudatuse ulatusel või keerukusel, vaid võimalikul kahjulikul mõju digielemente sisaldava toote küberriski profiilile ning seega oluliste nõuete rakendamisele.

Näide 44: tootja avaldab tarkvararakenduse uuenduse, millega lisatakse kasutaja meeldejätmise ehk püsiva sisselogimise võimalus, mis salvestab autentimistõendid kasutajamugavuse suurendamiseks lokaalselt. Kuigi selle funktsiooni ulatus on piiratud, toob see kaasa uusi riske, mis on seotud tõendite varguse, volitamata juurdepääsu ja seansikaaperdusega, mida ei võetud arvesse riskihindamise ajal. Uuendus mõjutab seega vastavust olulistele nõuetele. Tarkvararakendust on oluliselt muudetud.

Näide 45: tootja lisab olemasolevale digielemente sisaldavale tarkvaratootele uue logimis- ja diagnostikafunktsiooni, mis võimaldab eksportida rikkeotsingu otstarbel üksikasjalikke süsteemilogisid. Kuigi see funktsioon näib olevat ebaoluline, kogutakse ja salvestatakse selle tulemusena tundlikke kasutusandmeid krüpteerimata kujul, mis tekitab teabepaljangu riske, mida ei ole varem hinnatud ega maandatud. Muudatus võib seega oluliselt mõjutada digielemente sisaldava toote küberriski profiili. Digielemente sisaldavat tarkvaratoodet on oluliselt muudetud.

108. Kooskõlas küberkerksuse määruse põhjendusega 39 ei käsitata turvauuendusi üldjuhul oluliste muudatustena, kuna nende peamine otstarve on vähendada digielemente sisaldava tootega seotud küberriski taset. Turvauuendust, mis ei muuda toote sihtotstarvet ja ei tekita uusi küberriske, ei tohiks seega käsitada olulise muudatusena isegi juhul, kui kõnealuse uuenduse tulemusena võidakse teha märkimisväärseid tehnilisi muudatusi. See hõlmab olukordi, kui teatavaid funktsioone muudetakse või piiratakse üksnes kindlaks tehtud nõrkuste vähendamiseks ja olulistele nõuetele jätkuva vastavuse tagamiseks.

Näide 46: tootja rakendab turvauuenduse, et vähendada digielemente sisaldava toote koodibaasi nõrkust, parandades sisendi valideerimise vea, mis võib põhjustada puhvri ületäitumise, või parandades loogikavea, mis võimaldab seansi identifikaatori väära valideerimise teel autentimisest mööduda. Uuendusega muudetakse tarkvara sisemist teostust, mõjutamata kõnealuse toote sihtostarvet ega tekitamata uusi riske. Selle uuenduse ainus eesmärk on vähendada küberriski. Turvauuendust ei tohiks käsitada olulise muudatusena.

Näide 47: tootja võtab kasutusele turvauuenduse, millega tugevdatakse olemasolevat turvalisuse konfigureerimist, näiteks karmistatakse tulemüüri reegleid, keelatakse kasutamata võrgupordid, muudetakse administraatori vaikeparooli põhimõtteid või tehakse mitmikautentimine kohustuslikuks, kui kõnealune funktsioon oli juba saadaval või kavas. Kuigi uuendus võib mõjutada viisi, kuidas kasutajad digielemente sisaldavat toodet konfigureerivad või sellele juurdepääsu saavad, ei muuda see sihtotstarvet ning selle ainus eesmärk on suurendada turvaolekut. Turvauuendust ei tohiks käsitada olulise muudatusena.

Näide 48: tootja laseb turule digielemente sisaldava tarkvaratoote, mis tagab side turvalisuse, kasutades konfigureeritavat krüpteerimise raamistikku, mis toetab mitut krüptoalgoritmi ja võtme pikkust, nagu on kirjeldatud toote tehnilises dokumentatsioonis ja riskihindamises. Riskihindamine hõlmab kõiki digielemente sisaldavas tootes pakutavaid krüptograafilisi valikuid ja näeb ette teatavate algoritmide tulevast kasutusest kõrvaldamist. Riskihindamine hõlmab ka maandamismeetmeid, nagu krüptograafiline kohandatavus, sisemine võtmehaldus ja ühilduvuse testimine. Vastusena uutele krüptograafiaalastele suunistele võtab tootja kasutusele turvauuenduse, mis lülitab välja iganenud algoritmi ja aktiveerib tugevama, juba toetatud alternatiivi, tekitamata uut välist sõltuvust või muutmata andmevooge. Kuna uuendusega rakendatakse turvameede, mida nähti ette ja hinnati algse projekteerimise raames ning millega ei tekitata uusi küberriske, ei tohiks käsitada turvauuendust olulise muudatusena.

109. Samas võib turvauuenduse puhul olla tegemist olulise muudatusega juhul, kui hoolimata selle turvaeesmärgist on uuenduse tulemuseks digielemente sisaldava toote sihtotstarbe muutmine suuremas ulatuses, kui algselt ette nähti, või kui selle tulemusena tekivad uued või suuremad küberriskid. See võib olla nii näiteks juhul, kui uuendus muudab oluliselt kõnealuse toote piire või sõltuvusstruktuuri viisil, mida ei nähtud riskihindamise puhul ette, nt andmevoogude oluline muutmine või uute liideste lisamine, millele on väline juurdepääs.

Näide 49: tootja laseb turule digielemente sisaldava tarkvaratoote, mis on mõeldud kasutaja seadmesse salvestatud andmete kohalikuks krüpteerimiseks, võimaldades kasutajatel faile vastavalt vajadusele krüpteerida ja dekrüpteerida. Pärast krüpteerimise töövoos nõrkuse avastamist võtab tootja kasutusele turvauuenduse, millega kõrvaldatakse kohaliku krüpteerimise funktsioon ning nõutakse selle asemel, et kõik failid laaditaks üles tootja käitatavasse kaugkrüpteerimise teenusesse ning neid säilitatakse ja töödeldakse seal. Selle muudatuse tulemusena ei võimalda digielemente sisaldav toode enam kohalikku krüpteerimist, nagu oli algselt ette nähtud, ning toimib selle asemel kaugkrüpteerimise ja andmetöötluse teenusena. Kuigi uuendus tehakse turvalisuse kaalutlustel, muudab see olemuslikult kõnealuse toote sihtotstarvet viisil, mida ei ole riskihindamises ette nähtud, ning seega on tegemist olulise muudatusega.

Näide 50: tootja laseb turule digielemente sisaldava tarkvaratoote, mis tugineb väljakujunenud krüpteerimisprotokollile ja sisemiselt hallatavate võtmete elutsüklile, et tagada digielemente sisaldava toote komponentide vahelise side turvalisus. Vastusena uutele kindlaks tehtud krüptograafilistele nõrkustele võtab tootja kasutusele turvauuenduse, mis asendab olemasoleva krüpteerimismehhanismi teise protokolliga, mis nõuab kolmanda isiku käitatava välise võtmehaldusteenuse kasutamist. Selle muudatuse tulemusena muutuvad oluliselt digielemente sisaldava toote sõltuvused ja andmevood, võetakse kasutusele uued välisliidesed ning tuginetakse kolmanda isiku teenustele, mida ei ole riskihindamises arvesse võetud. Kuigi uuendus on ajendatud turvakaalutlustest, tekitatakse sellega uued küberriskid ning seega on tegemist olulise muudatusega.

110. Nagu on märgitud punktis 104 eespool, tuleks tarkvarauuenduse puhul hinnata olulise muudatuse olemasolu iga juhtumi puhul eraldi. Seda hindamist tehes võivad tootjad muu hulgas kaaluda, kas tarkvarauuenduse puhul kehtib järgmine:

a) sellega luuakse uued ründevektorid, näiteks täiendavad liidesed, sidekanalid, täitmiskeskkonnad või välised sõltuvused, mille kaudu ohud võivad realiseeruda;

b) see võimaldab uusi ründestsenaariume, sh näiteks võivad ilmneda uued viisid, kuidas saada lubamatu juurdepääs, manipuleerida, sekkuda või väärkasutada digielemente sisaldavat toodet või selle töödeldavaid andmeid;

c) see muudab varem kindlaks tehtud ründestsenaariumide rakendumise tõenäosust, näiteks vähendades vaeva või eksperdioskusi, mida on vaja nende ärakasutamiseks, suurendades kokkupuudet ebausaldusväärsete osalejatega või nõrgendades olemasolevaid kaitsemeetmeid;

d) see muudab varem kindlaks tehtud ründestsenaariumide võimalikku mõju, näiteks mõjutatud andmete või funktsioonide ulatust, tegevuslike, ohutuse või majanduslike tagajärgede tõsidusastet või suutlikkust intsidenti avastada, see kontrolli alla saada või sellest taastuda.

111. Mõnel juhul ei tekita tarkvarauuendus uusi ründevektoreid, ei võimalda uusi ründestsenaariume ja ei muuda oluliselt varem kindlaks tehtud ründestsenaariumide avaldumise tõenäosust või mõju. See võib näidata, et uuendusest ei teki uusi ega suuremaid küberturvalisuse riske, kui riskihindamise eeldused ja selle raames rakendatud maandamismeetmed on jätkuvalt kehtivad ja tõhusad. Seega on tõenäoline, et uuenduse puhul ei ole tegemist olulise muudatusega.

112. Samas võib tarkvarauuendus tekitada uusi ründevektoreid, võimaldada uusi ründestsenaariume või muuta oluliselt varem kindlaks tehtud ründestsenaariumide avaldumise tõenäosust või mõju. Sellistel juhtudel peaks tootja uuesti hindama digielemente sisaldava toote küberturvalisuse riske ja tegema kindlaks, kas olulised nõuded on jätkuvalt täidetud, sh kui uuendus põhjustab uusi või suuremaid riske, mida riskihindamises ei olnud ette nähtud.

113. See, kas tarkvarauuendust käsitatakse olulise muudatusena, on asjakohane, kui tehakse kindlaks, kas kehtivad küberkerksuse määrusest tulenevad teatavad kohustused, nagu on märgitud punktis 91. Kuid sellisest liigitamisest hoolimata vastutavad tootjad tarkvarauuenduste ja oma digielemente sisaldava toote turvalisuse eest toote toe kestuse vältel kooskõlas küberkerksuse määruse I lisa II osas märgitud nõrkuste käsitlemise nõuetega. Lisaks sellele peavad tootjad olenemata sellest, kas tarkvarauuendusi käsitatakse oluliste muudatustena või mitte, säilitama kõnealuse riskihindamise ja tehnilise dokumentatsiooni täpsust, terviklikkust ja pidevat ajakohasust kooskõlas artikli 13 lõikega 7 ja artikli 31 lõikega 2.

4.4. **Olulise muudatuse tagajärjed**

114. Muu osaleja kui juba turule lastud digielemente sisaldava toote algse tootja tehtud olulise muudatuse tagajärgi on käsitletud küberkerksuse määruse artiklites 21 ja 22. Artikkel 21 käsitleb importijaid ja turustajaid ning artikkel 22 käsitleb mis tahes füüsilist või juriidilist isikut, kes ei ole tootja, importija ega turustaja.

115. Kui olulise muudatuse teeb digielemente sisaldava toote algne tootja, siis tulenevad tagajärjed küberkerksuse määruse põhjenduses 41 osutatud laialdaselt juurdunud mõistest, mida on täpsemalt kirjeldatud sinise raamatu punktis 2.1. Selles punktis on märgitud, et toodet, mida on pärast turule laskmist oluliselt muudetud või täiustatud, tuleb pidada uueks tooteks juhul, kui selle algset toimivust, otstarvet või tüüpi on muudetud, muutunud on ohu iseloom või tõusnud on ohu tase ning digielemente sisaldav toode tehakse turul kättesaadavaks.

116. Sellest tulenevalt on üldiselt kehtestatud põhimõte, et kui digielemente sisaldava toote muutmise puhul on tegemist olulise muudatusega ja muudetud digielemente sisaldav toode tehakse turul kättesaadavaks, tuleb seda käsitada küberkerksuse määruse tähenduses uue digielemente sisaldava tootena. Seega loetakse oluliselt muudetud toote turul kättesaadavaks tegemist uueks turule laskmiseks. See kehtib olenemata sellest, kas olulise muudatuse teeb algne tootja või muu isik. Eesmärgiga tagada, et küberkerksuse määrust kohaldatakse olulist muudatust teha võivate osalejate eri kategooriate puhul ühtsel ja proportsionaalsel viisil, käsitlevad järgmised alapunktid olulist muudatust tegevale isikule tekkivaid kohustusi oluliselt muudetud digielemente sisaldava toote turule laskmisel. Digielemente sisaldava toote toe kestuse tagajärgi on käsitletud punktis *5 Toe kestus*.

4.4.1. *Muu isiku kui algse tootja tehtud oluline muudatus*

117. Artiklite 21 ja 22 kohaselt, kui juba turule lastud digielemente sisaldava toote olulise muudatuse teeb füüsiline või juriidiline isik, kes ei ole digielemente sisaldava toote tootja, siis käsitatakse isikut, kes teostab olulise muudatuse ja teeb muudetud digielemente sisaldava toote turul kättesaadavaks, muudetud digielemente sisaldava toote tootjana olenemata sellest, kas see isik osales kõnealuse toote algses projekteerimises või turule laskmises.

118. Artiklis 22 on täpsustatud, et muudatuse teinud isiku suhtes kohaldatakse artiklites 13 ja 14 sätestatud kohustusi ainult digielemente sisaldava toote selle osa puhul, mida on oluliselt muudetud, kui muudatus ei mõjuta digielemente sisaldava toote kui terviku küberturvalisust.

119. Kui oluline muudatus mõjutab vastavust olulistele nõuetele, kuid ei mõjuta negatiivselt digielemente sisaldava toote kui terviku küberturvalisust, siis kohaldatakse muudatuse teinud isiku suhtes artikleid 13 (sh kohustust tagada vastavus olulistele nõuetele ja teha vastavushindamismenetlus) ning 14 (teatamiskohustused) ainult digielemente sisaldava toote selle osa suhtes, mida on oluliselt muudetud ([16]). Lisaks sellele kohaldatakse küberkerksuse määrusest tulenevaid algse tootja kohustusi jätkuvalt turule lastud algse digielemente sisaldava toote suhtes, tagades järjepidevuse nõrkuste käsitlemisel ning muudatusteta osade nõuetele vastavuse.

120. Olulist muudatust ei tohiks ajada segamini integreerimisega, mille puhul isik paneb komponendid (sh vajaduse korral neid muutes) kokku uueks digielemente sisaldavaks tooteks, mille laseb ise turule. Sellistel juhtudel ei muuda integreerija juba teise tootja turule lastud digielemente sisaldavat toodet, vaid ta laseb selle asemel ise turule uue digielemente sisaldava toote. Integreerija on küberkerksuse määruse tähenduses kõnealuse uue digielemente sisaldava toote tootja ja ta on kohustatud täitma määrust täies ulatuses seoses digielemente sisaldava tootega tervikuna. Kui tootja integreerib komponendid, mille suhtes kohaldatakse küberkerksuse määrust, siis võib ta tugineda komponentide tootjate vastavust tõendavatele toimingutele, et hõlbustada oma toote vastavusse viimist küberkerksuse määruse nõuetega.

Näide 51: ettevõte ostab kolmandast isikust tarnijatelt mikrokontrolleri valmismoodulid ja ühenduvuskomponendid, arendab omandiõigusega kaitstud püsivara ja anduripaketi ning paneb need kokku digielemente sisaldavaks võrguühendusega põllumajanduslikuks seireseadmeks, mille ta laseb turule enda nime all. Kuigi ettevõte on muutnud aluseks olevaid mikrokontrolleri mooduleid ja kombineerinud neid teiste komponentidega, ei muuda ta oluliselt juba turule lastud digielemente sisaldavat toodet, vaid ta laseb selle asemel turule uue digielemente sisaldava toote. Ettevõte on küberkerksuse määruse tähenduses põllumajandusliku seireseadme tootja ja ta on kohustatud täitma määrust seoses selle seadmega tervikuna.

([16]) Kooskõlas sinise raamatu punktiga 2.1 ei ole „aspektides, mida muutmine ei mõjuta, [---] vaja korrata katseid ega koostada uusi dokumente. Toodet muutnud või muuta lasknud füüsilise või juriidilise isiku ülesanne on tõendada, et kõiki tehnilisi dokumente ei ole vaja ajakohastada. Toodet muutnud või muuta lasknud füüsiline või juriidiline isik peab tagama muudetud toote vastavuse ning koostama vastavusdeklaratsiooni, isegi kui ta lähtub juba tehtud katsetest ja tehnilisest dokumentatsioonist“.

121. Kui muu isiku kui algse tootja tehtud oluline muudatus mõjutab negatiivselt digielemente sisaldava toote kui terviku küberturvalisust, näiteks kuna muudatus ei ole enam sihipärane või ei piirdu konkreetse komponendi või allsüsteemiga, siis tuleks turul kättesaadavaks tehtud digielemente sisaldavat muudetud toodet käsitada uue digielemente sisaldava tootena, mille suhtes kohaldatakse tervikuna küberkerksuse määrust. Neil juhtudel on selle toote üldine küberriski profiil muutunud ja muudatust ei saa hinnata, käsitlemata digielemente sisaldavat toodet tervikuna. Muudatuse teinud isiku suhtes kohaldatakse artiklites 13 ja 14 sätestatud tootja kohustusi seoses digielemente sisaldava muudetud tootega tervikuna.

4.4.2. *Algse tootja tehtud oluline muudatus*

122. Kui olulise muudatuse teeb algne tootja, sh digielemente sisaldavate tarkvaratoodete järkjärgulise arendamise kontekstis, siis jääb kõnealune tootja küberkerksuse määruse tähenduses tootjaks. Oluliselt muudetud digielemente sisaldavat toodet käsitatakse aga uue turule lastud tootena.

123. Sinise raamatu punkti 2.1 kohaselt võib oluliselt muudetud digielemente sisaldava toote turule lasknud algne tootja taaskasutada olemasolevat dokumentatsiooni ja katsetulemusi digielemente sisaldava toote aspektide puhul, mida oluline muudatus ei mõjuta. Eriti juhul, kui tootja laseb turule digielemente sisaldava sama toote oluliselt muudetud versioonid, peaks vastavushindamismenetlus keskenduma digielemente sisaldava toote oluliselt muudetud osadele. Samuti peaks kolmanda poole tehtava vastavushindamise korral vastavushindamisasutus keskenduma oma hindamises oluliselt muudetud osadele. Digielemente sisaldava toote muutmata osade puhul võib ta taaskasutada olemasolevat dokumentatsiooni ja katsetulemusi.

124. Eelmises alapunktis märgitud proportsionaalsuse kaalutlusi kohaldatakse samal moel oluliste muudatuste suhtes, mille on teinud enne 11. detsembrit 2027 turule lastud digielemente sisaldava toote algne tootja. Selline algse tootja tehtud oluline muudatus ei nõua iseenesest, et tootja viiks enne seda kuupäeva turule lastud digielemente sisaldava toote täielikku vastavusse küberkerksuse määrusega, v.a juhul, kui muudatus mõjutab negatiivselt digielemente sisaldava toote kui terviku küberturvalisust. Kui muudatus ei mõjuta digielemente sisaldava toote kui terviku küberturvalisust, siis peaksid algse tootja kohustused, mis on seotud muudatusega, piirduma oluliselt muudetud osadega.

5. **TOE KESTUS**

125. Küberkerksuse määruse artikli 13 lõikes 8 nõutakse, et tootja määraks kindlaks toe kestuse, mille jooksul digielemente sisaldava toote, sh selle komponentide, nõrkusi käsitletakse tulemuslikult ja kooskõlas I lisa II osas sätestatud oluliste nõuetega. Toe kestus kajastab ajavahemikku, mille vältel digielemente sisaldav toode on eeldatavasti kasutuses (eeldatav kasutusaeg) ning see tuleks määrata kindlaks, võttes arvesse artikli 13 lõikes 8 sätestatud kriteeriume, eelkõige kasutajate mõistlikke ootusi, digielemente sisaldava toote olemust, sh selle sihtotstarvet, ning samuti asjakohaseid liidu õigusnorme, millega määratakse kindlaks digielemente sisaldavate toodete kasutusiga ([17]). Üldiselt tuleks neid kriteeriume võtta arvesse viisil, millega tagatakse toe kestuse kindlaksmääramisel proportsionaalsus.

([17]) Täiendavad kriteeriumid, mida võidakse artikli 13 lõike 8 kohaselt arvesse võtta, on tootjate poolt turule lastud sarnase funktsiooniga digielemente sisaldavate toodete toe kestus, kasutuskeskkonna kättesaadavus, põhifunktsioone täitvate ja kolmandatelt isikutelt hangitud integreeritud komponentide toe kestus ning küberkerksuse määruse kohaselt loodud halduskoostöörühma (ADCO rühm) ja komisjoni antud asjakohased suunised.

126. Artikli 13 lõikes 8 on samuti nõutud, et toe kestus oleks vähemalt viis aastat, v.a juhul, kui digielemente sisaldavat toodet kasutatakse eeldatavasti vähem kui viis aastat, millisel juhul vastab toe kestus eeldatavale kasutusajale. Minimaalne toe kestus on seega vaid kaitsemeede, millega tagatakse, et nõrkusi käsitletakse piisava aja jooksul, võimaldades samal ajal tootjatel võtta arvesse digielemente sisaldavaid tooteid, mille eeldatav kasutusaeg on tegelikult lühem. Selle kohta on esitatud täpsemad suunised põhjenduses 60, milles selgitatakse, et kui digielemente sisaldava toote mõistlikult eeldatav kasutusaeg on pikem kui viis aastat, siis peaks olema pikem ka toe kestus. Viieaastast toe kestust ei tohiks seega käsitada kõigi digielemente sisaldavate toodete puhul vaikimisi kasutatava ajavahemikuna. Selle asemel peaks tootja määrama kindlaks sobiliku toe kestuse, võttes arvesse artikli 13 lõikes 8 märgitud kriteeriume.

127. Artikli 13 lõikes 19 nõutakse, et tootjad märgiksid ostu ajal selgelt ja arusaadavalt toe kestuse lõppkuupäeva (vähemalt kuu ja aasta). Selles nõutakse samuti, et kui toe kestus on lõppenud, siis peab tootja kuvama kasutajatele selle kohta teate, kui see on digielemente sisaldava toote olemust arvestades tehniliselt teostatav. Selle kohustuse eesmärk on tagada kasutajatele läbipaistvus selle kohta, kui pikka turvatoe kestust nad võivad eeldada.

128. Digielemente sisaldavate tarkvaratoodete puhul, mida arendatakse ja antakse sageli välja järkjärguliselt ning mille puhul võidakse oluliselt muudetud versioone lasta sagedasti turule, tuleb toe kestust mõista sellest arendusmudelist lähtuvalt. Igal turule lastud digielemente sisaldava tarkvaratoote oluliselt muudetud versioonil peab olema artikli 13 lõike 8 nõuetele vastav teatatud toe kestus. See hõlmab minimaalset toe kestust vähemalt viis aastat, v.a juhul kui versiooni eeldatav kasutusaeg on tõendatavalt lühem, nagu on selgitatud ka põhjenduses 60. Punktis *5.1 Olulised muudatused ja toe kestus* on täpsemalt selgitatud, et kui oluline muudatus ei too kaasa muudatusi tegurites, millest lähtuvalt määrati algselt kindlaks digielemente sisaldava toote eeldatav kasutusaeg, siis jääb algne toe kestus muutumatuks (sh olukorras, kus järelejäänud toe kestus on lühem kui viis aastat).

129. Artikli 13 lõikega 10 võimaldatakse digielemente sisaldavate tarkvaratoodete puhul paindlikkust, lubades tootjatel teatavatel tingimustel tagada vastavuse I lisa II osa punktis 2 märgitud nõrkuste käsitlemise nõudele (nõrkustega tegelemine ja nende kõrvaldamine) ainult digielemente sisaldava tarkvaratoote viimati turule lastud versiooni puhul. See on lubatud juhul, kui varem turule lastud versioonide kasutajatel on tasuta juurdepääs viimasele turule lastud versioonile ja neil ei teki lisakulusid seoses riist- ja tarkvarakeskkonna kohandamisega, milles nad toote algversiooni kasutavad.

130. Artikli 13 lõike 10 otstarbel tuleks „lisakulude“ mõistet tõlgendada praktilisel ja proportsionaalsel viisil, võttes arvesse tarkvara hooldamise ja käitamise tarvapäraseid ning eeldatavaid tavasid. See ei hõlma mõistlikku tegevuskoormust, mis kaasneb tarkvarauuenduste kohaldamisega või turvalise tegevuskeskkonna säilitamisega, nagu personali tööaeg, korrapärane testimine, konfiguratsiooni kohandamine või aluseks oleva sõltuva tarkvara versioonitäiendid, mis on vajalikud kasutusaja lõppu jõudnud komponentide või teada olevate turvanõrkuste arvesse võtmiseks. Samas lisakulud osutavad koormusele, mis ületab seda, mida võiks tavapäraselt eeldada tarkvarauuenduste kontekstis, näiteks uue riistvara kohustuslik ostmine, taristu asendamine või kasutuskeskkonna olemuslikud muudatused.

131. Digielemente sisaldavate pidevalt muutuvate tarkvaratoodete puhul võivad tootjad lasta suhteliselt lühikeste ajavahemike järel turule järjestikused oluliselt muudetud versioonid ja eeldada, et kasutajad teevad korrapäraselt versioonitäiendusi. Neil juhtudel peab iga oluliselt muudetud versiooni teatatud toe kestus vastama turule laskmise ajal artikli 13 lõike 8 nõuetele. Teisisõnu peab tootja teatama kõnealuse oluliselt muudetud versiooni puhul uue toe kestuse. Kuid tootjad võivad tugineda artikli 13 lõikele 10, et lõpetada varasemate versioonide nõrkustega tegelemine ja nende kõrvaldamine, kui kasutajad saavad teha tasuta versioonitäienduse uuema versiooni

hankimiseks, ilma et neile tekiks eespool nimetatud viisil lisakulusid, isegi kui selle tulemuseks on kõnealuste varasemate versioonide lühem tegeliku toe kestus ([18]). Tootja suhtes kohaldatakse jätkuvalt muid I lisa II osa nõrkuste käsitlemise nõudeid ning samuti artikli 14 kohaseid teatamiskohustusi. Nagu on samuti selgitatud põhjenduses 40, hõlmavad need nõuded muu hulgas turule lastud digielemente sisaldava tarkvaratoote kõigi edasiste oluliselt muudetud versioonide puhul järgmist: i) nõrkuste avalikustamise koordineeritud poliitika säilitamine; ning ii) meetmed, mis hõlbustavad teabe jagamist võimalike nõrkuste kohta ([19]).

Näide 52: tootja laseb ELi turule nutitelefoni mudeli ja teatab toe kestuse X aastat alates turule laskmise kuupäevast, mille vältel ta tagab nõrkusi kõrvaldavaid turvauuendusi. Selle ajavahemiku jooksul annab tootja välja operatsioonisüsteemi korrapäraseid tarkvarauuendusi ja oluliselt muudetud versioone, mille kasutajad saavad tasuta installida, ilma et selleks oleks vaja uut riistvara.

Tootja võib kooskõlas artikli 13 lõikega 10 tegeleda selle nutitelefoni mudeli jaoks kättesaadavaks tehtud operatsioonisüsteemi viimase versiooni nõrkustega ja neid kõrvaldada, kui varasemaid versioone saab ajakohastada tasuta ja lisakuludeta. Toe kestuse ajal peab tootja täitma muid nõrkuste käsitlemise nõudeid, nagu nõrkuste koordineeritud avalikustamise ja teabe jagamise meetmed.

Näide 53: tootja laseb turule digielemente sisaldava äritarkvara toote ja annab iga mõne kuu tagant välja oluliselt muudetud versioonid, milles on tehtud turvatäiendusi, lisatud uusi funktsioone ning tagatud ühilduvus ajakohastatud operatsioonisüsteemide ja platvormidega. Iga versiooni turule laskmise ajal antakse teada toe kestus kooskõlas artikli 13 lõikega 8. Tootja eeldab, et kasutajad teevad tavapärase käitamise käigus korrapäraselt versioonitäiendusi, ja annab tasuta juurdepääsu uusimale versioonile. Versioonitäienduste tegemine võib nõuda mõistlikke operatiivseid pingutusi, näiteks testimist või konfiguratsiooni kohandamist, aga see ei tekita selliseid lisakulusid nagu uue riistvara ostmine või olemuslikud taristumuudatused. Selles kontekstis võib tootja tugineda artikli 13 lõikele 10, et lõpetada nõrkustega tegelemine ja nende kõrvaldamine varasemate versioonide puhul, kui kasutajatel on võimalik minna üle versioonitäienduse uusimale versioonile, ning jätkata muude nõrkuste käsitlemise nõuete täitmist kõigi edasiste oluliselt muudetud versioonide puhul.

5.1. **Olulised muudatused ja toe kestus**

132. Nagu on märgitud punktis 4.4 *Olulise muudatuse tagajärjed*, kui digielemente sisaldava toote muudatuse puhul on tegemist olulise muudatusega ja digielemente sisaldav muudetud toode tehakse turul kättesaadavaks, siis käsitatakse seda küberkerksuse määruse tähenduses uue tootena ja digielemente sisaldava oluliselt muudetud toote turul kättesaadavaks tegemist käsitatakse uue turule laskmisena. Seetõttu on kasulik selgitada mõju, mida kõnealune uus turule laskmine avaldab digielemente sisaldava oluliselt muudetud toote toe kestusele.

133. Digielemente sisaldava oluliselt muudetud toote toe kestus tuleks määrata kindlaks lähtuvalt kõnealuse toote eeldatavast kasutusajast, võttes arvesse küberkerksuse määruse artikli 13 lõikes 8 märgitud kriteeriume. Seetõttu peaks oluline muudatus kaasa tooma nende kriteeriumide alusel uuesti hindamise, aga selle tulemuseks ei ole toe kestuse automaatne taasalustamine või isegi pikendamine. Küsimus on selles, kas oluline muudatus mõjutab tegureid, mille alusel määrati algselt kindlaks toote eeldatav kasutusaeg ning seega ka algne toe kestus.

([18]) Tuleb pidada silmas, et artikli 13 lõike 19 kohaselt peavad tootjad, kui see on digielemente sisaldava toote olemust arvestades tehniliselt teostatav, kuvama kasutajale teate selle kohta, et tema digielemente sisaldava toote toe kestus on lõppenud. Seega, kui varasemate versioonide nõrkustega tegelemine ja nende kõrvaldamine lõpetatakse, siis eeldatakse, et kui see on tehniliselt teostatav, siis teavitatakse sellest kasutajaid, kes ei ole teinud versioonitäiendust uusima versiooni hankimiseks.

([19]) Tuleb märkida, et kui kasutajad saavad teha ilma lisakuludeta versioonitäienduse tarkvara uusima versiooni hankimiseks, siis võivad tootjad sellest hoolimata otsustada jätkuvalt tegeleda kõnealuse tarkvara varasemate versioonide nõrkustega ja neid kõrvaldada, sh tasu eest või muu kaubandusliku kokkuleppe alusel. Küberkerksuse määrus ei nõua, et tootjad tagaksid tasuta kõnealuste varasemate versioonide turvauuendusi.

134. Kui oluline muudatus ei mõjuta neid tegureid, jääb artikli 13 lõikes 8 sätestatud kriteeriumide alusel jätkuvalt kehtima algselt kindlaksmääratud eeldatav kasutusaeg, ning digielemente sisaldava muudetud toote toe kestus peaks olema vastavuses algselt turule lastud toote eeldatava allesoleva kasutusajaga. See on üldjuhul nii, kui eeldatav kasutusaeg määrati kindlaks eelkõige selliste tegurite põhjal, mida muudatus ei mõjuta, näiteks riistvarakomponentide füüsiline vastupidavus, kui oluline muudatus on seotud ainult tarkvarafunktsiooni või tagasüsteemi teenustega.

Näide 54: tootja laseb turule robottolmuimeja, mille eeldatav kasutusaeg on X aastat, mis on määratud kindlaks lähtuvalt digielemente sisaldava toote olemusest, sh riistvarakomponentide füüsilisest vastupidavusest ja kulumisomadustest ning võttes arvesse kasutajate mõistlikke ootusi toote kasutusea kohta. Tootja määrab toe kestuseks X aastat. Pärast Y aasta möödumist annab tootja välja tarkvarauuenduse, mille puhul on tegemist olulise muudatusega ning millega lisatakse uued puhastusrežiimid ja navigatsiooniomadused. Tarkvarauuendus ei mõjuta riistvara füüsilist vastupidavust ega kasutajate mõistlikke ootusi toote kasutusea kohta. Artikli 13 lõike 8 kriteeriumidest tuleneb seega jätkuvalt sama eeldatav kasutusaeg. Digielemente sisaldava muudetud toote toe kestus vastab algselt kindlaks määratud allesolevale eeldatavale kasutusajale.

Näide 55: tootja laseb turule digielemente sisaldava keeruka tööstusmasina pilvepõhise tagasüsteemiga, mille puhul on tegemist andmete kaugtöötlemise lahendusega. Eeldatav kasutusaeg on X aastat, mis määratakse kindlaks lähtuvalt kasutajate mõistlikest ootustest ja digielemente sisaldava toote olemusest, nagu masina riistvara füüsiline vastupidavus ja eeldatav kulumine. Toe kestuseks määratakse X aastat, mis vastab eeldatavale kasutusajale. Pärast Y aasta möödumist muudab tootja pilvepõhise tagasüsteemi (andmete kaugtöötlemise lahenduse) arhitektuuri, võttes kasutusele uued rakendusliidesed ja andmevood viisil, mis on käsitatav digielemente sisaldava toote olulise muudatusena, kuid mis ei muuda toote olemust ega mõjuta kasutajate ootusi. Artikli 13 lõike 8 kriteeriumid viitavad jätkuvalt samale eeldatavale kasutusajale. Digielemente sisaldava muudetud toote toe kestus vastab algselt kindlaks määratud allesolevale eeldatavale kasutusajale.

135. Kui oluline muudatus mõjutab tegureid, mis määrasid algselt kindlaks digielemente sisaldava toote eeldatava kasutusaja, siis peaks tootja arvutama uuesti toe kestuse, et kajastada uut eeldatavat kasutusaega, kohaldades vastavalt artikli 13 lõike 8 kriteeriume. See võib nii olla näiteks selliste riistvara uuenduste puhul, mis pikendavad toote eluiga, või toote põhitarkvara olulise ümberprogrammeerimise või -kirjutamise puhul, mis oluliselt muudab eeldatavat kasutusaega ([20]).

Näide 56: tootja laseb turule programmeeritava kontrolleri, mille eeldatav kasutusaeg on X aastat, mis määratakse kindlaks eelkõige lähtuvalt digielemente sisaldava toote olemusest ja aluseks oleva riistvara vastupidavusest. Toe kestus määratakse vastavalt sellele. Kui algsest turule laskmisest on möödunud mitu aastat, teeb tootja olulise muudatuse, mis seisneb programmeeritava kontrolleri sisseehitatud andmetöötlusplatvormi, sh protsessori, mälu ja käitusaegse keskkonna asendamises uue põlvkonna komponentidega, mis on projekteeritud märksa pikemaks kasutuseaks. Muudatuse tulemusena muutuvad kasutajate mõistlikud eeldused ja digielemente sisaldava toote olemus: programmeritava kontrolleri kasutaja võib nüüd mõistlikult eeldada, et programmeeritav kontroller jääb tootlikku kasutusse selle algselt teatatud eeldatavast kasutusajast pikemaks ajaks tänu uuele andmetöötlusplatvormile. Artikli 13 lõike 8 kriteeriumid osutavad seega pikemale eeldatavale kasutusajale ja tootja arvutab selle konkreetse programmeeritava kontrolleri toe kestuse sellest lähtuvalt uuesti.

6. **DIGIELEMENTE SISALDAVAD OLULISED JA KRIITILISE TÄHTSUSEGA TOOTED**

136. Küberkerksuse määruse artikli 7 lõikes 1 on märgitud, et digielemente sisaldavaid tooteid, millel on mõne kõnealuse määruse III lisas sätestatud tootekategooria põhifunktsioon, käsitatakse „digielemente sisaldavate oluliste toodetena“. III lisas liigitatakse olulised tooted omakorda digielemente sisaldavateks I ja II klassi olulisteks toodeteks. Samal moel on artikli 8 lõikes 1 on märgitud, et digielemente sisaldavad tooted, millel on mõne küberkerksuse määruse IV lisas sätestatud tootekategooria põhifunktsioon, käsitatakse „digielemente sisaldavate kriitilise tähtsusega toodetena“ ([21]).

([20]) Tuleb pidada silmas, nagu on märgitud punktis *4.1 Füüsiline parandamine,* et taastamise, hoolduse või parandamise toiminguid ei käsitata üldjuhul oluliste muudatustena.

([21]) Komisjoni rakendusmääruses (EL) 2025/2392 on esitatud oluliste ja kriitilise tähtsusega toodete kategooriate tehniline kirjeldus.

137. Digielemente sisaldava toote liigitamine oluliseks või kriitilise tähtsusega tooteks või vastupidi nn vaikekategooriasse kuuluvaks ([22]) on oluline vastavushindamismenetluse kindlaksmääramisel, mida tootja peab artikli 32 kohaselt järgima, enne kui ta saab lasta kõnealuse digielemente sisaldava toote turule. Eelkõige võivad vaikekategooriasse kuuluvad digielemente sisaldavad tooted alati tugineda moodulil A põhinevale sisekontrollimenetlusele (enesehindamine) ([23]). Digielemente sisaldavad I või II klassi olulised tooted ja digielemente sisaldavad kriitilise tähtsusega tooted peavad läbima rangema vastavushindamismenetluse. See ei hõlma digielemente sisaldavaid I või II klassi olulisi tooteid, mida käsitatakse turule lastud vaba ja avatud lähtekoodiga tarkvarana, mille puhul võivad tootjad artikli 32 lõike 5 kohaselt järgida vaikekategooria menetlusi.

138. Põhifunktsiooni mõiste on seega oluline, kui tootja määrab kindlaks kohaldatava vastavushindamise korra. Kuid seda mõistet ei ole küberkerksuse määruses otseselt määratletud. Digielemente sisaldavad tooted saavad täita mitmesuguseid funktsioone, millest mõned võivad täiendada toote põhifunktsiooni ja mis ei tohiks mõjutada toote liigitamist vaikekategooria tooteks, I klassi oluliseks tooteks, II klassi oluliseks tooteks või kriitilise tähtsusega tooteks. Seega on kasulik esitada rohkem suuniseid, et aidata tootjatel korraldada nõuetekohaselt asjakohaseid vastavushindamismenetlusi ning aidata turujärelevalveasutustel tagada küberkerksuse määruse nõuete ühtlustatud täitmine kõikjal ELis.

6.1. **Põhifunktsioon**

139. Digielemente sisaldava toote põhifunktsioon osutab kõnealuse toote peamistele omadustele ja tehnilisele võimekusele, ilma milleta ei saaks see täita oma sihtotstarvet. Seda on võimalik hinnata kõnealuse toote konkreetset konteksti ja kasutustingimusi silmas pidades, võttes muu hulgas arvesse teavet, mille tootja esitab toote kasutusjuhendis, reklaam- või müügimaterjalides või avaldustes ning tehnilises dokumentatsioonis.

Näide 57: digielemente sisaldav tarkvaratoode loob abstraktsioonikihi alusriistvara kohale ja haldab tarkvarakomponentide käitamist. Selle peamised funktsioonid on riistvara ja välisseadmete lähtestamine, protsessi ja mälu haldamine, sisestuse ja väljastuse juhtimine, plaanimine, ressursijaotus ning süsteemiteenuste ja rakendusliideste, mille kaudu rakendused suhtlevad seadme riist- ja tarkvararessurssidega, kättesaadavaks tegemine. Tehnilises dokumentatsioonis on märgitud, et digielemente sisaldav toode suunab arvutusressursse, toetab süsteemi konfigureerimist ning tagab standarditud liidesed tarkvaramoodulitele ja ühendatud välisseadmetele. Tootja rõhutab, et need võimekused võimaldavad platvormil toimida keskse tarkvarakeskkonnana, kus saab usaldusväärselt käitada rakendusi. Digielemente sisaldaval tootel on operatsioonisüsteemi põhifunktsioon, nagu on kirjeldatud rakendusmääruse (EL) 2025/2392 I lisa punktis 11.

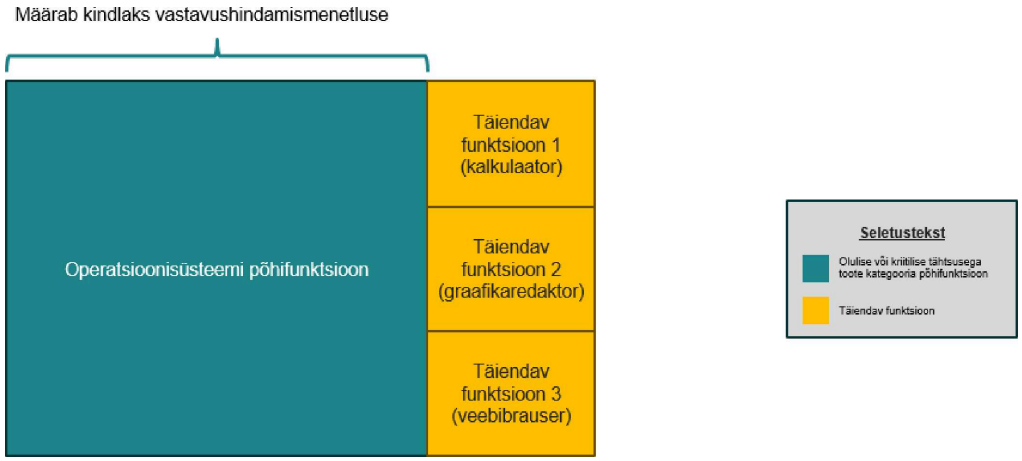
140. Digielemente sisaldava toote funktsioon piirdub harva selle põhifunktsiooniga, kuna digielemente sisaldavad tooted täidavad sageli, kui mitte alati, täiendavaid funktsioone, mis ei panusta toote põhifunktsiooni. See võib samuti hõlmata ka selliste komponentide lisamist, millel endil on muu digielemente sisaldava olulise või kriitilise tähtsusega toote funktsioon. Kuid asjaolu, et digielemente sisaldav toode täidab muid või täiendavaid funktsioone võrreldes nendega, mis on kirjas digielemente sisaldavate oluliste või kriitilise tähtsusega toodete tehnilises kirjelduses, ei takista iseenesest tootel omamast ühte sellist põhifunktsiooni.

([22]) Mõiste „vaikekategooria“ ei ole küberkerksuse määruses määratletud mõiste. Käesolevas dokumendis kasutatakse seda mõistet, et osutada digielemente sisaldavatele toodetele, millel ei ole küberkerksuse määruse III või IV lisas sätestatud tootekategooria põhifunktsiooni ning mille suhtes kohaldatakse seega artikli 32 lõikes 1 sätestatud vastavushindamise korda.

([23]) Tootja võib sellest hoolimata alati otsustada kohaldada rangemat vastavushindamismenetlust, nagu on sätestatud artikli 32 lõikes 1.

Joonis 2

Näide selle kohta, kuidas kohaldatava vastavushindamismenetluse määrab kindlaks põhifunktsioon ja mitte täiendavad funktsioonid



141. Digielemente sisaldav toode võib suuta täita olulise või kriitilise tähtsusega tootekategooria funktsioone, kuid selle põhifunktsioon võib sellest hoolimata erineda sellise tootekategooria põhifunktsioonist. Neil juhtudel ei liigitata sellist digielemente sisaldavat toodet digielemente sisaldavaks oluliseks või kriitilise tähtsusega tooteks. Nagu on sõnaselgelt sätestatud küberkerksuse määruse artikli 7 lõikes 1 digielemente sisaldavate oluliste toodete kohta (ning kohaldades sama loogikat digielemente sisaldavate kriitilise tähtsusega toodete puhul), ei muuda pelk digielemente sisaldava olulise või kriitilise tähtsusega toote integreerimine iseenesest digielemente sisaldavat toodet digielemente sisaldavaks oluliseks või kriitilise tähtsusega tooteks.

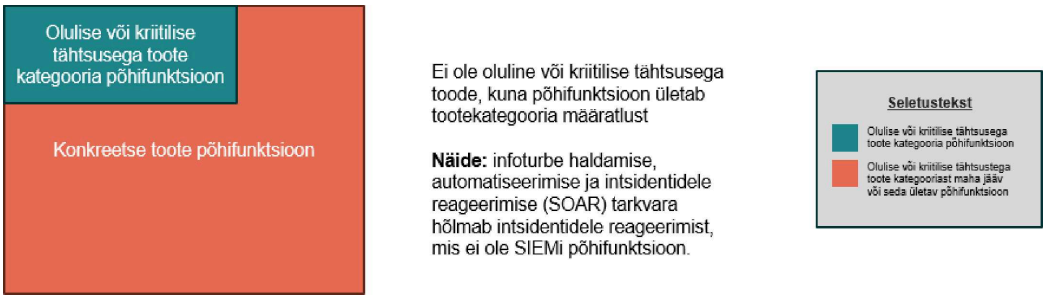
Näide 58: nutitelefoni integreeritakse operatsioonisüsteem, mis tagab rakendusmääruse (EL) 2025/2392 I lisa punktis 11 kirjeldatud funktsioonid. Kuigi operatsioonisüsteem võimaldab riistvararessursside haldamist ja tarkvararakenduste käitamist, on nutitelefonil tervikuna erinev põhifunktsioon (nt võimaldada kasutajatel suhelda ning saada juurdepääsu teabele ja teenustele). Pelgalt operatsioonisüsteemi integreerimine ei tähenda, et nutitelefonil on operatsioonisüsteemi põhifunktsioon.

142. Mõned digielemente sisaldavad tooted võivad sarnaneda olulise või kriitilise tähtsusega tootekategooriaga või kuuluda samasse üldisesse tooteperekonda, kuid nende põhifunktsioon võib märkimisväärselt ületada kõnealuse kategooria põhifunktsiooni või jääda sellest märkimisväärselt maha. See ei ole nii juhul, kui digielemente sisaldav toode sisaldab täiendavaid funktsioone, mis lihtsalt täiendavad või täiustavad põhifunktsiooni, mis ise vastab olulise või kriitilise tähtsusega tootekategooriale; sellistel juhtudel jääb digielemente sisaldavale tootele selle kategooria põhifunktsioon ja see liigitatakse vastavalt sellele. See hindamine peaks põhinema toote põhiomadustel ja tehnilisel võimekusel, mida vaadeldakse objektiivselt, võttes arvesse selle sihtotstarvet, ning mitte viisil, kuidas digielemente sisaldavat toodet kirjeldatakse või turundatakse, kui kõnealune kirjeldus ei kajasta toote tegelikke tehnilisi näitajaid.

Näide 59: infoturbe haldamise, automatiseerimise ja intsidentidele reageerimise (security orchestration, automation and response – SOAR) tarkvara on sageli võimeline täitma „turvateabe ja -sündmuste haldamise (security information and event management – SIEM) süsteemide“ kategooriasse kuuluvate digielemente sisaldavate toodete funktsioone, st koguma andmeid mitmest allikast, neid analüüsima ja leidma korrelatsioonid ning esitama neid turvaeesmärkidel rakendatava teabena. Kuid tarkvara põhifunktsioon ületab märkimisväärselt SIEMi põhifunktsiooni, hõlmates selle tehnilise võimekuse põhielementidena selliseid teenuseid nagu intsidentidele reageerimine. Seega ei käsitata SOARi tarkvara üldjuhul selliselt, et sellel on SIEMi süsteemide põhifunktsioon.

Joonis 3

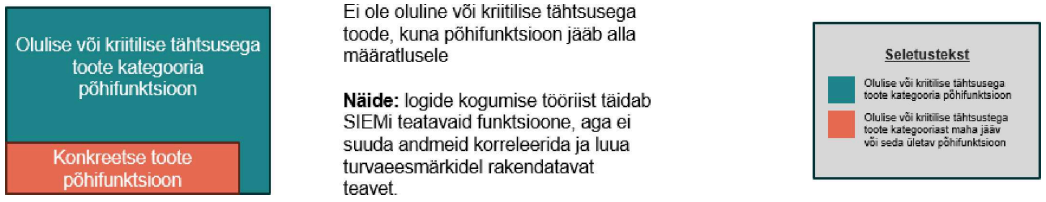
Näide digielemente sisaldava toote põhifunktsiooni kohta, mille elemendid ületavad märkimisväärselt olulise või kriitilise tähtsusega tootekategooria määratlust



Näide 60: teatavatel logide kogumis- ja visualiseerimisvahenditel on võime valmendada logi andmeid ja kuvada süsteemi sündmusi kajastavaid lihtsaid juhtpaneele. Kuigi need vahendid võivad toetada turvaseire toiminguid, jääb nende põhifunktsioon alla SIEMi süsteemide põhifunktsioonile, kuna need ei võimaldada leida andmete korrelatsioone ega paku praktiliselt rakendatavat teavet turvalisuse kohta. Seega ei käsitata kõnealuseid vahendeid üldjuhul selliselt, et neil on SIEMi süsteemide põhifunktsioon.

Joonis 4

Näide olukorrast, mille puhul digielemente sisaldava toote põhifunktsioon jääb märkimisväärselt alla olulise või kriitilise tähtsusega tootekategooria määratlusele

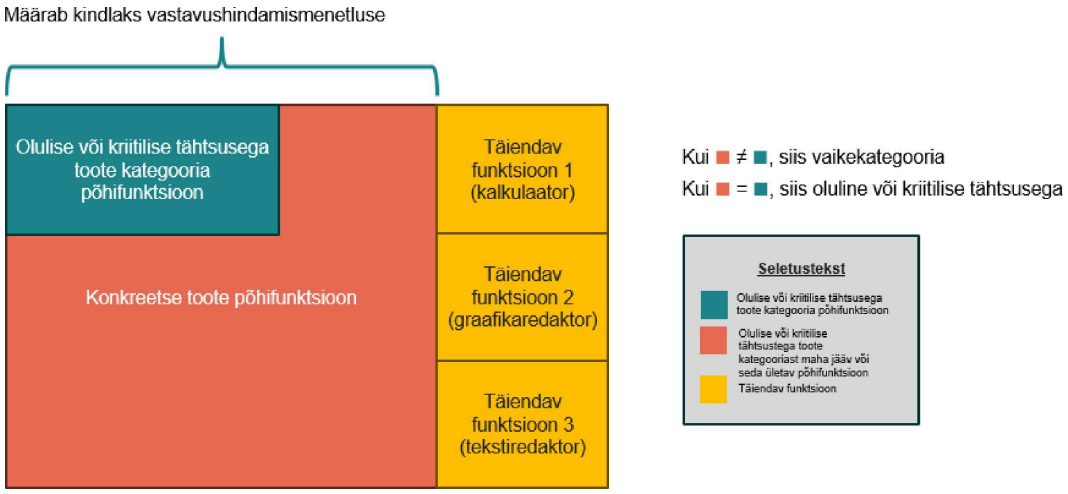


143. Tootja ei tohi esitada eksitavalt oma digielemente sisaldava toote põhifunktsiooni, et vältida digielemente sisaldavate oluliste või kriitilise tähtsusega toodete suhtes kohaldatava vastavushindamise korra rakendamist, näiteks rõhutades liigselt teatavate funktsioonide rolli või näidates neid tegelikust väiksemana, et toode ületaks märkimisväärselt teatavat põhifunktsiooni või jääks märkimisväärselt alla selle. See oleks nii näiteks juhul, kui esinevad selged ebakõlad reklaammaterjali, kasutusjuhendite ja tehnilise dokumentatsiooni vahel.

144. Digielemente sisaldaval tootel ei tohi olla kohaldatava vastavushindamise korra kindlaksmääramisel rohkem kui üks põhifunktsioon. Küberkerksuse määruse VII lisa kohaselt peavad tootjad kirjeldama toote tehnilise dokumentatsiooni osana nende digielemente sisaldava toote sihtotstarvet ja järgitud vastavushindamismenetlust. Toote põhifunktsioon tuleks seega selgelt kindlaks määrata. See võimaldab määrata õigesti kindlaks kohaldatava vastavushindamise korra ning turujärelevalveasutustel teha järelevalvet ja kontrollida, et määrust kohaldatakse õigesti.

Joonis 5

Näidis selle kohta, kuidas digielemente sisaldava konkreetse toote põhifunktsioon määrab kindlaks tooteklassi ja seeläbi kohaldatava vastavushindamismenetluse



145. Mõned digielemente sisaldavad tooted lastakse turule digielemente sisaldava ühe tootena, aga koosnevad eraldiseisvatest moodulitest, millel on erinevad funktsioonid. Kui tootja teeb need moodulid turul kättesaadavaks ka eraldi, näiteks juhul, kui neid pakutakse eraldi ostmiseks, litsentsimiseks või tellimiseks, siis on kõnealuste moodulite puhul tegemist eraldiseisvate digielemente sisaldavate toodetega. Seega tuleb need liigitada lähtuvalt nende vastavast põhifunktsioonist (ning seega tuleb nende suhtes kohaldada sobivat vastavushindamise korda lähtuvalt iga mooduli põhifunktsioonist). See ei piira moodulite tarnimist üksnes digielemente sisaldavasse tootesse integreeritud komponentidena, tegemata neid eraldiseisvalt kättesaadavaks; sellisel juhul määratakse põhifunktsioon kindlaks digielemente sisaldava integreeritud toote tasandil.

Näide 61: tootja laseb turule ühtse turvapaketi, millesse on koondatud mitu moodulit, sh SIEM, sissetungituvastuse süsteem ja analüüsimoodul. Tootja pakub neid mooduleid ka eraldi tellimuste alusel. Sellise stsenaariumi alusel on iga moodul eraldiseisev digielemente sisaldav toode ja liigitatakse lähtuvalt selle põhifunktsioonist. SIEMi mooduli suhtes kohaldatakse digielemente sisaldavate I klassi oluliste toodete vastavushindamise korda, kuna selle põhifunktsioon on „Turvateabe ja -sündmuste halduse (SIEM) süsteemid“. Sissetungituvastuse süsteemi suhtes kohaldatakse digielemente sisaldavate II klassi oluliste toodete vastavushindamise korda, kuna selle põhifunktsioon on „Tulemüürid, sissetungi tuvastamise ja ennetamise süsteemid“. Analüüsimooduli suhtes kohaldatakse digielemente sisaldavate vaikekategooriasse kuuluvate toodete vastavushindamise korda, kuna sellel ei ole olulise või kriitilise tähtsusega toote kategooria põhifunktsiooni.

146. Kui küberkerksuse määruse artiklis 32 sätestatud kohustused jäetakse täitmata, siis võidakse määrata haldustrahvid kooskõlas artikli 64 lõikega 3.

6.2. Digielemente sisaldavate oluliste ja kriitilise tähtsusega toodete vastavushindamine

147. Kui tootja on teinud kindlaks digielemente sisaldava toote põhifunktsiooni, siis peab ta tegema ühe kohaldatavatest vastavushindamismenetlustest. Tootja peab tagama, et digielemente sisaldav toode tervikuna vastab olulistele nõuetele, võttes vajadust mööda arvesse sellesse integreeritud komponentide või funktsioonide turvalisust.

148. Rangem vastavushindamismenetlus, milles osaleb kolmas isik (lähtuvalt moodulitest B+C, moodulist H või küberturvalisuse sertifitseerimise kavadest), on kohustuslik digielemente sisaldavate II klassi oluliste toodete puhul (v.a kui nende puhul on tegemist vaba ja avatud lähtekoodiga tarkvaraga kooskõlas artikli 32 lõikega 5) ning digielemente sisaldavate kriitilise tähtsusega toodete puhul ([24]). Samas peavad digielemente sisaldavad I klassi olulised tooted (v.a kui nende puhul on tegemist vaba ja avatud lähtekoodiga tarkvaraga kooskõlas artikli 32 lõikega 5) läbima kolmanda isiku vastavushindamismenetluse ainult juhul, kui tootja ei ole kohaldanud või on kohaldanud ainult osaliselt asjakohaseid harmoneeritud standardeid, mille viited on avaldatud *Euroopa Liidu Teatajas*, (edaspidi „harmoneeritud standardid"), ühtseid spetsifikatsioone, või Euroopa küberturvalisuse sertifitseerimise kava vähemalt märkimisväärsel usaldusväärsuse tasemel ([25]).

149. Seega selleks, et digielemente sisaldav I klassi oluline toode võiks läbida sisekontrollimenetluse, i) tuleb rakendada asjakohase harmoneeritud standardi kõiki kohaldatavaid nõudeid ning ii) standardi kohaldamisala peab hõlmama vähemalt kõiki kõnealuse toote põhifunktsiooniga seotud küberturvalisuse riske.

150. Digielemente sisaldava toote ulatus võib olla laiem kui asjakohases harmoneeritud standardis ette nähtud kohaldamisala ning kõnealused täiendavad funktsioonid võivad põhjustada erinevaid või täiendavaid küberriske. Tootja peab alati tegema artikli 13 lõike 2 kohase riskihindamise ning seejärel tuleks kontrollida, kas harmoneeritud standardi rakendamine hõlmab kõiki riske, mis on seotud digielemente sisaldava tootega. Kui standardi rakendamine ei hõlma kõiki riske, siis peaks tootja tagama muul viisil, et tema digielemente sisaldav toode vastab olulistele nõuetele.

151. Seega, kui digielemente sisaldava I klassi olulise toote tootja on kohaldanud asjakohast harmoneeritud standardit, mis hõlmab kõnealuse toote põhifunktsiooniga seotud riske, siis võib ta otsustada kasutada toote vastavuse tõendamiseks sisekontrollimenetlust. Tootja peab oma vastavushindamise toimingute osana siiski tõendama, et arvesse on võetud kõiki tema digielemente sisaldava toote puhul tekkivaid riske. Seega, kui harmoneeritud standardi ulatuse ja digielemente sisaldava toote kui terviku kohaldamisala vahel on erinevus, peab tootja siiski dokumenteerima, millised täiendavaid meetmeid ta on nende riskide maandamiseks võtnud.

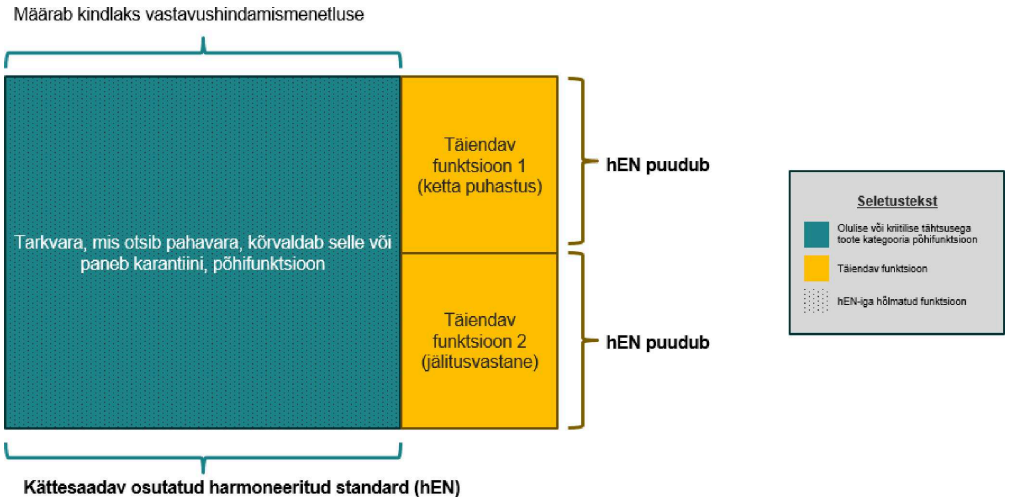
Näide 62: viirusetõrjetarkvara põhifunktsioon on pahavara otsimine, selle kõrvaldamine või karantiini panemine, nagu on märgitud rakendusmääruse (EL) 2025/2392 I lisa punktis 4. See digielemente sisaldav toode sisaldab ka täiendavaid funktsioone, nimelt ketta puhastamise funktsioon ja jälitusvastane funktsioon, mis kaitseb kasutajat internetis liikumisel. Tootja teeb riskihindamise, mis hõlmab digielemente sisaldavat toodet tervikuna, sh viirusetõrjetarkvara põhifunktsiooni, ketta puhastamise ja jälitusvastaseid funktsioone. Ta rakendab harmoneeritud standardit, mis hõlmab viirusetõrjetarkvara põhifunktsiooniga seotud riske, ning täiendavaid meetmeid lisafunktsioonidest tulenevate riskide maandamiseks. Tootja peab kasutama vastavushindamiseks sisekontrollimenetlust, mis hõlmab digielemente sisaldavat toodet tervikuna, sh ketta puhastamise ja jälitusvastaseid funktsioone.

([24]) See on samuti nii juhul, kui kasutatakse Euroopa küberturvalisuse sertifitseerimise kava vähemalt märkimisväärse usaldusväärsuse tasemega, kuna see nõuab kolmandast isikust sertifitseerimisasutuse osalemist.

([25]) Lühiduse huvides osutatakse käesoleva punkti ülejäänud osas ainult harmoneeritud standarditele, mille viited on avaldatud *Euroopa Liidu Teatajas*. Samas kehtivad need suunised ka artikli 27 lõike 2 kohaselt vastu võetud ühtsete spetsifikatsioonide puhul ning Euroopa küberturvalisuse sertifitseerimise kavade puhul, kui komisjon on nii kindlaks määranud delegeeritud õigusaktidega vastavalt artikli 27 lõikele 9.

Joonis 6

Näide selle kohta, kuidas ainult ühte põhifunktsiooni hõlmav osutatud harmoneeritud standard määrab kindlaks kohaldatava vastavushindamismenetluse



152. See kehtib ka juhul, kui digielemente sisaldavasse tootesse on integreeritud täiendav funktsioon, mis on ise muu digielemente sisaldav oluline või kriitilise tähtsusega toode. Tegelikult määrab selle, kas digielemente sisaldav toode kuulub oluliste või kriitiliste toodete kategooriasse (ja millist vastavushindamiskorda seetõttu kohaldatakse), just digielemente sisaldava toote kui terviku põhifunktsioon, mitte aga integreeritud komponentide funktsioonid. Näiteks kui digielemente sisaldaval tootel on digielemente sisaldava I klassi olulise toote põhifunktsioon, siis kohaldatakse kõnealuse toote kui terviku suhtes digielemente sisaldavate I klassi oluliste toodete suhtes kohaldatavat vastavushindamise korda isegi juhul, kui sellesse on integreeritud komponent, mis on ise digielemente sisaldav kriitilise tähtsusega toode. Neil juhtudel, kui tootja kohaldab harmoneeritud standardit, mis hõlmab kõnealuse toote põhifunktsiooniga seotud riske, võib ta kasutada sisekontrollimenetlust.

Näide 63: digielemente sisaldaval riistvaratootel on ruuteri põhifunktsioon, nagu on kirjeldatud rakendusmääruse (EL) 2025/2392 I lisa punktis 12. Kõnealusel digielemente sisaldaval tootel on ka täiendavad funktsioonid, sh tulemüüri võimekus, kuna sellesse on integreeritud tulemüüri komponent. Tootja teeb riskihindamise, mis hõlmab digielemente sisaldavat toodet tervikuna, sh ruuteri põhifunktsiooni ja tulemüüri funktsiooni. Ta rakendab harmoneeritud standardit, mis hõlmab ruuteri põhifunktsiooniga seotud riske, ning täiendavaid meetmeid lisafunktsioonidest tulenevate riskide maandamiseks. Näiteks võib tootja kohaldada tulemüüride harmoneeritud standardit, et hõlmata tulemüüri funktsiooniga seotud riske. Tootja võib kasutada vastavushindamiseks sisekontrollimenetlust, mis hõlmab digielemente sisaldavat toodet tervikuna, sh tulemüüri funktsiooni.

6.3. Nõuetele vastavuse eeldamise mõju

153. Küberkerksuse määruse artikli 27 lõikes 1 on märgitud, et digielemente sisaldavate toodete ja tootja rakendatud protsesside puhul, mis on vastavuses selliste harmoneeritud standardite või nende osadega, mille viited on avaldatud *Euroopa Liidu Teatajas*, eeldatakse vastavust küberkerksuse määruses sätestatud olulistele nõuetele, mida

nimetatud standardid või nende osad käsitlevad ([26]). Artikli 27 lõikega 5 laiendatakse sama nõuetele vastavuse eeldust digielemente sisaldavatele toodetele ja tootja rakendatud protsessidele, mis on vastavuses komisjoni rakendusaktidega kehtestatud ühtsete spetsifikatsioonidega, ning artikli 27 lõikega 8 kehtestatakse nõuetele vastavuse eeldus digielemente sisaldavate toodete ja tootja rakendatud protsesside puhul, mille kohta on välja antud ELi vastavusdeklaratsioon või sertifikaat vastavalt määruse (EL) 2019/881 alusel vastu võetud Euroopa küberturvalisuse sertifitseerimiskavale, kui see on sätestatud delegeeritud õigusaktidega vastavalt artikli 27 lõikele 9 ([27]).

154. Seega kui tootja on kohaldanud harmoneeritud standardit, mille viited on avaldatud *Euroopa Liidu Teatajas*, kehtib tema suhtes vastavuse eeldus kõnealuse standardiga hõlmatud riskide puhul. See võib olla nii näiteks juhul, kui osutatud harmoneeritud standard käsitleb kõiki digielemente sisaldava toote põhifunktsiooniga seotud riske ja tootel ei ole täiendavaid funktsioone, mis kujutaksid endast küberturvalisuse riske. Näiteks eeldatakse, et ruuterite harmoneeritud standard võtab arvesse vähemalt kõnealuste digielemente sisaldavate toodete põhifunktsiooniga seotud riske. Kui kõnealune toode ei sisalda täiendavaid funktsioone või kõnealused täiendavad funktsioonid ei tekita riske, mida ei ole standardis arvesse võetud, siis võib digielemente sisaldava toote puhul kohaldada vastavuse eelduse põhimõtet.

155. Punktides 151 ja 152 käsitletud juhtudel võib tootja kasutada sisekontrollimenetlust, kuna harmoneeritud standard hõlmab digielemente sisaldava toote põhifunktsiooniga seotud riske. Samas võib neis näidetes kirjeldatud digielemente sisaldavate toodete kohaldamisala olla laiem harmoneeritud standardite kohaldamisalast ja täiendavad funktsioonid võivad tekitada küberriske, mida ei ole sellises harmoneeritud standardis käsitletud. Seetõttu ei pruugi digielemente sisaldavate toodete puhul nende täiendavatele funktsioonidele laieneda vastavuse eelduse kohaldamine.

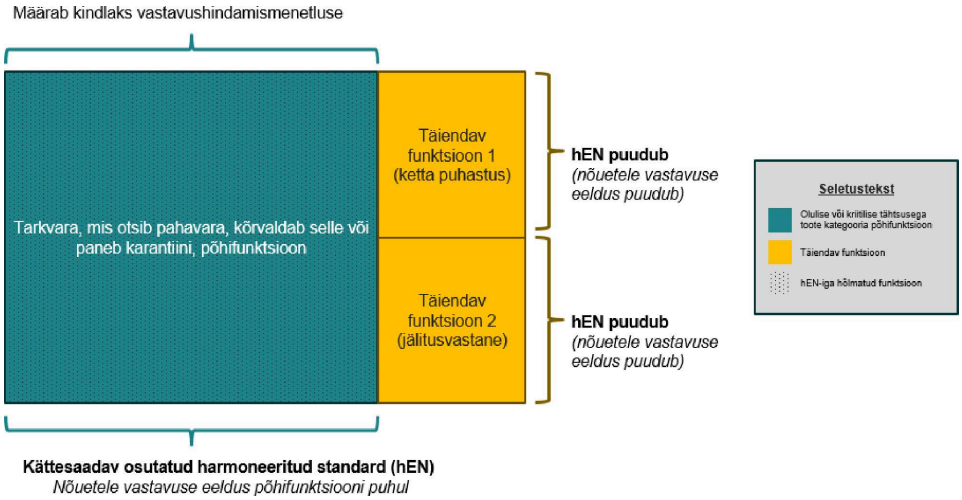
Näide 64: viirusetõrjetarkvara põhifunktsioon on pahavara otsimine, selle kõrvaldamine või karantiini panemine ning kõnealuse põhifunktsiooniga seotud riskid on hõlmatud harmoneeritud standardiga. See digielemente sisaldav toode sisaldab ka täiendavaid funktsioone, nimelt ketta puhastamise funktsiooni ja jälitusvastast funktsiooni, mis kaitseb kasutajat, kui ta kasutab internetti, mille riskid ei ole harmoneeritud standardiga hõlmatud. Kui kohaldatakse harmoneeritud standardit, siis võib tootja kasutada oma vastavushindamise jaoks sisekontrollimenetlust. Tootele kehtib vastavuse eeldus nende riskide puhul, mis on seotud toote põhifunktsiooniga, kuid mitte nende riskide puhul, mis on seotud täiendavate funktsioonidega.

([26]) Nagu on selgelt märgitud sinise raamatu punktis 4.1.2.2, isegi kui tootjad järgivad „[h]armoneeritud standardeid, mille viited on avaldatud *Euroopa Liidu Teatajas* avaldamise päeval, vastutavad nad jätkuvalt täiel määral kõikide oma toodetest tulenevate ohtude hindamise eest, et teha kindlaks, millised olulised (või muud) nõuded on asjakohased. Pärast sellist hindamist võib tootja otsustada kohaldada *Euroopa Liidu Teatajas* avaldamise päeval viidatud harmoneeritud standardites esitatud tehnilisi kirjeldusi, et rakendada harmoneeritud standardites kirjeldatud meetmeid ohtude vähendamiseks“.

([27]) Nagu on ka eespool märgitud, osutatakse lühiduse huvides käesoleva punkti ülejäänud osas ainult harmoneeritud standarditele, mille viited on avaldatud *Euroopa Liidu Teatajas*. Kuid samad suunised kehtivad ka ühtsete spetsifikatsioonide ning Euroopa küberturvalisuse sertifitseerimise kavade puhul.

Joonis 7

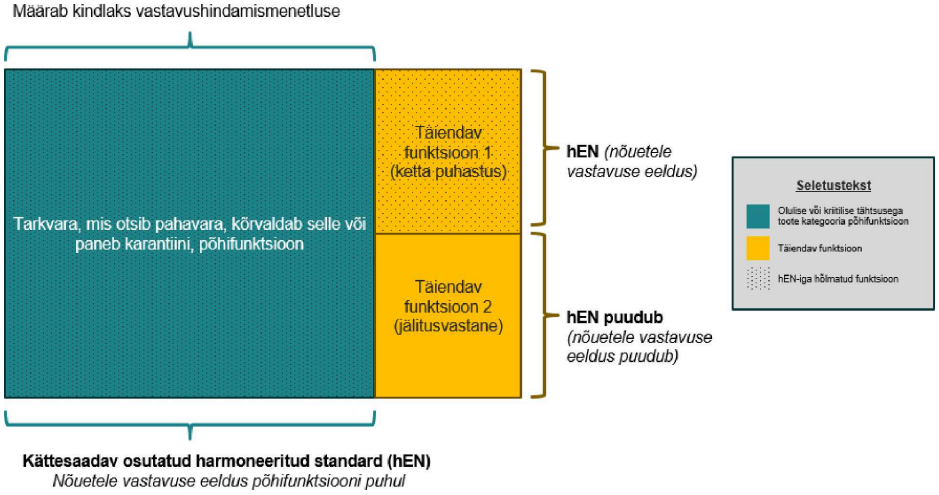
Harmoneeritud standard tagab nõuetele vastavuse eelduse põhifunktsiooni puhul, kuna see käsitleb kõiki selle põhifunktsiooniga seotud riske, kuid mitte täiendavate funktsioonide puhul



Näide 65: eelmises näites esitatud stsenaariumiga seoses on harmoneeritud standardit nüüd ajakohastatud, et see hõlmaks ka riske, mis on seotud ühe täiendava funktsiooniga, nimelt ketta puhastamise funktsiooniga, aga mitte teisega (s.o jälitusvastane funktsioon). Kui kohaldatakse harmoneeritud standardit, siis võib tootja kasutada oma vastavushindamise jaoks sisekontrolli-menetlust. Tootele kehtib vastavuse eeldus nende riskide puhul, mis on seotud toote põhifunktsiooniga ja ketta puhastamise funktsiooniga, aga mitte jälitusvastase funktsiooniga seotud riskide puhul.

Joonis 8

Harmoneeritud standard tagab nõuetele vastavuse eelduse põhifunktsiooni ja täiendava funktsiooni 1 puhul, kuna see käsitleb kõiki nende kahe funktsiooniga seotud riske, aga mitte täiendava funktsiooni 2 puhul



7. **KÜBERRISKIDE HINDAMINE NING DIGIELEMENTE SISALDAVATE TOODETE JA KOMPONENTIDE INTEGREERIMINE**

7.1. **Küberriskide hindamine ja nende maandamine**

156. Küberkerksuse määruse artikli 13 lõikes 2 sätestatud küberriskide hindamine nõuab, et tootjad teeksid kindlaks digielemente sisaldava toote asjakohased riskid ja hindaksid nende võimalikku mõju. Tootjad peavad samuti võtma sobilikud meetmed nende riskide maandamiseks kooskõlas I lisas märgitud oluliste nõuetega.

157. Organisatsiooni riskijuhtimise puhul hinnatakse riske üldjuhul lähtuvalt vastuvõetavuse kriteeriumidest, mis tulenevad organisatsiooni sisemistest eesmärkidest või riskinormist. Samas küberkerksuse määruse kohaselt tuleks järelejäänud küberriske hinnata lähtuvalt nõudest, et turule lastud digielemente sisaldava toote puhul tagatakse riskidest lähtuvalt asjakohane küberturvalisuse tase, võttes arvesse selle sihtotstarvet ja mõistlikult prognoositavat kasutamist.

158. Seega ei ole tootja sisemine riskitaluvus, äristrateegia või lihtsalt kulukaalutlused asjakohased selle kindlaks määramisel, kas riskid on maandatud. Artikli 13 lõigete 2 ja 3 kohaldamisel peavad tootjad suutma kindlaks teha, kas tuvastatud küberriske on piisavalt maandatud, rakendades I lisa I osa olulisi nõudeid, võttes arvesse sihtotstarvet, mõistlikult prognoositavat kasutamist ja kasutustingimusi, sh vajaduse korral kasutuskeskkonda (näiteks digielemente sisaldava toote kavandatud kasutajad) ja kaitstavaid varasid ning digielemente sisaldava toote eeldatavat kasutusaega.

159. Järelejäänud küberrisk on riskihindamise ja riskikäsitluse olemuslik tulemus. Võetakse arvesse, et küberriske ei saa tegelikkuses täielikult kõrvaldada. Kuid jääkriski olemasolu ei tähenda, et tootja võib oma äranägemise järgi leppida mis tahes riskiga. Digielemente sisaldava toote võib turule lasta ainult juhul, kui jääkriske on pärast asjakohaste meetmete võtmist piisavalt maandatud oluliste nõuete rakendamise teel, võttes arvesse digielemente sisaldava toote sihtotstarvet ja mõistlikult prognoositavat kasutamist.

160. Artikli 13 lõike 3 kohaselt peavad tootjad, kui küberriskid tehakse kindlaks, maandama neid sobilike meetmete abil, sh toote tasandil. Olenevalt asjaoludest võib see hõlmata näiteks ründepinna vähendamist, tehniliste kaitsemeetmete rakendamist, funktsioonide piiramist või kohandamist või digielemente sisaldava toote sihtotstarbe täpsemat määratlemist. Tootjad võivad samuti astuda samme, et kujundada digielemente sisaldava toote mõistlikult prognoositavat kasutamist, näiteks riskist teatamise, kasutajajuhiste või -liidese projekteerimise teel, et suunata kasutajate käitumist turvaliste kasutusviiside poole.

161. Küberkerksuse määruses ei nähta ette küberriski või vastutuse ülekandmist kasutajatele või kolmandatele isikutele, et korvata toote projekteerimise vajakajäämisi või õigustada küberriskide maandamata jätmist. Kohustus lasta turule turvaline digielemente sisaldav toode ja tõendada vastavust olulistele nõuetele jääb tootjale.

162. Kasutajatele antavat teavet ja juhiseid võib kasutada digielemente sisaldava toote turvalise kasutuselevõtu ja käitamise toetamiseks, sh juhul, kui tootja on otsustanud piirata kõnealuse toote kasutusotstarbe usaldusväärsete keskkondadega ja teavitada kasutajaid jääkriskidest viisil, mis on asjakohane, arvestades digielemente sisaldava toote olemust ja selle sihtkasutajaid.

Näide 66: tootja töötab välja tööstusliku anduri kasutamiseks usaldusväärses keskkonnas. Selleks et andur täidaks oma funktsioone õigesti, ei rakenda tootja meetmeid kaitseks anduri enda vastu suunatud füüsiliste rünnete eest. Riskihindamise käigus kindlaks tehtud seotud riskide maandamiseks piirab tootja anduri sihtotstarvet ainult usaldusväärsete keskkondadega, kus takistatakse lubamatut füüsilist juurdepääsu digielemente sisaldavale tootele. Kasutajatele esitatav teave ja juhised annavad selget teavet sensori kõnealuste kasutuspiirangute kohta viisil, mis on asjakohane lähtuvalt digielemente sisaldava toote olemusest ja selle sihtkasutajatest.

Näide 67: tootja arendab tarkvararakenduse, mis on mõeldud erialaseks kasutuseks hallatavates lauaarvutites ja mobiilseadmetes. Rakendus töötleb kohalikult salvestatud tundlikke andmeid ja kasutaja loodud sisu. Riskihindamise ajal teeb tootja kindlaks kõnealustele andmetele volitamata juurdepääsu riski, kui neid andmeid säilitakse seadmes avateksti kujul. Omandiõigusega kaitstud krüpteerimismehhanismi projekteerimise ja selle rakenduses kasutusele võtmise asemel otsustab tootja tugineda selle rakenduse käitamiseks ette nähtud operatsioonisüsteemi algsetele krüpteerimise ja võtmehalduse funktsioonidele, kuna operatsioonisüsteemi sisseehitatud krüptoteenused on lõpuni välja arendatud ja neid hooldatakse korrapäraselt.

163. Kui küberriskide hindamise käigus tehakse kindlaks riskid, mida ei saa sobilike meetmete abil piisavalt maandada, siis võib küberkerksuse määruse nõuete täitmiseks olla vaja muuta digielemente sisaldava toote projekteerimist, funktsioone või sihtotstarvet. Ainult kuludest või ärilisest otstarbekusest lähtuvad kaalutlused ei ole piisav alus nende riskide maandamata jätmiseks, kui selle tõttu ei vastaks digielemente sisaldav toode olulistele nõuetele.

7.2. **Digielemente sisaldavate toodete projekteerimine, arendamine ja tootmine sellisel viisil, et need tagaksid riskidest lähtuvalt asjakohase küberturvalisuse taseme**

164. Küberkerksuse määruse I lisa I osa punktis 1 osutatud oluliste küberturvalisuse nõuetega nähakse ette, et digielemente sisaldavad tooted tuleb projekteerida, arendada ja toota sellisel viisil, et need tagaksid riskidest lähtuvalt asjakohase küberturvalisuse taseme.

165. Selle olulise nõude eesmärk on maandada kõik küberriskid, mis on küberriskide hindamise osana kindlaks tehtud. Eelkõige hõlmab see küberriske, mida muidu ei käsitleta piisavalt I lisa I osa (välja arvatud punkt 1) oluliste nõuete rakendamisel. See oluline nõue erineb õiguslikust kohustusest teha küberriskide hindamine lähtuvalt artikli 13 lõikest 2.

166. Kui digielemente sisaldava toote kõiki asjakohaseid küberriske maandatakse, rakendades piisavad meetmed muude kui punkti 1 kohaste kohaldatavate oluliste nõuete arvesse võtmiseks, siis käsitatakse I lisa I osa punktis 1 osutatud olulisi nõudeid täidetuna. Samas kui küberriskide hindamise tulemusena tehakse kindlaks täiendavad riskid, mida kõnealuste meetmete abil ei ole piisavalt maandatud, siis peavad tootjad rakendama digielemente sisaldava toote puhul asjakohased meetmed kõnealuste riskide maandamiseks, et toode vastaks I lisa I osa punktis 1 osutatud olulistele nõuetele. Üldjuhul on muudele olulistele nõuetele vastavuse eeldatavaks tulemuseks vastavus sellele nõudele.

7.3. **Riskihindamine ja hoolsuskohustus välise sõltuvuse ning integreeritud komponentide puhul**

167. Küberkerksuse määrusega kehtestatakse kaks eraldiseisvat, kuid teineteist täiendavat kohustust tootjatele seoses küberriski juhtimisega. Esiteks nõutakse artikli 13 lõikega 2, et tootjad teeksid küberriskide hindamise digielemente sisaldava toote enda puhul. Teiseks kehtestatakse artikli 13 lõikega 5 kohustus täita integreeritud komponentide puhul hoolsuskohustust. Ühiselt on nende kahe kohustuse eesmärk tagada, et digielemente sisaldav toode jääb turvaliseks, sh juhul, kui see tugineb andmete kaugtöötlemise lahendustele, kaugteenustele või kolmanda isiku tark- või riistvarakomponentidele.

168. Küberriskide hindamine käsitleb selliste riskide tuvastamist ja juhtimist, mis võivad mõjutada digielemente sisaldavat toodet, sh tooteväliseid riske, mis võivad tuleneda välistest võrkudest, keskkonnateguritest või muudest välistest aspektidest, mis võivad mõjutada digielemente sisaldavat toodet või millest toode sõltub. Selliste väliste riskide puhul ei nõua küberkerksuse määrus, et tootjad kontrolliksid või juhiksid väliskeskkonda. Selle asemel peavad tootjad tegema sellised riskid kindlaks ja neid maandama digielemente sisaldava toote enda projekteerimise ja arendamise kaudu. See hõlmab I lisa I osas märgitud asjakohaste oluliste nõuete rakendamist ning vajaduse korral teabe ja juhiste esitamist kasutajatele integreerimise või kasutuselevõtu riskide kohta.

169. Tootja võib näiteks teha kindlaks riski, et loata isikud võivad saada toote kasutamise ajal juurdepääsu tagasüsteemidele, mis ei ole digielemente sisaldava toote enda osa, ning võivad proovida saata pahatahtlikke käske digielemente sisaldavale tootele. Sellised tagasüsteemid, kui need ei ole projekteerinud ja arendanud tootja või need ei ole tema vastutusel või kui need ei toeta ühte digielemente sisaldava toote funktsioonidest, ei ole andmete kaugtöötlemise lahendused ning seega jäävad küberkerksuse määruse kohaldamisel digielemente sisaldava toote kohaldamisalast välja. Sellest hoolimata nõutakse küberkerksuse määruses, et tootja maandaks neist tekkida võiva riski toote tasandil võetavate meetmete abil, näiteks nõudes kaugkäskude krüptoautentimist, millega kontrollitakse konfigureerimise muudatuste usaldusväärsust, või luues turvalisust käsitlevad logid või hoiatused, kui tuvastatakse ebatavaline käitumine. Samal moel, kui tootja teeb kindlaks riski, mis tuleneb sellise välise teenuse kättesaadavuse katkemisest, näiteks elektrikatkestuse või taristu tõrke tõttu, siis võidakse küberkerksuse määrusega nõuda küberriskide maandamise meetmete võtmist toote tasandil, nt tagamist, et elektrikatkestus ei põhjusta digielemente sisaldava toote üleminekut ebaturvalisse olekusse. Neil juhtudel reguleeritakse küberkerksuse määrusega seda, kuidas digielemente sisaldav toode neile välistele riskidele reageerib; sellega ei kehtestata kohustusi tagasüsteemide taristu korraldamise, selle töötajate ega käitamise kohta ning kõnealust taristut ei käsitata digielemente sisaldava toote osana.

170. Hoolsuskohustus on seotud digielemente sisaldava toote enda osadega, eelkõige kolmanda isiku tagatud integreeritud tark- ja riistvarakomponentidega. Tootjad peavad võtma sobilikke meetmeid, millega tagatakse, et kõnealused komponendid ei õõnesta digielemente sisaldava toote vastavust olulistele nõuetele. Seda on võimalik saavutada ainult juhul, kui määratakse kindlaks, millised nõuded seab digielemente sisaldav toode selle komponentidele, et saavutada oma küberturvalisuse eesmärgid, ning kontrollitakse riskipõhiselt, et need komponendid on kooskõlas toote vajadustega, nagu on märgitud ka põhjenduses 34.

171. Tootja peab kooskõlas oma küberriskide hindamisega tegema kindlaks nõuded, millele integreeritud komponent peaks vastama. Näiteks kui digielemente sisaldav toode tugineb krüptograafilistele funktsioonidele, uuendusmehhanismidele või turvalisele sidele, mille tagab komponent, siis peab tootja oma hoolsuskohustuse täitmise osana tegema kindlaks kõnealused vajadused ning kontrollima, et komponent vastab nendele. Sel otstarbel kasutatavad tõendid võivad hõlmata komponendi tootjalt saadud dokumentatsiooni, näiteks tehnilisi spetsifikatsioone, turvalisust käsitlevaid dokumente või asjakohaseid vastavust või usaldusväärsust käsitlevaid dokumente. Kui see on asjakohane, siis võib tootja samuti teha testid eesmärgiga kontrollida, et need komponendid täidavad asjakohaseid funktsioone nõuetekohaselt. Kuigi hoolsuskohustus on eraldiseisev õiguslik kohustus, toetab ja kindlustab see tootja võimet tõendada digielemente sisaldava toote kui terviku vastavust olulistele nõuetele.

172. Digielemente sisaldava toote kui terviku puhul tekkivate riskide hindamisel tuleb küberriskide hindamises arvesse võtta tooteväliseid elemente, näiteks keskkonnamõju, välist taristut, muid süsteeme või võrke, ning riske tuleb vajaduse korral maandada tootetasandi meetmete abil, et tagada digielemente sisaldava toote vastavus olulistele nõuetele. Riskihindamise osana tuleb arvesse võtta ka komponente, mis on digielemente sisaldavasse tootesse füüsiliselt või loogiliselt integreeritud, kuid mis on hangitud kolmandalt isikult. Nõuete täitmise tagamiseks peaks tootja käsitlema neid siiski väljastpoolt hangitud komponentidena, mille omadusi kontrollitakse hoolsuskohustuse alusel integreerimise ajal, kuna tootja ei pruugi olla neid ümber projekteerinud või edasi arendanud.

173. Sama loogika kehtib komponentide arendamise ja integreerimise ajal. Kui tootja arendab funktsioonid ise, peab ta olulised nõuded vahetult rakendama. Kui tootja integreerib teiste arendatud komponendid, peab ta hoolsuskohustuse kaudu tagama, et neid komponente saab kasutada viisil, millega tagatakse digielemente sisaldava toote kui terviku nõuetele vastavus. Mõlemal juhul jääb eesmärk samaks: digielemente sisaldav toode peab turule lastud kujul saavutama küberkerksuse määrusega nõutud sobiliku küberturvalisuse taseme, võttes arvesse küberturvalisuse riskihindamise käigus tuvastatud riske.

7.4. **Riskihindamiste ja vastavusdokumentatsiooni taaskasutamine digielemente sisaldavate tooterühmade puhul**

174. Tootjad võivad lasta turule sarnaseid digielemente sisaldavaid tooteid, näiteks sama tooterühma eri variante, mudeleid või konfiguratsioone. Kui sellistel digielemente sisaldavatel toodetel on sama arhitektuur, turvalisuse seisukohast oluline ülesehitus ja sihtotstarve ning neile avalduvad samad küberriskid, siis ei nõuta küberkerksuse määrusega, et tootjad kohtleksid iga varianti täiesti eraldiseisva digielemente sisaldava tootena riski- ja vastavushindamise otstarbel.

175. Neil juhtudel, kui kõik variandid on asjakohaste riskide ja oluliste nõuete seisukohast piisavalt hõlmatud, siis võivad tootjad tugineda järgmisele: i) küberkerksuse määruse artikli 13 lõike 2 kohaselt tehtud üks küberriskide hindamine, ii) üks tehniline dokumentatsioon ning iii) üks vastavushindamismenetlus. See võimaldab väljastada digielemente sisaldavate toodete rühma kohta ühe ELi vastavusdeklaratsiooni, kui selles on selgelt märgitud tootevariandid, mille suhtes seda kohaldatakse.

176. Määrav tähtsus on sellel, kas variantide erinevused on küberturvalisuse seisukohast olulised. Erinevused, mis ei mõjuta digielemente sisaldava toote küberturvalisuse omadusi, näiteks värvi, kuju või mälumahu erinevused või muude turvalisusega mitteseotud omaduste erinevused, ei nõua eraldi riski- või vastavushindamist. Samas võivad variandid teatavatel juhtudel erineda viisil, mis mõjutab oluliste nõuete rakendamist, näiteks erinevate sideliideste, tarkvaravirnade, uuendusmehhanismide või kaugühenduse kaudu. Neil juhtudel peavad need erinevused kajastuma riskihindamises ning vajaduse korral vastavushindamises ja tehnilises dokumentatsioonis.

177. Tootjatele jääb kohustus tagada, et riskihindamine ja sellega seotud dokumentatsioon kajastavad täpselt turule lastud digielemente sisaldavaid tooteid. Kui uue variandiga tekitatakse uued küberriskid või muudetakse oluliste nõuete rakendamise viisi, siis tuleb olemasolevat riskihindamist ja vastavuse dokumentatsiooni sellest lähtuvalt ajakohastada. Ühele vastavushindamisele tuginemine on võimalik ainult selles ulatuses, milles digielemente sisaldavate toodete küberturvalisuse omadused ei ole erinevad.

8. **ANDMETE KAUGTÖÖTLUS**

178. Küberkerksuse määruse artikli 3 punktis 1 on digielemente sisaldav toode määratletud kui „tarkvara- või riistvaratoode ja selle andmete kaugtöötluslahendused, kaasa arvatud tarkvara- ja riistvarakomponendid, mis lastakse turule eraldi“. Sellest lähtuvalt peab tootja käsitama digielemente sisaldavat toodet tervikuna, sh selle andmete kaugtöötluslahendusi. Näiteks kui ta tõendab, et digielemente sisaldav toode vastab I lisas sätestatud olulistele nõuetele, siis tuleb võtta arvesse andmete kaugtöötluslahendusi, alates riskihindamisest (artikli 13 lõige 2). Sama kehtib juhul, kui käsitletakse elutsükliga seotud kohustusi, näiteks aktiivselt ärakasutatavatest nõrkustest ja tõsistest intsidentidest teatamine (artikkel 14).

179. Käesolevate suuniste eesmärk on pakkuda tootjatele täiendavat tuge selle kindlaksmääramisel, kas nende digielemente sisaldaval tootel on andmete kaugtöötluslahendus, nagu on määratletud küberkerksuse määruses, ning kuidas sel puhul järgida oma nõuete täitmise kohustusi. Pärast küberkerksuse määruses esitatud määratluste ja põhjenduste esialgset analüüsi esitatakse käesolevates suunistes küsimused, millest tootjad saavad lähtuda, kui nad teevad kindlaks, kas nende digielemente sisaldav toode hõlmab andmete kaugtöötluslahendust (vt punkt *8.1 Mida käsitatakse digielemente sisaldava toote andmete kaugtöötluslahendusena?*). Seejärel täpsustatakse andmete kaugtöötluslahenduse tehnilisi tagajärgi ja kuidas hinnata vastavust küberkerksuse määrusele (vt punkt *8.2 Andmete kaugtöötluslahenduste ja kolmandate isikute lahendustele tuginemise praktiline ja tehniline mõju*).

180. Artikli 3 punktis 2 on määratletud andmete kaugtöötlus kui „andmetöötlus, mis toimub distantsilt ja mille jaoks tootja on projekteerinud ja välja töötanud tarkvara või mille jaoks on selline tarkvara projekteeritud ja välja töötatud tootja vastutusel ning mille puudumine ei laseks digielemente sisaldaval tootel täita üht oma funktsiooni“. Andmete kaugtöötluslahendus on seega määratletud andmete kaugtöötluse tarkvaraelementidena („elektroonilise infosüsteemi osa, mis koosneb arvutikoodist“, nagu on määratletud artikli 3 punktis 4). Digielemente sisaldava toote kohaldamisala ei hõlma riistvara, millele andmete kaugtöötlus võib tugineda.

181. Põhjendustes 11 ja 12 on täpsemalt selgitatud, kuidas seda mõistet tuleks tõlgendada. Põhjenduses 11 on selgitatud et andmete kaugtöötluslahenduse hõlmamise eesmärk on, et „tootjad on sellised tooted igakülgselt piisavalt turvanud, olenemata sellest, kas andmeid töödeldakse või salvestatakse kohapeal kasutaja seadmes või tootja poolt kaugühenduse teel“. Selles on samuti märgitud, et „[k]äesoleva määruse kohaldamisalasse kuuluvaid andmete kaugtöötluslahendusi käsitlevad nõuded ei hõlma seega tehnilisi, operatiiv- ega korralduslikke meetmeid, mille eesmärk on ohjata riske, mis ohustavad tootja võrgu- ja infosüsteemide turvalisust tervikuna“.

182. Seega tuleneb põhjendusest 11, et eesmärk ei ole hõlmata küberkerksuse määruse nõuetega organisatsiooni kogu IT-taristut, vaid ainult tarkvarakomponente, mis võimaldavad andmetöötluslahenduse täitmist. Näiteks sisemisi süsteeme, mis on seotud tootja enda inimressursside, palgamaksete, kliendisuhete haldamise, pidevintegratsiooni/pidevvalmiduse konveieritega ning turvauuenduste jaotamisega servasõlmedesse, ei tohiks käsitada andmete kaugtöötluslahendustena. Samal moel jäävad süsteemid, mis on seotud auditeerimise ja katsetegevusega, näiteks läbistustestimine, ohujaht ja punaste tiimide kasutamine, väljapoole digielemente sisaldava toote määratlust, nagu seda käsitletakse küberkerksuse määruses. On oluline märkida, et kuigi digielemente sisaldava toote turvalisuse kohta mõjusate ja korrapäraste testide ja läbivaatamiste tegemine on küberkerksuse määruse I lisa II osa punktis 3 sätestatud oluline nõue, ei tähenda see, et sellist tegevust tuleb käsitada digielemente sisaldava toote andmete kaugtöötluslahendusena.

183. Põhjendus 12 keskendub pilvteenustele ja täpsustab asjaolud, mille puhul võib pilvteenuseid käsitada andmete kaugtöötluslahendusena. Põhjenduse lõpus juhitakse tähelepanu sellele, et pilvandmetöötlusteenused ja pilvteenuste mudelid kuuluvad direktiivi (EL) 2022/2555 (küberturvalisuse 2. direktiiv) ([28]) kohaldamisalasse, millega kehtestatakse küberturvalisuse riskijuhtimise nõuded pilvandmetöötlusteenuste osutajatele. Neid nõudeid täpsustatakse komisjoni rakendusmääruses (EL) 2024/2690 ([29]).

8.1. **Mida käsitatakse digielemente sisaldava toote andmete kaugtöötluslahendusena?**

184. Artikli 3 punktis 2 esitatud andmete kaugtöötluse määratlus tugineb seega kolmele elemendile: i) kas andmetöötlus toimub „distantsilt“, ii) kas kõnealuse andmetöötluse puudumine takistaks digielemente sisaldaval tootel täita üht oma funktsiooni ning iii) kas tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel. Järgmised kolm alapunkti käsitlevad neid asjaolusid üksikasjalikumalt.

([28]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (ELT L 333, 27.12.2022, lk 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Komisjoni 17. oktoobri 2024. aasta rakendusmäärus (EL) 2024/2690, millega kehtestatakse seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate ning internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite, sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega direktiivi (EL) 2022/2555 kohaldamise eeskirjad, mis puudutavad küberturvalisuse riskijuhtimismeetmete tehnilisi ja metoodilisi nõudeid ja selliste juhtude täpsemat kindlaksmääramist, mille korral peetakse intsidenti oluliseks (ELT L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Mõiste „distantsilt“ määratlus*

185. Artikli 3 lõikes 2 kasutatud mõiste „distantsilt“ on asjakohane, aga mitte piisav, et teha kindlaks, kas digielemente sisaldav toode hõlmab andmete kaugtöötluslahendust. Võttes samuti arvesse mitmesuguseid lahendusi, mis võivad olla selle mõistega hõlmatud, ei ole võimalik esitada mõiste „distantsilt“ ammendavat määratlust. Tootja peab hindama iga juhtumit eraldi.

186. Küberkerksuse määruse põhjenduses 11 on nimetatud andmeid, mida töödeldakse või salvestatakse „tootja poolt kaugühenduse teel“ erinevalt andmetest, mida töödeldakse või salvestatakse „kohapeal kasutaja seadmes“. Andmete kaugtöötlus toimub üldjuhul väljaspool digielemente sisaldava toote kasutajakeskkonda või organisatsiooni tegevuskeskkonda (erialase kasutaja puhul). See ei takista samas töötlemise toimumist ka seadme läheduses (servtöötlus). Andmeülekanne võib toimuda kaabli kaudu (nt Etherneti kaabel) või traadita ühenduse (nt Wi-Fi, Bluetooth) teel. Pilvandmetöötlus, sh servtöötlus on „distantsilt“ andmetöötluse tavapärane näide. Näiteks kui kasutaja saab pilvepõhisele funktsioonile juurdepääsu mobiilirakenduse abil, siis toimub osa andmetöötlusest pilves, väljaspool kasutajakeskkonda.

187. On oluline märkida, et andmete kaugtöötluslahendust ei käitata ilmtingimata kolmanda isiku pilvetaristus. Tootja ruumides kohapeal asuvates serverites toimuv andmete kaugtöötlus võib samuti olla andmete kaugtöötluslahendus. Teisisõnu võib enda ruumides ja privaatpilves käitatav lahendus olla sama tõenäosusega andmete kaugtöötluslahendus kui avalikus pilves ja ruumidest väljaspool käitatav lahendus.

188. Kaks määrava tähtsusega küsimust, mille mõlema vastus peab olema jaatav ja mis määravad kindlaks, kas andmetöötlust käsitatakse küberkerksuse määruse alusel andmete kaugtöötluslahendusena, on esitatud allpool, punktides *8.1.2* ja *8.2*. Kui mõlema küsimuse vastus on jaatav, siis on andmete kaugtöötluse puhul tegemist andmete kaugtöötluslahendusega.

8.1.2. *Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni?*

189. Nagu on märgitud artikli 3 punktis 2 esitatud andmete kaugtöötluse määratluses, peaks selleks, et andmete distantsilt töötlemist käsitataks andmete kaugtöötluslahendusena, takistama selle puudumine digielemente sisaldaval tootel täita üht selle funktsiooni. Selles määratluses kasutatud funktsiooni mõiste ei piirdu digielemente sisaldava toote põhifunktsiooni ega sihtotstarbega, kuna küberkerksuse määrusega ei ole kehtestatud sellist piirangut. Küberkerksuse määruse kohaldamisalasse kuuluvad funktsioonid on nii funktsioonid, mis täidavad otseselt digielemente sisaldava toote sihtotstarvet, nagu seda kogevad kasutajad, kui ka funktsioonid, mis toetavad toote üldist toimivust.

190. Näited funktsioonidest, mille puhul võib toimuda andmetöötlus distantsilt ja mille tõrge takistaks digielemente sisaldaval tootel täita üht selle funktsioonidest, on järgmised: i) seadmele käskluste saatmine, ii) failide sünkroniseerimine, iii) kasutaja kaasamine, iv) konfigureerimine (digielemente sisaldava toote individualiseerimine), v) automaatne uuenduste jaotamine, sh funktsiooniuuendused ja turbepaigad, vi) identiteedi- ja pääsuhaldus.

191. Mõnel juhul saavad kasutajad kasutada funktsiooni nii kaugmeetodil kui ka käsitsi (nt lambipirni lülitamine rakenduse abil või käsitsi). Selle variandi olemasolu ei välista funktsiooni kaugtäitmisega seotud andmetöötluse käsitamist andmete kaugtöötluslahendusena. Selle funktsiooni kaugtäitmist käsitatakse samuti digielemente sisaldava toote pakutavate funktsioonide osana.

192. Seevastu juhul, kui digielemente sisaldava toote teatava andmetöötluse puudumine ei takista sellel täita üht selle funktsioonidest, siis ei käsitata kõnealust töötlust andmete kaugtöötluslahendusena küberkerksuse määruse tähenduses. See hõlmab näiteks ainult statistika või tulevase tootearenduse otstarbel kogutud telemeetria andmete kauganalüüsi.

193. Sellegipoolest, isegi kui andmetöötlus ei toeta digielemente sisaldava toote mingit funktsiooni, võib tootjatel olla vajalik kaaluda oma küberriskide hindamise raames, kas need kaugkomponendid tekitavad digielemente sisaldavale tootele riske (nt võttes arvesse toote kasutuskeskkonda) ning maandama neid riske sobilikul viisil (nt toote tasandil võetavate maandamismeetmete abil).

194. Veebisaidid on konkreetne juhtum, mida on vaja täpsemalt selgitada, nagu on selgitatud ka *punktis 2.1 Turule laskmine*. Veebisaidid ei hõlma andmete kaugtöötluslahendust, kui need ei toeta ühe digielemente sisaldava toote funktsiooni täitmist, nagu on selgitatud küberkerksuse määruse põhjenduses 11. Ei piisa sellest, kui veebisait sisaldab teavet digielemente sisaldava toote kohta, et seda käsitataks andmete kaugtöötluslahendust hõlmavana, isegi kui toode suunab sellisele veebisaidile. Näiteks kasutajate suunamist välisele veebilehele, mis esitab kasutajatele teavet ja juhiseid, ei käsitata andmete kaugtöötluslahendusena. Samas võib olla veebisait hõlmatud andmete kaugtöötluslahenduse määratlusega, kui see võimaldab või toetab digielemente sisaldava toote funktsiooni. Näiteks autentimisportaali, mis väljastab mandaadid või identsustõendid, mis on vajalikud digielemente sisaldava toote kasutamiseks, käsitataks andmete kaugtöötluslahendusena (kui täidetud on ka muud selle määratluse kriteeriumid).

8.1.3. *Kas tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel?*

195. Küberkerksuse määruse artikli 3 punktis 2 esitatud andmete kaugtöötluse määratluses täpsustatakse samuti, et kõnealuse andmete kaugtöötluse tarkvara peab olema projekteerinud ja välja töötanud tootja või seda peab olema tehtud tema vastutusel. Tootja poolt (asutusesiseselt) täies mahus väljatöötatud ja projekteeritud andmete kaugtöötlust käsitataks loomulikult andmete kaugtöötluslahendusena. See oleks nii samuti juhul, kui tootjad tuginevad lahenduse väljatöötamiseks ja projekteerimiseks asutusevälisele teenuseosutajale (s.o „tema vastutusel“). Fraas „tootja vastutusel“ osutab kaugtöötluse lahendustele, mis on sihtotstarbeliselt loodud tootja jaoks. Neil juhtudel ei hangi tootja ainult olemasoleva digielemente sisaldava toote või teenuse litsentsi, mida teenuseosutaja pakub oma klientidele, või selle mõnevõrra muudetud versioone. „[T]ootja vastutusel“ tähendab, et tarkvara loob ainult tootja või see luuakse tema nimel lähtuvalt tema esitatud projektidest ja spetsifikatsioonidest.

196. Andmete kaugtöötluslahenduse mõistmisel ei ole see, kes lahendust käitab, määrav tegur, kuna küberkerksuse määruses osutatakse ainult andmete kaugtöötluslahenduse projekteerimisele ja väljatöötamisele. See on kooskõlas küberkerksuse määruse lähenemisviisiga, mille puhul on nõuded ja kohustused kehtestatud tootjatele ja mitte digielemente sisaldava toote käitamisele. Kui tootjad projekteerivad ja töötavad välja lahendusi, mida käitab seejärel kolmas isik, siis jäävad nad vastutavaks selle eest, et nende turule lastud digielemente sisaldav toode vastab küberkerksuse määruse olulistele nõuetele.

197. On vaja eristada juhtumeid, kui projekteerimise ja väljatöötamisega tegelevad tootjad (või see toimub nende vastutusel) ning juhtumeid, kui tuginetakse kolmanda isiku lahendustele, mis ei ole tootjate projekteeritud ega välja töötatud (või seda ei ole tehtud nende vastutusel). Näitena on kasulik käsitleda kõige tavapärasemaid pilvteenuse mudeleid, millega tagatakse erineval määral kasutaja kontroll ja millele on samuti osutatud küberkerksuse määruse põhjenduses 12, nimelt tarkvara teenusena (SaaS), platvorm teenusena (PaaS) ja taristu teenusena (IaaS).

198. Kolmanda isiku IaaS-lahenduse (taristu teenusena) puhul ei halda ega kontrolli tootja aluseks olevaid füüsilisi ega virtuaalseid ressursse (nagu alusriistvara ja pilvteenuse osutaja hüperviisor), aga ta saab võtta kasutusele ja käitada nende ressursside abil oma äranägemisel valitud tarkvara, näiteks operatsioonisüsteeme ja rakendusi. Kõnealuse tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel ning seda võidakse seega käsitada andmete kaugtöötluslahendusena (kui see vastab määratluse muudele elementidele).

199. Kolmanda isiku PaaS-lahenduse (platvorm teenusena) puhul võtab tootja kasutusele enda (loodud või omandatud) rakenduse, kasutades programmeerimiskeelt ja täitmiskeskkonda, mille on taganud pilvteenuse osutaja, ning integreerib selle rakenduse oma digielemente sisaldavasse tootesse. Tootjal on kontroll rakenduse ning võimalik, et täitmiskeskkonna konfiguratsioonisätete üle. Kõnealuse rakenduse on seega projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel ning seda võidakse seega käsitada andmete kaugtöötluslahendusena (kui see vastab määratluse muudele elementidele).

200. Kolmanda isiku SaaS-lahenduse (tarkvara teenusena) puhul pakub sellise lahenduse pakkuja tootjale täielikult väljatöötatud rakendust, mis integreeritakse tootja digielemente sisaldavasse tootesse. Tootjal on piiratud võime hallata kasutajapõhise rakenduse konfiguratsioonisätteid. Rakendust ei ole seega projekteerinud ega välja töötanud tootja ning seda ei ole tehtud tema vastutusel.

201. Sellest hoolimata, kui teatavad elemendid ei vasta andmete kaugtöötluslahenduse määratlusele (näiteks hüperviisor kolmanda isiku IaaS-taristu puhul, operatsioonisüsteem kolmanda isiku PaaS-lahenduse puhul või kolmanda isiku SaaS-rakendus), kuid need on integreeritud digielemente sisaldavasse tootesse viisil, mis mõjutab selle turvalisust, siis tuleks neid lahendusi käsitada samalaadsena kolmanda isiku komponentidega. Tootja peab tuvastama ja hindama nimetatud elementide integreerimisega seotud riskid ja nendega tegelema, rakendades digielemente sisaldava tootele endale olulisi nõudeid. Seda võib vajaduse korral toetada turvafunktsioonidega, mille teeb kättesaadavaks pilvteenuse osutaja oma jagatud vastutuse mudeli alusel, kui tootja kasutab või konfigureerib neid funktsioone kindlaks tehtud riskide maandamiseks. Lisaks sellele eeldatakse, et tootja täidab komponentide turvalisusega seotud hoolsuskohustust, mis on samaväärne artikli 13 lõikes 5 osutatud hoolsuskohustusega, viisil, mis on proportsionaalne riskiga, mida kauglahendus kujutab endast digielemente sisaldava toote turvalisusele.

202. Seega on olukord kokkuvõtlikult järgmine.

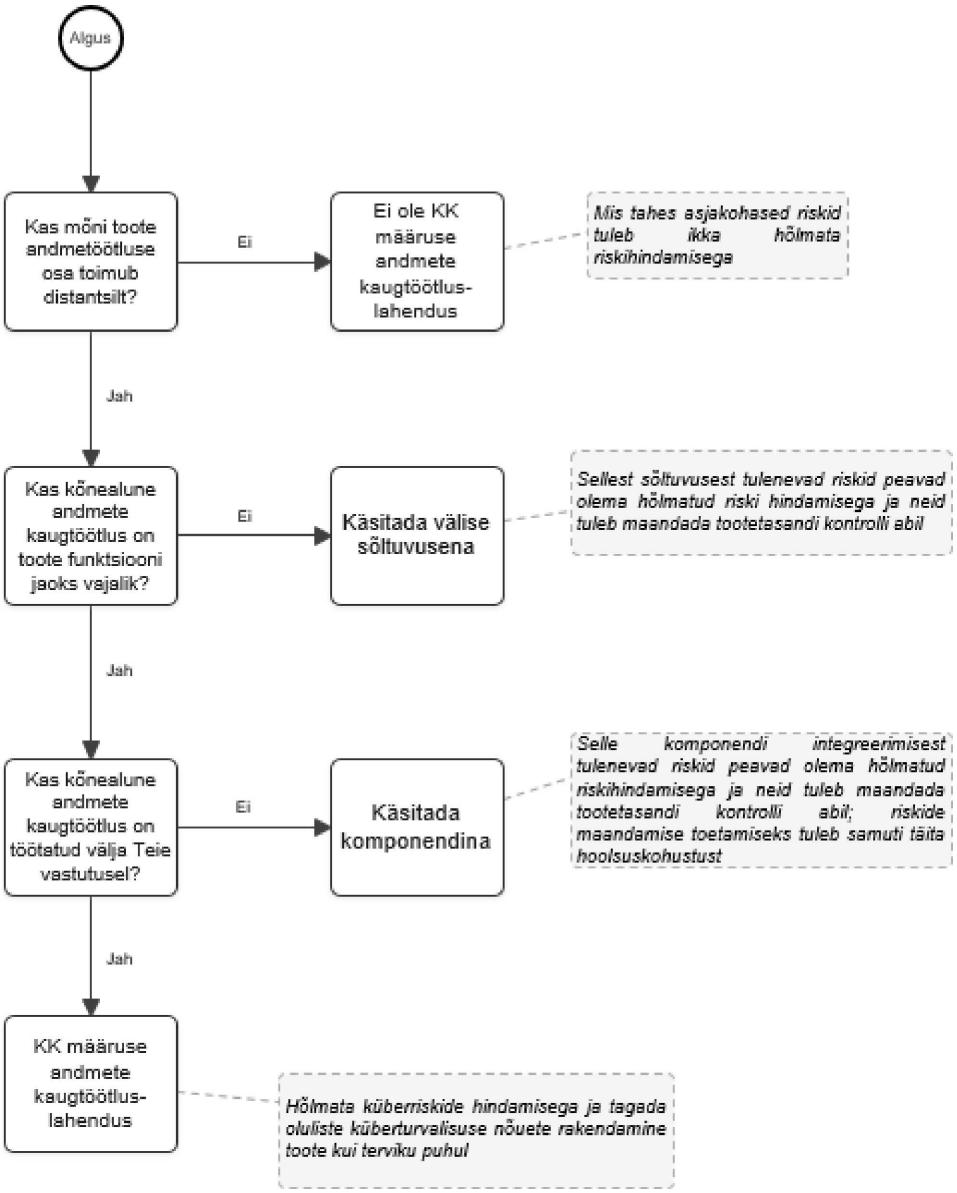
a) Selleks et andmetöötluse puhul oleks tegemist andmete kaugtöötluslahendusega, peab vastus nii punktis *8.1.2 Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni?* kui ka punktis *8.1.3 Kas tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel?* esitatud küsimusele olema jaatav.

b) Kui vastus punktis *8.1.2 Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni?* esitatud küsimusele on eitav, siis peaksid tootjad hindama oma riskihindamise osana riske, mis tulenevad kõnealuse andmetöötluse olemasolust.

c) Kui vastus punktis *8.1.2 Kas kõnealuse andmetöötluse puudumine takistab digielemente sisaldaval tootel täita üht oma funktsiooni?* esitatud küsimusele on jaatav, aga vastus *8.1.3 Kas tarkvara on projekteerinud ja välja töötanud tootja või seda on tehtud tema vastutusel?* küsimusele on eitav, siis peaksid tootjad käsitama kolmanda isiku lahendust komponendina. Tootjad peaksid riskihindamise osana hindama riske, mis tulenevad sellise lahenduse integreerimisest, ning neid vastavalt maandama. Tootjad peaksid samuti täitma hoolsuskohustust.

Joonis 9

Kujundlik vooskeem, mille alusel saab määrata kindlaks, kas digielemente sisaldav toode sisaldab andmete kaugtöötluslahendusi



8.2. Andmete kaugtöötluslahenduste ja kolmandate isikute lahendustele tuginemise praktiline ja tehniline mõju

203. Küberkerksuse määrus järgib riskipõhist lähenemisviisi, mis tuleneb artikli 13 lõigetest 2 ja 3 ning samuti I lisa I osa esimesest olulisest nõudest mille kohaselt „[d]igielemente sisaldavaid tooteid tuleb projekteerida, arendada ja toota sellisel viisil, et need tagaksid riskidest lähtuvalt asjakohase küberturvalisuse taseme.“ Seega tuleks võtta arvesse riskipõhist lähenemisviisi, kui küberkerksuse määruse nõudeid kohaldatakse andmete kaugtöötluslahenduste ning digielemente sisaldavatesse toodetesse integreeritud kolmanda isiku teenustest tulenevate riskide maandamise suhtes.

204. Esiteks peaks tootja i) märkima tehnilises dokumentatsioonis, et tema digielemente sisaldaval tootel on andmete kaugtöötluslahendus või see tugineb kolmanda isiku kauglahendustele ning ii) kirjeldama neid lahendusi. Kui sama andmete kaugtöötluslahendus toetab mitut digielemente sisaldavat toodet, siis tuleb andmete kaugtöötluslahendus märkida iga toote tehnilises dokumentatsioonis. Mitut digielemente sisaldavat toodet teenindavat andmete kaugtöötluslahendust käsitlevat dokumentatsiooni võib kasutada uuesti kõnealuste eri toodete vastavushindamise puhul.

205. Nagu on märgitud põhjenduses 11, peaks andmete kaugtöötluslahendus, mis on digielemente sisaldava toote osa ja mille suhtes kohaldatakse seega toote vastavushindamist, piirduma tarkvaramoodulitega, mis vastutavad digielemente sisaldava toote funktsioonide eest, ning liidestega, mida need moodulid kasutavad väliste teenuste puhul. Täiendavaid tagasüsteeme, mis teostavad edasist töötlemist ja millega digielemente sisaldav toode otseselt kokku ei puutu, ei käsitata andmete kaugtöötluslahendustena.

206. Sellest hoolimata jäävad kõnealused tagasüsteemid välisteks sõltuvusteks, mida tuleb hinnata küberriskide hindamise osana ja maandada tootetasandi meetmete abil. Tootja tehtav riskihindamine peaks võtma arvesse: i) andmete kaugtöötluslahendusega seotud riske, ii) riske, mis on seotud kolmanda isiku kauglahendustele (mis on samalaadsed kolmanda isiku komponentidega) tuginemisega, ning iii) riske, mis on seotud tootekeskkonnaga (nt alusriistvara). Tootjad peaksid rakendama kõnealuste riskide maandamiseks digielemente sisaldava toote enda turvakontrolle.

207. Lisaks sellele võib vastavushindamise ja/või kolmanda isiku kaugteenustega seotud hoolsuskohustuse täitmise osana kasutada tootja hinnangu toetuseks uuesti järgmisi loetelu kohaseid tõendusmaterjale (loetelu ei ole ammendav):

a) tõendid komisjoni rakendusmäärusest (EL) 2024/2690 tulenevate kohustuste täitmise kohta;

b) tõendid komisjoni määrusest (EL) 2022/2554 (DORA) tulenevate kohustuste täitmise kohta;

c) Euroopa küberturvalisuse sertifitseerimise kava alusel saadud vastavusdeklaratsioon või sertifikaat (vastu võetud määruse (EL) 2019/881 (küberturvalisuse määrus) alusel);

d) tõendid standardile ISO/IEC 27017:2015 või ISO/IEC 27001:2022 vastavuse kohta.

208. Viimaks peavad tootjad kolmandast isikust kaugteenuse osutajaga suheldes rakendama kõige sobilikumaid turvameetmeid lähtuvalt oma riskihindamisest (ning mida vajaduse korral toetab pakkuja jagatud vastutuse mudel). Need leevendusmeetmed peaksid hõlmama nende digielemente sisaldavate toodete turvakontrolli ja kolmandast isikust pakkuja enda tagatud turvameetmete kinnitamist (hoolsuskohustus). Üks meetod kõnealuste riskide maandamiseks võib olla turvalisuse tagatiste kaasamine nende teenustasemelepetesse kolmandast isikust pakkujatega. Kolmandast isikust kaugteenuste pakkujate tagatud lahenduste olulist muudatust ei tohiks käsitada digielemente sisaldava toote olulise muudatusena, kuna kõnealused aspektid ei kuulu tootja vastutuse alla. Kuid oma hoolsuskohustuse täitmise osana ning kolmandast isikust pakkujate kasutamisest tulenevate riskide nõuetekohaseks maandamiseks julgustatakse tootjaid tagama, et nende kolmandast isikust pilvteenuse osutajad hoiaksid neid piisavalt kursis mis tahes muudatustega, mida kõnealused teenuseosutajad oma lahendustes teevad. Selle teabe alusel võib tootjatel tekkida vajadus muuta oma riskihindamist. Ajakohastatud riskihindamise puhul tuleks võtta arvesse, kas kolmandast isikust teenuseosutajad annavad jätkuvalt piisavad küberturvalisuse tagatised ning kas toote tasandi turvakontroll on endiselt piisav. Mõnel juhul võib tootjatel tekkida vajadus muuta kõnealust kontrolli või vahetada kolmandast isikust teenuseosutajaid.

8.3. **Andmete kaugtöötluslahenduste kasutusmallid**

Tootjatele täiendavate praktiliste suuniste esitamiseks on käesolevas punktis kirjeldatud väljamõeldud kasutusmalle, mis käsitlevad digielemente sisaldavaid tüüpilisi tooteid, mis tuginevad andmete kaugtöötlusele, ning seda, kas kõnealuse töötlemise puhul on tegemist andmete kaugtöötluslahendustega küberkerksuse määruse tähenduses.

8.3.1. *Mobiilpanganduse rakendus*

Finantssektori ettevõtja laseb turule mobiilpanganduse rakenduse. Rakenduse tagasüsteemid toetavad muu hulgas autentimist, autoriseerimist, kontohaldust ja makseid. Finantssektori ettevõtja kasutab hübriidstrateegiat, tuginedes asutusesisesele taristule ning samuti kolmanda isiku kauglahendustele rakenduse funktsioonide toetamiseks. Need on muu hulgas järgmised.

Finantssektori ettevõtja enda hallatav taristu

— Klient avab mobiilpanganduse rakenduse ja ta autenditakse pangaliidese kaudu, mis on finantsasutuse hallatav lahendus, mille on töötanud välja finantssektori ettevõtja, kes võtab vastu rakenduse päringuid ja annab sobilikud vastused. Pangaliides kontrollib kliendi isikut, esitades päringu kontohaldussüsteemi, ning annab rakendusele juurdepääsu.

— Klient algatab rakenduse kaudu ülekande. Rakendus edastab juhised pangaliidesele, mis esitab vastava taotluse arvestusraamatu süsteemile.

— Kontohaldussüsteem ja arvestusraamatu süsteem, mis on mõlemad finantsasutuse enda hallatavad, kuid pangaliidesest loogiliselt eraldatud, registreerivad tehingu.

— Arvestusraamatu süsteem saadab tehingu oleku pangaliidesele, mis kuvab tulemuse kliendile.

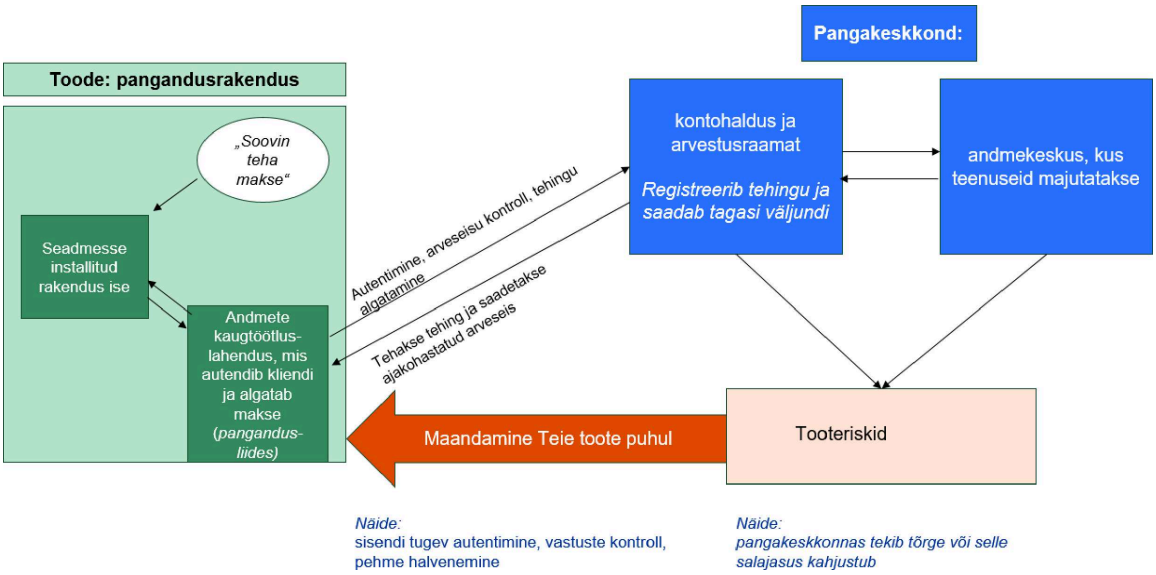
Mõju andmete kaugtöötluslahendusele

— Pangaliides on vajalik, et rakendus täidaks oma funktsioone, nimelt autendiks kliendi, esitaks kliendile juhiseid, sh makse ja ülekande juhised, ning saadaks tagasi sellest tuleneva staatuse. Pangaliides on projekteeritud ja arendatud tootja vastutuse all. Kuna vastus punktides eespool esitatud mõlemale küsimusele on jaatav, käsitatakse pangaliidest andmete kaugtöötluslahendusena. See peab seetõttu olema hõlmatud küberriskide hindamisega ning digielemente sisaldava toote kui terviku oluliste nõuete rakendamisega. Juhiste edasine töötlemine pärast esitamist, eelkõige tehingu registreerimist kontohalduse ja arvestusraamatu süsteemi, arveldamist ja kliiringut, toimub süsteemides, millega rakendus otseselt kokku ei puutu, ning seega ei ole sellest lähtuvalt tegemist andmete kaugtöötluslahendustega.

— Kontohaldussüsteemi ja arvestusraamatu süsteemi puhul ei ole tegemist pangandusrakenduse andmete kaugtöötluslahendusega. Rakendus ei suhtle nendega otseselt (ja suhtleb selle asemel pangaliidesega, mis tugineb omakorda neile). Kuigi nende kättesaadavus võib olla vajalik funktsiooni täitmiseks, hõlmab küberkerksuse määrus ainult neid süsteemi osi, mis suhtlevad otseselt digielemente sisaldava tootega. Need jäävad seega küberkerksuse määruse otstarbel andmete kaugtöötluslahenduse määratlusest välja. Kuid kõnealused süsteemid jäävad väliseks sõltuvuseks, mis võivad põhjustada digielemente sisaldavale tootele olulisi küberriske. Näiteks arvestusraamatu süsteemi kahjustamine võib võimaldada ründajal mõjutada tehingu tulemusi, mis seejärel rakenduses kuvatakse. Tootja peab seega tegema kindlaks need riskid ja hindama neid küberriskide hindamise osana ning maandama neid toote tasandil võetavate meetmete abil, näiteks tagasüsteemi liideste tugeva autentimise, tehinguandmete tervikluse kaitse, turvaliste sidekanalite ja rakenduse saadud vastuste kontrollimise teel.

Joonis 10

Andmete kaugtöötluslahendusele tugineva pangandusrakenduse kujundlik väljendus



Kolmanda isiku tarkvara teenusena klienditoe otstarbel

— Finantssektori ettevõtja integreerib oma rakendusse klienditoe vestluslahenduse, mille on välja töötanud ja mida käitab kolmandast isikust pakkuja; kolmandast isikust pakkuja on kirjutanud vestlusserveri koodi, loonud kasutajaliidese ning käitab taristut, kus vestlus toimub (s.o tarkvara teenusena mudel).

— Kui klient esitab tugiteenuse päringu, siis ühendab rakendus kliendi kolmanda isiku teenusega, et luua vestlusseanss ning hallata sõnumite voogu, andmata kolmandale isikule juurdepääsu panganduse tuumsüsteemidele.

Mõju andmete kaugtöötluslahendusele

— Klienditoe vestluse lahendus on vajalik, et digielemente sisaldav toode täidaks üht oma funktsiooni, aga seda ei ole projekteerinud ega arendanud finantssektori ettevõtja ja see ei kuulu tema vastutusalasse ning seega ei ole tegemist andmete kaugtöötluslahendusega. Kuid seda tuleks käsitada kolmanda isiku komponendina. Kõnealusele kolmanda isiku teenusele tuginemine võib tekitada küberriske pangandusrakendusele, näiteks kui ründaja kasutaks vestluskanalit pangana esinemiseks või kasutajatele pahatahtliku sisu saatmiseks. Finantssektori ettevõtja peab võtma neid riske arvesse oma küberriskide hindamises ja maandama neid tootetasandil võetavate meetmete abil, näiteks eraldades vestluse funktsiooni panganduse põhifunktsioonidest, kontrollides andmevooge ja valideerides sisu. SaaS-lahenduse (tarkvara teenusena) puhul tuleb samuti täita hoolsuskohustust.

8.3.2. *Nutitermostaat*

Nutitermostaat võimaldab kasutajatel määrata oma kodu temperatuuri mobiilirakenduse abil. Mobiilirakendus ja nutitermostaat tuginevad andmete vahetamiseks (nt temperatuuri tõstmise taotlus) ja andmete salvestamiseks (nt kasutajaeelistused) andmete kaugtöötlusele. Need funktsioonid töötati välja ja projekteeriti tootja vastutusel, kuid need toimivad kolmanda isiku pakutava füüsilise ja virtuaalse taristu baasil (kolmanda isiku taristu teenusena)

Kuna nutitermostaat ei suudaks täita oma nutifunktsioone ilma andmete kaugtöötluseta, takistaks selle puudumine digielemente sisaldaval tootel täita üht või enamat selle funktsiooni. Lisaks sellele arendati ja projekteeriti tarkvara nutitermostaadi tootja vastutusel. Seega on andmete kaugtöötluse puhul tegemist andmete kaugtöötluslahendusega, nagu see on määratletud küberkerksuse määruses.

Küberkerksuse määruse nõuete täitmise eesmärgil peab nutitermostaadi tootja dokumenteerima andmete kaugtöötluslahenduse ning samuti kolmanda isiku taristule teenusena tuginemise digielemente sisaldava toote tehnilises dokumentatsioonis, sealhulgas esitama üksikasjad lepingu alusel osutatava teenuse kohta. Tootja peab võtma neid elemente arvesse riskihindamises, mis hõlmab digielemente sisaldava toote sihtotstarvet ja mõistikult prognoositavat kasutamist. Tootja rakendab küberkerksuse määruse olulisi nõudeid lähtuvalt andmete kaugtöötluslahenduse riskidest. Kolmanda isiku IaaS-lahenduse (taristu teenusena) puhul peab tootja tagama, et kolmandast isikust pakkuja tagatud turvameetmed on sobilikud ja/või võtma taristu puhul asjakohaseid meetmeid. Neist esimese puhul võib tootja näiteks küsida tõendeid küberturvalisuse 2. direktiivi kohustuste täitmise kohta.

8.3.3. *E-luger*

E-lugeri tarkvara tootja kasutab kolmanda isiku tarkvara teenusena salvestusteenust, et salvestada klientide ostetud e-raamatuid ning anda neile juurdepääs oma raamatutele. Selle salvestusteenuse puudumine takistaks digielemente sisaldaval tootel täita üht selle funktsioonidest, kuid kolmanda isiku tarkvara teenusena salvestusteenus ei ole tootja arendatud ega kuulu tema vastutuse alla ning tarkvara teenusena pakkuja teeb selle kasutajatele kõigi kasutusmallide jaoks kättesaadavaks.

Tarkvara teenusena salvestusteenus ei vasta andmete kaugtöötluslahenduse määratlusele. Kuid e-lugeri tootja tugineb kõnealusele välisele teenusele oma digielemente sisaldava toote toimimiseks ning peab seega võtma sellega seotud riske arvesse oma küberriskide hindamises. E-lugeri tootja peaks käsitama teenusena pakutavat tarkvara komponendina. Tootja peab rakendama asjakohaseid tootetasandi turvameetmeid, nagu turvaline autentimine, krüpteerimine ja salvestusteenusega toimuva side tervikluse kaitse. Tarkvara teenusena pakkuja valimisel ja integreerimisel täidetav hoolsuskohustus toetab samuti tootja kohustusi, et digielemente sisaldav toode tervikuna vastaks olulistele nõuetele.

8.3.4. *Tööstusrobot*

Tööstusroboti ülesandeks on detailide haaramine. Robot saadab kaamerate abil kogutud teabe kaugteenusele, mille on projekteerinud ja arendanud tootja. See teenus töötab kolmandast isikust teenuseosutaja (kolmanda isiku taristu teenusena) pakutaval füüsilisel ja virtuaalsel taristul. Pilvteenus arvutab detaili asukoha kaamera edastatud andmete põhjal ja saadab robotile käskluse detailide haaramiseks.

Sellise andmetöötluse puudumisel ei suudaks tööstusrobot detaile haarata ja seega täita üht oma funktsiooni. Lisaks sellele on taristul käitatava tarkvara projekteerinud ja arendanud tootja. Tootja projekteeritud ja arendatud tarkvara vastab andmete kaugtöötluslahenduse määratlusele.

Tööstusroboti tootja peab dokumenteerima andmete kaugtöötluslahenduse ning samuti kolmanda isiku taristule teenusena tuginemise digielemente sisaldava toote tehnilises dokumentatsioonis (sh lepingu alusel osutatava teenuse üksikasjad). Tootja peab võtma neid elemente arvesse ka riskihindamises, mis hõlmab digielemente sisaldava toote sihtotstarvet ja mõistikult prognoositavat kasutamist. Tootja rakendab digielemente sisaldava toote, sh selle andmete kaugtöötluslahenduse suhtes küberkerksuse määruse olulisi nõudeid lähtuvalt riskidest. Hoolsuskohustuse täitmine taristu teenusena pakkuja valimisel toetab samuti tootja kohustuste täitmist. Tootja võib näiteks küsida tõendeid küberturvalisuse 2. direktiivi kohustuste täitmise kohta.

8.3.5. *Mobiilivõrk*

Nutitelefon tugineb 5G-võrgule, et pakkuda oma kasutajatele internetiühendust, telefonikõnesid ja sõnumeid (mobiilside). Mobiilivõrku arendavad ja projekteerivad telekommunikatsioonioperaatorid. Võrk koosneb väikese raadiusega tugijaamadest ja mobiilsidemastidest ning muudest võrguseadmetest.

Digielemente sisaldav toode peaks suutma võrguga nõuetekohaselt ühenduda; see on üks selle funktsioonidest. See, kas võrk on kasutuses või mitte, ei ole siiski asjakohane, et teha kindlaks, kas digielemente sisaldav toode toimib nõuetekohaselt. Võrk on vaid sidekanal ega ole vajalik digielemente sisaldava toote võrguga nõuetekohase ühenduse loomise funktsiooni täitmiseks. Samuti ei käsitata Etherneti kaablit, ruuterit ega Wi-Fi signaali andmetöötlusena, mille puudumine takistaks digielemente sisaldaval tootel täita üht selle funktsiooni, vaid pigem side/ühenduvuse võimaldajana.

Seega ei vasta mobiilivõrk andmete kaugtöötluslahenduse määratlusele. Võrku ei tohiks käsitada kolmanda isiku komponendina, kuna digielemente sisaldavasse tootesse ei ole integreeritud tarkvara ning toode lihtsalt tugineb sellele võrgule. Seega ei ole tootjal vaja täita võrguteenuse osutaja puhul hoolsuskohustuse nõudeid.

9. **LISAELEMENDID**

9.1. **Teatamiskohustus**

209. Küberkerksuse määruse artikli 14 lõigete 1 ja 3 kohaselt peab tootja teavitama samal ajal koordinaatoriks määratud CSIRTi ja ENISAt i) oma digielemente sisaldava toote mis tahes aktiivselt ärakasutatavast nõrkusest, millest ta on teada saanud, ning ii) digielemente sisaldava toote turvalisust mõjutavatest mis tahes tõsistest intsidentidest, millest ta on teada saanud.

210. Artikli 69 lõike 3 ja artikli 71 lõike 2 teise lause kohaselt kohaldatakse artikli 14 täitmise kohustust alates 11. septembrist 2026 kõigi digielemente sisaldavate toodete suhtes, mis kuuluvad küberkerksuse määruse kohaldamisalasse, sh enne 11. detsembrit 2027 turule lastud digielemente sisaldavate toodete suhtes. Lisaks sellele jääb teatamiskohustus erinevalt nõrkuste käsitlemise kohustustest, mis kehtivad toe kestuse vältel, kehtima pärast digielemente sisaldava toote toe kestuse lõppu. Kui digielemente sisaldav toode lasti turule enne 11. detsembrit 2027 või kui selle toe kestus on lõppenud, siis ei pea tootja täitma nõrkuste käsitlemise kohustusi, mis on sätestatud I lisa II osas.

211. Tuleb pidada silmas, et nendest sündmustest teatamise kohustus tekib siis, kui tootja saab teada nõrkuse aktiivsest ärakasutamisest või tõsise intsidendi toimumisest, mis on seadnud ohtu digielemente sisaldava toote turvalisuse. Seega peaksid suunised selle kohta, millal loetakse tootja teadlikuks saanuks, aitama tootjatel teha kindlaks hetke, alates millest hakatakse arvestama kohaldatavaid teatamistähtaegu.

212. Tootjate suhtes võidakse kohaldada võrreldavaid teatamiskohustusi eri ELi õigusaktide alusel. Selleks et „teadlikust saamise“ tähendust tõlgendataks järjepidevalt ja et aidata tootjatel neid kohustusi täita, on käesolevad suunised viidud vastavusse komisjoni rakendusmääruse (EL) 2024/2690 põhjendusega 31 ning isikuandmete kaitse üldmääruse alusel isikuandmetega seotud rikkumisest teatamise suuniste 9/2022 jaotisega II(A).

213. Mõnel juhul avastab tootja kahtlase sündmuse või juhib kolmas isik, näiteks üksikisik, klient, üksus, asutus, meediaorganisatsioon või muu allikas tootja tähelepanu võimalikule intsidendile või nõrkusele. Neil juhtudel peaks tootja kahtlast sündmust viivitamata hindama, et teha kindlaks, kas selle puhul on tegemist aktiivselt ärakasutatava nõrkuse või tõsise intsidendiga, mis mõjutab digielemente sisaldava toote turvalisust. Seetõttu loetakse, et tootja on asjast teadlikuks saanud siis, kui ta on pärast sellist esmast hindamist mõistlikult veendunud, et: i) tema digielemente sisaldavas tootes esinevat nõrkust kasutatakse aktiivselt ära või ii) on toimunud tõsine intsident, mis on ohustanud tema digielemente sisaldava toote turvalisust.

214. Seega oleneb ajahetk, millal tootjat käsitatakse asjast teadlikuks saanuna, konkreetse aktiivselt ärakasutatava nõrkuse või tõsise intsidendi asjaoludest. Mõnel juhul on algusest peale suhteliselt selge, et nõrkust kasutatakse aktiivselt ära või et tõsine intsident mõjutab digielemente sisaldava toote turvalisust. Muudel juhtudel võib võtta aega, et teha kindlaks, kas digielemente sisaldaval tootel on nõrkus ja kas seda nõrkust kasutab ära kuritahtlik isik või kas intsident mõjutab digielemente sisaldava toote turvalisust. Siiski tuleks rõhku panna kiirele tegutsemisele esmasel hindamisel, millega tehakse kindlaks, kas need tingimused on tõepoolest täidetud, eelkõige kui nõrkus võib tekitada märkimisväärse riski, ning kui see on nii, siis võtta parandusmeetmeid ning anda sellest teada kooskõlas küberkerksuse määrusega.

215. Lisaks sellele nõuab teatamiskohustuste struktuur, et tootjad ajakohastaksid oma teadaandeid järk-järgult, sedamööda, kuidas nende sisejuurdlused edenevad ning nende arusaam aktiivselt ärakasutatavast nõrkusest või intsidendist muutub üksikasjalikumaks. Eelkõige peavad tootjad esitama põhjendamatu viivituseta ning igal juhul 24 tunni jooksul teada saamisest eelhoiatuse teavituse, mis sisaldab piiratud teavet. Seejärel tuleb teavituse osana esitada põhjendamatu viivituseta ning igal juhul 72 tunni jooksul alates teada saamisest lisateavet (edaspidi „72 tunni jooksul teavitamine“). Terviklik aruanne tuleb esitada 14 päeva jooksul pärast aktiivselt ärakasutatava nõrkuse jaoks parandus- või maandamismeetme kättesaadavaks muutumisest, või ühe kuu möödumisel 72 tunni jooksul teavitamisest tõsiste intsidentide korral.

216. Nagu on märgitud ka punktis *3.3.1 Vaba ja avatud lähtekoodiga tarkvara pidev toetus ning elujõulisuse tagamine,* peavad avatud lähtekoodiga tarkvara korraldajad samuti teatama aktiivselt ärakasutatavatest nõrkustest kooskõlas artikli 24 lõikega 3 ([30]). See kohustus kehtib aktiivselt ärakasutatavast nõrkusest teada saamisel ja mitte lihtsalt juhul, kui selle üksuse korraldatavas vaba ja avatud lähtekoodiga koodibaasis on nõrkus. Kuna vaba ja avatud lähtekoodiga tarkvara on üldjuhul integreeritud järgnevates etappides muudesse digielemente sisaldavatesse toodetesse, saab korraldaja tegelikkuses tõenäoliselt aktiivsest ärakasutamisest teada kolmandate isikute teadaannete alusel, milles tehakse kindlaks muudesse digielemente sisaldavatesse toodetesse integreeritud vaba ja avatud lähtekoodiga tarkvara komponentide ärakasutamine. See võib olla nii näiteks juhul, kui digielemente sisaldava toote tootja teeb kindlaks tema tootesse integreeritud vaba ja avatud lähtekoodiga tarkvara komponendi aktiivse ärakasutamise ja annab sellest teada kõnealuse komponendi korraldajale või kui kasutaja või turbeuurija leiab tõendeid digielemente sisaldavasse tootesse integreeritud vaba ja avatud lähtekoodiga tarkvara komponendi ärakasutamise kohta ning teatab sellest aktiivsest ärakasutamisest komponendi korraldajale.

217. Tuleks samuti täpsustada, et kuna aktiivselt ärakasutatavatest nõrkustest teatamise kohustus kehtib ajal, kui tootja saab teada aktiivsest ärakasutamisest, ei pea tootja teatama nõrkustest, mille aktiivsest ärakasutamisest ta sai teada juba enne 11. septembrit 2026 (mis on kuupäev, alates milles teatamiskohustus hakkab kehtima). Küberkerksuse määrusega ei nõuta seega nendest nõrkustest tagasiulatuvat teatamist. Samas kehtib kohustus juhul, kui tootja sai nõrkusest teada enne 11. septembrit 2026, aga ta ei olnud siis teadlik selle mis tahes aktiivsest ärakasutamisest (kuna seda ei olnud veel toimunud või kuna tootja ei olnud sellest teada saanud). Kui seejärel toimub pärast 11. septembrit 2026 aktiivne ärakasutamine või tootja saab sellest teada, siis käsitatakse seda nõrkust aktiivselt ärakasutatud nõrkusena, mille puhul kehtib teatamiskohustus.

218. Samal moel peab tootja teatama ainult tema digielemente sisaldavates toodetes esinevatest aktiivselt ärakasutatavatest nõrkustest. Kui digielemente sisaldavas tootes esineb aktiivselt ärakasutatav nõrkus, mis on omistatav kolmanda isiku komponendile, siis peab digielemente sisaldava toote tootja teatama sellest aktiivselt ärakasutatavast nõrkusest. Kui aga tootja on kursis, et kolmanda isiku komponent sisaldab nõrkust, kuid kõnealust nõrkust kas i) ei saa tema digielemente sisaldavas tootes ära kasutada (nt kuna nõrkusega koodini ei ole võimalik jõuda) või ii) seda ei ole tema digielemente sisaldavas tootes ära kasutatud, siis ei ole selle nõrkuse puhul tegemist tema digielemente sisaldavas tootes esineva aktiivselt ärakasutatava nõrkusega ja seega ei kehti selle puhul kõnealuse tootja teatamiskohustus. Kõnealune tootja võib siiski teatada sellest nõrkusest vabatahtlikkuse alusel kooskõlas küberkerksuse määruse artikliga 15. Samuti tuleb täita küberkerksuse määruse I lisa II osa nõrkuste käsitlemise nõudeid ning teatada nõrkusest seda komponenti tootvale või hooldavale isikule või üksusele kooskõlas artikli 13 lõikega 6, nagu on täpsemalt selgitatud punktis *9.2.1 Algse projektiga seotud isikute teavitamine ja turvaparanduste jagamine.*

([30]) Selles ulatuses, mille korraldaja osaleb digielemente sisaldava toote arenduses.

219. Pärast aktiivselt ärakasutatavast nõrkustest või tõsisest intsidendist teada saamist peavad tootjad kooskõlas artikli 14 lõikega 8 samuti teavitama mõjutatud kasutajaid ning vajaduse korral kõiki kasutajaid. Kui nad seda piisava aja jooksul ei tee, siis võivad teate saanud CSIRTid esitada selle teabe kasutajatele, kui seda peetakse proportsionaalseks ja vajalikuks, et vältida või maandada nõrkuse või intsidendi mõju.

220. Kooskõlas küberkerksuse määruse riskipõhise lähenemisviisiga kohaldatakse artikli 14 lõikes 8 sätestatud kohustust teavitada kasutajaid riskipõhisel ja proportsionaalsel viisil. Eelkõige ei tulene aktiivselt ärakasutatava nõrkuse või tõsise intsidendi kohta teabe esitamisest, et kõnealune teave tuleb teha üldsusele kättesaadavaks või valimatult avalikustada. Kui see on asjakohane ning võttes arvesse digielemente sisaldava toote olemust, mõjutatud kasutajaid ning nõrkuse või intsidendi võimalikku mõju, võivad tootjad avalikustada üksikasjaliku teabe asjakohastele kasutajatele või klientidele. See on eelkõige nii digielemente sisaldavate toodete puhul, mida kasutatakse tundlikus või üliolulises keskkonnas, kus üldsuse arutelu tehniliste üksikasjade teemal võib iseenesest suurendada küberriske või soodustada täiendavat ärakasutamist.

221. Kui nõrkusega on piisavalt tegeletud või selle mõju leevendatud, siis võib olla asjakohane laialdasem arutelu. See oleks nii näiteks juhul, kui arutelu aitab suurendada üldist teadlikkust või võimaldab kasutajatel kontrollida, et nende digielemente sisaldavad tooted ei ole enam mõjutatud. Neil juhtudel peaks jääma mis tahes laiema arutelu üksikasjalikkuse tase ja ajastus proportsionaalseks ning selle puhul tuleks võtta arvesse ärakasutamise jääkriske, digielemente sisaldava toote olemust ning asjasse puutuvate kasutajate huve. Lisaks sellele nõutakse I lisa II osa punktis 4, et tootjad avalikustaksid üldsusele teabe parandatud nõrkuste kohta, kui turvauuendus on kättesaadavaks tehtud.

9.2. **Nõrkuste käsitlemine**

9.2.1. *Algse projektiga seotud isikute teavitamine ja turvaparanduste jagamine*

222. Küberkerksuse määruse artikli 13 lõikes 6 nõutakse, et tootjad teataksid integreeritud komponentide nõrkustest kõnealust komponenti tootvale või hooldavale isikule või üksusele (edaspidi „algse projektiga seotud isiku teavitamine“).

223. Tootjad peavad teavitama algse projektiga seotud isikut ainult nende integreeritud komponendi versiooni puhul. Kui komponenti tootev või hooldav isik või üksus on võtnud kasutusele turvapoliitika, koordineeritud nõrkuste avalikustamise protsessid või nõrkustest teatamise määratud kanalid, siis peaksid tootjad esitama teateid nende kaudu, eelkõige kui parandamata nõrkuste enneaegne teatamine võib suurendada küberriske. Algse projekti hooldajate koormuse vähendamiseks, eelkõige avatud lähtekoodiga projektide puhul, ei ole tootjad samuti kohustatud neid teavitama, kui neil on võimalik veenduda, et komponenti tootev või hooldav isik või üksus on selle nõrkuse olemasolust teadlik. Tootjaid kutsutakse üles võtma mõistlikke meetmeid, et vältida topeltaruannete esitamist, näiteks kontrollides üldsusele kättesaadavaid nõrkuste andmebaase, projektipõhiseid turvanõuandeid või pikka aega kasutusel olnud probleemide jälgimise vahendeid enne algse projektiga seotud isikute teavitamist.

224. Tootjad peavad algse projektiga seotud isikuid teavitama ainult nendest nõrkustest, mis on olemas integreeritud komponendis endas, ning mitte nõrkustest, mis on olemas komponendi ning tootja arendatud muu koodi või muude komponentide integreerimise kombinatsiooni tulemusena. Sellest hoolimata võib tekkida olukordi, kui komponendi integreerimine konkreetsesse digielemente sisaldavasse tootesse toob esile kõnealuse komponendi teatava käitumise, omavahelise mõju või turvalisuse seisukohast olulised omadused, mis ei olnud eraldiseisvalt ilmsed või kergesti kindlaks tehtavad. Neil juhtudel kutsutakse tootjaid üles esitama selle teabe komponenti tootvale või hooldavale isikule või üksusele, et edendada häid nõrkuste käsitlemise tavasid, mille eesmärk on soodustada komponendi ökosüsteemi üldise turvalisuse tulemuslikku parandamist ja täiustamist.

225. Lõpuks ei nõuta tootjatelt nõrkusest teatamist ka algse projektiga seotud isikutele, kui komponendil ei ole enam hooldajat või kui tootja ei tugine uute versioonide või turvaparanduste puhul enam algsele hooldajale. Neil juhtudel julgustatakse tootjat sellest hoolimata teavitama selle komponendi kasutajaid mõistlike alternatiivsete meetmete abil, näiteks läbi olemasolevate kogukonna mehhanismide (nagu meililistid või probleemihalduse süsteemid) või läbi nõrkusi käsitlevate avalike registrite.

226. Artikli 13 lõike 6 kohaselt peavad lisaks sellele tootjad, kes on integreeritud komponendi nõrkusega tegelemiseks välja töötanud tarkvara muudatuse, jagama seda tarkvara muudatust (edaspidi „turvaparandus“) komponenti tootva või hooldava isiku või üksusega (edaspidi „jagamine algse projektiga seotud isikutega“)

227. Kui tootjad peavad jagama turvaparandust artikli 13 lõike 6 alusel, siis tuleks see parandus, kui see on asjakohane, esitada masinloetavas vormingus, lihtsasti kontrollitaval viisil ning, kui see on asjakohane, siis peaks komponenti tootev või hooldav isik või üksus selle integreerima. Kui komponent on vaba ja avatud lähekoodiga komponent, siis tuleks turvaparandust jagada viisil, mis on kooskõlas selle komponendi litsentsiga, näiteks jagades seda sama litsentsi alusel või litsentsi alusel, mis võimaldab hooldajal levitada parandust oma litsentsi all. Kui selle komponendi hooldajal on suunised turvaparanduste jagamise viisi kohta, siis peaks tootja järgima neid suuniseid.

228. Küberkerksuse määrusega ei nõuta siiski tootjatelt, et nad tagaksid, et komponenti tootev või hooldav isik või üksus nõustuks ilmtingimata nende turvaparandustega. Nad ei pea samuti tagama, et need parandused integreeritakse kindlasti komponendi koodihoidlasse, näiteks kui hooldaja eelistab kasutada probleemi lahendamiseks muud varianti. Samal moel ei pea tootjad nõustuma pakutud parandusega, mille on välja töötanud komponendi hooldaja, ning võivad eelistada lahendada probleemi muul sobilikul viisil.

229. Teatavatel juhtudel võib komponenti tootev või hooldav isik olla juba taganud nõrkuse kõrvaldamiseks turvaparanduse, aga tootja kasutab erinevat leevendusstrateegiat (näiteks võttes kasutusele erineva konfiguratsiooni). Neil juhtudel ei nõuta küberkerksuse määrusega tootjalt eelneva etapi süsteemi mõne muu osa muudatuse jagamist. Tootjat kutsutakse siiski üles seda tegema, kui see võib aidata komponenti hooldavat isikut või üksust.

9.2.2. *Teadaolevad ärakasutatavad nõrkused*

230. Küberkerksuse määruse I lisa I osa ühes olulises nõudes on märgitud, et artikli 13 lõikes 2 osutatud küberriskide hindamise alusel ning kui see on kohaldatav, tuleb digielemente sisaldavad tooted teha turul kättesaadavaks ilma teadaolevate ärakasutatavate nõrkusteta.

231. Artikli 3 punktis 41 on ärakasutatav nõrkus määratletud kui „nõrkus, mida vastaspool võib praktilistes käitamistingimustes tulemuslikult ära kasutada“. Kõik nõrkused ei ole praktilistes käitamistingimustes ärakasutatavad ja mõnda nõrkust saab ära kasutada ainult teoreetilistes tingimustes (nt laboris või matkimise käigus) ning/või mitte tingimustel, mis tekivad digielemente sisaldava toote käitamiskeskkonnas.

232. Küberkerksuse määrusega nõutakse, et tootjatel oleksid kehtestatud asjakohased põhimõtted ja kord, et käsitleda ja kõrvaldada võimalikke sisemiste või väliste allikate teatatud nõrkusi (artikli 13 lõige 8). Siiski ei ole seal sõnaselgelt täpsustatud, millal tuleks lugeda, et tootja on teadlik ärakasutatavast nõrkusest, millest tuleneb kohustus täita seda olulist nõuet turule laskmise ajal.

233. Nõrkust tuleks käsitada teada olevana, kui see on loetletud asjakohases üldsusele kättesaadavas nõrkuste andmebaasis, näiteks direktiivi (EL) 2022/2555 artikli 12 lõike 2 kohaselt loodud Euroopa nõrkuste andmebaasis või muus tuntud nõrkuste andmebaasis.

234. Lisaks sellele võib nõrkus olla teada, kui tootjale on sellest teada antud mitteavaliku teabe kaudu, näiteks turbeuurija koordineeritud avalikustamise või tootja enda sisemise katsetamise ja analüüsi teel, sh näiteks kasutades tehisintellektipõhiseid teenuseid. Samuti võib nõrkus olla teada, kui sellest on avalikult ja märgatavalt teatatud usaldusväärsetes meediaväljaannetes, sh erialastes küberturvalisuse väljaannetes või üldises massiteabevahendites.

235. Siiski ei tähenda lihtsalt fakt, et nõrkusest on teatatud või see on leitud, et see on praktilistes tingimustes ärakasutatav või esineb asjaomase konkreetse digielemente sisaldava toote puhul. Tootja peab seda uurima ning tegema kindlaks kõnealuse teabe õigsuse ja kehtivuse tema enda toote puhul, mis sisaldab digielemente. Seega võib nõrkusest esimese teatamise ja selle kinnitamise vahele jääda piiratud ajavahemik. Nagu on märgitud punktis *9.1 Teatamiskohustus*, tuleks rõhku panna kiirele tegutsemisele asjaolude uurimisel ja probleemile reageerimisel.

236. Lisaks sellele kehtib tootjate kohustus täita I lisa I osas sätestatud olulisi nõudeid turule laskmise hetkel kooskõlas artikli 13 lõikega 1. Tegelikkuses võidakse avastada uus võimalik ärakasutatav nõrkus digielemente sisaldava toote arendustsükli viimastes etappides, sh vahetult enne selle turustusahelasse lisamist (ja seega turule laskmist).

237. Kuna kohustus lasta digielemente sisaldavaid tooteid turule ilma teadaolevate ärakasutatavate nõrkusteta on riskipõhine kohustus, on tootja ülesanne teha kindlaks, kas küberriskide hindamise põhjal saab digielemente sisaldava toote turvaliselt turule lasta kooskõlas küberkerksuse määrusega. Teise võimalusena võib tootja otsustada, et teatavaks saanud uus nõrkus tuleb kõrvaldada enne, kui digielemente sisaldava toote saab turule lasta. Selle kindlaksmääramisel peaksid tootjad võtma arvesse nõrkuse tõsidust, ärakasutatavust ja võimalikku mõju ning samuti digielemente sisaldavast tootest endast tekkivaid riske, kui see on kasutuses. Nad võivad samuti võtta arvesse riske, mis tulenevad toote turulelaskmise edasilükkamisest kuni nõrkuse parandamiseni, näiteks kuna uus versioon kõrvaldab samuti muid ärakasutatavaid nõrkusi või see on vajalik elutähtsate süsteemide jätkuvaks käitamiseks. Igal juhul, kui digielemente sisaldav toode on turule lastud, siis jääb tootjale kohustus käsitleda nõrkusi tulemuslikult ning kooskõlas I lisa II osas sätestatud nõrkuste käsitlemise nõuetega.

9.2.3. *Mõjusad ja korrapärased testid ja läbivaatamised*

238. I lisa II osa punktis 3 nõutakse, et tootjad teeksid digielemente sisaldava toote mõjusaid ja korrapäraseid teste ja läbivaatamisi selle toe kestuse jooksul. Korrapäraste testide tegemine ei nõua muutmata testikampaania mehaanilist kordamist kindlate ajavahemike järel. See tähendab, et tuleb korrapäraselt läbi vaadata, kas uued sisendid, näiteks uued kindlaks tehtud ohud või uued avastatud nõrkused, nõuavad olemasolevate testide ajakohastamist ning vastavate testide rakendamist.

239. Läbivaatamise sagedus, põhjalikkus ja sisu peaks olema proportsionaalne digielemente sisaldava toote riskiprofiiliga, selle muutumisega aja jooksul ning ohupildi seisundiga. Kui läbivaatamise tulemusena tehakse kindlaks määratud testi mõjutavad uued asjakohased sisendid, tuleks koostada uued või muudetud testid ning need toote puhul rakendada eesmärgiga tagada, et ükski nõrkus ei jää kõrvaldamata. See võib hõlmata olemasolevate testide uuesti tegemist, kui digielemente sisaldava toote muudatuse tõttu muutub asjakohaseks selline testimine, näiteks regressioontest.

240. Kui läbivaatamise käigus sellist sisendit kindlaks ei tehta, siis ei ole vaja koostada täiendavaid teste. Muud nõrkuste käsitlemise kohustused, sh tekkivate riskide puhul nõrkuste käsitlemine ja kõrvaldamine, jäävad samal ajal kehtima.

9.3. **Koosmõju muude õigusaktidega**

9.3.1. *Määrus (EL) 2019/2144 ja määrus (EL) nr 168/2013*

241. Küberkerksuse määruse artikli 2 lõike 2 punktis c on sätestatud, et seda määrust ei kohaldata digielemente sisaldavate toodete suhtes, mille suhtes kohaldatakse määrust (EL) 2019/2144. Määrust (EL) 2019/2144 kohaldatakse „määruse (EL) 2018/858 artiklis 4 määratletud M-, N- ja O-kategooria sõidukite ning selliste sõidukite jaoks konstrueeritud ja ehitatud süsteemide, osade ja eraldi tehniliste seadmestike suhtes".

242. Samal moel on komisjoni delegeeritud määrusega (EL) 2025/1535 arvatud küberkerksuse määruse kohaldamisalast välja digielemente sisaldavad tooted, mis kuuluvad määruse (EL) nr 168/2013 kohaldamisalasse. Määrust (EL) nr 168/2013 kohaldatakse L-kategooria sõidukite ning „nimetatud sõidukite jaoks konstrueeritud ja valmistatud süsteemide, osiste ja eraldi seadmestike ning osade ja lisaseadmete suhtes" (artikli 2 lõige 1).

243. Küberkerksuse määrust ei kohaldata sõidukite suhtes, mille suhtes kohaldatakse neid määrusi. Lisaks sellele on vaja täiendavaid selgitusi kõnealuste sõidukite jaoks konstrueeritud ja valmistatud süsteemide, osiste ja eraldi seadmestike ning osade ja lisaseadmete (käesoleva punkti otstarbel „komponendid") erandi kohaldamisala kohta, kui neid käsitatakse digielemente sisaldavate toodetena küberkerksuse määruse tähenduses.

244. Ollakse seisukohal, et kõnealuste komponentide suhtes ei kohaldata küberkerksuse määrust, kui need on ainult konstrueeritud ja valmistatud määrustega (EL) 2019/2144 ja (EL) nr 168/2013 hõlmatud sõidukitesse integreerimiseks. See kehtib olenemata sellest, kas kõnealuse komponendi tootja müüb selle otse sõiduki tootjale või autotööstuse tarneahela muule ettevõtjale, kui komponent on selgelt mõeldud ja sobilik ainult lõpuks kõnealustesse sõidukitesse integreerimiseks.

245. Samas kohaldatakse küberkerksuse määrust tootja suhtes, kes müüb tavapäraseid komponente, mis on digielemente sisaldavad tooted, mida saab integreerida eri liiki toodetesse ja mitte ainult kõnealuste määrustega hõlmatud sõidukitesse.

246. Hindamine, kas komponent lastakse küberkerksuse määruse tähenduses turule, peab põhinema selle kättesaadavaks tegemise objektiivsetel tingimustel. Kui tootja pakub komponenti, mis ei ole sobilik ainult kõnealustesse sõidukitesse lõplikuks integreerimiseks, turustusmeetodite kaudu, mis on avatud muudele klientidele lisaks autotööstuse tarneahelale, näiteks üldised jaemüügipunktid või internetimüügi kanalid, mis võtavad vastu tellimusi üldsuselt, siis kuulub see komponent küberkerksuse määruse kohaldamisalasse, olenemata selle sihtotstarbe kohta esitatud väidetest. Neil juhtudel ei saa komponenti käsitada sellisena, et see on konstrueeritud ja valmistatud ainult määrustega (EL) 2019/2144 ja (EL) nr 168/2013 hõlmatud sõidukitesse integreerimise eesmärgil, ning tootja peab täitma küberkerksuse määruse nõudeid. Seevastu ainult autotööstuse tarneahelat hõlmavate piiratud, ettevõtjatevaheliste jaotuskanalite kasutamine võib osutada sellele, et need on konstrueeritud ja valmistatud ainult kõnealuse integreerimise eesmärgil.

9.3.2. *ELi tüübihindamissertifikaatide kehtivus (artikli 69 lõige 1)*

247. Küberkerksuse määruse artikli 69 lõikes 1 on märgitud, et „ELi tüübihindamissertifikaadid ja tüübikinnitusotsused, mis on välja antud seoses küberturvalisuse nõuetega digielemente sisaldavatele toodetele, mille suhtes kohaldatakse muid liidu ühtlustamisõigusakte kui käesolevat määrust, kehtivad kuni 11. juunini 2028, välja arvatud juhul, kui need aeguvad enne seda kuupäeva või kui sellistes muudes liidu ühtlustamisõigusaktides on sätestatud teisiti; sel juhul jäävad need kehtima kõnealuste õigusaktide kohaselt."

248. Kõnealuste sertifikaatide ja otsuste jätkuvat kehtivust tuleks mõista selliselt, et need piirduvad küberriskide ja vastavate nõuetega, mida on käsitletud asjakohastes liidu ühtlustamisõigusaktides, mille alusel need välja anti. Nende riskide puhul ei ole tootjad kohustatud vastavalt küberkerksuse määrusele vastavust uuesti hindama ega tõendama artikli 69 lõikes 1 osutatud kehtivusaja vältel digielemente sisaldavate toodete puhul, mille nad kavatsevad turule lasta 11. detsembrist 2027 kuni 11. juunini 2028 ([31]). See on nii seoses väljastatud sertifikaatide ja otsustega, mille puhul nõutakse kohaldatavates liidu ühtlustamisõigusaktides, et tootja korraldaks vastavushindamismenetluse teada antud asutuse kaudu, ning kui tootja on otsustanud seda vabatahtlikult teha.

249. Seega ei vabasta muude liidu ühtlustamisõigusaktide alusel kehtiva sertifikaadi või otsuse olemasolu tootjaid küberkerksuse määruse alusel tervikliku küberriskide hindamise tegemisest (ega muudest sellest tulenevatest kohustustest). Selle asemel võimaldab see neil tugineda olemasolevatele sertifikaatidele tõendina nende vastavushindamismenetluse nõuete täitmise kohta selles ulatuses, milles vastavaid küberriske on juba maandatud. Kui sertifikaat või otsus kehtib muude liidu ühtlustamisõigusaktide alusel kauem kui 11. juunini 2028, siis võib tootja sellest hoolimata tugineda küberkerksuse määruse otstarbel sellele sertifikaadile või otsusele ainult kuni 11. juunini 2028.

250. Kui artikli 13 lõike 2 kohaselt tehtud küberriskide hindamise tulemusena tehakse kindlaks täiendavad riskid, mida ei käsitletud olemasoleva sertifikaadi või otsuse aluseks olevates küberturvalisuse nõuetes, siis jääb tootjatele kohustus tegeleda nende riskidega kooskõlas küberkerksuse määrusega. Neil juhtudel eeldab nõuetele vastavus kindlaks tehtud lünkade hindamist ja kõrvaldamist, olenemata olemasoleva sertifikaadi või otsuse jätkuvast kehtivusest.

251. Seda võib näitlikustada juhtumi abil, mil digitaalseid elemente sisaldava toote suhtes kohaldatakse küberturvalisuse nõudeid, mis on sätestatud komisjoni delegeeritud määruses (EL) 2022/30, millega täiendatakse direktiivi 2014/53/EL, (edaspidi „raadioseadmete direktiivi delegeeritud määrus“) ning kui ELi tüübihindamise sertifikaat või tüübikinnitusotsus on väljastatud nende nõuete alusel. Sel juhul jääb sertifikaat või otsus kooskõlas artikli 69 lõikega 1 kehtima küberriskide puhul, mida on kõnealuses sertifikaadis käsitletud ja mis on seotud direktiivi 2014/53/EL (edaspidi „raadioseadmete direktiiv“) küberturvalisuse oluliste nõuetega.

252. Neil juhtudel ei pea tootjad kõnealuste sertifikaatidega juba käsitletud kõnealuste riskide puhul küberkerksuse määruse kohaldamisel hindama uuesti või tõendama uuesti vastavust seni, kuni asjakohane sertifikaat või otsus kehtib, ning igal juhul mitte pärast 11. juunit 2028. See hõlmab näiteks küberriske, mis on seotud võrgu kaitsmise, isikuandmete ja eraelu puutumatuse kaitse või pettuste vältimisega (selles ulatuses, milles need riskid on hõlmatud kõnealuse sertifikaadiga), mis on seotud raadioseadmete direktiivi küberturvalisuse nõuetega ning kajastuvad vastavushindamises.

253. Kuid kui küberkerksuse määruse artikli 13 lõike 2 kohaselt tehtud küberriskide hindamise tulemusena tehakse kindlaks täiendavad küberriskid, mida ei käsitletud nendes sertifikaatides, siis jääb tootjatele kohustus käsitleda neid riske kooskõlas küberkerksuse määrusega. See võib näiteks hõlmata riske, mis on seotud nõrkuste käsitlemise protsessidega, andmete minimeerimisega ning ründepinna vähendamisega või muude tootepõhiste küberturvalisuse aspektidega, mida ei ole neis sertifikaatides käsitletud või mida ei ole igal juhul käsitletud raadioseadmete direktiivi küberturvalisuse olulistes nõuetes.

254. Seega ei tõenda raadioseadmete direktiivi alusel kehtiva ELi tüübihindamise sertifikaadi või tüübikinnitusotsuse olemasolu selle küberturvalisust käsitlevate oluliste nõuete puhul iseenesest täielikku vastavust küberkerksuse määrusele. Selle asemel võimaldab see tootjatel tugineda kõnealusele sertifikaadile või otsusele nõuete täitmise tõendina vastavate riskide puhul, tagades samal ajal, et mis tahes allesolevaid või uusi kindlaks tehtud riske hinnatakse ja maandatakse küberkerksuse määruse kohaselt.

([31]) Enne 11. detsembrit 2027 turule lastud digielemente sisaldavate toodete suhtes kohaldatakse liidu õigusakte, mis kehtisid nende turule laskmise ajal, ning kui need vastasid nõuetele, siis on neid võimalik müüa ja kasutusele võtta, v.a juhul, kui neis tehakse 11. detsembril 2027 või pärast seda olulisi muudatusi. Vt turule laskmise ja turul kättesaadavaks tegemise mõistete selgitusi ka käesoleva dokumendi punktis *2.1 Turule laskmine* ning sinise raamatu 2. peatükis.

255. Samal moel, kui digielemente sisaldava toote suhtes kohaldatakse küberturvalisusega seotud olulisi tervisekaitse- ja ohutusnõudeid, mis on sätestatud määruses (EL) 2023/1230 (edaspidi „masinate määrus“), mis on täielikult kohaldatav alates 20. jaanuarist 2027, ja kui ELi tüübihindamise sertifikaat või tüübikinnitusotsus on väljastatud kõnealuste nõuete alusel, siis jääb kõnealune sertifikaat või otsus masinate määrusega hõlmatud küberriskide puhul kehtima kooskõlas küberkerksuse määruse artikli 69 lõikega 1.

256. See kehtib eelkõige küberturvalisuse aspektide puhul, mis on seotud rikkumise eest kaitsmise ning juhtsüsteemide ohutuse ja töökindlusega, nagu on märgitud masinate määruse III lisa punktides 1.1.9 ja 1.2.1. Nende riskide puhul ei pea tootjad küberkerksuse määruse otstarbel hindama uuesti või tõendama uuesti vastavust seni, kuni asjakohane sertifikaat või otsus kehtib, ning igal juhul mitte pärast 11. juunit 2028. See kehtib selles ulatuses, milles neid riske on maandatud masinate määruse kohase vastavushindamise raames.

257. Nagu ka eespool nimetatud raadioseadmete direktiivi küberturvalisuse oluliste nõuete puhul, kui küberkerksuse määruse artikli 13 lõike 2 kohase küberriskide hindamise tulemusena tehakse kindlaks täiendavad küberriskid, mis ei ole hõlmatud masinate määruse kohaselt väljastatud asjakohase sertifikaadiga ja mis on seotud kõnealuse määruse küberohutuse nõuetega, siis jääb tootjatele kohustus maandada neid riske kooskõlas küberkerksuse määrusega.