Publicatieblad
van de Europese Unie

NL
C-serie

C/2026/6013

17.11.2026

MEDEDELING VAN DE COMMISSIE

Richtsnoeren van de Commissie over de toepassing van Verordening (EU) 2024/2847 (verordening cyberweerbaarheid)

(C/2026/6013)

Inhoudsopgave

Bladzijde

1. INLEIDING 3
   - 1.1. De verordening cyberweerbaarheid 3
   - 1.2. Doel van de richtsnoeren 3
2. TOEPASSINGSGEBIED 4
   - 2.1. In de handel brengen 4
   - 2.2. Software als product met digitale elementen 5
   - 2.3. Computercode 6
   - 2.4. Combinatie van hardware en software die een product met digitale elementen vormen 7
   - 2.5. Gegevensverbinding 8
   - 2.6. Complexe systemen 8
   - 2.7. Producten met digitale elementen die zijn ontworpen voordat de verordening cyberweerbaarheid van toepassing werd 9
3. VRIJE EN OPENSOURCESOFTWARE 11
   - 3.1. Bepalen of vrije en opensourcesoftware onder iemands verantwoordelijkheid valt 12
   - 3.2. Bepalen of vrije en opensourcesoftware in de EU in de handel wordt gebracht 13
     - 3.2.1. Een prijs in rekening brengen 13
     - 3.2.2. Tegeldemaking van andere diensten of diensten waarvoor persoonsgegevens moeten worden verwerkt 13
     - 3.2.3. Ondersteunende diensten 14
     - 3.2.4. Donaties 15
     - 3.2.5. Financiering van vrije en opensourcesoftware 15
     - 3.2.6. Entiteiten zonder winstoogmerk die zijn opgericht om doelstellingen zonder winstoogmerk te verwezenlijken 16
     - 3.2.7. Integratie door andere fabrikanten 16
   - 3.3. Opensourcesoftwarestewards 16
     - 3.3.1. Langdurige ondersteuning en waarborging van de levensvatbaarheid van FOSS 17
   - 3.4. Contribuanten en downstreamtoepassingen 18
   - 3.5. Illustratieve scenario's 19
4. INGRIJPENDE WIJZIGINGEN EN RESERVEONDERDELEN 21
   - 4.1. Fysieke reparatie 22
   - 4.2. Reserveonderdelen 23
   - 4.3. Software-updates als ingrijpende wijzigingen 24

4.4. Gevolgen van een ingrijpende wijziging 27
4.4.1. Ingrijpende wijzigingen uitgevoerd door een andere persoon dan de oorspronkelijke fabrikant .. 28
4.4.2. Door de oorspronkelijke fabrikant uitgevoerde ingrijpende wijzigingen 29
5. ONDERSTEUNINGSPERIODE 29
5.1. Ingrijpende wijzigingen en de ondersteuningsperiode 31
6. Belangrijke en kritieke producten met digitale elementen 32
6.1. Basisfunctionaliteit 33
6.2. Conformiteitsbeoordeling voor belangrijke en kritieke producten met digitale elementen 36
6.3. Gevolgen voor het vermoeden van conformiteit 38
7. BEOORDELING VAN CYBERBEVEILIGINGSRISICO'S EN INTEGRATIE VAN PRODUCTEN MET DIGITALE ELEMENTEN EN COMPONENTEN 41
7.1. Over de evaluatie en behandeling van cyberbeveiligingsrisico's 41
7.2. Over het zodanig ontwerpen, ontwikkelen en produceren van producten met digitale elementen dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen 42
7.3. Risicobeoordeling en passende zorgvuldigheid met betrekking tot externe afhankelijkheden en geïntegreerde componenten 42
7.4. Hergebruik van risicobeoordelingen en conformiteitsdocumentatie voor families van producten met digitale elementen 44
8. GEGEVENSVERWERKING OP AFSTAND 44
8.1. Wat wordt beschouwd als een oplossing voor gegevensverwerking op afstand voor een product met digitale elementen? 45
8.1.1. Het begrip "op afstand" 46
8.1.2. Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren? 46
8.1.3. Is de software ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant? 47
8.2. Praktische en technische gevolgen van oplossingen voor gegevensverwerking op afstand en afhankelijkheid van oplossingen van derden 49
8.3. Praktijkvoorbeelden van oplossingen voor gegevensverwerking op afstand 50
8.3.1. Mobiele bankapplicatie 51
8.3.2. Slimme thermostaat 52
8.3.3. E-reader 53
8.3.4. Industriële robot 53
8.3.5. Cellulair netwerk 53
9. AANVULLENDE ELEMENTEN 54
9.1. Meldingsplicht 54
9.2. Respons op kwetsbaarheden 56
9.2.1. Upstream melden en beveiligingsoplossingen delen 56
9.2.2. Bekende uitbuitbare kwetsbaarheden 57
9.2.3. Doeltreffende en regelmatige tests en evaluaties 58
9.3. Raakvlakken met andere wetgeving 59
9.3.1. Verordening (EU) 2019/2144 en Verordening (EU) nr. 168/2013 59
9.3.2. Geldigheid van EU-typeonderzoekscertificaten (artikel 69, lid 1) 59

1. **INLEIDING**

1.1. **De verordening cyberweerbaarheid**

1. Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (verordening cyberweerbaarheid) ([1]) is op 10 december 2024 in werking getreden. De verordening heeft tot doel de aanpak van cyberbeveiliging door de Unie te versterken, de cyberweerbaarheid op EU-niveau aan te pakken en de werking van de interne markt te verbeteren door een uniform rechtskader vast te stellen voor essentiële cyberbeveiligingsvereisten voor het in de EU in de handel brengen van producten met digitale elementen, alsook tijdens de levenscyclus van een product met digitale elementen.

2. De verordening cyberweerbaarheid is gebaseerd op het nieuwe wetgevingskader van de EU (NWK) dat is vastgesteld in Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 en Besluit nr. 768/2008/EG van het Europees Parlement en de Raad van 9 juli 2008 betreffende een gemeenschappelijk kader voor het verhandelen van producten en tot intrekking van Besluit 93/465/EEG van de Raad ([2]).

3. Het markttoezicht en de handhaving worden uitgevoerd door de nationale markttoezichtautoriteiten. Op producten met digitale elementen die vallen binnen het toepassingsgebied van de verordening cyberweerbaarheid is Verordening (EU) 2019/1020 van het Europees Parlement en de Raad van 20 juni 2019 betreffende markttoezicht en conformiteit van producten en tot wijziging van Richtlijn 2004/42/EG en de Verordeningen (EG) nr. 765/2008 en (EU) nr. 305/2011 van toepassing. De Commissie en het Agentschap van de Europese Unie voor cyberbeveiliging (Enisa) ondersteunen marktdeelnemers en lidstaten bij de toepassing van de verordening cyberweerbaarheid.

1.2. **Doel van de richtsnoeren**

4. Volgens artikel 26, lid 1, van de verordening cyberweerbaarheid is de Commissie verplicht richtsnoeren te publiceren om de marktdeelnemers te helpen bij de toepassing van de verordening, met bijzondere aandacht voor de wijze waarop de naleving door kleine, middelgrote en micro-ondernemingen kan worden vergemakkelijkt. In artikel 26, lid 2, wordt beschreven welke aspecten in elk geval in de richtsnoeren aan bod moeten komen. Het gaat onder meer om: i) het toepassingsgebied van de verordening cyberweerbaarheid (met name oplossingen voor gegevensverwerking op afstand en vrije en opensourcesoftware); ii) het begrip "ondersteuningsperioden"; iii) de wisselwerking tussen de verordening cyberweerbaarheid en andere EU-wetgeving, en iv) het begrip "ingrijpende wijziging".

5. Op 3 december 2025 heeft de Commissie een reeks veelgestelde vragen (FAQ's) gepubliceerd, die bedoeld zijn om marktdeelnemers te helpen zich voor te bereiden op de uitvoering van de verordening cyberweerbaarheid ([3]).

6. Deze richtsnoeren zijn bedoeld om marktdeelnemers te helpen bij de naleving van de verordening cyberweerbaarheid en om de activiteiten van markttoezichtautoriteiten, aanmeldende autoriteiten en aangemelde instanties te ondersteunen, teneinde de geharmoniseerde handhaving van de verordening cyberweerbaarheid in de hele Unie te waarborgen. Deze richtsnoeren zijn niet bedoeld om het gehele toepassingsgebied van de verordening cyberweerbaarheid te bestrijken, maar veeleer om duidelijkheid te verschaffen over de grondgedachte achter bepaalde belangrijke bepalingen en over de wijze waarop deze in de praktijk kunnen worden toegepast. Deze richtsnoeren hebben betrekking op de verordening cyberweerbaarheid en zijn niet van toepassing op andere EU-wetgeving.

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

([2]) Het werkprogramma van de Commissie voor 2026 voorziet in de presentatie van "Europese productwetgeving", waarbij het NWK en de regels inzake markttoezicht en normalisatie worden geactualiseerd: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52025DC0870.

([3]) De veelgestelde vragen kunnen worden gedownload via de website van de Commissie over de uitvoering van de verordening cyberweerbaarheid, vanaf de speciale webpagina met veelgestelde vragen.

7. Bij de voorbereiding van deze richtsnoeren zijn belanghebbenden uitgebreid geraadpleegd, waaronder de deskundigengroep inzake cyberbeveiliging van producten met digitale elementen ([4]) en via een openbare raadpleging die tussen 3 maart en 13 april 2026 is gehouden ([5]).

8. Deze richtsnoeren zijn niet bindend voor marktdeelnemers of andere actoren die onder de verordening cyberweerbaarheid vallen. Een bindende uitlegging van de verordening cyberweerbaarheid komt uitsluitend toe aan het Hof van Justitie van de Europese Unie. Niettemin wordt in deze richtsnoeren de interpretatie van de verordening cyberweerbaarheid door de Commissie uiteengezet, teneinde de naleving te ondersteunen en bij te dragen tot de doeltreffende uitvoering van de verordening. Voorts bevatten de richtsnoeren een aantal voorbeelden ter illustratie van de toepassing van specifieke bepalingen. Deze voorbeelden zijn echter niet bedoeld ter vervanging van een beoordeling per geval, wat altijd nodig zal zijn om rekening te houden met de specifieke kenmerken van elk individueel geval.

9. Overeenkomstig artikel 26 van de verordening cyberweerbaarheid kan de Commissie overwegen verdere richtsnoeren uit te vaardigen, met inbegrip van richtsnoeren voor fabrikanten die onder de verordening cyberweerbaarheid en andere harmonisatiewetgeving van de Unie of andere daarmee verband houdende rechtshandelingen van de Unie vallen. Deze richtsnoeren kunnen bijvoorbeeld betrekking hebben op vragen over de wisselwerking tussen de verordening cyberweerbaarheid en Verordening (EU) 2024/1689 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie (“AI-verordening”) en Verordening (EU) 2022/2554 betreffende digitale operationele weerbaarheid voor de financiële sector (“DORA-verordening”).

2. **TOEPASSINGSGEBIED**

2.1. **In de handel brengen**

10. De verordening cyberweerbaarheid is van toepassing op producten met digitale elementen die op de EU-markt worden aangeboden. Het begrip “op de markt aanbieden” wordt gedefinieerd in artikel 3, punt 22), van de verordening cyberweerbaarheid als “het in het kader van een handelsactiviteit, al dan niet tegen betaling, verstrekken van een product met digitale elementen met het oog op distributie of gebruik op de markt van de Unie”. Overeenkomstig artikel 3, punt 21), wordt een product met digitale elementen in de EU in de handel gebracht wanneer het voor het eerst op de markt wordt aangeboden.

11. De meest recente editie van “De Blauwe Gids: richtlijnen voor de uitvoering van de productvoorschriften van de EU” ([6]) (hierna te noemen: “de Blauwe Gids”), die in 2022 is gepubliceerd, biedt richtsnoeren om het inzicht in de productvoorschriften van de EU en de uniforme toepassing ervan in de verschillende sectorale rechtskaders die zijn afgestemd op het nieuwe wetgevingskader (NWK), zoals de verordening cyberweerbaarheid, te vergemakkelijken. De Blauwe Gids geeft aan dat de begrippen “in de handel brengen” en “op de markt aanbieden” moeten worden opgevat als een verwijzing naar “elk product afzonderlijk, niet […] een type product, of het nu als een losse eenheid of in serie is vervaardigd” (punt 2.3).

12. Voor meer “traditionele” producten met digitale elementen die onder het NWK vallen, zoals hardware in de vorm van machines of radioapparatuur met digitale elementen, is het begrip “in de handel brengen” goed ingeburgerd en biedt de Blauwe Gids verdere richtsnoeren om te verduidelijken wanneer dergelijke producten worden geacht in de handel te zijn gebracht. De “beknopte voorbeelden” in punt 2.12 van de Blauwe Gids geven verdere voorbeelden van het begrip “in de handel brengen”.

13. Gezien de aard van immateriële producten met digitale elementen, zoals opzichzelfstaande software, zijn echter verdere richtsnoeren nodig over wanneer dergelijke producten met digitale elementen worden geacht in de handel te zijn gebracht. Zodra de productiefase van de software is voltooid en het product met digitale elementen aan potentiële gebruikers op de EU-markt wordt aangeboden, kan de fabrikant ervan worden geacht meerdere kopieën van hetzelfde softwareproduct met digitale elementen te hebben vervaardigd en deze te hebben geleverd voor distributie of gebruik. In tegenstelling tot materiële producten met digitale elementen is opzichzelfstaande software niet onderworpen aan fysieke productie- of voorraadbeperkingen: elke handeling waarbij de software op de markt

([4]) Deskundigengroep inzake cyberbeveiliging van producten met digitale elementen in het register van deskundigengroepen van de Commissie en andere adviesorganen.
([5]) Openbare raadpleging over de ontwerprichtsnoeren van de Commissie over de verordening cyberweerbaarheid.
([6]) Mededeling van de Commissie, “De Blauwe Gids van 2022: richtlijnen voor de uitvoering van de productvoorschriften van de EU”, 2022/C 247/01 (PB C 247 van 29.6.2022, blz. 1).

wordt aangeboden om te worden gedownload of verspreid, leidt ertoe dat een nieuwe identieke kopie voor de gebruiker wordt gecreëerd. Zolang deze versie van de software niet zodanig wordt gewijzigd dat dit gevolgen heeft voor de naleving van de verordening cyberweerbaarheid, wordt het in de EU in de handel brengen geacht te hebben plaatsgevonden op het moment van het eerste aanbod voor distributie of gebruik. De mogelijkheid om deze versie van het softwareproduct met digitale elementen daarna te downloaden of te verspreiden, moet daarom worden beschouwd als een geval waarin dit softwareproduct met digitale elementen op de markt wordt aangeboden ([7]).

14. Daarom moet een opzichzelfstaand softwareproduct met digitale elementen worden geacht in de handel te zijn gebracht wanneer de productiefase ervan is voltooid en die software in het kader van een handelsactiviteit voor het eerst wordt geleverd voor distributie of gebruik op de EU-markt. De fabrikant moet worden geacht meerdere kopieën van hetzelfde softwareproduct met digitale elementen tegelijkertijd in de handel te hebben gebracht. Hoewel meerdere kopieën van dezelfde software individuele producten met digitale elementen blijven, worden zij derhalve geacht tegelijkertijd in de handel te worden gebracht, ongeacht wanneer het bezit of het gebruik van elke afzonderlijke kopie aan een andere natuurlijke of rechtspersoon wordt overgedragen. Wanneer de fabrikant software op de markt aanbiedt in verschillende varianten die verschillen wat betreft de componenten, configuraties of ingeschakelde functionaliteiten ervan (bv. versies voor verschillende besturingssystemen of bundels met verschillende sets functies), kunnen die varianten echter niet worden beschouwd als meerdere kopieën van hetzelfde softwareproduct met digitale elementen. Daarom moeten zij met het oog op het in de handel brengen als afzonderlijke producten met digitale elementen worden behandeld.

Voorbeeld 1: op 1 januari 2028 levert bedrijf A voor het eerst via haar website versie 1.0.0 van haar software X voor distributie. Diezelfde dag koopt klant 1 een kopie van versie 1.0.0 van software X. Op 15 januari 2028 koopt klant 2 een kopie van versie 1.0.0 van software X. Beide kopieën van versie 1.0.0 van software X worden op 1 januari 2028 in de handel gebracht.

15. Gezien de iteratieve aard van softwareontwikkeling, moet verder worden verduidelijkt dat latere iteraties van een softwareproduct met digitale elementen worden beschouwd als nieuw in de handel gebracht wanneer die iteraties kunnen worden aangemerkt als een "ingrijpende wijziging" van een softwareproduct met digitale elementen dat reeds in de handel is gebracht, zoals aangegeven in overweging 41 van de verordening cyberweerbaarheid. Voor iteraties die niet als ingrijpende wijzigingen kunnen worden aangemerkt, hoeft de fabrikant geen nieuwe conformiteitsbeoordelingsprocedure uit te voeren en wordt de datum van het in de handel brengen van die software derhalve niet gewijzigd. Zie punt 4 voor meer informatie over het begrip "ingrijpende wijziging".

Voorbeeld 2: op 1 januari 2028 levert bedrijf A voor het eerst via haar website versie 1.0.0 van software X voor distributie. Diezelfde dag koopt klant 1 een kopie van versie 1.0.0 van software X. Op 15 januari 2028 geeft bedrijf A een bijgewerkte versie 1.0.1 van software X uit die geen ingrijpende wijziging vormt. Op 30 januari 2028 koopt klant 2 een kopie van versie 1.0.1 van software X. Zowel versie 1.0.0 als versie 1.0.1 van software X wordt geacht op 1 januari 2028 in de handel te zijn gebracht.

16. De richtsnoeren in de punten 13, 14 en 15 zijn uitsluitend van toepassing voor zover het product met digitale elementen opzichzelfstaande software is. Dit is bijvoorbeeld niet het geval wanneer de software wordt gecombineerd met hardware, zoals besproken in punt 2.4, "Combinatie van hardware en software die een product met digitale elementen vormen".

2.2. **Software als product met digitale elementen**

17. In artikel 3, punt 1), van de verordening cyberweerbaarheid wordt een product met digitale elementen gedefinieerd als "een software- of hardwareproduct en zijn oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht". Deze producten met digitale elementen vallen binnen het toepassingsgebied van de verordening cyberweerbaarheid wanneer het beoogde doel of het redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke gegevensverbinding met een apparaat of netwerk omvat.

([7]) Overeenkomstig artikel 13, lid 11, kunnen fabrikanten openbare softwarearchieven bijhouden om de toegang van gebruikers tot historische versies te verbeteren. In die gevallen worden gebruikers duidelijk en op gemakkelijk toegankelijke wijze geïnformeerd over de risico's in verband met het gebruik van niet-ondersteunde software.

18. De verordening cyberweerbaarheid kan daarom betrekking hebben op een reeks producten met digitale elementen, waaronder: i) opzichzelfstaande software, zoals apps en computerprogramma's, zowel digitaal als fysiek verspreid; ii) hardware met ingebedde software (bv. apparatuur voor het internet der dingen, laptops, tablets); iii) opzichzelfstaande hardware (bv. geïntegreerde schakelingen, moederborden), en iv) elke combinatie van hardware en software die afzonderlijk wordt geleverd, maar bedoeld is om samen te worden gebruikt.

19. Opzichzelfstaande software valt derhalve binnen het toepassingsgebied van de verordening cyberweerbaarheid wanneer deze in de handel wordt gebracht als een product met digitale elementen. Het is nuttig een onderscheid te maken tussen softwareproducten met digitale elementen die onder de verordening cyberweerbaarheid vallen en de verlening op afstand van diensten die niet onder het toepassingsgebied van de verordening cyberweerbaarheid vallen.

20. Om binnen het toepassingsgebied van de verordening cyberweerbaarheid te vallen, moet een softwareproduct met digitale elementen aan een gebruiker worden verstrekt, door die gebruiker worden verkregen en worden gebruikt op of als onderdeel van een elektronisch informatiesysteem aan de kant van de gebruiker. Software die wordt gedownload, geïnstalleerd of anderszins aan de gebruiker wordt geleverd en die op het elektronische informatiesysteem van de gebruiker wordt gebruikt, voldoet aan deze criteria, ook wanneer deze bijvoorbeeld de vorm aanneemt van een browserextensie of een applicatie die met behulp van webtechnologie is ontwikkeld, maar voor lokaal gebruik wordt geleverd.

21. Software die op afstand wordt uitgevoerd en waartoe de gebruiker alleen toegang heeft, is daarentegen niet louter op die basis een product met digitale elementen. In overwegingen 11 en 12 van de verordening cyberweerbaarheid wordt dit onderscheid in feite gemaakt door uit te leggen dat verwerking of opslag op afstand alleen onder de verordening cyberweerbaarheid valt voor zover het noodzakelijk is opdat een product met digitale elementen zijn functies vervult (d.w.z. via het concept van gegevensverwerking op afstand zoals gedefinieerd in artikel 3, punt 2), en niet zelf als een product met digitale elementen. Dit is doorgaans het geval voor webapplicaties, met inbegrip van progressieve webapps, waartoe uitsluitend toegang wordt verkregen via een webbrowser. Hetzelfde geldt voor websites: hoewel websites in beperkte mate technisch kunnen worden beheerd en uitgevoerd op het apparaat van de gebruiker, volgt uit overweging 12 van de verordening cyberweerbaarheid dat websites zelf niet als producten met digitale elementen moeten worden beschouwd en alleen binnen het toepassingsgebied van de verordening cyberweerbaarheid vallen wanneer zij de functionaliteit van een product met digitale elementen ondersteunen, d.w.z. voor zover zij als gegevensverwerking op afstand kunnen worden aangemerkt (zoals nader toegelicht in punt *8*, en met name punt *8.1.2*, "Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren?").

Voorbeeld 3: een mobiele applicatie die een gebruiker downloadt van een appstore en installeert op zijn smartphone, wordt aan de gebruiker geleverd en wordt uitgevoerd op het apparaat van de gebruiker en is derhalve een product met digitale elementen. Wanneer het in het kader van een handelsactiviteit in de handel wordt gebracht, kan het onder het toepassingsgebied van de verordening cyberweerbaarheid vallen.

Voorbeeld 4: een desktopapplicatie die is gebouwd met behulp van webtechnologie, maar is verpakt voor lokale installatie, wordt aan de gebruiker geleverd en wordt uitgevoerd op het apparaat van de gebruiker, en is derhalve een product met digitale elementen. Wanneer het in het kader van een handelsactiviteit in de handel wordt gebracht, kan het onder het toepassingsgebied van de verordening cyberweerbaarheid vallen.

Voorbeeld 5: een webapplicatie waartoe de gebruiker uitsluitend via een webbrowser toegang heeft, is geen product met digitale elementen. Tenzij het de functionaliteit van een product met digitale elementen ondersteunt, valt het niet onder het toepassingsgebied van de verordening cyberweerbaarheid. Een applicatie die aan de gebruiker wordt geleverd als lokaal geïnstalleerde client die op het apparaat van de gebruiker wordt uitgevoerd, is daarentegen een product met digitale elementen. Wanneer het in het kader van een handelsactiviteit in de handel wordt gebracht, kan het onder het toepassingsgebied van de verordening cyberweerbaarheid vallen.

Indien die client voor de uitvoering van een of meer van zijn functies gebruikmaakt van gegevensverwerking op afstand die voldoet aan de definitie van gegevensverwerking op afstand, maakt die gegevensverwerking op afstand ook deel uit van het product met digitale elementen.

Voorbeeld 6: een website die uitsluitend informatie aan bezoekers weergeeft en de functionaliteit van een product met digitale elementen niet ondersteunt, is zelf geen product met digitale elementen. De website valt derhalve niet onder het toepassingsgebied van de verordening cyberweerbaarheid.

2.3. **Computercode**

22. Het is ook nuttig om te verduidelijken of broncode een softwareproduct met digitale elementen kan vormen. In de verordening cyberweerbaarheid wordt "software" gedefinieerd als "het deel van een elektronisch informatiesysteem dat uit computercode bestaat" (artikel 3, punt 4)). Computercode kan de vorm aannemen van i) machinecode, d.w.z. een reeks rechtstreeks door de processor van een computer uitgevoerde instructies in binair formaat, of ii) broncode, d.w.z. een reeks instructies en statements die in een programmeertaal zijn geschreven en die door een computer moeten worden gecompileerd of geïnterpreteerd om te worden uitgevoerd. De definitie van software in de verordening cyberweerbaarheid heeft betrekking op beide.

23. Een andere vraag is of een bepaalde levering van computercode neerkomt op het in de Unie in de handel brengen van een product met digitale elementen, waarvoor een levering in het kader van een handelsactiviteit moet plaatsvinden. Dit is voor broncode vaak niet het geval. Zo wordt een natuurlijke of rechtspersoon die vrije en opensourcecomputercode in openbaar toegankelijke gegevensbanken deelt, voor de toepassing van de verordening cyberweerbaarheid over het algemeen niet geacht die code op de EU-markt te brengen (zoals nader wordt besproken in punt *3*, "Vrije en opensourcesoftware"). Onafgewerkte code die tijdens de ontwerp- en ontwikkelingsfase van een product met digitale elementen wordt gedeeld (bv. voor tests of beoordelingen), wordt ook niet geacht in de handel te zijn gebracht voor de toepassing van de verordening cyberweerbaarheid, aangezien de productiefase ervan niet is voltooid. Ook voorbeeldcode of code voor demonstratiedoeleinden die als onderdeel van instructie- of opleidingsmateriaal wordt verstrekt, wordt voor de toepassing van de verordening cyberweerbaarheid niet als in de handel gebracht beschouwd ([8]).

24. Wanneer een fabrikant zijn klanten daarentegen computercode verstrekt als een product met digitale elementen, wordt die code geacht in de handel te zijn gebracht, ongeacht of het machinecode of broncode betreft ([9]).

Voorbeeld 7: bedrijf A geeft een broncodelicentie af aan bedrijf B voor een aanpasbaar intern platform en verstrekt die broncode in een tekstbestand. Zelfs indien die broncode vóór gebruik verder moet worden aangepast en gecompileerd door bedrijf B, brengt bedrijf A die broncode in de handel en is zij derhalve onderworpen aan de verordening cyberweerbaarheid. Bedrijf A is niet verantwoordelijk voor de naleving van de verordening cyberweerbaarheid bij de latere aanpassingen en compilatie van die code door bedrijf B.

2.4. **Combinatie van hardware en software die een product met digitale elementen vormen**

25. Of software deel uitmaakt van een product met digitale elementen, moet niet worden bepaald door hoe of wanneer die software aan de gebruiker wordt geleverd, maar door de vraag of de software, in het licht van het beoogde doel en het redelijkerwijs te voorziene gebruik van het product, noodzakelijk is opdat het product met digitale elementen zijn beoogde functies kan vervullen. Wanneer een hardwareproduct met digitale elementen is ontworpen om te werken met specifieke software die door dezelfde fabrikant wordt verstrekt om zijn functies uit te voeren, vormen die hardware en software samen het product met digitale elementen. Software die nodig is om een product met digitale elementen te bedienen, te configureren, te controleren of te gebruiken overeenkomstig het beoogde doel ervan, maakt derhalve deel uit van het product met digitale elementen, zelfs indien deze wordt verkregen via een afzonderlijk kanaal (bv. een appstore, een downloadlink of een ander digitaal kanaal nadat het hardwareproduct met digitale elementen in de handel is gebracht). Het in de handel brengen ervan vindt dus plaats op hetzelfde tijdstip als het in de handel brengen van eenheden van de hardwareproducten met digitale elementen.

Voorbeeld 8: een netwerkprinter wordt in de handel gebracht als hardwareproduct met digitale elementen, terwijl de softwaredrivers die nodig zijn om afdruktaken te verzenden, het apparaat te configureren en de werking ervan te beheren, beschikbaar worden gesteld voor download vanaf de website van de fabrikant. Hoewel de printer en de drivers via verschillende kanalen worden geleverd, vormen zij samen één enkel product met digitale elementen, omdat de printer zonder de drivers niet aan zijn beoogde doel kan voldoen.

Voorbeeld 9: een draagbaar fitnessapparaat ("wearable") wordt in de handel gebracht om de hartslag en activiteit van een gebruiker te meten, terwijl een door de fabrikant verstrekte smartphoneapplicatie nodig is om de metingen en voortgang weer te geven en de configuratie van het apparaat mogelijk te maken. Hoewel de applicatie afzonderlijk wordt gedownload via een appstore, vormen de wearable en de applicatie samen één product met digitale elementen, omdat zij ontworpen en bedoeld zijn om samen de functionaliteit van het product met digitale elementen te leveren.

([8]) Er zij ook aan herinnerd dat artikel 4, lid 3, fabrikanten toestaat onafgewerkte software op de markt aan te bieden die niet aan de verordening voldoet, zoals alfa- of bètaversies of release candidates, op voorwaarde dat de onafgewerkte software niet langer beschikbaar wordt gesteld dan nodig is om deze te testen en feedback te verzamelen.

([9]) Anderzijds moet worden opgemerkt dat computercode zelf voor de toepassing van het productaansprakelijkheidsrecht geen product is en dat fabrikanten die dergelijke code in de handel brengen derhalve niet aansprakelijk kunnen worden gesteld op grond van Richtlijn (EU) 2024/2853 (de richtlijn productaansprakelijkheid). In overweging 13 van die richtlijn staat dat "[i]nformatie [...] echter niet als een product [mag] worden beschouwd en de productaansprakelijkheidsregels [...] daarom niet van toepassing [mogen] zijn op de inhoud van digitale bestanden, zoals mediabestanden of e-boeken of de loutere broncode van software". Dit sluit niet uit dat fabrikanten aansprakelijk kunnen worden gesteld op grond van het nationale recht inzake onrechtmatige daad.

2.5. **Gegevensverbinding**

26. In artikel 2, lid 1, wordt gesteld dat de verordening cyberweerbaarheid van toepassing is op "op de markt aangeboden producten met digitale elementen waarvan het beoogde doel of het redelijkerwijs voorzienbaar gebruik een directe of indirecte logische of fysieke gegevensverbinding met een apparaat of netwerk omvat". Het toepassingsgebied van de verordening cyberweerbaarheid wordt daarom niet bepaald door de loutere aanwezigheid van elektronica, maar door het vermogen van een product met digitale elementen om digitale informatie uit te wisselen.

27. Hoewel de termen "logische verbinding" en "fysieke verbinding" in artikel 3 worden gedefinieerd, geeft de verordening cyberweerbaarheid geen definitie van "gegevensverbinding" of "digitale gegevens". Het is daarom nuttig om een interpretatie te geven van wat een gegevensverbinding is, teneinde de grens van het toepassingsgebied van de verordening cyberweerbaarheid te verduidelijken. Deze grens is met name belangrijk om producten met digitale elementen die louter gebruikmaken van elektrische signalen te onderscheiden van producten die betrokken zijn bij digitale communicatie en daarom worden blootgesteld aan cyberbeveiligingsrisico's.

28. Op het meest basale niveau houdt een gegevensverbinding in dat informatie in binaire vorm wordt doorgegeven, d.w.z. als reeks van nullen (0) en enen (1). Het simpelweg in- en uitschakelen van een output (d.w.z. 0/1) vormt op zich geen gegevensverbinding indien die toestanden niet bedoeld zijn om gegevens weer te geven of niet door een digitale input worden gelezen. Voor het bestaan van een gegevensverbinding moeten de binaire toestanden doelbewust door een bron als informatie worden gecodeerd en op de plaats van bestemming als informatie kunnen worden gedecodeerd. Met andere woorden, er moet een afzender zijn die opzettelijk digitale symbolen genereert volgens een bepaald schema, en een ontvanger die deze symbolen als gegevens kan interpreteren. Wanneer elektrische of elektronische signalen uitsluitend worden gebruikt om een functie te activeren of in te schakelen, zonder digitaal gecodeerde informatie te versturen, bestaat er geen gegevensverbinding voor de doeleinden van het verordening cyberweerbaarheid en valt het product met digitale elementen derhalve niet onder het toepassingsgebied van artikel 2, lid 1.

2.6. **Complexe systemen**

29. Producten met digitale elementen die binnen het toepassingsgebied van de verordening cyberweerbaarheid vallen, bestaan mogelijk niet alleen uit afzonderlijke apparaten of softwarecomponenten, maar kunnen ook uit complexe systemen bestaan, waaronder systemen met meerdere hardware- en softwarecomponenten die samenwerken om een bepaalde functie uit te voeren. Wanneer een dergelijk systeem als één product met digitale elementen in de handel wordt gebracht, vormt het een product met digitale elementen in de zin van de verordening cyberweerbaarheid.

30. Dergelijke complexe systemen worden vaak gekenmerkt door lange ontwerp- en ontwikkelingscycli, met contracten die mogelijk zijn ondertekend voordat de verordening cyberweerbaarheid van toepassing wordt, een lange operationele levensduur en een hoge mate van technische en organisatorische complexiteit. Dergelijke systemen, die in de handel worden gebracht nadat de verordening cyberweerbaarheid in werking is getreden, kunnen afhankelijk zijn van componenten die in de handel zijn gebracht voordat de verordening cyberweerbaarheid in werking is getreden, van gevestigde architecturen of van veelgebruikte interoperabiliteitsnormen, met inbegrip van normen waarnaar wordt verwezen in andere EU-wetgeving of sectorspecifieke kaders. Als gevolg daarvan kan het moeilijk of onevenredig bezwarend zijn om bepaalde technische kenmerken van die systemen te wijzigen zonder afbreuk te doen aan het beoogde doel, de veiligheid, de betrouwbaarheid of de interoperabiliteit met bestaande infrastructuur.

31. Deze kenmerken op zich sluiten complexe systemen niet uit van het toepassingsgebied van de verordening cyberweerbaarheid. Zij illustreren veeleer de toepassing van de risicogebaseerde benadering van de verordening cyberweerbaarheid, die het mogelijk maakt om naleving op verschillende manieren aan te tonen, afhankelijk van de kenmerken en beperkingen van het product met digitale elementen, overeenkomstig artikel 13, lid 3, van de verordening cyberweerbaarheid. Die kenmerken maken deel uit van het beoogde doel en de operationele context ervan en zijn daarom relevant bij de beoordeling van de naleving van de essentiële cyberbeveiligingsvereisten (de "essentiële vereisten"). Met name wordt in overweging 55 uitdrukkelijk erkend dat bepaalde essentiële eisen mogelijk niet volledig verenigbaar zijn met de aard van een product met digitale elementen. Dit kan bijvoorbeeld het geval zijn wanneer naleving verplichte interoperabiliteitsvereisten of de goede werking van het systeem zou ondermijnen.

32. Bijgevolg moeten fabrikanten cyberbeveiligingsrisico's aanpakken op basis van de in artikel 13, lid 2, bedoelde beoordeling van cyberbeveiligingsrisico's. Zoals ook uiteengezet in overweging 55, zijn specifieke essentiële vereisten in sommige gevallen niet van toepassing of kan daaraan niet worden voldaan door de uitvoering van

geavanceerde beveiligingsmaatregelen, bijvoorbeeld vanwege het beoogde doel van het systeem, op grond waarvan het product met digitale elementen moet interageren met bestaande afhankelijkheden of bepaalde interoperabiliteitsvereisten moet volgen. In dergelijke gevallen moeten fabrikanten die specifieke beperkingen identificeren en documenteren, de bijbehorende risico's beoordelen en passende alternatieve of compenserende risicobeperkende maatregelen nemen, zodat de beveiliging van het product met digitale elementen niet wordt ondermijnd. Daartoe spelen zowel de in artikel 31 bedoelde technische documentatie als de in bijlage II bedoelde informatie en instructies voor de gebruiker een sleutelrol bij het transparant beschrijven van de vastgestelde beperkingen, de bijbehorende cyberbeveiligingsrisico's en de uitgevoerde risicobeperkende maatregelen. Overeenkomstig de verplichting om de risicobeoordeling tijdens de ondersteuningsperiode bij te werken, moeten fabrikanten ook periodiek opnieuw beoordelen of dergelijke beperkingen nog steeds bestaan. Indien dergelijke beperkingen na verloop van tijd kunnen worden opgeheven of verminderd, moeten fabrikanten het product met digitale elementen dienovereenkomstig bijwerken, zodat het kan evolueren naar een passend niveau van cyberbeveiliging ([10]).

Voorbeeld 10: een fabrikant brengt een product met digitale elementen in de handel dat communiceert met externe systemen met behulp van een netwerkprotocol. Als onderdeel van de toepassing van de essentiële vereisten bepaalt de fabrikant op basis van de cyberbeveiligingsrisicobeoordeling dat het gebruik van een beveiligd communicatieprotocol noodzakelijk is om de vertrouwelijkheid en integriteit van de door het product met digitale elementen uitgewisselde gegevens te waarborgen.

Het beoogde doel ervan omvat echter interoperabiliteit met bestaande systemen die alleen een ouder of minder beveiligd protocol ondersteunen. In dergelijke gevallen kan de fabrikant dat protocol uitvoeren wanneer dit noodzakelijk is om interoperabiliteit tot stand te brengen, op voorwaarde dat de bijbehorende cyberbeveiligingsrisico's met andere middelen worden geïdentificeerd en beperkt.

Indien het technisch haalbaar is dat het product met digitale elementen zowel het beveiligde protocol als het minder beveiligde protocol ondersteunt, wordt van de fabrikant verwacht dat hij het beveiligde protocol toepast en het standaardgebruik ervan mogelijk maakt. Het minder veilige protocol zou alleen mogen worden toegestaan wanneer dat nodig is voor interoperabiliteit.

Voorbeeld 11: een fabrikant van een systeem voor industriële automatisering koopt een aantal microcontrollers voordat de verordening cyberweerbaarheid van toepassing wordt. De fabrikant voert de cyberbeveiligingsrisicobeoordeling uit voor zijn systeem voor industriële automatisering dat in de handel wordt gebracht nadat de verordening cyberweerbaarheid van toepassing is geworden. Op basis van die cyberbeveiligingsrisicobeoordeling stelt de fabrikant geen specifieke cyberbeveiligingsrisico's vast in verband met het gebruik van een van die microcontrollers. De fabrikant integreert deze in zijn systeem voor industriële automatisering en zorgt ervoor dat het product met digitale elementen als geheel (het systeem voor industriële automatisering) aan de essentiële vereisten voldoet.

2.7. **Producten met digitale elementen die zijn ontworpen voordat de verordening cyberweerbaarheid van toepassing werd**

33. In sommige gevallen zal een fabrikant, nadat de verordening cyberweerbaarheid op 11 december 2027 van toepassing wordt, eenheden van een product met digitale elementen in de handel brengen die zijn vervaardigd overeenkomstig een type of model dat is ontworpen en ontwikkeld vóór de datum van toepassing van de verordening cyberweerbaarheid. In dergelijke gevallen vereist de naleving van deze verordening niet noodzakelijkerwijs dat die eenheden van het product met digitale elementen opnieuw worden ontworpen. De fabrikant moet overeenkomstig artikel 13, lid 2, van de verordening cyberweerbaarheid een beoordeling van de cyberbeveiligingsrisico's uitvoeren om op basis van het beoogde doel en het redelijkerwijs te voorziene gebruik van het product met digitale elementen te bepalen welke van de essentiële vereisten van deel I van bijlage I van toepassing zijn op dat product met digitale elementen, en hoe die vereisten worden uitgevoerd.

34. Wanneer uit die risicobeoordeling blijkt dat het product met digitale elementen reeds passende en doeltreffende beveiligingsmaatregelen omvat om de relevante risico's aan te pakken, kan de fabrikant zich op die bestaande maatregelen baseren om de naleving van de verordening cyberweerbaarheid aan te tonen. De verordening cyberweerbaarheid legt op zich geen verplichting op om nieuwe beveiligingskenmerken in te voeren of het product met digitale elementen opnieuw te ontwerpen wanneer dit niet nodig is om de vastgestelde risico's aan te pakken.

([10]) Er zij op gewezen dat de overwegingen in dit lid in voorkomend geval van toepassing kunnen zijn op alle producten met digitale elementen die onder het toepassingsgebied van de verordening cyberweerbaarheid vallen, en niet alleen op "complexe systemen".

35. Niettemin blijft de fabrikant onderworpen aan de verplichtingen van de verordening cyberweerbaarheid. Deze omvatten waarborgen, voordat het product met digitale elementen in de handel wordt gebracht, dat de toepasselijke conformiteitsbeoordelingsprocedure is uitgevoerd, de EU-conformiteitsverklaring is opgesteld en de CE-markering is aangebracht. De naleving van die vereisten staat los van de vraag of het ontwerp van het product met digitale elementen als gevolg van de risicobeoordeling zou moeten worden gewijzigd. Voor producten met digitale elementen die vóór de datum van toepassing van de verordening cyberweerbaarheid zijn ontworpen, maar na die datum in de handel zijn gebracht, moet, wanneer de fabrikant niet kan aantonen hoe tijdens de ontwerp- en ontwikkelingsfase van het product met digitale elementen rekening is gehouden met de risicobeoordeling, de verplichting van artikel 13, lid 2, worden opgevat als een verplichting voor fabrikanten om een cyberbeveiligingsrisicobeoordeling uit te voeren en op basis daarvan aan te tonen dat het product met digitale elementen passende beveiligingsmaatregelen omvat om cyberbeveiligingsrisico's tot een minimum te beperken, incidenten te voorkomen en de gevolgen ervan tot een minimum te beperken, onder meer met betrekking tot de gezondheid en veiligheid van gebruikers.

36. Bijgevolg kunnen producten met digitale elementen die zijn ontworpen voordat de verordening cyberweerbaarheid van toepassing werd, in het kader van de verordening cyberweerbaarheid zonder hernieuwd ontwerp in de handel worden gebracht, mits de fabrikant aan de hand van de cyberbeveiligingsrisicobeoordeling en de technische documentatie kan aantonen dat het product met digitale elementen een passend cyberbeveiligingsniveau bereikt in het licht van het beoogde doel en het redelijkerwijs voorzienbare gebruik ervan en voldoet aan de essentiële vereisten op het gebied van cyberbeveiliging.

37. Voorts is het nuttig de toepassing van conformiteitsbeoordelingsverplichtingen te verduidelijken voor fabrikanten van producten met digitale elementen die in de handel worden gebracht ná de datum van toepassing van de verordening cyberweerbaarheid, maar die zijn vervaardigd overeenkomstig een type of model dat vóór die datum is ontworpen en ontwikkeld. Overeenkomstig artikel 13, lid 12, moet de fabrikant via de desbetreffende conformiteitsbeoordelingsprocedure aantonen dat zijn product met digitale elementen in overeenstemming is met de toepasselijke essentiële vereisten en daartoe bewijsmateriaal opnemen in de technische documentatie van het product (punt 6 van bijlage VII).

38. De toepassing van dergelijke vereisten moet echter worden geïnterpreteerd in het licht van de cyberbeveiligingsrisicobeoordeling en het cyberbeveiligingsrisicoprofiel van het product met digitale elementen. Met name in het geval van producten met digitale elementen die vóór de datum van toepassing van de verordening cyberweerbaarheid zijn ontworpen (maar ná die datum in de handel zijn gebracht) en onderworpen zijn aan de conformiteitsbeoordelingsprocedures van artikel 32, lid 1, mag, indien uit de risicobeoordeling blijkt dat het product met digitale elementen reeds passende en doeltreffende beveiligingsmaatregelen omvat om de risico's van dat product aan te pakken, de verplichting om in het kader van de conformiteitsbeoordelingsprocedure bewijsmateriaal te verstrekken niet worden opgevat als een verplichting voor de fabrikant om testresultaten te verstrekken met betrekking tot de oorspronkelijke ontwerp- en ontwikkelingsfasen van dergelijke producten met digitale elementen. Dit zou niet nodig zijn, aangezien het niet zou bijdragen tot het vergroten van de beveiliging van het product met digitale elementen zelf. Wanneer tests niettemin nodig zouden zijn, wordt van fabrikanten niet verwacht dat zij bewijs leveren van tests die op alle productvarianten zijn uitgevoerd, maar kunnen zij dergelijke tests groeperen per familie van producten met digitale elementen, zoals nader wordt besproken in punt 7.4, "Hergebruik van risicobeoordelingen en conformiteitsdocumentatie voor families van producten met digitale elementen".

39. Niettemin moet de fabrikant aantonen hoe hij voldoet aan de procedures inzake de respons op kwetsbaarheden van deel II van bijlage I, moet hij zijn risicobeoordeling actueel houden overeenkomstig artikel 13, lid 3, en moet hij voldoen aan alle andere verplichtingen van de verordening cyberweerbaarheid, onder meer door gebruikers informatie en instructies te verstrekken overeenkomstig artikel 13, lid 18.

Voorbeeld 12: een fabrikant brengt een microcontroller in de handel die vóór de datum van toepassing van de verordening cyberweerbaarheid is ontworpen en ontwikkeld. De microcontroller is bedoeld om te worden geïntegreerd in een reeks elektronische producten met digitale elementen, waaronder producten met digitale elementen met connectiviteitsfuncties.

Alvorens nieuwe eenheden van de microcontroller in de handel te brengen nadat de verordening cyberweerbaarheid van toepassing is geworden, voert de fabrikant een cyberbeveiligingsrisicobeoordeling uit overeenkomstig artikel 13, lid 2. Op basis van het beoogde doel van de microcontroller en het redelijkerwijs te voorziene gebruik ervan stelt de fabrikant relevante cyberbeveiligingsrisico's vast, zoals ongeoorloofde toegang, manipulatie van software of gegevens en misbruik van beschikbare interfaces.

Uit de resultaten van de risicobeoordeling blijkt dat de microcontroller, zoals oorspronkelijk ontworpen, reeds passende en doeltreffende beveiligingsmaatregelen omvat om de vastgestelde risico's aan te pakken. De fabrikant concludeert derhalve dat het product met digitale elementen voldoet aan de toepasselijke essentiële vereisten van deel I van bijlage I en dat het niet nodig is de beveiligingsfuncties opnieuw te ontwerpen of in te voeren.

Wanneer niet kan worden aangetoond hoe tijdens de oorspronkelijke ontwerp- en ontwikkelingsfase rekening is gehouden met een cyberbeveiligingsrisicobeoordeling, documenteert de fabrikant een actuele cyberbeveiligingsrisicobeoordeling en licht hij toe hoe het bestaande ontwerp en de bestaande maatregelen de vastgestelde risico's beperken. De fabrikant is niet verplicht het opstellen van historische ontwerp- of testdocumentatie te herhalen, aangezien dit niet zou bijdragen tot een betere cyberbeveiliging van het product met digitale elementen. Indien verschillende varianten van de microcontroller gebaseerd zijn op hetzelfde ontwerp en hetzelfde cyberbeveiligingsrisicoprofiel hebben, kan de fabrikant zich ook baseren op representatief bewijsmateriaal voor de relevante productfamilie.

De fabrikant waarborgt ook de naleving van de vereisten inzake de respons op kwetsbaarheden van deel II van bijlage I, onder meer door processen in stand te houden om kwetsbaarheden aan te pakken en te verhelpen en door de beoordeling van cyberbeveiligingsrisico's te evalueren overeenkomstig artikel 13, lid 3.

In deze omstandigheden mag de microcontroller die vóór de datum van toepassing van de verordening cyberweerbaarheid is ontworpen, zonder hernieuwd ontwerp in de handel worden gebracht, mits de fabrikant aan de hand van de beoordeling van de cyberbeveiligingsrisico's en de technische documentatie kan aantonen dat hij een passend cyberbeveiligingsniveau bereikt in het licht van het beoogde doel en het redelijkerwijs voorzienbare gebruik ervan en voldoet aan de toepasselijke essentiële vereisten.

3. **VRIJE EN OPENSOURCESOFTWARE**

40. Zoals in punt *2.1*, "In de handel brengen", in herinnering is gebracht, is de verordening cyberweerbaarheid van toepassing op producten met digitale elementen die in het kader van een handelsactiviteit voor het eerst op de EU-markt worden aangeboden (d.w.z. "in de handel worden gebracht"), alsook op alle daaropvolgende gevallen waarin hetzelfde product met digitale elementen op de markt wordt aangeboden. In de Blauwe Gids (punt 2.2) wordt verduidelijkt dat onder "handelsactiviteit" moet worden verstaan het leveren van goederen, al dan niet tegen betaling, in een bedrijfsgerelateerde context en dat dit alleen per geval kan worden beoordeeld, rekening houdend met de regelmaat van de leveringen, de kenmerken van het product, de intenties van de leverancier enz.

41. Levering in het kader van een handelsactiviteit wordt gekenmerkt door een reeks omstandigheden, die uitvoerig worden gedocumenteerd in de Blauwe Gids en in herinnering worden gebracht in overweging 15 van de verordening cyberweerbaarheid. Daarbij kan het onder meer gaan om het rechtstreeks in rekening brengen van een prijs, "maar ook door het in rekening brengen van een prijs voor technische ondersteuningsdiensten indien die prijs niet alleen dient om de gemaakte kosten te dekken, door een intentie van tegeldemaking, bijvoorbeeld door het aanbieden van een softwareplatform waarmee de fabrikant andere diensten te gelde maakt, door als voorwaarde voor gebruik de verwerking van persoonsgegevens te eisen voor andere redenen dan uitsluitend de verbetering van de beveiliging, compatibiliteit of interoperabiliteit van de software, of door donaties te accepteren die de kosten van het ontwerp, de ontwikkeling en de levering van een product met digitale elementen overstijgen" (overweging 15) ([11]).

42. De verordening cyberweerbaarheid erkent echter de specifieke kenmerken van de verschillende manieren waarop "vrije en opensourcesoftware" (FOSS) wordt ontwikkeld en gepubliceerd en biedt enkele richtsnoeren om te helpen vaststellen of FOSS een product met digitale elementen is dat in de handel wordt gebracht (d.w.z. in het kader van een handelsactiviteit) in de zin van de verordening cyberweerbaarheid. Dit wordt in overweging 18 toegelicht: "Bij het bepalen van het handels- of niet-handelskarakter van die activiteit mag derhalve geen rekening worden gehouden met de loutere omstandigheden waaronder het product met digitale elementen is ontwikkeld of met de wijze waarop de ontwikkeling ervan is gefinancierd. Meer in het bijzonder mag voor de toepassing van deze verordening en voor de marktdeelnemers die onder deze verordening vallen, om een duidelijk onderscheid te maken tussen de ontwikkelings- en leveringsfase, de levering van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en die niet door de fabrikanten te gelde worden gemaakt, niet als een handelsactiviteit worden beschouwd."

([11]) Er zij ook aan herinnerd dat, hoewel producten met digitale elementen vaak (ook) via de verwerking van persoonsgegevens te gelde worden gemaakt, de bescherming van persoonsgegevens een grondrecht is en dat persoonsgegevens daarom niet als een goed kunnen worden beschouwd, zoals aangegeven in overweging 24 van Richtlijn 2019/770 van het Europees Parlement en de Raad van 20 mei 2019 betreffende bepaalde aspecten van overeenkomsten voor de levering van digitale inhoud en digitale diensten (PB L 136 van 22.5.2019, blz. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Daarom is het nuttig i) te verduidelijken wat FOSS is; ii) te bepalen wanneer deze geacht wordt onder de verantwoordelijkheid van een natuurlijke of rechtspersoon te vallen, en iii) voorbeelden te geven om belanghebbenden te helpen begrijpen wanneer de distributie van FOSS wordt gezien als "in de handel brengen". Wanneer FOSS niet in de handel wordt gebracht, valt deze buiten het toepassingsgebied van de verordening cyberweerbaarheid, tenzij de entiteit die deze uitgeeft een rechtspersoon is die voldoet aan de definitie van "opensourcesoftwaresteward" (hierna "steward" genoemd) uit hoofde van artikel 3, punt 14). In dat geval gelden enkel de verplichtingen van artikel 24.

44. In artikel 3, punt 48), wordt vrije en opensourcesoftware gedefinieerd als "software waarvan de broncode openlijk wordt gedeeld en die beschikbaar wordt gesteld onder een vrije en opensourcelicentie die voorziet in alle rechten om die vrij toegankelijk, bruikbaar, wijzigbaar en herdistr[ib]ueerbaar te maken". Hoewel in deze richtsnoeren geen specifieke vrije en opensourcelicenties worden genoemd die verenigbaar zijn met de definitie van artikel 3, punt 48), volgt uit de formulering van die bepaling dat alleen software die cumulatief aan beide voorwaarden voldoet, voor de toepassing van de verordening cyberweerbaarheid als FOSS kan worden aangemerkt: i) de software moet beschikbaar worden gesteld onder een vrije en opensourcelicentie die voorziet in alle rechten als bedoeld in artikel 3, punt 48) en ii) de broncode ervan moet openlijk worden gedeeld.

45. Het vereiste dat de licentie bepaalt dat de software "vrij toegankelijk, bruikbaar, wijzigbaar en herdistr[ib]ueerbaar" moet zijn, weerspiegelt de traditionele opvatting van FOSS, namelijk dat gebruikers toegang moeten hebben tot de broncode, deze zonder onnodige beperkingen moeten kunnen gebruiken, deze moeten kunnen wijzigen en originele of gewijzigde versies moeten kunnen herdistribueren. Toegang tot de broncode is derhalve een noodzakelijke voorwaarde voor de uitoefening van de andere rechten: zonder toegang tot de broncode is het praktisch niet mogelijk de software te wijzigen of op zinvolle wijze te hergebruiken.

46. Artikel 3, punt 48), gaat echter verder dan alleen te verwijzen naar de licentievoorwaarden, aangezien het artikel uitdrukkelijk het vereiste bevat dat de broncode "openlijk wordt gedeeld". Het begrip "openlijk […] gedeeld" geeft aan dat de broncode openbaar moet worden gemaakt ("upstream" of "downstream"), en niet louter op beperkte of voorwaardelijke basis wordt verstrekt. Bijgevolg mag software die onder een vrije en opensourcelicentie wordt gedistribueerd, maar waarvan de broncode alleen wordt gedeeld (of mag worden gedeeld) met betalende klanten of een beperkte groep gebruikers, niet worden beschouwd als FOSS in de zin van artikel 3, punt 48). Voor de toepassing van de verordening cyberweerbaarheid mag daarom alleen software waarvan de broncode openbaar beschikbaar is en die in licentie is gegeven op grond van een vrije en opensourcelicentie die voorziet in alle rechten als bedoeld in artikel 3, punt 48), als FOSS worden aangemerkt.

3.1. **Bepalen of vrije en opensourcesoftware onder iemands verantwoordelijkheid valt**

47. In de verordening cyberweerbaarheid worden belangrijke verantwoordelijkheden opgelegd aan marktdeelnemers die producten met digitale elementen op de EU-markt leveren. In de verordening wordt de fabrikant gedefinieerd als de natuurlijke of rechtspersoon die onder zijn naam of merk producten met digitale elementen levert, en dat doet in het kader van een handelsactiviteit (waardoor het product in de handel wordt gebracht). Evenzo is een importeur de in de Unie gevestigde natuurlijke of rechtspersoon die een product met digitale elementen levert van een persoon die buiten de EU is gevestigd, en dat doet in het kader van een handelsactiviteit (waardoor het product in de handel wordt gebracht). De verplichtingen van stewards gelden voor de rechtspersoon die FOSS levert die bestemd is voor handelsactiviteiten ([12]), maar deze niet in de handel brengt in de zin van de verordening cyberweerbaarheid.

48. Om te bepalen of een natuurlijke of rechtspersoon FOSS in de EU in de handel brengt, moet daarom eerst worden verduidelijkt of die natuurlijke of rechtspersoon de FOSS daadwerkelijk levert. Om de toepasselijke verplichtingen uit hoofde van de verordening cyberweerbaarheid correct vast te stellen, is het van essentieel belang om te bepalen of de natuurlijke of rechtspersoon inderdaad de handeling van het leveren van FOSS verricht. Zoals in overweging 18 in herinnering is gebracht, is de verordening cyberweerbaarheid in feite niet van toepassing op natuurlijke of rechtspersonen die met broncode bijdragen aan producten met digitale elementen die als FOSS worden aangemerkt en niet onder hun verantwoordelijkheid vallen.

([12]) Dit is een noodzakelijke, maar niet voldoende voorwaarde voor een rechtspersoon om als opensourcesoftwaresteward te worden aangemerkt, aangezien de definitie van artikel 3, punt 14), aanvullende voorwaarden bevat waaraan een rechtspersoon moet voldoen om als steward te worden aangemerkt.

49. Gezien de specifieke kenmerken van de ontwikkeling van FOSS, waar vaak meerdere contribuanten bij betrokken zijn, waarbij sprake is van modellen voor gedecentraliseerde samenwerking en het leveren van een bijdrage en deelnemen aan de besluitvorming gescheiden processen zijn, is het nuttig te verduidelijken dat FOSS wordt geacht "onder de verantwoordelijkheid" te vallen van natuurlijke of rechtspersonen die de FOSS publiceren en primaire controle uitoefenen over de beslissingen met betrekking tot de ontwikkeling, release en distributie ervan (vaak "onderhouder" genoemd). Personen die met broncodes een bijdrage leveren, maar die geen controle hebben over releases, routekaarten of bestuursbesluiten, worden als "contribuanten" beschouwd; in dergelijke gevallen valt de FOSS niet onder hun verantwoordelijkheid, ook al hebben zij er met code aan bijgedragen. Het loutere bestaan van technische toestemmingen, zoals het verlenen van toegang, volstaat niet om aan te tonen dat de FOSS onder de verantwoordelijkheid van die persoon valt; de verantwoordelijkheid ligt bij degenen die de FOSS publiceren en controleren.

Voorbeeld 13: een individuele ontwikkelaar of een werknemer van een bedrijf dient een "pull"- of "merge"-verzoek met een beveiligingspatch of een nieuwe functie in bij een FOSS-project. De onderhouders van het project beoordelen de code, aanvaarden deze en voegen deze samen in het hoofdregister, waarna deze in een nieuwe release wordt opgenomen. In dit scenario is de persoon die het pull-verzoek heeft ingediend een "contribuant" en niet onderworpen aan de verordening cyberweerbaarheid. Hoewel deze persoon met broncode heeft bijgedragen, oefent deze geen primaire zeggenschap uit over de beslissingen inzake ontwikkeling, release of distributie.

3.2. **Bepalen of vrije en opensourcesoftware in de EU in de handel wordt gebracht**

50. Zodra is vastgesteld dat FOSS onder de verantwoordelijkheid van een natuurlijke of rechtspersoon valt, moet worden vastgesteld of die persoon de FOSS in het kader van een handelsactiviteit levert, wat dus "in de handel brengen" vormt.

3.2.1. *Een prijs in rekening brengen*

51. Wanneer de natuurlijke of rechtspersoon die FOSS levert een prijs aanrekent voor de software zelf (bv. door een prijs aan te rekenen voor de vooraf gecompileerde binaries), brengt die persoon een product met digitale elementen in de handel. De persoon die FOSS in de handel brengt, is derhalve een fabrikant in het kader van de verordening cyberweerbaarheid.

52. Vaak leveren fabrikanten van FOSS gratis versies van die software (vaak "community"-versies genoemd), waarvan de codebase (bijna) identiek is aan de betaalde versie. Die producten met digitale elementen zijn echter verschillende producten: de betaalde versie wordt op een of andere manier te gelde gemaakt (bv. door een prijs in rekening te brengen of via andere middelen zoals besproken in dit punt) en wordt daarom geacht in de handel te zijn gebracht, waardoor de verplichtingen van de fabrikant in werking treden. De gratis versie (of community-versie) wordt niet te gelde gemaakt en wordt daarom niet beschouwd als in de handel gebracht voor de toepassing van de verordening cyberweerbaarheid. Dit is ook het geval wanneer de betaalde versie een "verbeterde" commerciële versie is, die de codebase van de gratis verstrekte versie uitbreidt of die versie integreert in een breder product met digitale elementen (bv. zoals in het geval van het "open core"-model).

53. Indien de persoon die de community-versie levert een rechtspersoon is, is die rechtspersoon ook onderworpen aan de verplichtingen van stewards voor de versie die hij gratis levert (de community-versie). Indien de entiteit een natuurlijke persoon is, valt de gratis verstrekte versie (de community-versie) niet binnen het toepassingsgebied van de verordening cyberweerbaarheid.

3.2.2. *Tegeldemaking van andere diensten of diensten waarvoor persoonsgegevens moeten worden verwerkt*

54. Een natuurlijke of rechtspersoon die FOSS publiceert, kan deze ook in de handel brengen (d.w.z. leveren in het kader van een handelsactiviteit) wanneer hij de software verstrekt waarmee hij andere producten met digitale elementen of diensten te gelde maakt, of wanneer hij als voorwaarde voor het gebruik de verwerking van persoonsgegevens vereist om andere redenen dan uitsluitend om de beveiliging, compatibiliteit of interoperabiliteit van de software te verbeteren.

Voorbeeld 14: een natuurlijke of rechtspersoon publiceert een vrije en opensourcemarktplaatsapplicatie. De applicatie is gratis beschikbaar en stelt gebruikers in staat via deze applicatie goederen of diensten te kopen. De app stelt de persoon die de app heeft gepubliceerd in staat andere producten met digitale elementen en diensten die via de app worden aangeboden, te gelde te maken (bv. via advertenties, commissie of abonnementskosten). Daarom wordt de applicatie geacht in het kader van een handelsactiviteit in de handel te zijn gebracht.

Voorbeeld 15: een natuurlijke of rechtspersoon publiceert een vrije en opensource-VPN. De applicatie is gratis beschikbaar, maar biedt gebruikers de mogelijkheid te betalen om toegang te krijgen tot extra servers of speciale IP-adressen. Die applicatie stelt die persoon in staat om andere via die applicatie aangeboden diensten te gelde te maken, zodat die applicatie wordt geacht in het kader van een handelsactiviteit in de handel te zijn gebracht.

Voorbeeld 16: een natuurlijke of rechtspersoon publiceert een vrije en opensource-applicatie voor fitness tracking. De applicatie is gratis beschikbaar, maar het gebruik ervan is afhankelijk van de verwerking van persoonsgegevens van gebruikers voor doeleinden zoals gerichte reclame of analyse die geen verband houdt met de beveiliging, compatibiliteit of interoperabiliteit van de software. Door een dergelijke gegevensverwerking als voorwaarde voor het gebruik te stellen, wordt de applicatie dus geacht in het kader van een handelsactiviteit in de handel te zijn gebracht.

3.2.3. *Ondersteunende diensten*

55. Het enkele feit dat een natuurlijke of rechtspersoon die FOSS publiceert, ook betaalde ondersteunende diensten aanbiedt die daarmee verband houden, betekent als zodanig niet dat het product met digitale elementen wordt geleverd in het kader van een handelsactiviteit. Ondersteunende diensten kunnen activiteiten omvatten zoals consultancy, opleiding of professionele diensten in verband met het gebruik, de documentatie, de configuratie en de inzet van de software door een klant.

56. Doorslaggevend is of de toegang tot de FOSS zelf (d.w.z. de levering van het product met digitale elementen), met inbegrip van het onderhoud ervan, afhankelijk is van een vergoeding, in plaats van louter het aanbieden van professionele diensten rond een vrij beschikbaar product met digitale elementen, zoals aangegeven in overweging 18 van de verordening cyberweerbaarheid ("de levering van producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en die niet door de fabrikanten te gelde worden gemaakt, [mag] niet als een handelsactiviteit worden beschouwd"). Wanneer de FOSS vrij kan worden gedownload en geïnstalleerd en gebruikers er facultatief voor kunnen kiezen om professionele diensten afzonderlijk aan te schaffen, wordt die FOSS niet geacht in de handel te zijn gebracht.

57. In sommige gevallen is voor de toegang tot een specifieke versie van het product met digitale elementen, met inbegrip van bepaalde voordelen zoals technische bijstand of optimalisering van de prestaties, daarentegen wel een vergoeding verschuldigd. In dergelijke gevallen vormt deze bepaling een te gelde gemaakte levering van een product met digitale elementen dat in het kader van een handelsactiviteit wordt geleverd, en wordt het product derhalve geacht in de handel te zijn gebracht. Dit omvat gevallen waarin een betaalde editie of "enterprise"-versie op de markt wordt aangeboden in het kader van een commerciële overeenkomst, ongeacht of functioneel gelijkwaardige software ook gratis beschikbaar is onder een vrije en opensourcelicentie.

Voorbeeld 17: een natuurlijke of rechtspersoon publiceert een vrij en opensourcebesturingssysteem dat een betaalde versie van dat besturingssysteem aanbiedt die ondersteunende diensten omvat, zoals technische bijstand of optimalisering van de prestaties. De betaalde versie van het besturingssysteem wordt geacht in het kader van een handelsactiviteit in de handel te zijn gebracht.

Voorbeeld 18: een natuurlijke of rechtspersoon publiceert een vrij en opensource-opdrachtregelinstrument. Het instrument is vrij toegankelijk en iedereen kan het downloaden en installeren. Die natuurlijke of rechtspersoon biedt afzonderlijk professionele diensten aan, zoals facultatieve adviesdiensten om gebruikers op te leiden en te ondersteunen bij de installatie en het gebruik van het instrument. Die FOSS wordt niet beschouwd als in de handel gebracht in de zin van de verordening cyberweerbaarheid.

58. Met name in het geval van natuurlijke personen die FOSS publiceren, zou het aanbieden van technische bijstand die rechtstreeks gebundeld wordt met toegang tot het product met digitale elementen nog steeds niet als een handelsactiviteit kunnen worden aangemerkt indien, zoals aangegeven in overweging 15 van de verordening cyberweerbaarheid, de in rekening gebrachte prijs alleen dient om de gemaakte kosten te dekken. Dergelijke gemaakte kosten omvatten verschillende kosten in verband met het ontwerp, de ontwikkeling en het onderhoud van die software, met inbegrip van de redelijke kosten van levensonderhoud van de persoon. Een natuurlijke persoon die FOSS publiceert en technische bijstand verleent om zijn kosten te dekken en een billijke vergoeding te verkrijgen, mag dus niet louter op die basis worden geacht die software in de Unie in de handel te brengen.

59. Een natuurlijke of rechtspersoon die technische bijstand aanbiedt in verband met FOSS die niet onder zijn verantwoordelijkheid valt, wordt niet geacht die software in de handel te brengen, tenzij die persoon de FOSS overeenkomstig artikel 22 ingrijpend wijzigt in het kader van de verlening van die bijstand.

Voorbeeld 19: een dienstverlener publiceert geen FOSS, maar helpt een klant deze op zijn eigen server te installeren. De dienstverlener doet dit zonder een ingrijpende wijziging van die FOSS door te voeren. De dienstverlener wordt derhalve niet geacht de FOSS in de handel te brengen.

3.2.4. *Donaties*

60. Natuurlijke of rechtspersonen die FOSS-projecten publiceren, vermelden regelmatig hoe gebruikers van die software vrijwillig geld kunnen doneren om de uitgever(s) van het project te bedanken en ook om ervoor te zorgen dat het project actief wordt onderhouden.

61. Zoals aangegeven in overweging 15 van de verordening cyberweerbaarheid mag "[h]et aanvaarden van schenkingen zonder winstoogmerk […] niet worden beschouwd als een handelsactiviteit". Het louter opnemen van een link naar een donatieplatform of soortgelijke instrumenten voor het inzamelen van donaties mag niet worden beschouwd als winstoogmerk, zelfs niet wanneer het via donaties geïnde bedrag hoger is dan de kosten in verband met het ontwerp, de ontwikkeling en de levering van een product met digitale elementen. Het bedrag omvat een redelijke vergoeding voor de contribuanten die door een rechtspersoon worden ingeschakeld en/of de redelijke kosten van levensonderhoud van een natuurlijke persoon. Donaties fluctueren naar hun aard in de loop van de tijd, en daarom moet een zekere mate van flexibiliteit worden toegepast bij de beoordeling of FOSS die uitsluitend via donaties in geld wordt uitgedrukt, wordt geacht in de handel te zijn gebracht. FOSS die alleen met donaties wordt ondersteund, zal daarom waarschijnlijk niet worden beschouwd als in de handel gebracht in de zin van de verordening cyberweerbaarheid.

Voorbeeld 20: een natuurlijke of rechtspersoon publiceert een FOSS-instrument in een openbaar onlineregister, zodat iedereen het kan downloaden, gebruiken, wijzigen en opnieuw distribueren onder een vrije en opensourcelicentie. De uitgever nodigt gebruikers uit om via een donatieplatform vrijwillig een donatie te doen om de verdere ontwikkeling en het onderhoud van het project te ondersteunen. De toegang tot de software, de broncode en de updates ervan is niet afhankelijk van het doen van een donatie. Die FOSS wordt niet geacht te zijn geleverd in het kader van een handelsactiviteit en wordt niet geacht in de handel te zijn gebracht in de zin van de verordening cyberweerbaarheid.

62. Niettemin zijn er gevallen waarin FOSS die met donaties wordt ondersteund, kan worden geacht in de handel te zijn gebracht. Dit is het geval wanneer, op basis van een algemene beoordeling van de omstandigheden, de donaties feitelijk gelijkwaardig zijn aan het in rekening brengen van een prijs om toegang te krijgen tot het product met digitale elementen of bepaalde functionaliteiten ervan. Dit kan met name het geval zijn wanneer de toegang tot de FOSS, tot essentiële functies of tot updates in de praktijk afhankelijk wordt gesteld van het doen van een donatie, of wanneer donaties gepaard gaan met contractuele voordelen of exclusieve voordelen die verder gaan dan "community"-voordelen (voor de gemeenschap).

Voorbeeld 21: een natuurlijke of rechtspersoon publiceert een softwareproduct met digitale elementen onder een vrije en opensourcelicentie, maar verstrekt alleen downloadbare releases en beveiligingsupdates aan gebruikers die een donatie doen. Gebruikers die geen donatie doen, hebben geen toegang tot de meest recente versie van de software.

In dit geval zijn de donaties feitelijk een voorwaarde voor toegang tot het product met digitale elementen en komen zij dus neer op het in rekening brengen van een prijs. Deze FOSS wordt derhalve geacht in de handel te zijn gebracht in de zin van de verordening cyberweerbaarheid.

Voorbeeld 22: een natuurlijke of rechtspersoon maakt de broncode van FOSS openbaar, maar maakt vooraf gecompileerde binaries, regelmatige updates en gegarandeerde beveiligingsoplossingen alleen beschikbaar voor donoren. In dit geval houden de donaties verband met de toegang tot essentiële aspecten van het product met digitale elementen en vormen zij een vergoeding voor de levering van dat product. Deze FOSS wordt derhalve geacht in het kader van een handelsactiviteit in de handel te zijn gebracht.

3.2.5. *Financiering van vrije en opensourcesoftware*

63. Het enkele feit dat een derde de ontwikkeling van FOSS heeft betaald, gesponsord of anderszins heeft gefinancierd, is op zich niet bepalend voor de vraag of die FOSS in de handel wordt gebracht. In het FOSS-ecosysteem is het gebruikelijk dat individuele ontwikkelaars, stichtingen of "communities" (gemeenschappen) financiering ontvangen van bedrijven, overheidsinstanties of andere sponsoren om aan specifieke functionaliteiten te werken, bugs te verhelpen of kritieke componenten te onderhouden. Deze financiering kan vele vormen aannemen, waaronder subsidies, "bug bounties" (beloning voor het opsporen van bugs), sponsoring, dienstencontracten of betaald ontwikkelingswerk.

64. Zoals al is aangegeven, wordt in artikel 18 van de verordening cyberweerbaarheid verduidelijkt dat bij het bepalen van het handels- of niet-handelskarakter van die activiteit geen rekening mag worden gehouden met de loutere omstandigheden waaronder het product met digitale elementen is ontwikkeld of met de wijze waarop de ontwikkeling ervan is gefinancierd.

65. Wanneer de FOSS openlijk wordt gedeeld en voor iedereen vrij beschikbaar wordt gesteld voor toegang, gebruik, wijziging en herdistributie, zou het feit dat een commerciële entiteit mogelijk voor dat project heeft betaald, geen factor zijn bij de vaststelling of de software in de handel wordt gebracht. Als die FOSS niet anderszins te gelde wordt gemaakt, mag deze niet worden beschouwd als in de handel gebracht. Wanneer het bedrijf dat de ontwikkeling van de FOSS heeft gefinancierd (en elk ander bedrijf) deze integreert in zijn product met digitale elementen, moet dat bedrijf passende zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5, van de verordening cyberweerbaarheid.

Voorbeeld 23: een individuele ontwikkelaar publiceert een FOSS-project en onderhoudt het actief. Fabrikant A verzoekt de individuele ontwikkelaar een specifieke functie voor die FOSS toe te voegen en financiert die ontwikkeling. De ontwikkelaar voegt de functie toe aan de FOSS-codebase, deelt deze functie openlijk en stelt haar vrij beschikbaar zodat iedereen er toegang toe heeft en de functie kan gebruiken, wijzigen en herdistribueren. De individuele ontwikkelaar wordt niet geacht die FOSS in de handel te hebben gebracht. Indien de fabrikant de FOSS integreert in zijn product met digitale elementen, moet hij passende zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5.

3.2.6. *Entiteiten zonder winstoogmerk die zijn opgericht om doelstellingen zonder winstoogmerk te verwezenlijken*

66. Wanneer een rechtspersoon die FOSS publiceert, een organisatie zonder winstoogmerk is die "zodanig is opgezet dat alle inkomsten na aftrek van kosten worden aangewend om doelstellingen zonder winstoogmerk te verwezenlijken" (overweging 18 van de verordening cyberweerbaarheid), wordt de FOSS die hij publiceert niet geacht in de handel te zijn gebracht. Wanneer die rechtspersoon voldoet aan de definitie van "steward", is hij onderworpen aan de overeenkomstige verplichtingen (artikel 24 van de verordening cyberweerbaarheid).

Voorbeeld 24: een rechtspersoon publiceert een vrije en opensourcebrowser die rechtstreeks te gelde wordt gemaakt via partnerschappen met zoekmachines, maar al zijn inkomsten na het betalen van de kosten worden gebruikt voor doelstellingen zonder winstoogmerk. De browser wordt niet beschouwd als in de handel gebracht in de zin van de verordening cyberweerbaarheid. De rechtspersoon die hem publiceert, is onderworpen aan de verplichtingen die van toepassing zijn op stewards.

3.2.7. *Integratie door andere fabrikanten*

67. In sommige gevallen wordt FOSS gepubliceerd door een duidelijk identificeerbare natuurlijke of rechtspersoon, maar die FOSS is "bestemd […] om door andere fabrikanten in hun eigen producten met digitale elementen te worden verwerkt". In dergelijke gevallen wordt die FOSS niet geacht in de EU in de handel te zijn gebracht, tenzij hij ook te gelde wordt gemaakt door de persoon die hem publiceert (d.w.z. de oorspronkelijke fabrikant), in overeenstemming met de vorige punten van deze richtsnoeren.

68. Wanneer die FOSS niet in de handel wordt gebracht, zou de rechtspersoon die deze uitgeeft, onderworpen zijn aan de verplichtingen van stewards, indien hij duurzaam steun verleent, in overeenstemming met de definitie van "steward".

Voorbeeld 25: een rechtspersoon publiceert een FOSS-bibliotheek voor gebruikersinterfaces van gebouwen. Hij maakt de levering van die bibliotheek niet te gelde, maar integreert deze in een van zijn producten met digitale elementen (die op zijn beurt in de handel wordt gebracht). De bibliotheek wordt niet beschouwd als in de handel gebracht in de zin van de verordening cyberweerbaarheid, maar is bestemd om te worden geïntegreerd in producten met digitale elementen. De rechtspersoon die de bibliotheek publiceert, is de steward ervan.

Voorbeeld 26: een rechtspersoon brengt een besturingssysteem op de markt en publiceert ook FOSS-bibliotheken als referentie-implementaties voor gebruikers van dat besturingssysteem. De rechtspersoon maakt de FOSS-bibliotheken, die bestemd zijn om te worden geïntegreerd in andere producten met digitale elementen, niet te gelde. De rechtspersoon die ze publiceert, is een steward van die FOSS-bibliotheken.

3.3. **Opensourcesoftwarestewards**

69. De verordening cyberweerbaarheid introduceert de nieuwe juridische categorie "opensourcesoftwaresteward" in het licht van "het belang voor cyberbeveiliging bij veel producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en die worden gepubliceerd, maar niet op de markt worden aangeboden in de zin van [de verordening cyberweerbaarheid]" (overweging 19 van de verordening cyberweerbaarheid).

70. In sommige gevallen wordt FOSS gepubliceerd, maar niet op de markt aangeboden in de zin van de verordening cyberweerbaarheid door een rechtspersoon die "als oogmerk of doelstelling heeft om systematisch en duurzaam ondersteuning te verlenen voor de ontwikkeling van […] vrije en opensourcesoftware [die] voor handelsactiviteiten bestemd zijn, en die de levensvatbaarheid van die producten waarborgt" (artikel 3, punt 14), van de verordening cyberweerbaarheid). In dergelijke gevallen is deze rechtspersoon onderworpen aan de verplichtingen van stewards.

71. Een “steward” wordt gedefinieerd als “een rechtspersoon die geen fabrikant is” omdat een fabrikant per definitie de natuurlijke of rechtspersoon is die producten met digitale elementen onder zijn eigen naam of handelsmerk in de handel brengt. Een rechtspersoon kan alleen een steward zijn voor producten met digitale elementen die als FOSS kunnen worden aangemerkt en die worden gepubliceerd, maar niet op de markt worden aangeboden in de zin van de verordening cyberweerbaarheid. Het begrip “steward” is derhalve van toepassing op specifieke gevallen van FOSS die “uiteindelijk bestemd zijn voor handelsactiviteiten, zoals voor integratie in handelsdiensten of in te gelde gemaakte producten met digitale elementen” (overweging 19 van de verordening cyberweerbaarheid ([13])), maar niet op de markt worden aangeboden in de zin van de verordening cyberweerbaarheid, en waarvoor de rechtspersoon die deze FOSS uitgeeft, systematische ondersteuning waarborgt.

72. Het zijn van een steward voor één specifieke FOSS betekent niet dat die rechtspersoon noodzakelijkerwijs ook een steward is voor andere FOSS die hij publiceert. Evenzo betekent het zijn van een fabrikant van één specifieke FOSS niet dat de rechtspersoon mogelijk geen steward is voor andere FOSS. Dit omvat het verstrekken van “community”-versies van dezelfde FOSS, zoals beschreven in punt *3.2.1*, “Een prijs in rekening brengen”.

73. Een rechtspersoon kan dus tegelijkertijd een steward zijn voor één specifieke FOSS (waarbij de steward systematisch en duurzaam ondersteuning biedt en de levensvatbaarheid van de software waarborgt) en een fabrikant voor een andere specifieke FOSS (waarbij hij deze in de handel brengt). Met andere woorden, het kan zo zijn dat dezelfde juridische entiteit verschillende rollen moet vervullen voor verschillende FOSS-projecten.

74. Voor elke specifieke FOSS die hij publiceert, moet de rechtspersoon nagaan of die FOSS wordt geacht in de handel te zijn gebracht in de zin van de verordening cyberweerbaarheid. Zo ja, dan is de rechtspersoon de fabrikant van de software. Indien de FOSS niet wordt geacht in de handel te zijn gebracht, kan de rechtspersoon de steward zijn, indien de software bestemd is voor handelsactiviteiten en indien de rechtspersoon de software onderhoudt overeenkomstig de definitie van steward ([14]).

3.3.1. *Langdurige ondersteuning en waarborging van de levensvatbaarheid van FOSS*

75. In overweging 19 wordt toegelicht dat het verlenen van langdurige ondersteuning voor de ontwikkeling van een product met digitale elementen het volgende kan omvatten (maar niet beperkt is tot): i) het hosten en beheren van samenwerkingsplatforms voor softwareontwikkeling; ii) het hosten van broncode of software; iii) het besturen of beheren van producten met digitale elementen die als FOSS worden aangemerkt, en iv) het aansturen van de ontwikkeling van dergelijke producten met digitale elementen.

76. Dit kan bijvoorbeeld het geval zijn voor een juridische entiteit die FOSS ontwikkelt voor integratie in de eigen producten met digitale elementen en deze vervolgens publiceert zonder de FOSS in de handel te brengen. Dit wordt ook besproken in punt *3.2.7*, “Integratie door andere fabrikanten”. In dat geval is de rechtspersoon geen fabrikant van de software, maar kan hij daarvoor wel een steward zijn. Daarnaast wordt, zoals ook uiteengezet in de vorige punten, een rechtspersoon die een vrije (of community-)versie en een te gelde gemaakte versie van dezelfde FOSS publiceert, beschouwd als een steward van de vrije (of community-)versie, en als een fabrikant van de te gelde gemaakte versie.

77. Evenzo is een juridische entiteit die een FOSS te gelde maakt, maar een entiteit zonder winstoogmerk is waarvan de winst na aftrek van kosten wordt gebruikt om doelstellingen zonder winstoogmerk te verwezenlijken (en waarvan de FOSS derhalve niet in de handel wordt gebracht in de zin van de verordening cyberweerbaarheid, zoals besproken in punt *3.2.6*, “Entiteiten zonder winstoogmerk die zijn opgericht om doelstellingen zonder winstoogmerk te verwezenlijken”), een steward van de FOSS die zij publiceert.

78. Bovendien bieden bepaalde stichtingen samenwerkingsplatforms met verschillende vormen van governance die fabrikanten in staat stellen regelmatig bij te dragen aan de ontwikkeling van FOSS en/of die regelmatig door fabrikanten worden gefinancierd. Dergelijke stichtingen moeten worden beschouwd als stewards met betrekking tot specifieke FOSS die bestemd zijn voor handelsactiviteiten en waarvoor de stichting langdurige ondersteuning biedt. Zoals uiteengezet in punt *3.3*, “Opensourcesoftwarestewards”, kan een dergelijke stichting echter niet worden onderworpen aan verplichtingen uit hoofde van de verordening cyberweerbaarheid voor andere specifieke FOSS die zij host, in gevallen waarin zij geen systematische ondersteuning biedt voor een specifieke FOSS, zij de levensvatbaarheid ervan niet waarborgt en/of specifieke software niet bestemd is voor handelsactiviteiten.

([13]) Dit begrip is ook opgenomen in de formulering “voor handelsactiviteiten bestemd” in de definitie van “opensourcesoftwaresteward” in artikel 3, punt 14), van de verordening cyberweerbaarheid.

([14]) De rechtspersoon kan ook niet zijn onderworpen aan verplichtingen uit hoofde van de verordening cyberweerbaarheid in gevallen waarin: i) een specifieke FOSS niet in de handel wordt gebracht in de zin van de verordening cyberweerbaarheid en ii) de rechtspersoon niet voldoet aan de definitie van steward met betrekking tot die specifieke FOSS.

79. Het soort "langdurige ondersteuning" dat stichtingen en soortgelijke organisaties aan specifieke FOSS-projecten verlenen, kan sterk verschillen. Zo bieden bepaalde juridische entiteiten alleen niet-technische ondersteuning, zoals het beheren van de branding van projecten, het vaststellen van governanceregels, het organiseren van "community"-evenementen of het inzamelen van donaties. Andere entiteiten voorzien ook in de onderliggende IT-infrastructuur die nodig is om het project uit te voeren, zoals het hosten van registers voor broncode, het aanbieden van versiecontrolesystemen of het genereren van sleutels voor ondertekening. Andere gaan verder wat betreft het soort steun dat zij verlenen door actief technische middelen aan het project bij te dragen, bijvoorbeeld door ontwikkelaars in dienst te nemen, ontwikkelingswerkzaamheden te coördineren, codes te evalueren of combineren, releases te beheren of kwetsbaarheidsverslagen en beveiligingspatches te behandelen. Hoewel alle juridische entiteiten die in het kader van de verordening cyberweerbaarheid als stewards worden aangemerkt, moeten voldoen aan de verplichtingen van artikel 24, leden 1 en 2, varieert de mate waarin de verplichtingen van artikel 14, leden 1, 3 en 8, van toepassing zijn op die juridische entiteiten afhankelijk van het soort steun dat zij verlenen, overeenkomstig artikel 24, lid 3.

80. Een steward die alleen niet-technische ondersteuning biedt, is bijvoorbeeld per definitie niet betrokken bij de ontwikkeling van het product met digitale elementen en is daarom niet verplicht actief uitgebuite kwetsbaarheden te melden. Die steward voorziet ook niet in netwerk- en informatiesystemen voor de ontwikkeling van dergelijke producten met digitale elementen, en is daarom niet verplicht ernstige incidenten te melden aan Enisa en de CSIRT's of aan getroffen gebruikers. Wanneer de steward echter kennis krijgt van een actief uitgebuite kwetsbaarheid (bv. via een verslag uit externe bronnen, zoals beveiligingsonderzoekers), moet hij de informatie delen met de onderhouders van het product met digitale elementen, in overeenstemming met zijn cyberbeveiligingsbeleid. De onderhouders van de producten met digitale elementen en/of de stewards moeten ook overwegen de kwetsbaarheid op vrijwillige basis te melden, overeenkomstig artikel 15.

81. Anderzijds moet een steward, wanneer hij de onderliggende IT-infrastructuur voor bepaalde producten met digitale elementen ter beschikking stelt, Enisa en de CSIRT's overeenkomstig artikel 14, lid 3, in kennis stellen van ernstige incidenten in verband met die infrastructuur die gevolgen hebben voor de beveiliging van producten met digitale elementen. In voorkomend geval moeten ook alle gebruikers worden geïnformeerd (bv. via een algemene aankondiging). Zoals aangegeven in het vorige punt, moet de steward, hoewel hij niet verplicht is actief uitgebuite kwetsbaarheden waarvan hij kennis krijgt, te melden, de correcte aanpak van kwetsbaarheden bevorderen en vrijwillige melding overeenkomstig artikel 15 overwegen.

82. Tot slot moet een steward die ook technische middelen ter beschikking stelt voor specifieke producten met digitale elementen: i) overeenkomstig artikel 14, lid 1, melding doen van actief uitgebuite kwetsbaarheden waarvan hij kennis krijgt en ii) in voorkomend geval alle gebruikers te informeren. Voor zover de steward ook een directe relatie heeft met de getroffen gebruikers, is hij ook verplicht hen rechtstreeks te informeren, overeenkomstig artikel 14, lid 8.

83. Wanneer een entiteit ophoudt op langdurige basis systematische ondersteuning te verlenen voor een specifieke FOSS, kan het zijn dat zij niet langer voldoet aan de definitie van steward en dus niet langer onderworpen is aan de overeenkomstige verplichtingen. In dergelijke gevallen wordt die entiteit aangemoedigd om de wijziging van haar status voor die specifieke FOSS duidelijk mee te delen.

84. In bepaalde situaties kan een entiteit die zich voor een specifiek project heeft ingezet, besluiten dat project rechtstreeks te gelde te maken, waarbij het product met digitale elementen in de handel wordt gebracht en de verplichtingen van de fabrikant uit hoofde van de verordening cyberweerbaarheid in werking treden. In dergelijke omstandigheden kan die entiteit worden aangemerkt als de fabrikant van het product met digitale elementen vanaf de datum waarop zij het in de handel brengt (maar niet met betrekking tot eerdere versies waarvoor zij als steward optrad).

3.4. **Contribuanten en downstreamtoepassingen**

85. Zoals reeds vermeld in punt *3.1*, "Bepalen of vrije en opensourcesoftware onder iemands verantwoordelijkheid valt", is in de verordening cyberweerbaarheid verduidelijkt dat zij niet van toepassing is "op natuurlijke of rechtspersonen die met broncode bijdragen aan producten met digitale elementen die als vrije en opensourcesoftware worden aangemerkt en niet onder hun verantwoordelijkheid vallen" (overweging 18).

86. Fabrikanten van producten met digitale elementen die FOSS-componenten integreren in hun eigen producten met digitale elementen, worden ook niet verantwoordelijk voor de individuele naleving van de verordening cyberweerbaarheid door dergelijke componenten, zelfs niet wanneer de fabrikanten met broncode bijdragen aan het onderhoud ervan.

87. Evenzo heeft het loutere feit dat fabrikanten FOSS-componenten integreren in hun eigen (te gelde gemaakte) producten met digitale elementen geen gevolgen voor de status van die FOSS-component in het kader van de verordening cyberweerbaarheid. Onderhouders van FOSS-componenten die niet in de handel worden gebracht, hebben geen verplichtingen ten aanzien van andere entiteiten die dergelijke componenten in hun producten met digitale elementen kunnen integreren. Of de verordening cyberweerbaarheid van toepassing is op een bepaalde FOSS-component, hangt uitsluitend af van de vraag of de natuurlijke of rechtspersoon die de component publiceert, deze in de handel brengt.

88. Niettemin moeten fabrikanten van producten met digitale elementen waarin FOSS-componenten zijn geïntegreerd, voldoen aan de verordening cyberweerbaarheid voor hun eigen producten met digitale elementen. Zij hebben overeenkomstig artikel 13, lid 5, ook een zorgvuldigheidsverplichting ten aanzien van de FOSS-componenten die zij integreren. Daarnaast moeten zij kwetsbaarheden in geïntegreerde componenten melden en beveiligingsoplossingen delen overeenkomstig artikel 13, lid 6. Zie punt *9.2.1*, "Rapportage upstream en delen van beveiligingsoplossingen", voor meer informatie over dit onderwerp.

3.5. **Illustratieve scenario's**

89. De onderstaande voorbeelden zijn volledig hypothetisch en alleen bedoeld ter illustratie van de verschillende gevallen die in de bovenstaande punten zijn toegelicht.

Voorbeeld 27: individuele ontwikkelaar A heeft FOSS ontwikkeld. Ontwikkelaar A publiceert die FOSS onder de eigen naam of het eigen handelsmerk, maar brengt geen prijs in rekening voor het gebruik ervan. De software wordt openlijk gedeeld en is voor iedereen vrij toegankelijk voor toegang, gebruik, wijziging en herdistributie. Ontwikkelaar A heeft er ook een link naar een platform voor het inzamelen van vrijwillige donaties bij geplaatst.

De bedrijven B, C en D integreren die FOSS in hun eigen producten met digitale elementen. Om lopend onderhoud te ondersteunen, doen de bedrijven B, C en D vrijwillige donaties aan ontwikkelaar A. Deze donaties stellen ontwikkelaar A in staat het project actief te onderhouden.

Die FOSS wordt niet in de handel gebracht in de zin van de verordening cyberweerbaarheid. Ontwikkelaar A heeft geen verplichtingen uit hoofde van de verordening cyberweerbaarheid. De bedrijven B, C en D moeten overeenkomstig artikel 13, lid 5, passende zorgvuldigheid betrachten bij de integratie van die FOSS in hun eigen producten met digitale elementen.

Voorbeeld 28: stichting zonder winstoogmerk F publiceert een FOSS-component voor integratie in andere handelsproducten met digitale elementen. Stichting F verbindt zich ertoe die FOSS langdurig te ondersteunen om de levensvatbaarheid en het gebruik ervan te waarborgen. De bedrijven A, B en C integreren die FOSS in hun eigen producten met digitale elementen. De bedrijven A en B dragen vrijwillig een deel van de tijd van hun ontwikkelaars bij aan de ontwikkeling en het onderhoud van FOSS-projecten binnen stichting F, ook voor die FOSS.

Aangezien stichting F een entiteit zonder winstoogmerk is die zodanig is opgericht dat haar winst na aftrek van kosten wordt gebruikt om doelstellingen zonder winstoogmerk te verwezenlijken, wordt de FOSS niet geacht in de handel te zijn gebracht in de zin van de verordening cyberweerbaarheid. Stichting F is de steward van de FOSS en is onderworpen aan de overeenkomstige verplichtingen van artikel 24. De bedrijven A, B en C moeten overeenkomstig artikel 13, lid 5, passende zorgvuldigheid betrachten bij de integratie van die FOSS in hun eigen producten met digitale elementen.

Voorbeeld 29: bedrijf A heeft een FOSS-component ontwikkeld voor integratie in zijn eigen producten met digitale elementen. Bedrijf A publiceert deze FOSS ook afzonderlijk onder de eigen naam of het eigen handelsmerk en onderhoudt deze actief. Het brengt echter geen kosten in rekening voor het gebruik en maakt het ook niet op andere manieren te gelde. De bedrijven B, C en D integreren die FOSS in hun eigen producten met digitale elementen en dragen vrijwillig een deel van de tijd van hun ontwikkelaars bij aan het onderhoud ervan.

Die FOSS wordt niet geacht in de handel te zijn gebracht in de zin van de verordening cyberweerbaarheid. Bedrijf A is niet de fabrikant ervan, maar de steward. De bedrijven B, C en D moeten overeenkomstig artikel 13, lid 5, passende zorgvuldigheid betrachten wanneer zij de FOSS integreren in hun eigen producten met digitale elementen.

Voorbeeld 30: bedrijf A publiceert een FOSS onder de eigen naam of het eigen handelsmerk en biedt deze aan als een betaalde versie, die bepaalde voordelen omvat, zoals technische bijstand of optimalisering van de prestaties. Ontwikkelaars van de bedrijven B, C en D dragen bij aan het onderhoud van de FOSS, maar deze blijft onder zeggenschap van bedrijf A.

Bedrijf A wordt beschouwd als fabrikant van die FOSS ([15]). *De bedrijven B, C en D zijn voor die specifieke FOSS niet onderworpen aan verplichtingen uit hoofde van de verordening cyberweerbaarheid. Indien zij die FOSS integreren in hun eigen producten met digitale elementen, moeten zij passende zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5.*

Voorbeeld 31: bedrijf A publiceert een FOSS onder de eigen naam of het eigen handelsmerk en zorgt voor het lopende onderhoud om de levensvatbaarheid ervan op lange termijn te waarborgen, zodat die software kan worden geïntegreerd in producten met digitale elementen van andere bedrijven. Bedrijf A brengt geen kosten in rekening voor het gebruik ervan, verwerkt geen persoonsgegevens die het via het product met digitale elementen verzamelt, of verkoopt geen ondersteunende diensten in verband met de publicatie van de FOSS.

Bedrijf B draagt code en de tijd van ontwikkelaars bij aan het onderhoud van de FOSS, maar distribueert deze niet in het kader van een handelsactiviteit. Bedrijf B biedt onafhankelijk van de distributie van de FOSS technische ondersteuningsdiensten aan. Bedrijf A wordt geacht de steward voor die FOSS te zijn, terwijl bedrijf B voor die FOSS geen verplichtingen uit hoofde van de verordening cyberweerbaarheid heeft.

Voorbeeld 32: een FOSS-component wordt gepubliceerd door een entiteit zonder winstoogmerk die zodanig is opgericht dat alle winst na aftrek van kosten wordt gebruikt om doelstellingen zonder winstoogmerk te verwezenlijken. De entiteit verleent langdurige ondersteuning om de levensvatbaarheid van het project op lange termijn te waarborgen. Het onderhoud wordt gefinancierd met overheidsmiddelen, zoals onderzoekssubsidies. Aanvullende ontwikkelingen, waaronder nieuwe functionaliteiten, worden gefinancierd door middel van donaties en specifieke projecten, die worden uitgevoerd in partnerschap met fabrikanten die die FOSS integreren in hun producten met digitale elementen. Dergelijke functionaliteiten worden opgenomen in de codebase van de FOSS.

De entiteit zonder winstoogmerk die de FOSS publiceert, wordt beschouwd als de steward voor die FOSS-component. Een fabrikant die heeft bijgedragen tot de ontwikkeling van bepaalde functionaliteiten, wordt niet de fabrikant van die FOSS-component. Wanneer de fabrikant die FOSS-component integreert in zijn eigen product met digitale elementen, moet hij passende zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5.

Voorbeeld 33: een entiteit zonder winstoogmerk die zodanig is opgericht dat alle inkomsten na aftrek van kosten worden gebruikt om doelstellingen zonder winstoogmerk te verwezenlijken, publiceert een softwareontwikkelingskit ("Software Development Kit", SDK) voor FOSS en zorgt voor het voortdurende onderhoud ervan. De SDK wordt openlijk gedeeld en is voor iedereen vrij toegankelijk voor toegang, gebruik, wijziging en herdistributie. De financiering wordt verstrekt door middel van lidmaatschapsbijdragen die worden betaald aan de entiteit zonder winstoogmerk, en ontwikkelaars die in dienst zijn van aangesloten organisaties dragen bij met code en andere middelen voor de ontwikkeling van de SDK. Fabrikanten gebruiken de SDK als component om andere producten met digitale elementen te bouwen.

De entiteit zonder winstoogmerk die de SDK publiceert, is de steward ervan. De leden van de stichting zijn niet verantwoordelijk voor de naleving van de verordening cyberweerbaarheid door de SDK. Wanneer fabrikanten de SDK gebruiken om hun eigen product met digitale elementen te bouwen, moeten zij passende zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5.

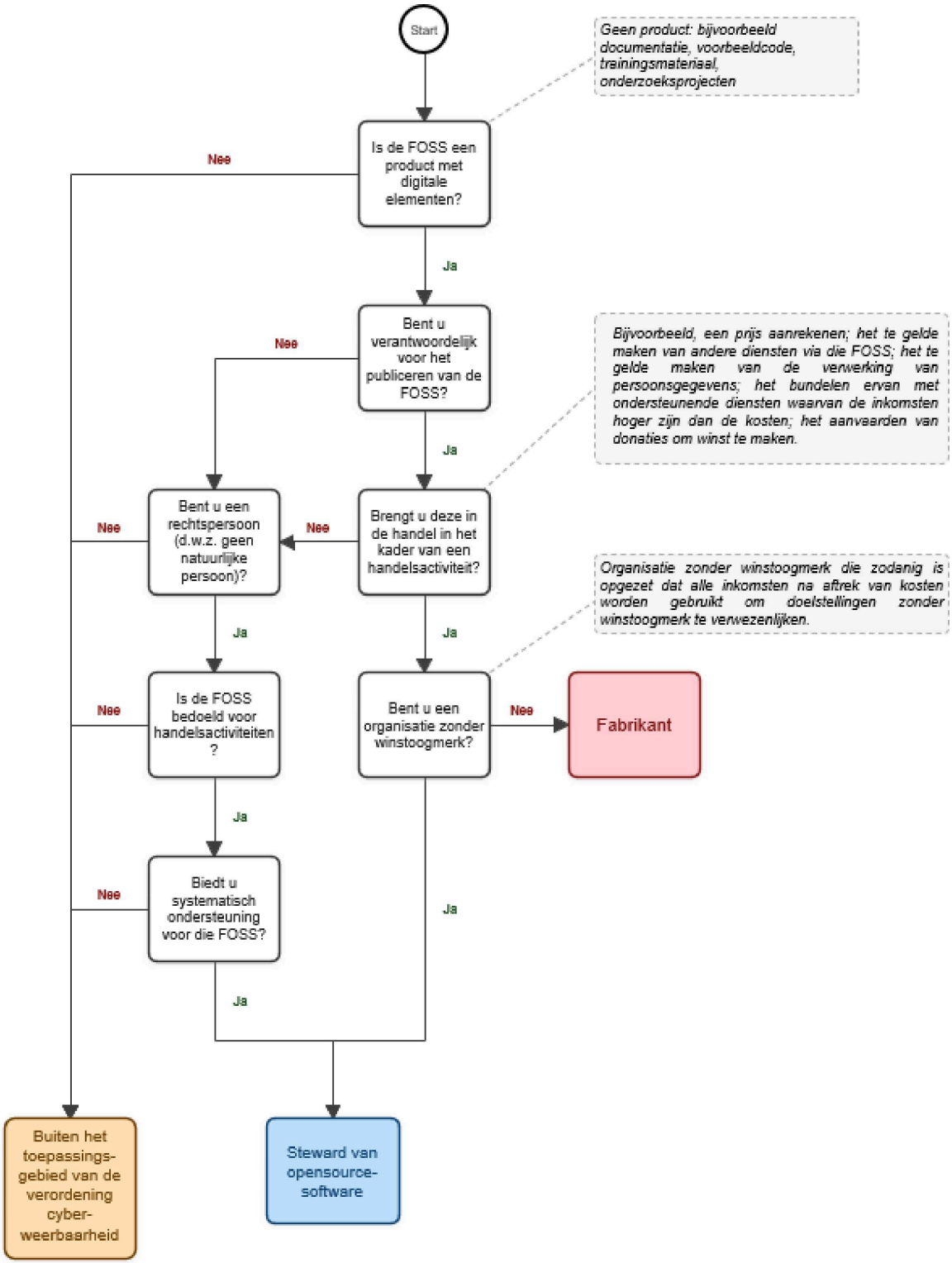
Voorbeeld 34: een individuele ontwikkelaar publiceert een FOSS-bibliotheek in een openbaar pakkettenregister voor een bepaalde programmeertaal en onderhoudt deze actief. In de pakketdocumentatie voegt de ontwikkelaar een link toe om donaties in te zamelen. Een fabrikant downloadt die bibliotheek gratis uit het register en integreert deze in zijn eigen product met digitale elementen.

De individuele ontwikkelaar en het pakketregister hebben geen verplichtingen uit hoofde van de verordening cyberweerbaarheid. De fabrikant die de bibliotheek integreert, moet de nodige zorgvuldigheid betrachten overeenkomstig artikel 13, lid 5.

([15]) Tenzij bedrijf A een entiteit zonder winstoogmerk is die zodanig is opgericht dat alle winst na aftrek van kosten wordt gebruikt om doelstellingen zonder winstoogmerk te verwezenlijken, in welk geval het de steward van die FOSS zou zijn.

Figuur 1:

gestileerd stroomschema dat aangeeft hoe vrije en opensourcesoftware onder de verordening cyberweerbaarheid valt



4. INGRIJPENDE WIJZIGINGEN EN RESERVEONDERDELEN

90. In artikel 3, punt 30), van de verordening cyberweerbaarheid wordt een “ingrijpende wijziging” gedefinieerd als een wijziging van het product met digitale elementen nadat het in de handel is gebracht, die i) gevolgen heeft voor de conformiteit van het product met digitale elementen met de essentiële cyberbeveiligingsvereisten van deel I van bijlage I of ii) leidt tot een wijziging van het beoogde doel waarvoor het product met digitale elementen is beoordeeld.

91. Het begrip “ingrijpende wijziging” is relevant voor het bepalen van de verplichtingen krachtens de verordening cyberweerbaarheid in een aantal gevallen, waaronder de volgende:

a) overeenkomstig artikel 21 wordt een importeur of distributeur die een reeds in de handel gebracht product met digitale elementen ingrijpend wijzigt, beschouwd als de fabrikant ervan;

b) overeenkomstig artikel 22 wordt elke natuurlijke of rechtspersoon die een ingrijpende wijziging uitvoert aan een product met digitale elementen en het op de markt aanbiedt, beschouwd als de fabrikant ervan;

c) overeenkomstig artikel 69, lid 2, wordt elke natuurlijke of rechtspersoon die na 11 december 2027 een ingrijpende wijziging uitvoert aan een product met digitale elementen dat vóór 11 december 2027 in de handel is gebracht en in de handel brengt, beschouwd als de fabrikant ervan;

d) voor fabrikanten van producten met digitale elementen die na 11 december 2027 in de handel zijn gebracht, om te bepalen of een product met digitale elementen een nieuwe conformiteitsbeoordelingsprocedure moet ondergaan als gevolg van wijzigingen die na die datum zijn aangebracht, met name in het licht van het iteratieve karakter van softwareontwikkeling.

92. Daarom is het belangrijk richtsnoeren te verstrekken om marktdeelnemers te helpen begrijpen wanneer hardware- of softwarewijzigingen als ingrijpende wijzigingen kunnen worden aangemerkt.

4.1. **Fysieke reparatie**

93. Zoals vermeld in overweging 42 van de verordening cyberweerbaarheid leidt “[h]et “opknappen”, het “onderhoud” en de “reparatie” als gedefinieerd in artikel 2, punten 18), 19) en 20), van Verordening (EU) 2024/1781 van het Europees Parlement en de Raad [...] van een product met digitale elementen, […] niet noodzakelijkerwijs tot een ingrijpende wijziging van het product, bijvoorbeeld als het beoogde doel en de functies niet worden gewijzigd en het risiconiveau ongewijzigd blijft. De verbetering van een product met digitale elementen door de fabrikant kan echter leiden tot veranderingen in het ontwerp en de ontwikkeling van dat product en kan derhalve van invloed zijn op het beoogde doel en de conformiteit ervan met de vereisten van deze verordening”. Dit is in overeenstemming met punt 2.1 van de Blauwe Gids, waarin eraan wordt herinnerd dat “[e]en product dat in belangrijke mate is gewijzigd of gereviseerd nadat het in gebruik is genomen, […] als een nieuw product [moet] worden beschouwd als: i) de oorspronkelijke prestaties, het oorspronkelijke doel of het oorspronkelijke type zijn gewijzigd zonder dat dit bij de initiële risicobeoordeling was voorzien; ii) de aard van het gevaar is veranderd of het risiconiveau is gestegen op basis van de relevante harmonisatiewetgeving van de Unie; en iii) het product op de markt wordt aangeboden (of in gebruik wordt genomen indien de toepasselijke wetgeving ook de ingebruikneming bestrijkt). Dit moet per geval worden beoordeeld rekening houdend met de doelstelling van de wetgeving en het type producten dat onder die wetgeving valt”.

94. Opknap-, onderhouds- en reparatiewerkzaamheden die leiden tot fysieke wijzigingen van producten met digitale elementen die reeds in de handel zijn gebracht, vormen niet noodzakelijkerwijs ingrijpende wijzigingen. Daarom moet per geval worden beoordeeld of een dergelijke fysieke wijziging van invloed is op de conformiteit van het product met digitale elementen met de essentiële eisen van deel I van bijlage I, of leidt tot een wijziging van het beoogde doel van het product dat onder de cyberbeveiligingsrisicobeoordeling valt.

95. Het vervangen van defecte of versleten onderdelen door onderdelen die beter presteren (bv. vanwege de technische vooruitgang of omdat het oude onderdeel niet langer wordt geproduceerd) leidt op zich niet tot een ingrijpende wijziging van het gerepareerde product met digitale elementen. Dit gebeurt alleen als de prestatiewijziging of de manier waarop het gerepareerde product met digitale elementen werkt i) van invloed is op de conformiteit ervan met de essentiële vereisten of ii) leidt tot een wijziging van het beoogde doel die niet onder de risicobeoordeling viel.

Voorbeeld 35: de fabrikant van een computerserver voert een reparatie uit en vervangt een defect RAM door een nieuw RAM dat beter presteert. De conformiteit van de server met de essentiële vereisten wordt niet beïnvloed. De server presteert beter, maar de nieuwe prestaties blijven binnen het beoogde gebruik van de server zoals in aanmerking genomen in de cyberbeveiligingsrisicobeoordeling. De computerserver wordt niet als ingrijpend gewijzigd beschouwd.

4.2. **Reserveonderdelen**

96. In artikel 2, lid 6, van de verordening cyberweerbaarheid is bepaald dat reserveonderdelen die bestemd zijn als vervanging van identieke componenten en die zijn vervaardigd volgens dezelfde specificaties als de componenten die zij beogen te vervangen, niet onder de verordening cyberweerbaarheid vallen. In overweging 29 staat verder dat de vrijstelling zowel betrekking heeft op reserveonderdelen die bedoeld zijn voor de producten met digitale elementen die vóór de datum van toepassing van deze verordening werden aangeboden, als op reserveonderdelen die reeds een conformiteitsbeoordelingsprocedure op grond van deze verordening hebben ondergaan.

97. De vrijstelling van artikel 2, lid 6, van de verordening cyberweerbaarheid moet aldus worden opgevat dat zij alleen van toepassing is wanneer het reserveonderdeel specifiek wordt geleverd ter reparatie van een reeds in de handel gebracht product met digitale elementen of om de duurzaamheid ervan te verlengen (vóór of na 11 december 2027). Wanneer een product met digitale elementen wordt geleverd als een opzichzelfstaand product, zonder enig verband met het onderhoud of de reparatie van een reeds bestaand product met digitale elementen, wordt het in de handel gebracht in de zin van de verordening cyberweerbaarheid en mag het niet worden beschouwd als een reserveonderdeel dat binnen het toepassingsgebied van artikel 2, lid 6, valt. Het doel van het onderhoud of de reparatie moet blijken uit de context van de levering, bijvoorbeeld door identificatie van het product met digitale elementen of de productfamilie in de bestelling of offerte, of door levering via aftersales- of servicekanalen. Ondersteunend bewijsmateriaal in die zin moet ook ter beschikking van de markttoezichtautoriteiten worden gehouden. Het feit dat een product met digitale elementen technisch gezien kan worden gebruikt om een component te vervangen, is op zich niet voldoende om het onder de vrijstelling te laten vallen wanneer dergelijke elementen ontbreken.

98. Wanneer een reserveonderdeel identiek is aan een onderdeel dat reeds onderdeel uitmaakt van een product met digitale elementen dat hetzij vóór de datum van toepassing van de verordening cyberweerbaarheid in de handel is gebracht, hetzij overeenkomstig de verordening cyberweerbaarheid in de handel is gebracht, is dat reserveonderdeel zelf dus niet onderworpen aan de verordening cyberweerbaarheid.

99. Bij de beoordeling of een reserveonderdeel als identiek aan een component moet worden beschouwd, moet de nadruk liggen op de functionele rol ervan in het product met digitale elementen en op de kenmerken die relevant kunnen zijn voor cyberbeveiliging. Hoewel altijd een beoordeling per geval nodig is, beletten verschillen die geen invloed hebben op de beveiligingskenmerken of het cyberbeveiligingsrisicoprofiel van de component op zich niet dat dat reserveonderdeel binnen het toepassingsgebied van artikel 2, lid 6, van de verordening cyberweerbaarheid valt.

100. Verschillen in kenmerken die relevant zijn voor de cyberbeveiliging van het onderdeel, zoals algoritmen, protocollen, cryptografische mechanismen, toegangscontrolefuncties of andere kenmerken die relevant zijn voor de beveiliging, kunnen daarentegen betekenen dat het nieuwe onderdeel niet kan worden beschouwd als identiek aan het onderdeel dat het moet vervangen.

101. Wanneer een reserveonderdeel niet identiek is aan het oorspronkelijke onderdeel, vormt dat reserveonderdeel een opzichzelfstaand product met digitale elementen en is het derhalve onderworpen aan de verordening cyberweerbaarheid. In dergelijke gevallen moet de naleving van de essentiële vereisten worden beoordeeld in het licht van het beoogde doel van de vervangende component. Van bijzonder belang is de functie van de vervangende component om de compatibiliteit of interoperabiliteit met een bestaand product met digitale elementen te waarborgen, ook wanneer dat product een product met digitale elementen is dat vóór de inwerkingtreding van de verordening cyberweerbaarheid in de handel is gebracht. Indien vanwege dat beoogde doel of die technische beperkingen redelijkerwijs niet aan bepaalde essentiële vereisten kan worden voldaan, moet de fabrikant dit in de cyberbeveiligingsrisicobeoordeling tot uiting brengen en passende alternatieve of compenserende risicobeperkende maatregelen nemen om de beveiliging van het product met digitale elementen niet te ondermijnen. Zoals ook besproken in punt *2.6*, "Complexe systemen", spelen zowel de technische documentatie als de informatie en instructies voor de gebruiker een belangrijke rol bij het transparant beschrijven van de vastgestelde beperkingen, de bijbehorende cyberbeveiligingsrisico's en de uitgevoerde risicobeperkende maatregelen. Zoals uiteengezet in punt *4.1*, "Fysieke reparatie", leidt het vervangen van defecte of versleten onderdelen door onderdelen die beter presteren op zich niet tot een ingrijpende wijziging van het gerepareerde product met digitale elementen.

Voorbeeld 36: een fabrikant heeft verbonden controllers in de EU in de handel gebracht. In één geval werd de controller in 2026 in de handel gebracht, vóór de datum van toepassing van de verordening cyberweerbaarheid. In een ander geval werd de controller in 2028 in overeenstemming met de verordening cyberweerbaarheid in de handel gebracht. In 2028 bleek een digitale communicatiemodule bij beide soorten controllers niet goed te werken. De fabrikant levert als reserveonderdeel een vervangingsmodule die identiek is en volgens dezelfde specificaties als het origineel is vervaardigd.

In beide gevallen valt de vervangingsmodule binnen het toepassingsgebied van de vrijstelling van artikel 2, lid 6. Het reserveonderdeel valt zelf niet onder de verordening cyberweerbaarheid, ook al is het een product met digitale elementen, omdat het een identieke component in een product met digitale elementen vervangt. De reparatie vormt geen ingrijpende wijziging van het product met digitale elementen.

Voorbeeld 37: een fabrikant heeft in 2026, vóór de datum van toepassing van de verordening cyberweerbaarheid, een verbonden industriële controller in de EU in de handel gebracht. In 2028 werkt een communicatiechip in die controller niet meer goed. Aangezien de fabrikant die chip niet langer vervaardigt, levert hij als reserveonderdeel een nieuwere chip met een gelijkwaardige functionaliteit, maar met een andere cryptografische uitvoering en een geactualiseerd beveiligd opstartmechanisme, om de compatibiliteit en de continue werking te handhaven.

In dit geval kan de vervangende chip niet als identiek worden beschouwd, aangezien de verschillen in de cryptografische uitvoering en het beveiligde opstartmechanisme van invloed zijn op de cyberbeveiligingseigenschappen van de chip. De chip komt derhalve niet in aanmerking voor de vrijstelling van artikel 2, lid 6, en vormt een product met digitale elementen dat onder de verordening cyberweerbaarheid valt. De conformiteit van het vervangende onderdeel moet worden beoordeeld in het licht van het beoogde doel ervan, met inbegrip van de rol ervan bij het waarborgen van de interoperabiliteit met het product met digitale elementen dat vóór de inwerkingtreding van de verordening cyberweerbaarheid in de handel is gebracht.

Voorbeeld 38: een fabrikant brengt in 2028 een controller voor slimme gebouwen in de handel in overeenstemming met de verordening cyberweerbaarheid. In 2029 werkt de draadloze module in die controller niet meer goed. Aangezien de fabrikant die module niet meer vervaardigt, levert hij als reserveonderdeel een nieuwe module die dezelfde functie vervult met gebruikmaking van dezelfde communicatieprotocollen en beveiligingsmechanismen, maar die gebaseerd is op een andere chipset en beschikt over geactualiseerde firmware die de kenmerken die relevant kunnen zijn voor cyberbeveiliging, niet wijzigt.

In dat geval kan de vervangende module als identiek worden beschouwd. De module komt derhalve in aanmerking voor de vrijstelling van artikel 2, lid 6, en is niet onderworpen aan de verordening cyberweerbaarheid.

102. De vrijstelling voor reserveonderdelen is van toepassing ongeacht of het reserveonderdeel een component in een product met digitale elementen vervangt of een volledig product met digitale elementen vervangt dat zelf deel uitmaakt van een groter product, ook wanneer dat grotere product met digitale elementen uit verschillende geïntegreerde componenten bestaat, mits het vervangende onderdeel specifiek als reserveonderdeel wordt geleverd, zoals in de voorgaande punten is uitgelegd.

Voorbeeld 39: in 2027 brengt een fabrikant een industrieel automatiseringssysteem in de handel dat een programmeerbare logische controller (PLC) als een van zijn componenten omvat. In 2031 werkt de processor (CPU) van de PLC niet meer goed. De fabrikant biedt twee reparatiemogelijkheden: i) de levering van een vervangende CPU-eenheid, die als identiek aan de oorspronkelijk geïnstalleerde CPU kan worden beschouwd of ii) de levering van een volledige vervangende PLC, die als identiek aan de oorspronkelijk geïnstalleerde PLC kan worden beschouwd. In beide gevallen wordt de vervanging als reserveonderdeel geleverd via het servicekanaal van de fabrikant en wordt het systeem voor industriële automatisering waarvoor de vervanging is bedoeld, duidelijk geïdentificeerd. In beide gevallen valt de vervanging binnen het toepassingsgebied van de vrijstelling van artikel 2, lid 6, ongeacht of de vervanging betrekking heeft op een component in de PLC, dan wel op de PLC als geheel.

4.3. **Software-updates als ingrijpende wijzigingen**

103. Softwareontwikkeling is iteratief van aard, waarbij reeds in de handel gebrachte softwareproducten met digitale elementen regelmatig en voortdurend worden bijgewerkt. In dit verband is het nuttig meer richtsnoeren te verstrekken om te bepalen wanneer software als ingrijpend gewijzigd moet worden beschouwd. Dergelijke richtsnoeren zijn met name bedoeld om fabrikanten van softwareproducten met digitale elementen die hun eigen producten wijzigen, te helpen bepalen of die wijzigingen een ingrijpende wijziging vormen.

104. In overweging 39 wordt aangegeven dat een product met digitale elementen ingrijpend wordt gewijzigd wanneer een wijziging het niveau van het cyberbeveiligingsrisico wijzigt en wanneer een dergelijk gewijzigd of extra risico door de fabrikant niet in aanmerking is genomen bij zijn risicobeoordeling en bijgevolg bij de uitvoering van de essentiële vereisten. Een fabrikant moet daarom per geval beoordelen of een software-update nieuwe of verhoogde cyberbeveiligingsrisico's met zich meebrengt en of dergelijke risico's reeds in zijn risicobeoordeling aan bod zijn gekomen.

105. Wanneer een fabrikant nieuwe functionaliteiten in een product met digitale elementen invoert die leiden tot een wijziging van het beoogde doel van het product als geheel, is het waarschijnlijk dat de fabrikant dergelijke wijzigingen niet in aanmerking heeft genomen in zijn risicobeoordeling. In dergelijke omstandigheden zou de wijziging over het algemeen als een ingrijpende wijziging worden aangemerkt.

Voorbeeld 40: een fabrikant brengt een dashboard in de handel dat gegevens van machines verzamelt en trends en waarschuwingen weergeeft, zonder dat hij dergelijke machines kan bedienen. Vervolgens ontwikkelt de fabrikant een nieuwe versie van dat dashboard, waarbij functionaliteiten worden ingevoerd die hem in staat stellen de machines te bedienen, onder meer door na een storing de operationele parameters aan te passen en de machines te herstarten. Als gevolg van deze wijzigingen is het beoogde doel van het dashboard verder geëvolueerd dan in de risicobeoordeling was voorzien, waarbij dit doel is verschoven van een instrument voor situationeel bewustzijn naar een product met digitale elementen dat bedoeld is om operationele controle uit te oefenen over andere apparaten. Het dashboard is daarom ingrijpend gewijzigd.

Voorbeeld 41: een fabrikant brengt een softwaretoepassing voor consumenten in de handel die bedoeld is om persoonsgegevens, zoals e-mails, berichten of documenten, te organiseren en weer te geven en om basisfuncties voor zoeken en filteren te ondersteunen. De fabrikant voert vervolgens een update in die de toepassing in staat stelt gebruikersinhoud automatisch te analyseren om gedragsprofielen te genereren en geautomatiseerde beslissingen te nemen die van invloed zijn op de prioritering, onderdrukking of aanbeveling van inhoud zonder tussenkomst van de gebruiker. Als gevolg van deze wijziging verschuift het beoogde doel van de software van een door de gebruiker gecontroleerd instrument voor informatiebeheer naar een geautomatiseerd besluitvormingssysteem, wat niet was voorzien in de risicobeoordeling. De toepassing is derhalve ingrijpend gewijzigd.

106. Tegelijkertijd is het echter mogelijk dat een fabrikant geleidelijk nieuwe functionaliteiten invoert die reeds in de risicobeoordeling zijn opgenomen of die op zich het cyberbeveiligingsrisicoprofiel van het product met digitale elementen niet wijzigen. Dit kan bijvoorbeeld het geval zijn wanneer de fabrikant heeft geanticipeerd op de ontwikkeling van die functionaliteiten, de bijbehorende risico's reeds heeft beschreven en beoordeeld en passende risicobeperkende maatregelen heeft genomen om ervoor te zorgen dat voortdurend aan de essentiële vereisten wordt voldaan. Dit kan ook het geval zijn wanneer de nieuwe functionaliteiten geen wijzigingen doorvoeren die nieuwe of verhoogde risico's met zich meebrengen. Dergelijke actualiseringen mogen daarom niet als ingrijpende wijzigingen worden beschouwd, aangezien zij het cyberbeveiligingsrisico niet vergroten en bijgevolg de uitvoering van de essentiële vereisten niet wijzigen.

Voorbeeld 42: een berichtenapplicatie wordt in eerste instantie gelanceerd met een functionaliteit die beperkt is tot één-op-één berichtenuitwisseling. De risicobeoordeling van de fabrikant heeft betrekking op de latere invoering van groepsberichten, met inbegrip van bijvoorbeeld de toegenomen complexiteit van de routering van berichten. In een latere update voegt de fabrikant een groepschatfunctie toe, samen met beheerderscontroles en moderatie-instrumenten die reeds in het oorspronkelijke ontwerp waren voorzien en beoordeeld. De update implementeert functionaliteiten die binnen het toepassingsgebied van het oorspronkelijke beoogde doel en de risicobeoordeling vallen. De berichtenapplicatie is dus niet ingrijpend gewijzigd.

Voorbeeld 43: er wordt een productiemonitoringsysteem in de handel gebracht met read-onlydashboards ingeschakeld, terwijl de systeemarchitectuur wel geautomatiseerde controlefuncties bevat, maar deze uitgeschakeld blijven. De risicobeoordeling van de fabrikant heeft uitdrukkelijk betrekking op de toekomstige activering van geautomatiseerde controleketens, met inbegrip van de cyberbeveiligingsrisico's in verband met gesloten-ketencontrole, alsook op waarborgen zoals mechanismen om acties van bedieners op te heffen en noodinstellingen. In een latere update schakelt de fabrikant de automatische controlefuncties in en activeert hij de veiligheidscontroles zoals oorspronkelijk beoordeeld. Het productiecontrolesysteem is derhalve niet ingrijpend gewijzigd.

107. Omgekeerd kunnen zelfs beperkte of schijnbaar kleine nieuwe functionaliteiten aanzienlijke cyberbeveiligingsrisico's met zich meebrengen die van invloed zijn op de naleving van de essentiële vereisten. De beoordeling van een ingrijpende wijziging moet daarom niet worden gebaseerd op de omvang of complexiteit van de wijziging, maar op de mogelijke nadelige gevolgen ervan voor het cyberbeveiligingsrisicoprofiel van het product met digitale elementen en bijgevolg op de uitvoering van de essentiële vereisten.

Voorbeeld 44: een fabrikant introduceert een update van een softwaretoepassing waarbij een "onthoud mij"- of een permanente loginfunctie wordt toegevoegd die authenticatietokens lokaal opslaat om het gebruiksgemak te verbeteren. Hoewel de functionaliteit beperkt is qua omvang, brengt zij nieuwe risico's met zich mee in verband met de diefstal van tokens, ongeoorloofde toegang en het overnemen van sessies, die niet in aanmerking zijn genomen in de risicobeoordeling. De update heeft dus gevolgen voor de naleving van de essentiële vereisten. De softwaretoepassing is ingrijpend gewijzigd.

Voorbeeld 45: een fabrikant voegt een nieuwe logboek- en diagnosefunctie toe aan een bestaand softwareproduct met digitale elementen, waardoor gedetailleerde systeemlogbestanden kunnen worden geëxporteerd voor probleemoplossingsdoeleinden. Hoewel de functionaliteit gering lijkt, heeft dit tot gevolg dat gevoelige operationele gegevens in een onversleuteld formaat worden verzameld en opgeslagen, waardoor risico's op blootstelling van gegevens ontstaan die niet eerder zijn beoordeeld of beperkt. De wijziging kan daarom aanzienlijke gevolgen hebben voor het cyberbeveiligingsrisicoprofiel van het product met digitale elementen. Het softwareproduct met digitale elementen is ingrijpend gewijzigd.

108. Overeenkomstig overweging 39 van de verordening cyberweerbaarheid mogen beveiligingsupdates over het algemeen niet als ingrijpende wijzigingen worden beschouwd, aangezien zij in de eerste plaats tot doel hebben het niveau van cyberbeveiligingsrisico's in verband met het product met digitale elementen te verminderen. Een beveiligingsupdate die het beoogde doel van dat product niet wijzigt en geen nieuwe cyberbeveiligingsrisico's met zich meebrengt, mag daarom niet als een ingrijpende wijziging worden beschouwd, zelfs niet wanneer die update aanzienlijke technische wijzigingen kan inhouden. Dit houdt onder meer in dat bepaalde functionaliteiten worden gewijzigd of beperkt, uitsluitend met het oog op het beperken van vastgestelde kwetsbaarheden en het waarborgen van de voortdurende naleving van de essentiële vereisten.

Voorbeeld 46: een fabrikant voert een beveiligingsupdate uit om een kwetsbaarheid in de codebase van een product met digitale elementen aan te pakken door een fout bij invoervalidatie te corrigeren die ertoe kan leiden dat de buffer vol loopt, of door een logische fout te verhelpen die het omzeilen van de authenticatie door onjuiste validatie van sessietokens mogelijk maakt. De update wijzigt de interne implementatie van de software zonder het beoogde doel van dat product te beïnvloeden of het aan nieuwe gevaren bloot te stellen. Een dergelijke update is uitsluitend bedoeld om het cyberbeveiligingsrisico te verminderen. De beveiligingsupdate mag niet als een ingrijpende wijziging worden beschouwd.

Voorbeeld 47: een fabrikant introduceert een beveiligingsupdate die de bestaande beveiligingsconfiguraties versterkt, door bijvoorbeeld de firewallregels aan te scherpen, ongebruikte netwerkpoorten te deactiveren, het standaardwachtwoordbeleid van de beheerder te wijzigen of multifactorauthenticatie verplicht te stellen, waarbij een dergelijke functionaliteit reeds beschikbaar of gepland was. Hoewel de update van invloed kan zijn op de wijze waarop gebruikers het product met digitale elementen configureren of er toegang toe hebben, wordt het beoogde doel ervan niet gewijzigd en dient de update uitsluitend om de beveiligingspositie ervan te verbeteren. De beveiligingsupdate mag niet als een ingrijpende wijziging worden beschouwd.

Voorbeeld 48: een fabrikant brengt een softwareproduct in de handel met digitale elementen dat de communicatie beveiligt met behulp van een configureerbaar versleutelingskader ter ondersteuning van meerdere cryptografische algoritmen en sleutelmaten, zoals beschreven in de technische documentatie en risicobeoordeling van het product. De risicobeoordeling heeft betrekking op alle cryptografische opties in het product met digitale elementen en anticipeert op de toekomstige veroudering van bepaalde algoritmen. De risicobeoordeling omvat ook risicobeperkende maatregelen, zoals cryptografische flexibiliteit, intern sleutelbeheer en compatibiliteitstests. Als reactie op opkomende cryptografische richtsnoeren voert de fabrikant een beveiligingsupdate uit die een verouderd algoritme uitschakelt en een sterker, reeds ondersteund alternatief activeert, zonder nieuwe externe afhankelijkheden in te voeren of gegevensstromen te wijzigen. Aangezien de update uitvoering geeft aan een beveiligingsmaatregel die was voorzien en beoordeeld als onderdeel van het oorspronkelijke ontwerp, en geen nieuwe cyberbeveiligingsrisico's met zich meebrengt, mag de beveiligingsupdate niet als een ingrijpende wijziging worden beschouwd.

109. Een beveiligingsupdate kan daarentegen als een ingrijpende wijziging worden aangemerkt indien de update, ondanks de beveiligingsdoelstelling ervan, ertoe leidt dat het beoogde doel van het product met digitale elementen wordt gewijzigd ten opzichte van wat oorspronkelijk was voorzien of nieuwe of verhoogde cyberbeveiligingsrisico's met zich meebrengt. Dit kan bijvoorbeeld het geval zijn wanneer een update de grenzen of afhankelijkheidsstructuur van dat product wezenlijk wijzigt op een wijze die niet in de risicobeoordeling is voorzien, bijvoorbeeld door gegevensstromen wezenlijk te wijzigen of nieuwe extern bereikbare interfaces toe te voegen.

Voorbeeld 49: een fabrikant brengt een softwareproduct met digitale elementen in de handel dat bedoeld is om lokale bestandsversleuteling te bieden voor gegevens die op een apparaat van een gebruiker zijn opgeslagen, zodat gebruikers bestanden op verzoek kunnen versleutelen en ontsleutelen. Na de ontdekking van een kwetsbaarheid in de versleutelingsworkflow voert de fabrikant een beveiligingsupdate uit waarbij de lokale versleutelingsfunctionaliteit wordt verwijderd en in plaats daarvan alle bestanden moeten worden geüpload naar, opgeslagen in en verwerkt door een door de fabrikant beheerde versleutelingsdienst op afstand. Als gevolg van deze wijziging voert het product met digitale elementen niet langer lokale versleuteling uit zoals oorspronkelijk bedoeld, maar functioneert het in plaats daarvan als een versleutelings- en gegevensverwerkingsdienst op afstand. Hoewel de update om veiligheidsredenen wordt uitgevoerd, wordt hiermee het beoogde doel van dat product fundamenteel gewijzigd, op een wijze die niet in de risicobeoordeling is voorzien, en kan de update derhalve als een ingrijpende wijziging worden aangemerkt.

Voorbeeld 50: een fabrikant brengt een softwareproduct met digitale elementen in de handel dat gebaseerd is op een vastgesteld versleutelingsprotocol en een intern beheerde sleutellevenscyclus ter beveiliging van de communicatie tussen componenten van het product met digitale elementen. Als reactie op het vinden van nieuwe zwakke punten in het cryptografiesysteem voert de fabrikant een beveiligingsupdate uit die het bestaande versleutelingsmechanisme vervangt door een ander protocol dat het gebruik van een door een derde beheerde externe sleutelbeheerdienst vereist. Als gevolg van deze wijziging worden de afhankelijkheden en gegevensstromen van het product met digitale elementen wezenlijk gewijzigd, waarbij nieuwe externe interfaces en de afhankelijkheid van diensten van derden worden ingevoerd, die beide in de risicobeoordeling niet in aanmerking zijn genomen. Hoewel de update bedoeld is om de beveiliging te verbeteren, brengt zij nieuwe cyberbeveiligingsrisico's met zich mee en kan zij daarom als een ingrijpende wijziging worden aangemerkt.

110. Zoals vermeld in punt 104, moet per geval worden beoordeeld of een software-update een ingrijpende wijziging vormt. Bij het uitvoeren van deze beoordeling kunnen fabrikanten op niet-uitputtende wijze nagaan of de software-update:

a) nieuwe dreigingsvectoren introduceert, zoals aanvullende interfaces, communicatiekanalen, uitvoeringsomgevingen of externe afhankelijkheden waardoor zich dreigingen kunnen voordoen;

b) nieuwe aanvalsscenario's mogelijk maakt, waaronder bijvoorbeeld nieuwe manieren waarop ongeoorloofde toegang tot, manipulatie van, inmenging in of misbruik van het product met digitale elementen, of van door het product verwerkte gegevens, mogelijk zou kunnen zijn;

c) de waarschijnlijkheid van eerder vastgestelde aanvalsscenario's wijzigt, bijvoorbeeld door de inspanningen of deskundigheid die nodig zijn om van zwakheden misbruik te maken te verminderen, de blootstelling aan onbetrouwbare actoren te vergroten of bestaande waarborgen te verzwakken;

d) de mogelijke gevolgen van eerder vastgestelde aanvalsscenario's wijzigt, met inbegrip van bijvoorbeeld de omvang van de getroffen gegevens of functies, de ernst van de operationele, veiligheidsgerichte of economische gevolgen, of het vermogen om incidenten op te sporen, de gevolgen ervan te beperken of ervan te herstellen.

111. In sommige gevallen worden met een software-update geen nieuwe dreigingsvectoren geïntroduceerd, worden geen nieuwe aanvalsscenario's mogelijk gemaakt en wordt de kans op of ernst van gevolgen van eerder vastgestelde aanvalsscenario's niet wezenlijk groter. Dit kan erop wijzen dat de update geen nieuwe of verhoogde cyberbeveiligingsrisico's met zich meebrengt, op voorwaarde dat de veronderstellingen en risicobeperkende maatregelen waarop de risicobeoordeling is gebaseerd, geldig en doeltreffend blijven. Het is daarom waarschijnlijk dat de update niet als een ingrijpende wijziging kan worden aangemerkt.

112. Omgekeerd kan een software-update nieuwe dreigingsvectoren introduceren, nieuwe aanvalsscenario's mogelijk maken of de kans op of ernst van gevolgen van bestaande aanvalsscenario's wezenlijk wijzigen. In dergelijke gevallen moet de fabrikant de cyberbeveiligingsrisico's van het product met digitale elementen opnieuw beoordelen en bepalen of nog steeds aan de essentiële vereisten wordt voldaan, met inbegrip van de vraag of de update nieuwe of verhoogde risico's met zich meebrengt die niet in de risicobeoordeling zijn opgenomen.

113. Of een software-update als een ingrijpende wijziging kan worden aangemerkt, is relevant om te kunnen bepalen of bepaalde verplichtingen uit hoofde van de verordening cyberweerbaarheid van toepassing zijn, zoals uiteengezet in punt 91. Ongeacht die kwalificatie blijven fabrikanten echter verantwoordelijk voor het waarborgen van de beveiliging van software-updates en van hun product met digitale elementen tijdens de ondersteuningsperiode, overeenkomstig de vereisten inzake de respons op kwetsbaarheden van deel II van bijlage I bij de verordening cyberweerbaarheid. Bovendien moeten fabrikanten, ongeacht of software-updates al dan niet als ingrijpende wijzigingen kunnen worden aangemerkt, de risicobeoordeling en de technische documentatie nauwkeurig, volledig en voortdurend actueel houden, overeenkomstig artikel 13, lid, 7, en artikel 31, lid 2.

4.4. **Gevolgen van een ingrijpende wijziging**

114. De gevolgen van een ingrijpende wijziging die wordt uitgevoerd door een andere actor dan de oorspronkelijke fabrikant van een product met digitale elementen dat reeds in de handel is gebracht, worden behandeld in de artikelen 21 en 22 van de verordening cyberweerbaarheid. Artikel 21 heeft betrekking op importeurs en distributeurs, terwijl artikel 22 betrekking heeft op elke andere natuurlijke of rechtspersoon dan de fabrikant, importeur of distributeur.

115. Wanneer de ingrijpende wijziging wordt uitgevoerd door de oorspronkelijke fabrikant van het product met digitale elementen, vloeien de gevolgen voort uit het algemeen aanvaarde concept van ingrijpende wijziging als bedoeld in overweging 41 van de verordening cyberweerbaarheid en worden zij nader uitgewerkt in punt 2.1 van de Blauwe Gids. In dat punt is bepaald dat een product dat na het in de handel brengen ervan ingrijpende wijzigingen of een revisie heeft ondergaan, als een nieuw product moet worden beschouwd wanneer de oorspronkelijke prestaties, het oorspronkelijke doel of het oorspronkelijke type ervan zijn gewijzigd, de aard van het gevaar is gewijzigd of het risiconiveau is verhoogd, en het product met digitale elementen op de markt wordt aangeboden.

116. Het algemeen vastgestelde gevolg is derhalve dat, wanneer een wijziging van een product met digitale elementen als een ingrijpende wijziging kan worden aangemerkt en het gewijzigde product met digitale elementen op de markt wordt aangeboden, het voor de toepassing van de verordening cyberweerbaarheid als een nieuw product met digitale elementen moet worden behandeld. Bijgevolg wordt het op de markt aanbieden van het ingrijpend gewijzigde product aangemerkt als het nieuw in de handel brengen. Dit geldt ongeacht of de ingrijpende wijziging door de oorspronkelijke fabrikant of door een andere persoon wordt uitgevoerd. Om ervoor te zorgen dat de verordening cyberweerbaarheid op uniforme en evenredige wijze wordt toegepast op de verschillende categorieën actoren die een ingrijpende wijziging kunnen uitvoeren, wordt in de volgende punten ingegaan op de daaruit voortvloeiende verplichtingen van de persoon die de ingrijpende wijziging uitvoert wanneer het ingrijpend gewijzigde product met digitale elementen in de handel wordt gebracht. De gevolgen voor de ondersteuningsperiode van het product met digitale elementen worden behandeld in punt 5, "Ondersteuningsperiode".

4.4.1. *Ingrijpende wijzigingen uitgevoerd door een andere persoon dan de oorspronkelijke fabrikant*

117. Overeenkomstig de artikelen 21 en 22 moet, wanneer een ingrijpende wijziging van een reeds in de handel gebracht product met digitale elementen wordt uitgevoerd door een andere natuurlijke of rechtspersoon dan de fabrikant van het product met digitale elementen, de persoon die de ingrijpende wijziging uitvoert en het gewijzigde product met digitale elementen op de markt aanbiedt, worden beschouwd als de fabrikant van het gewijzigde product met digitale elementen, ongeacht of die persoon betrokken was bij het oorspronkelijke ontwerp of het in de handel brengen van dat product.

118. In artikel 22 wordt verder verduidelijkt dat de persoon die de wijziging uitvoert, alleen onderworpen is aan de verplichtingen van de artikelen 13 en 14 met betrekking tot het deel van het product met digitale elementen waarop de ingrijpende wijziging betrekking heeft, indien die wijziging geen gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel.

119. Wanneer een ingrijpende wijziging gevolgen heeft voor de naleving van de essentiële vereisten, maar geen negatieve gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel, is de persoon die de wijziging uitvoert alleen onderworpen aan de artikelen 13 (met inbegrip van de verplichting om de naleving van de essentiële vereisten te waarborgen en een conformiteitsbeoordelingsprocedure uit te voeren) en 14 (meldingsplicht) met betrekking tot het deel van het product met digitale elementen dat ingrijpend is gewijzigd ([16]). Bovendien blijven de verplichtingen van de oorspronkelijke fabrikant uit hoofde van de verordening cyberweerbaarheid van toepassing op het oorspronkelijke product met digitale elementen dat in de handel wordt gebracht, waardoor de continuïteit van de respons op kwetsbaarheden en de naleving voor de ongewijzigde delen worden gewaarborgd.

120. Een geval van ingrijpende wijziging mag niet worden verward met gevallen van integratie, waarbij een persoon componenten assembleert (onder meer, in voorkomend geval, door ze te wijzigen) tot een nieuw product met digitale elementen dat hij zelf in de handel brengt. In dergelijke gevallen wijzigt de integrerende persoon een product met digitale elementen dat reeds door een andere fabrikant in de handel is gebracht, niet; hij brengt veeleer een nieuw product met eigen digitale elementen in de handel. De integrerende persoon is de fabrikant van dat nieuwe product met digitale elementen voor de toepassing van de verordening cyberweerbaarheid en moet de verordening in haar geheel naleven met betrekking tot het product met digitale elementen als geheel. Wanneer de fabrikant componenten integreert die onder de verordening cyberweerbaarheid vallen, kan hij vertrouwen op de nalevingsactiviteiten van de fabrikanten van componenten om zijn eigen naleving van de verordening cyberweerbaarheid te vergemakkelijken.

Voorbeeld 51: een bedrijf koopt kant-en-klare modules voor microcontrollers en connectiviteitscomponenten van externe leveranciers, ontwikkelt eigen firmware en een sensorpakket en assembleert deze tot een verbonden landbouwmonitoringproduct met digitale elementen dat het onder eigen naam in de handel brengt. Hoewel het bedrijf de onderliggende modules voor de microcontrollers heeft gewijzigd en deze met andere componenten heeft gecombineerd, is dit geen ingrijpende wijziging van het reeds in de handel gebrachte product met digitale elementen; veeleer wordt hier een nieuw product met digitale elementen in de handel gebracht. Het bedrijf is de fabrikant van de landbouwmonitor voor de toepassing van de verordening cyberweerbaarheid en moet de verordening naleven met betrekking tot de landbouwmonitor als geheel.

([16]) In overeenstemming met punt 2.1 van de Blauwe Gids is het "niet noodzakelijk de tests te herhalen en nieuwe documentatie op te stellen voor de aspecten waarop de wijziging geen invloed heeft. Het is de verantwoordelijkheid van de natuurlijke of rechtspersoon die de veranderingen aan het product aanbrengt of laat aanbrengen om aan te tonen dat niet alle elementen van de technische documentatie moeten worden aangepast. De natuurlijke of rechtspersoon die veranderingen aan het product aanbrengt of laat aanbrengen, is verantwoordelijk voor de conformiteit van het gewijzigde product en stelt een conformiteitsverklaring op, zelfs indien hij gebruikmaakt van bestaande tests en technische documentatie".

121. Wanneer een ingrijpende wijziging door een andere persoon dan de oorspronkelijke fabrikant negatieve gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel, bijvoorbeeld omdat de wijziging niet langer gericht is op of beperkt is tot een specifieke component of een specifiek subsysteem, moet het op de markt aangeboden gewijzigde product met digitale elementen worden behandeld als een nieuw product met digitale elementen dat in zijn geheel onder de verordening cyberweerbaarheid valt. In dergelijke gevallen is het algemene cyberbeveiligingsrisicoprofiel van dat product gewijzigd en kan de wijziging niet worden beoordeeld zonder het product met digitale elementen als geheel in aanmerking te nemen. De persoon die de wijziging uitvoert, is onderworpen aan de in de artikelen 13 en 14 vastgestelde verplichtingen van de fabrikant met betrekking tot het gewijzigde product met digitale elementen als geheel.

4.4.2. *Door de oorspronkelijke fabrikant uitgevoerde ingrijpende wijzigingen*

122. Wanneer de ingrijpende wijziging wordt uitgevoerd door de oorspronkelijke fabrikant, onder meer in het kader van de iteratieve ontwikkeling van softwareproducten met digitale elementen, blijft die fabrikant de fabrikant voor de toepassing van de verordening cyberweerbaarheid. Het ingrijpend gewijzigde product met digitale elementen moet echter worden beschouwd als nieuw in de handel gebracht.

123. Overeenkomstig punt 2.1 van de Blauwe Gids kan de oorspronkelijke fabrikant die het ingrijpend gewijzigde product met digitale elementen in de handel brengt, bestaande documentatie en tests hergebruiken voor aspecten van het product met digitale elementen waarop de ingrijpende wijziging geen invloed heeft. Met name wanneer de fabrikant ingrijpend gewijzigde versies van hetzelfde product met digitale elementen in de handel brengt, moet de conformiteitsbeoordelingsprocedure gericht zijn op de ingrijpend gewijzigde delen van het product met digitale elementen. Evenzo moet de conformiteitsbeoordelingsinstantie, wanneer een conformiteitsbeoordeling door een derde partij wordt uitgevoerd, haar beoordeling toespitsen op de ingrijpend gewijzigde delen. Voor ongewijzigde delen van het product met digitale elementen kunnen bestaande documentatie en testresultaten worden hergebruikt.

124. De in het vorige punt uiteengezette evenredigheidsoverwegingen zijn ook van toepassing op ingrijpende wijzigingen die worden uitgevoerd door de oorspronkelijke fabrikant van een product met digitale elementen dat vóór 11 december 2027 in de handel is gebracht. Een dergelijke ingrijpende wijziging door de oorspronkelijke fabrikant vereist op zich niet dat de fabrikant het volledige product met digitale elementen dat vóór die datum in de handel is gebracht, volledig in overeenstemming brengt met de verordening cyberweerbaarheid, tenzij de wijziging negatieve gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel. Indien de wijziging geen gevolgen heeft voor de cyberbeveiliging van het product met digitale elementen als geheel, moeten de verplichtingen van de oorspronkelijke fabrikant met betrekking tot de wijziging worden beperkt tot de ingrijpend gewijzigde onderdelen.

5. **ONDERSTEUNINGSPERIODE**

125. Op grond van artikel 13, lid 8, van de verordening cyberweerbaarheid moeten fabrikanten de ondersteuningsperiode bepalen waarin de kwetsbaarheden van het product met digitale elementen, met inbegrip van de componenten ervan, doeltreffend en in overeenstemming met de essentiële vereisten van deel II van bijlage I worden aangepakt. De ondersteuningsperiode weerspiegelt de periode waarin het product met digitale elementen naar verwachting in gebruik zal zijn (de verwachte gebruikstijd), en moet worden bepaald in het licht van de criteria van artikel 13, lid 8, met name de redelijke verwachtingen van gebruikers, de aard van het product met digitale elementen, met inbegrip van het beoogde doel ervan, en het relevante Unierecht dat de levensduur van producten met digitale elementen bepaalt ([17]). Al met al moeten dergelijke criteria in aanmerking worden genomen op een wijze die de evenredigheid bij het bepalen van de ondersteuningsperiode waarborgt.

([17]) Er kan rekening worden gehouden met aanvullende criteria, overeenkomstig artikel 13, lid 8, zoals de ondersteuningsperioden voor producten met digitale elementen met een soortgelijke functionaliteit die door andere fabrikanten in de handel worden gebracht, de beschikbaarheid van de operationele omgeving, de ondersteuningsperioden voor geïntegreerde componenten die kernfuncties leveren en afkomstig zijn van derden, alsook relevante richtsnoeren van de bij de verordening cyberweerbaarheid opgerichte speciale administratieve-samenwerkingsgroep (ADCO) en de Commissie.

126. In artikel 13, lid 8, is voorts bepaald dat de ondersteuningsperiode ten minste vijf jaar moet bedragen, tenzij het product met digitale elementen naar verwachting minder dan vijf jaar in gebruik zal zijn, in welk geval de ondersteuningsperiode overeenkomt met de verwachte gebruikstijd. De minimale ondersteuningsperiode fungeert daarom alleen als waarborg en zorgt ervoor dat kwetsbaarheden gedurende een voldoende lange periode worden aangepakt, terwijl fabrikanten rekening kunnen houden met producten met digitale elementen met werkelijk kortere verwachte gebruikstijden. Overweging 60 bevat meer richtsnoeren in dit verband en hierin wordt verduidelijkt dat producten met digitale elementen waarvan redelijkerwijs kan worden verwacht dat zij langer dan vijf jaar in gebruik zullen zijn, dienovereenkomstig langere ondersteuningsperioden moeten hebben. Een ondersteuningsperiode van vijf jaar mag daarom niet worden beschouwd als de standaardperiode voor alle producten met digitale elementen. In plaats daarvan moet de fabrikant een passende ondersteuningsperiode bepalen in het licht van de in artikel 13, lid 8, bedoelde criteria.

127. Op grond van artikel 13, lid 19, moeten fabrikanten op het moment van aankoop op duidelijke en begrijpelijke wijze de einddatum van de ondersteuningsperiode (ten minste de maand en het jaar) vermelden. Ook moeten fabrikanten na afloop van de ondersteuningsperiode een kennisgeving aan gebruikers tonen, indien dit technisch haalbaar is in het licht van de aard van het product met digitale elementen. Deze verplichting is bedoeld om gebruikers transparantie te bieden met betrekking tot hoelang zij beveiligingsondersteuning kunnen verwachten.

128. In het geval van softwareproducten met digitale elementen, die vaak iteratief worden ontwikkeld en uitgebracht en waarbij in de loop van de tijd vaak ingrijpend gewijzigde versies in de handel kunnen worden gebracht, moet de ondersteuningsperiode worden uitgelegd in het licht van dit ontwikkelingsmodel. Voor elke ingrijpend gewijzigde versie van een softwareproduct met digitale elementen dat in de handel wordt gebracht, moet een ondersteuningsperiode worden vermeld die voldoet aan artikel 13, lid 8. Dit omvat de minimale ondersteuningsperiode van ten minste vijf jaar, tenzij de verwachte gebruikstijd van die versie aantoonbaar korter is, zoals ook wordt verduidelijkt in overweging 60. In punt *5.1*, "Ingrijpende wijzigingen en de ondersteuningsperiode", wordt verder verduidelijkt dat wanneer de ingrijpende wijziging niet leidt tot veranderingen in de factoren die oorspronkelijk de verwachte gebruiksduur van het product met digitale elementen hebben bepaald, de oorspronkelijke ondersteuningsperiode ongewijzigd blijft (d.w.z. ook in gevallen waarin de resterende ondersteuningsperiode minder dan vijf jaar bedraagt).

129. Artikel 13, lid 10, biedt flexibiliteit voor softwareproducten met digitale elementen door fabrikanten onder bepaalde voorwaarden toe te staan de naleving van het vereiste inzake de respons op kwetsbaarheden van deel II, punt 2, van bijlage I (kwetsbaarheden aanpakken en verhelpen) te waarborgen, alleen voor de versie van het softwareproduct met digitale elementen die het laatst in de handel is gebracht. Dit is toegestaan wanneer gebruikers van eerder in de handel gebrachte versies kosteloos toegang hebben tot de laatst in de handel gebrachte versie en geen extra kosten hoeven te maken om de hardware- en softwareomgeving waarin zij de oorspronkelijke versie van dat product gebruiken, aan te passen.

130. Voor de toepassing van artikel 13, lid 10, moet het begrip "extra kosten" op praktische en evenredige wijze worden uitgelegd, rekening houdend met normale en verwachte praktijken op het gebied van het onderhoud en de werking van de software. Het gaat hierbij niet om redelijke operationele inspanningen die inherent zijn aan de toepassing van software-updates of het onderhoud van een beveiligde operationele omgeving, zoals arbeidstijd van personeel, regelmatige tests, aanpassingen van de configuratie of upgrades van onderliggende softwareafhankelijkheden die nodig zijn voor componenten die het einde van hun levensduur hebben bereikt of voor het aanpakken van bekende kwetsbaarheden in de beveiliging. Met "extra kosten" worden daarentegen lasten bedoeld die verder gaan dan wat normaal gesproken kan worden verwacht in het kader van software-updates, zoals de verplichte aankoop van nieuwe hardware, de vervanging van infrastructuur of fundamentele veranderingen in de operationele omgeving.

131. Voor voortdurend evoluerende softwareproducten met digitale elementen kunnen fabrikanten met relatief korte tussenpozen opeenvolgende ingrijpend gewijzigde versies in de handel brengen en verwachten dat gebruikers deze regelmatig upgraden. In dergelijke gevallen moet de opgegeven ondersteuningsperiode voor elke ingrijpend gewijzigde versie voldoen aan artikel 13, lid 8, op het moment dat deze versie in de handel wordt gebracht. Met andere woorden, de fabrikant moet voor die ingrijpend gewijzigde versie een nieuwe ondersteuningsperiode opgeven. Fabrikanten kunnen echter een beroep doen op artikel 13, lid 10, om kwetsbaarheden voor eerdere versies niet langer aan te pakken en te verhelpen zodra gebruikers kosteloos en zonder extra kosten zoals

hierboven vermeld kunnen upgraden naar een recentere versie, zelfs als dit leidt tot een kortere doeltreffende ondersteuningsperiode voor die eerdere versies ([18]). De fabrikant blijft onderworpen aan de andere eisen inzake de respons op kwetsbaarheden van deel II van bijlage I, en aan de meldingsplicht van artikel 14. Zoals ook uiteengezet in overweging 40, omvatten deze vereisten voor alle daaropvolgende ingrijpend gewijzigde versies van het in de handel gebrachte softwareproduct met digitale elementen onder meer: i) de beschikking over een beleid inzake de gecoördineerde bekendmaking van kwetsbaarheden, en ii) maatregelen om het delen van informatie over mogelijke kwetsbaarheden te vergemakkelijken ([19]).

Voorbeeld 52: een fabrikant brengt een model smartphone in de EU in de handel en geeft een ondersteuningsperiode van X jaar aan vanaf de datum van het in de handel brengen, waarin de fabrikant beveiligingsupdates verstrekt om kwetsbaarheden aan te pakken. Tijdens die periode brengt de fabrikant regelmatig software-updates en ingrijpend gewijzigde versies van het besturingssysteem uit, die gebruikers kosteloos kunnen installeren zonder dat nieuwe hardware nodig is.

De fabrikant kan overeenkomstig artikel 13, lid 10, kwetsbaarheden aanpakken en verhelpen voor de meest recente versie van het besturingssysteem die voor dat model smartphone beschikbaar wordt gesteld, op voorwaarde dat het mogelijk is eerdere versies kosteloos en zonder extra kosten te upgraden. Voor de duur van de ondersteuningsperiode blijft de fabrikant onderworpen aan de andere vereisten inzake de respons op kwetsbaarheden, zoals gecoördineerde bekendmaking van kwetsbaarheden en maatregelen voor het delen van informatie over mogelijke kwetsbaarheden.

Voorbeeld 53: een fabrikant brengt een "enterprise"-softwareproduct met digitale elementen in de handel en publiceert om de paar maanden ingrijpend gewijzigde versies waarin verbeteringen van de beveiliging, nieuwe functionaliteiten en compatibiliteit met geactualiseerde besturingssystemen en platforms tot uiting komen. Elke versie wordt in de handel gebracht met een opgegeven ondersteuningsperiode overeenkomstig artikel 13, lid 8. De fabrikant verwacht van de gebruikers dat zij als onderdeel van hun normale gebruik regelmatig een upgrade uitvoeren en biedt gratis toegang tot de meest recente versie. Het uitvoeren van upgrades kan een redelijke operationele inspanning vergen, zoals tests of configuratieaanpassingen, maar brengt geen extra kosten met zich mee, zoals de aankoop van nieuwe hardware of fundamentele wijzigingen in de infrastructuur. In dit verband kan de fabrikant een beroep doen op artikel 13, lid 10, om kwetsbaarheden voor eerdere versies niet langer aan te pakken en te verhelpen zodra gebruikers kunnen upgraden naar de meest recente versie, en tegelijkertijd voor alle latere ingrijpend gewijzigde versies te blijven voldoen aan de andere eisen inzake de respons op kwetsbaarheden.

5.1. **Ingrijpende wijzigingen en de ondersteuningsperiode**

132. Zoals uiteengezet in punt 4.4, "Gevolgen van een ingrijpende wijziging", moet een wijziging van een product met digitale elementen die als een ingrijpende wijziging kan worden aangemerkt en het gewijzigde product met digitale elementen op de markt wordt aangeboden, voor de toepassing van de verordening cyberweerbaarheid als een nieuw product worden behandeld, en wordt het op de markt aanbieden van het ingrijpend gewijzigde product met digitale elementen beschouwd als nieuw in de handel brengen. Daarom is het nuttig te verduidelijken welk effect dit nieuwe in de handel brengen heeft op de ondersteuningsperiode van het ingrijpend gewijzigde product met digitale elementen.

133. De ondersteuningsperiode van een ingrijpend gewijzigd product met digitale elementen moet worden bepaald op basis van de verwachte gebruikstijd van dat product, in het licht van de criteria van artikel 13, lid 8, van de verordening cyberweerbaarheid. Een ingrijpende wijziging moet daarom opnieuw worden beoordeeld aan de hand van die criteria, maar leidt niet automatisch tot een herziening of zelfs verlenging van de ondersteuningsperiode. De relevante vraag is of de ingrijpende wijziging van invloed is op de factoren die oorspronkelijk bepalend waren voor de verwachte gebruikstijd van dat product en dus voor de oorspronkelijke ondersteuningsperiode.

([18]) Er zij aan herinnerd dat fabrikanten overeenkomstig artikel 13, lid 19, indien dat in verband met de aard van het product met digitale elementen technisch haalbaar is, verplicht zijn gebruikers door de weergave van een notificatie ervan op de hoogte te stellen dat hun product met digitale elementen het einde van de ondersteuningsperiode heeft bereikt. Daarom wordt verwacht dat wanneer het aanpakken en verhelpen van kwetsbaarheden voor eerdere versies wordt stopgezet, gebruikers die geen upgrade naar de nieuwste versie hebben uitgevoerd, worden geïnformeerd, indien dit technisch haalbaar is.

([19]) Er zij op gewezen dat wanneer gebruikers zonder extra kosten kunnen upgraden naar de meest recente versie van de software, fabrikanten er niettemin voor kunnen kiezen kwetsbaarheden in eerdere versies van die software te blijven aanpakken en verhelpen, eventueel tegen betaling of in het kader van andere commerciële regelingen. De verordening cyberweerbaarheid verplicht fabrikanten niet om kosteloos beveiligingsupdates voor dergelijke eerdere versies te verstrekken.

134. Indien de ingrijpende wijziging geen invloed heeft op die factoren, blijven de criteria van artikel 13, lid 8, wijzen op dezelfde verwachte gebruikstijd als oorspronkelijk bepaald, en moet de ondersteuningsperiode van het gewijzigde product met digitale elementen in overeenstemming zijn met de resterende verwachte gebruikstijd van het product zoals oorspronkelijk in de handel gebracht. Dit zal doorgaans het geval zijn wanneer de verwachte gebruikstijd voornamelijk is bepaald op grond van factoren die door de wijziging niet veranderen, zoals de fysieke duurzaamheid van hardwarecomponenten, waarbij de ingrijpende wijziging alleen betrekking heeft op de softwarefunctionaliteit of back-enddiensten.

Voorbeeld 54: een fabrikant brengt een robotstofzuiger in de handel met een verwachte gebruiksduur van X jaar, bepaald op basis van de aard van het product met digitale elementen, met inbegrip van de kenmerken op het gebied van fysieke duurzaamheid en slijtage van de hardwarecomponenten, en rekening houdend met redelijke verwachtingen van de gebruiker ten aanzien van de levensduur van dat product. De fabrikant stelt de ondersteuningsperiode vast op X jaar. Na Y jaar brengt de fabrikant een software-update uit die kan worden aangemerkt als een ingrijpende wijziging, waarbij nieuwe schoonmaakmodi en navigatiekenmerken worden toegevoegd. De software-update heeft geen invloed op de fysieke duurzaamheid van de hardware en heeft geen verandering van redelijke verwachtingen van de gebruiker ten aanzien van de levensduur van dat product tot gevolg. De criteria van artikel 13, lid 8, geven dus nog steeds dezelfde verwachte gebruikstijd aan. De ondersteuningsperiode van het gewijzigde product met digitale elementen is in overeenstemming met de resterende verwachte gebruikstijd zoals oorspronkelijk bepaald.

Voorbeeld 55: een fabrikant brengt een complex product met digitale elementen voor een industrieel apparaat in de handel, met een back-end in de cloud die een oplossing voor gegevensverwerking op afstand vormt. De verwachte gebruiksduur is X jaar, bepaald in het licht van redelijke verwachtingen van de gebruiker en de aard van het product met digitale elementen, zoals de fysieke duurzaamheid van de hardware van het apparaat en de verwachte slijtage. De ondersteuningsperiode wordt afgestemd op die verwachte gebruikstijd en bepaald op X jaar. Na Y jaar herstructureert de fabrikant de back-end in de cloud (de oplossing voor gegevensverwerking op afstand), waarbij nieuwe API's en gegevensstromen worden ingevoerd op een wijze die kan worden aangemerkt als een ingrijpende wijziging van het product met digitale elementen, maar waarbij de aard van dat product niet wordt gewijzigd en de verwachtingen van de gebruiker niet worden beïnvloed. De criteria van artikel 13, lid 8, geven dus nog steeds dezelfde verwachte gebruikstijd aan. De ondersteuningsperiode van het gewijzigde product met digitale elementen is in overeenstemming met de resterende verwachte gebruikstijd zoals oorspronkelijk bepaald.

135. Indien de ingrijpende wijziging van invloed is op de factoren die oorspronkelijk de verwachte gebruikstijd van het product met digitale elementen hebben bepaald, moet de fabrikant de ondersteuningsperiode opnieuw berekenen om de nieuwe verwachte gebruikstijd weer te geven, waarbij hij de criteria van artikel 13, lid 8, dienovereenkomstig toepast. Dit kan bijvoorbeeld het geval zijn bij het revitaliseren van hardwarewijzigingen die de operationele levensduur van dat product verlengen, of bij een ingrijpende herprogrammering of herschrijving van de basissoftware van dat product, waardoor de verwachte gebruikstijd ervan wezenlijk wijzigt ([20]).

Voorbeeld 56: een fabrikant brengt een programmeerbare logische controller (PLC) in de handel met een verwachte gebruiksduur van X jaar, die voornamelijk wordt bepaald op basis van de aard van het product met digitale elementen en de duurzaamheid van de onderliggende hardware. De ondersteuningsperiode wordt dienovereenkomstig vastgesteld. Enkele jaren na het voor het eerst in de handel brengen, voert de fabrikant een ingrijpende wijziging uit die bestaat in de vervanging van het ingebedde computerplatform van de PLC, met inbegrip van de processor, het geheugen en de runtime-omgeving, door een nieuwe generatie componenten die zijn ontworpen om aanzienlijk langer mee te gaan. Als gevolg van de wijziging veranderen de redelijke verwachtingen van gebruikers en de aard van het product met digitale elementen: de gebruiker van de PLC kan nu redelijkerwijs verwachten dat de PLC ook ná de oorspronkelijk opgegeven verwachte gebruikstijd, ondersteund door het nieuwe computerplatform, in gebruik zal zijn. De criteria van artikel 13, lid 8, wijzen daarom op een langere verwachte gebruikstijd en de fabrikant herberekent de ondersteuningsperiode voor die specifieke PLC dienovereenkomstig.

6. **BELANGRIJKE EN KRITIEKE PRODUCTEN MET DIGITALE ELEMENTEN**

136. In artikel 7, lid 1, van de verordening cyberweerbaarheid is bepaald dat producten met digitale elementen die de belangrijkste functionaliteit van een in bijlage III bij de verordening vermelde productcategorie hebben, worden beschouwd als "belangrijke producten met digitale elementen". In bijlage III worden belangrijke producten met digitale elementen verder onderverdeeld in klasse I en klasse II. Evenzo is in artikel 8, lid 1, bepaald dat producten met digitale elementen die de basisfunctionaliteit van een in bijlage IV bij de verordening cyberweerbaarheid vermelde productcategorie hebben, worden beschouwd als "kritieke producten met digitale elementen" ([21]).

([20]) Er zij aan herinnerd dat, zoals aangegeven in punt *4.1*, "Fysieke reparatie", opknap-, onderhouds- of reparatiewerkzaamheden over het algemeen niet als ingrijpende wijzigingen worden beschouwd.

([21]) Uitvoeringsverordening (EU) 2025/2392 van de Commissie bevat de technische beschrijving van de categorieën belangrijke en kritieke producten.

137. De indeling van een product met digitale elementen als belangrijk of kritiek of, omgekeerd, als behorend tot de standaardcategorie ([22]), is van belang bij het bepalen van de conformiteitsbeoordelingsprocedure die de fabrikant overeenkomstig artikel 32 moet volgen voordat hij dat product met digitale elementen in de handel kan brengen. Met name met betrekking tot producten met digitale elementen in de standaardcategorie kan altijd worden vertrouwd op de internecontroleprocedure op basis van module A ("zelfbeoordeling") ([23]). Belangrijke producten met digitale elementen van klasse I of II en kritieke producten met digitale elementen zijn onderworpen aan strengere conformiteitsbeoordelingsprocedures. Dit omvat geen belangrijke in de handel gebrachte producten met digitale elementen van klasse I of II die als vrije en opensourcesoftware kunnen worden aangemerkt, waarvoor fabrikanten overeenkomstig artikel 32, lid 5, de procedures van de standaardcategorie mogen volgen.

138. Het begrip basisfunctionaliteit is daarom essentieel voor de fabrikant om de toepasselijke conformiteitsbeoordelingsregeling te bepalen. Dit begrip wordt in de verordening cyberweerbaarheid echter niet expliciet gedefinieerd. Producten met digitale elementen kunnen een reeks functies vervullen, waarvan sommige een aanvulling kunnen vormen op de basisfunctionaliteit van dat product, en die geen invloed zouden moeten hebben op de indeling van het product als standaard/belangrijk klasse I/belangrijk klasse II/kritiek. Het is daarom nuttig meer richtsnoeren te verstrekken om fabrikanten te helpen de relevante conformiteitsbeoordelingsprocedures correct uit te voeren en om markttoezichtautoriteiten te helpen de geharmoniseerde handhaving van de verordening cyberweerbaarheid in de hele EU te waarborgen.

6.1. **Basisfunctionaliteit**

139. De basisfunctionaliteit van een product met digitale elementen heeft betrekking op de basiskenmerken en technische capaciteiten van dat product, zonder welke het niet zou kunnen voldoen aan het beoogde doel ervan. Dit kan worden beoordeeld in het licht van de specifieke context en gebruiksvoorwaarden van het product, waarbij onder meer rekening wordt gehouden met de informatie die de fabrikant verstrekt in de gebruiksinstructies, de promotie- of verkoopmaterialen en verklaringen, alsook in de technische documentatie.

Voorbeeld 57: een softwareproduct met digitale elementen biedt een abstractielaag boven op de onderliggende hardware en beheert de uitvoering van softwarecomponenten. De belangrijkste kenmerken ervan zijn het inschakelen van hardware en randapparatuur, proces- en geheugenbeheer, input-outputcontrole, planning, toewijzing van middelen en het openzetten van systeemdiensten en applicatieprogramma-interfaces (API's) om interactie tussen applicaties en de hardware- en softwarehulpbronnen van het apparaat mogelijk te maken. Uit de technische documentatie blijkt dat het product met digitale elementen computercapaciteit regelt, systeemconfiguraties handhaaft en gestandaardiseerde interfaces biedt voor softwaremodules en aangesloten randapparatuur. De fabrikant benadrukt dat deze functionaliteiten het platform in staat stellen te fungeren als de centrale softwareomgeving waarop applicaties op betrouwbare wijze kunnen draaien. Het product met digitale elementen heeft de basisfunctionaliteit van een besturingssysteem, zoals beschreven in punt 11 van bijlage I bij Uitvoeringsverordening (EU) 2025/2392.

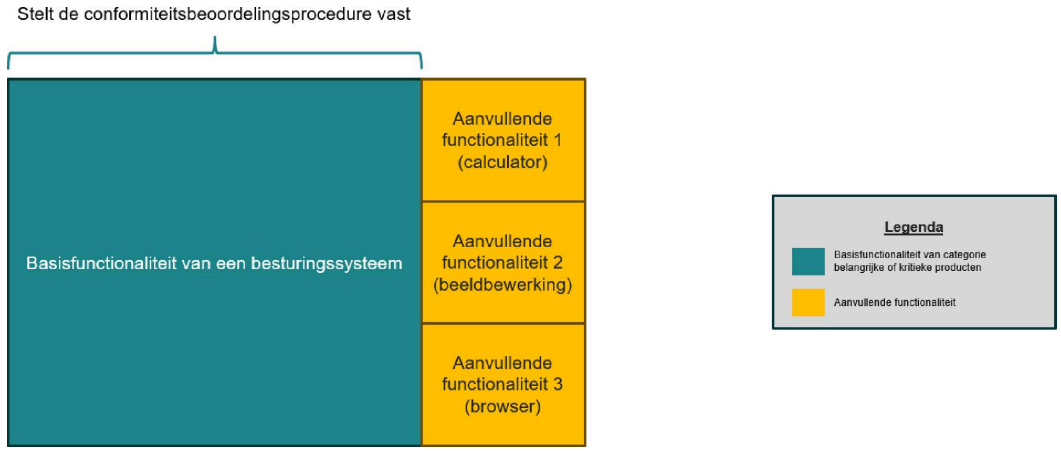
140. De functionaliteit van een product met digitale elementen is zelden beperkt tot de basisfunctionaliteit ervan, aangezien producten met digitale elementen vaak — zo niet altijd — aanvullende functies vervullen die niet bijdragen tot de basisfunctionaliteit van het product. Dit kan ook inhouden dat componenten worden geïntegreerd die zelf de functionaliteit hebben van een ander belangrijk of kritiek product met digitale elementen. Het feit dat een product met digitale elementen andere of aanvullende functies vervult dan die welke zijn beschreven in de technische beschrijvingen van belangrijke of kritieke producten met digitale elementen, belet op zich echter niet dat het product een dergelijke basisfunctionaliteit heeft.

([22]) De standaardcategorie is als begrip niet gedefinieerd in de verordening cyberweerbaarheid. Het gebruik van het begrip in dit document heeft betrekking op producten met digitale elementen die niet de basisfunctionaliteit hebben van een productcategorie die is opgenomen in de bijlagen III of IV bij de verordening cyberweerbaarheid, en die bijgevolg onderworpen zijn aan de conformiteitsbeoordelingsregeling van artikel 32, lid 1.

([23]) De fabrikant kan er niettemin altijd voor kiezen een strengere conformiteitsbeoordelingsprocedure toe te passen, zoals bepaald in artikel 32, lid 1.

Figuur 2:

illustratie van de wijze waarop de basisfunctionaliteit, en niet de aanvullende functionaliteiten, de toepasselijke conformiteitsbeoordelingsprocedure bepaalt



141. Een product met digitale elementen kan de functies van een belangrijke of kritieke productcategorie vervullen, maar toch een andere basisfunctionaliteit hebben dan die van een dergelijke productcategorie. In die gevallen zou dat product met digitale elementen niet kunnen worden aangemerkt als een belangrijk of kritiek product met digitale elementen. Zoals uitdrukkelijk vermeld in artikel 7, lid 1, van de verordening cyberweerbaarheid voor belangrijke producten met digitale elementen (en met toepassing van dezelfde logica voor kritieke producten met digitale elementen), maakt de loutere integratie van een belangrijk of kritiek product met digitale elementen het product met digitale elementen op zich niet tot een belangrijk of kritiek product met digitale elementen.

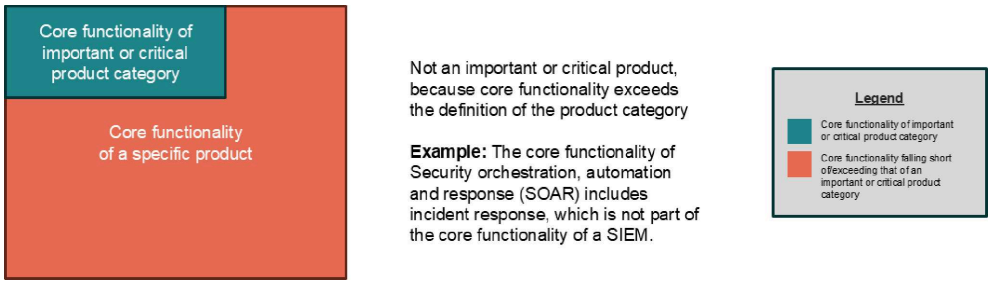
Voorbeeld 58: een smartphone integreert een besturingssysteem dat de in punt 11 van bijlage I bij Uitvoeringsverordening (EU) 2025/2392 beschreven functies biedt. Hoewel het besturingssysteem het beheer van hardware en de uitvoering van softwaretoepassingen mogelijk maakt, heeft de smartphone als geheel een andere basisfunctionaliteit (bv. die om gebruikers in staat te stellen te communiceren en toegang te krijgen tot informatie en diensten). De loutere integratie van een besturingssysteem betekent niet dat de smartphone de basisfunctionaliteit van een besturingssysteem heeft.

142. Sommige producten met digitale elementen kunnen vergelijkbaar zijn met een belangrijke of kritieke productcategorie of tot dezelfde algemene productfamilie behoren, maar hun basisfunctionaliteit kan aanzienlijk breder zijn dan of aanzienlijk achterblijven bij de basisfunctionaliteit van die categorie. Dit is niet het geval wanneer een product met digitale elementen aanvullende functionaliteiten bevat die louter de basisfunctionaliteit aanvullen of verbeteren, die zelf overeenkomt met die uit de categorie belangrijke of kritieke producten; in dergelijke gevallen behoudt het product met digitale elementen de basisfunctionaliteit van die categorie en wordt het dienovereenkomstig ingedeeld. Deze beoordeling moet gebaseerd zijn op de basiskenmerken en technische capaciteiten van dat product, objectief beschouwd in het licht van het beoogde doel ervan, en niet op de wijze waarop het product met digitale elementen wordt beschreven of in de handel wordt gebracht, indien die beschrijving de werkelijke technische kenmerken van het product niet weerspiegelt.

Voorbeeld 59: software voor beveiliging, automatisering en respons (SOAR) kan vaak de functies vervullen van producten met digitale elementen in de categorie "Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)", d.w.z. uit meerdere bronnen gegevens verzamelen, deze gegevens analyseren en correleren en ze dan presenteren als bruikbare informatie voor beveiligingsdoeleinden. De basisfunctionaliteit van de software is echter aanzienlijk breder dan die van een SIEM, en omvat ook diensten zoals incidentrespons als basiselementen van de technische capaciteiten ervan. Daarom wordt SOAR-software over het algemeen niet geacht de basisfunctionaliteit van SIEM-systemen te hebben.

Figuur 3:

illustratie van de basisfunctionaliteit van een product met digitale elementen die aanzienlijk verder gaat dan de definitie van een belangrijke of kritieke productcategorie



Voorbeeld 60: bepaalde instrumenten voor het verzamelen en visualiseren van logbestanden hebben de mogelijkheid om loggegevens te verwerken en basisdashboards met systeemgebeurtenissen weer te geven. Hoewel deze instrumenten activiteiten op het gebied van beveiligingsmonitoring kunnen ondersteunen, blijft hun basisfunctionaliteit achter bij die van SIEM-systemen, aangezien zij geen gegevenscorrelatie uitvoeren en evenmin bruikbare beveiligingsinzichten verschaffen. Daarom mogen dergelijke instrumenten over het algemeen niet worden geacht de basisfunctionaliteit van SIEM-systemen te hebben.

Figuur 4:

illustratie van de basisfunctionaliteit van een product met digitale elementen die aanzienlijk achterblijft bij de definitie van een belangrijke of kritieke productcategorie

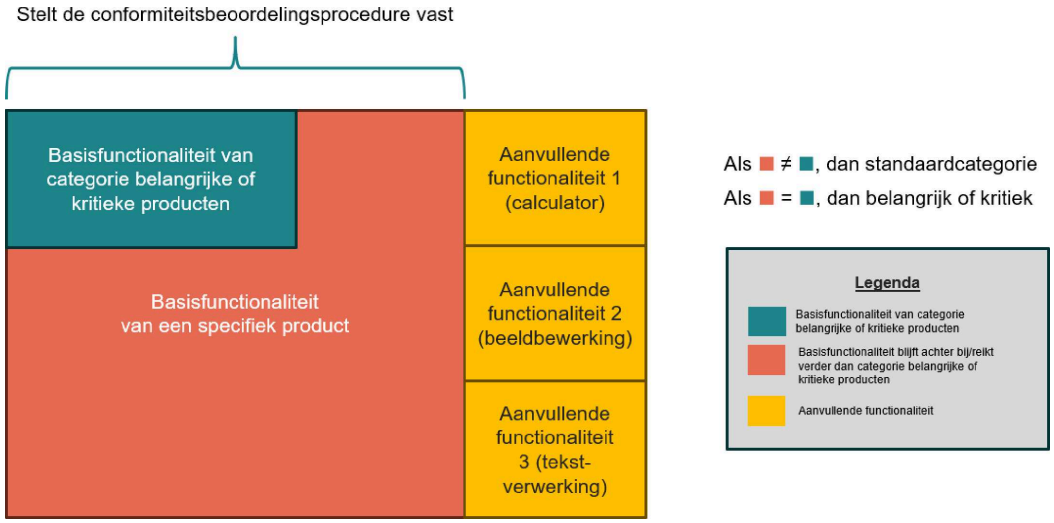


143. Een fabrikant mag de basisfunctionaliteit van zijn product met digitale elementen niet verkeerd voorstellen om de conformiteitsbeoordelingsregeling te omzeilen die van toepassing is op belangrijke of kritieke producten met digitale elementen, bijvoorbeeld door de rol van bepaalde functionaliteiten veel groter of juist kleiner te maken, zodat het product aanzienlijk breder is dan of achterblijft bij een bepaalde basisfunctionaliteit. Dit zou bijvoorbeeld het geval zijn wanneer er duidelijke inconsistenties zijn tussen promotiemateriaal, de gebruikshandleiding en technische documentatie.

144. Een product met digitale elementen mag voor het bepalen van de toepasselijke conformiteitsbeoordelingsregeling niet meer dan één basisfunctionaliteit hebben. Overeenkomstig bijlage VII bij de verordening cyberweerbaarheid moeten fabrikanten, als onderdeel van de technische documentatie van een product, het beoogde doel van hun product met digitale elementen en de door hen gevolgde conformiteitsbeoordelingsprocedure beschrijven. De basisfunctionaliteit van het product moet daarom duidelijk worden omschreven. Dit maakt het mogelijk de toepasselijke conformiteitsbeoordelingsregeling correct vast te stellen en stelt markttoezichtautoriteiten in staat hierop toezicht te houden en te controleren of de verordening correct wordt toegepast.

Figuur 5:

illustratie van de wijze waarop de basisfunctionaliteit van een specifiek product met digitale elementen de productklasse en dus de toepasselijke conformiteitsbeoordelingsprocedure bepaalt



145. Sommige producten met digitale elementen worden in de handel gebracht als afzonderlijke producten met digitale elementen, maar bestaan uit afzonderlijke modules met afzonderlijke functionaliteiten. Wanneer een fabrikant die modules ook afzonderlijk op de markt aanbiedt, zoals wanneer zij als afzonderlijke aankoop, licentie of abonnement worden aangeboden, vormen die modules opzichzelfstaande producten met digitale elementen op zich. Als zodanig moeten zij worden ingedeeld op basis van hun respectieve basisfuncties (en dus worden onderworpen aan de passende conformiteitsbeoordelingsregeling op basis van de basisfuncties van elke module). Dit doet geen afbreuk aan modules die uitsluitend als componenten van een geïntegreerd product met digitale elementen worden geleverd en niet afzonderlijk op de markt worden aangeboden; in dergelijke gevallen wordt de basisfunctionaliteit bepaald op het niveau van het geïntegreerde product met digitale elementen.

Voorbeeld 61: een fabrikant brengt een uniform beveiligingspakket in de handel dat meerdere modules combineert, waaronder een SIEM, een inbraakdetectiesysteem en een analysemodule. De fabrikant biedt deze modules ook aan in de vorm van afzonderlijke abonnementen. In dit scenario is elke module een afzonderlijk product met digitale elementen en wordt zij ingedeeld op basis van haar eigen basisfunctionaliteit. De SIEM-module is onderworpen aan de conformiteitsbeoordelingsregeling voor belangrijke producten met digitale elementen van klasse I, aangezien de basisfunctionaliteit ervan die van "Security information and event management-systemen (SIEM) (beveiligingsinformatie en evenementenbeheer)" is. Het inbraakdetectiesysteem is onderworpen aan de conformiteitsbeoordelingsregeling voor belangrijke producten met digitale elementen van klasse II, aangezien de basisfunctionaliteit ervan die van "Firewalls, intrusion detection and prevention systems (firewalls, inbraakdetectiesystemen en inbraakpreventiesystemen)" is. De analysemodule is onderworpen aan de conformiteitsbeoordelingsregeling voor "standaardproducten" met digitale elementen, aangezien de basisfunctionaliteit ervan niet die van een categorie belangrijke of kritieke producten is.

146. Niet-naleving van de verplichtingen van artikel 32 van de verordening cyberweerbaarheid kan leiden tot administratieve geldboeten overeenkomstig artikel 64, lid 3.

6.2. Conformiteitsbeoordeling voor belangrijke en kritieke producten met digitale elementen

147. Zodra de fabrikant de basisfunctionaliteit van zijn product met digitale elementen heeft bepaald, moet hij een van de toepasselijke conformiteitsbeoordelingsprocedures uitvoeren. De fabrikant moet ervoor zorgen dat het product met digitale elementen als geheel aan de essentiële vereisten voldoet, in voorkomend geval rekening houdend met de beveiliging van de componenten of functionaliteiten die erin zijn geïntegreerd.

148. Een strengere conformiteitsbeoordelingsprocedure, waar een derde bij betrokken is (op basis van module B + C, module H of regelingen voor cyberbeveiligingscertificering), is verplicht voor belangrijke producten met digitale elementen van klasse II (met uitzondering van producten die overeenkomstig artikel 32, lid 5, als vrije en opensourcesoftware worden aangemerkt) en voor kritieke producten met digitale elementen ([24]). Daarentegen hoeven belangrijke producten met digitale elementen van klasse I (met uitzondering van producten die overeenkomstig artikel 32, lid 5, als vrije en opensourcesoftware worden aangemerkt) alleen een conformiteitsbeoordelingsprocedure door een derde te ondergaan indien de fabrikant relevante geharmoniseerde normen waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt (hierna "geharmoniseerde normen" genoemd), gemeenschappelijke specificaties of Europese regelingen voor cyberbeveiligingscertificering op ten minste zekerheidsniveau "substantieel" niet of slechts gedeeltelijk heeft toegepast ([25]).

149. Om een belangrijk product met digitale elementen van klasse I in aanmerking te laten komen voor de internecontroleprocedure, moeten daarom i) alle toepasselijke vereisten van een relevante geharmoniseerde norm worden toegepast en ii) moet het toepassingsgebied van de norm ten minste alle cyberbeveiligingsrisico's in verband met de basisfunctionaliteit van dat product bestrijken.

150. Het toepassingsgebied van het product met digitale elementen kan breder zijn dan het toepassingsgebied waarin de desbetreffende geharmoniseerde norm voorziet, en dergelijke aanvullende functies kunnen andere of aanvullende cyberbeveiligingsrisico's met zich meebrengen. De fabrikant is altijd verplicht een risicobeoordeling uit te voeren overeenkomstig artikel 13, lid 2, en moet bijgevolg controleren of de toepassing van een geharmoniseerde norm alle risico's dekt die verbonden zijn aan het product met digitale elementen. Wanneer de toepassing van de norm niet alle risico's dekt, moet de fabrikant er via andere middelen voor zorgen dat zijn product met digitale elementen aan de essentiële vereisten voldoet.

151. Als de fabrikant van een belangrijk product met digitale elementen van klasse I een relevante geharmoniseerde norm heeft toegepast die de risico's in verband met de basisfunctionaliteit van dat product dekt, kan hij besluiten gebruik te maken van de internecontroleprocedure om de conformiteit van het product aan te tonen. In het kader van zijn conformiteitsbeoordelingsactiviteiten zal de fabrikant nog steeds moeten aantonen dat alle risico's die van toepassing zijn op zijn product met digitale elementen worden aangepakt. Wanneer er een kloof bestaat tussen de dekking van de geharmoniseerde norm en het toepassingsgebied van het product met digitale elementen als geheel, moet de fabrikant dus nog steeds documenteren welke aanvullende maatregelen hij heeft genomen om die risico's aan te pakken.

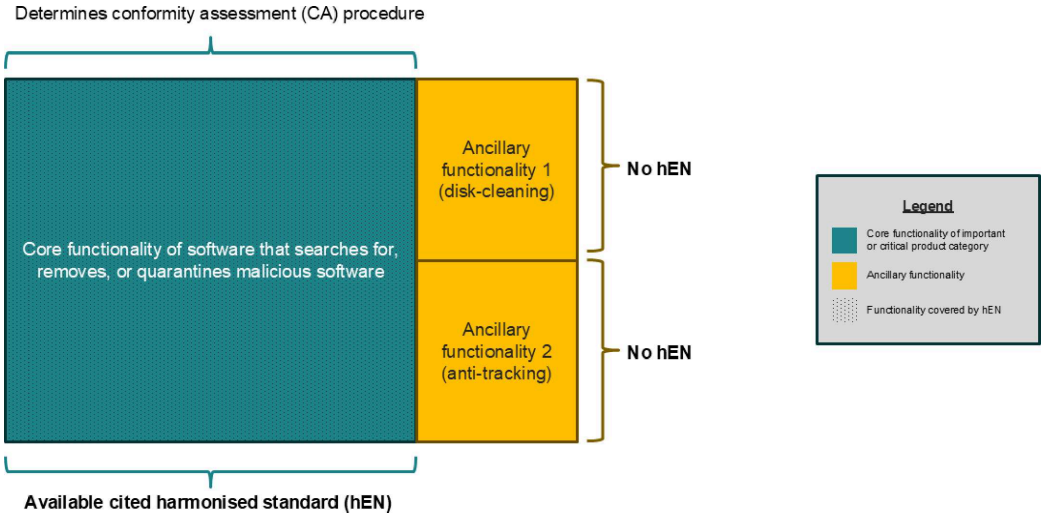
Voorbeeld 62: antivirussoftware heeft de basisfunctionaliteit van software waarmee kwaadaardige software wordt opgespoord en verwijderd of in quarantaine geplaatst, zoals beschreven in punt 4 van bijlage I bij Uitvoeringsverordening (EU) 2025/2392. Dat product met digitale elementen bevat ook aanvullende kenmerken, namelijk een functie voor schijfopruiming en traceerbescherming die de gebruiker beschermt wanneer deze op het internet aan het surfen is. De fabrikant voert een risicobeoordeling uit die betrekking heeft op het product met digitale elementen in zijn geheel, met inbegrip van de basisfunctionaliteit van virusbestrijding en de functies van schijfopruiming en traceerbescherming. De fabrikant past een geharmoniseerde norm toe die de risico's in verband met de basisfunctionaliteit van virusbestrijding dekt, alsook aanvullende maatregelen om risico's als gevolg van aanvullende functies aan te pakken. De fabrikant mag voor zijn conformiteitsbeoordeling gebruikmaken van de internecontroleprocedure, die betrekking heeft op het product met digitale elementen als geheel, met inbegrip van de functies schijfopruiming en traceerbescherming.

([24]) Dit is ook het geval wanneer gebruik wordt gemaakt van een Europese regeling voor cyberbeveiligingscertificering met een zekerheidsniveau dat ten minste "substantieel" is, aangezien de betrokkenheid van een externe certificeringsinstantie vereist is.

([25]) Kortheidshalve wordt in de rest van dit punt alleen verwezen naar geharmoniseerde normen waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt. Dezelfde richtsnoeren zijn echter ook van toepassing op gemeenschappelijke specificaties die zijn vastgesteld overeenkomstig artikel 27, lid 2, en op Europese regelingen voor cyberbeveiligingscertificering indien gespecificeerd door de Commissie via gedelegeerde handelingen overeenkomstig artikel 27, lid 9.

Figuur 6:

illustratie van de wijze waarop het gebruik van een aangehaalde geharmoniseerde norm die alleen betrekking heeft op de basisfunctionaliteit bepaalt welke conformiteitsbeoordelingsprocedure van toepassing is



152. Dit is ook het geval wanneer het product met digitale elementen een aanvullende functie integreert die zelf die van een ander belangrijk of kritiek product met digitale elementen is. In feite is het de basisfunctionaliteit van het product met digitale elementen als geheel, en niet de functionaliteit van de geïntegreerde componenten afzonderlijk, die bepaalt of het product met digitale elementen tot de belangrijke of kritieke productcategorie (en dus tot de toepasselijke conformiteitsbeoordelingsregeling) behoort. Indien een product met digitale elementen bijvoorbeeld de basisfunctionaliteit heeft van een belangrijk product met digitale elementen van klasse I, is dat product als geheel onderworpen aan de conformiteitsbeoordelingsregeling die van toepassing is op belangrijke producten met digitale elementen van klasse I, ook al integreert het een component die zelf een kritiek product met digitale elementen is. In deze gevallen, waarin de fabrikant een geharmoniseerde norm toepast die de risico's dekt die verbonden zijn aan de basisfunctionaliteit van dat product, mag hij gebruikmaken van de internecontrole-procedure.

Voorbeeld 63: een hardwareproduct met digitale elementen heeft de basisfunctionaliteit van een router, zoals beschreven in punt 12 van bijlage I bij Uitvoeringsverordening (EU) 2025/2392. Dat product met digitale elementen bevat ook aanvullende functionaliteiten, waaronder firewallcapaciteiten, aangezien het een firewallcomponent integreert. De fabrikant voert een risicobeoordeling uit die betrekking heeft op het product met digitale elementen in zijn geheel, met inbegrip van de basisfunctionaliteit van de router en de firewallfunctionaliteit. De fabrikant past een geharmoniseerde norm toe die de risico's in verband met de basisfunctionaliteit van de router bestrijkt, alsook aanvullende maatregelen om de risico's als gevolg van aanvullende functies aan te pakken. De fabrikant kan bijvoorbeeld de geharmoniseerde norm voor firewalls toepassen om de risico's in verband met de firewallfunctionaliteit af te dekken. De fabrikant mag voor zijn conformiteitsbeoordeling gebruikmaken van de internecontrole-procedure, die betrekking heeft op het product met digitale elementen als geheel, met inbegrip van de firewallfunctionaliteit.

6.3. Gevolgen voor het vermoeden van conformiteit

153. In artikel 27, lid 1, van de verordening cyberweerbaarheid wordt bepaald dat producten met digitale elementen en processen die door de fabrikant zijn ingesteld en in overeenstemming zijn met geharmoniseerde normen of delen daarvan waarvan de referenties in het *Publicatieblad van de Europese Unie* (PBEU) zijn bekendgemaakt, worden geacht conform te zijn met de essentiële vereisten van de verordening cyberweerbaarheid die door die normen of delen daarvan worden bestreken ([26]). In artikel 27, lid 5, wordt hetzelfde vermoeden van conformiteit uitgebreid tot

([26]) Zoals duidelijk vermeld in punt 4.1.2.2 van de Blauwe Gids, blijven "[i]n harmonisatiewetgeving […] fabrikanten altijd, zelfs als zij geharmoniseerde normen gebruiken waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, volledig verantwoordelijk […] voor het beoordelen van alle risico's van hun producten zodat zij weten welke essentiële (of andere) eisen relevant zijn. Na deze beoordeling kan de fabrikant beslissen de technische specificaties die zijn opgenomen in de geharmoniseerde normen, waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, toe te passen om de in de geharmoniseerde normen gespecificeerde "risicobeperkingsmaatregelen" te nemen".

producten met digitale elementen en processen die door de fabrikant zijn ingesteld en conform zijn met gemeenschappelijke specificaties die door de Commissie door middel van uitvoeringshandelingen zijn vastgesteld, en in artikel 27, lid 8, wordt het vermoeden van conformiteit bepaald voor producten met digitale elementen en processen die door de fabrikant zijn ingesteld en waarvoor een EU-conformiteitsverklaring of -certificaat is afgegeven in het kader van een op grond van Verordening (EU) 2019/881 vastgestelde Europese cyberbeveiligings-certificeringsregeling, indien dit is gespecificeerd door middel van gedelegeerde handelingen overeenkomstig artikel 27, lid 9 ([27]).

154. Wanneer de fabrikant een geharmoniseerde norm heeft toegepast waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt, geniet hij derhalve een vermoeden van conformiteit voor de risico's die onder die norm vallen. Dit kan bijvoorbeeld het geval zijn wanneer de geharmoniseerde norm waarnaar wordt verwezen, betrekking heeft op alle risico's in verband met de basisfunctionaliteit van een product met digitale elementen en er geen aanvullende functionaliteiten zijn die cyberbeveiligingsrisico's inhouden. Zo wordt verwacht dat de geharmoniseerde norm voor routers ten minste betrekking zal hebben op de risico's die verbonden zijn aan de basisfunctionaliteit van deze producten met digitale elementen. Indien een dergelijk product geen aanvullende functionaliteiten bevat of indien deze aanvullende functionaliteiten geen risico's inhouden die niet door de norm worden gedekt, kan het product met digitale elementen profiteren van het vermoeden van conformiteit.

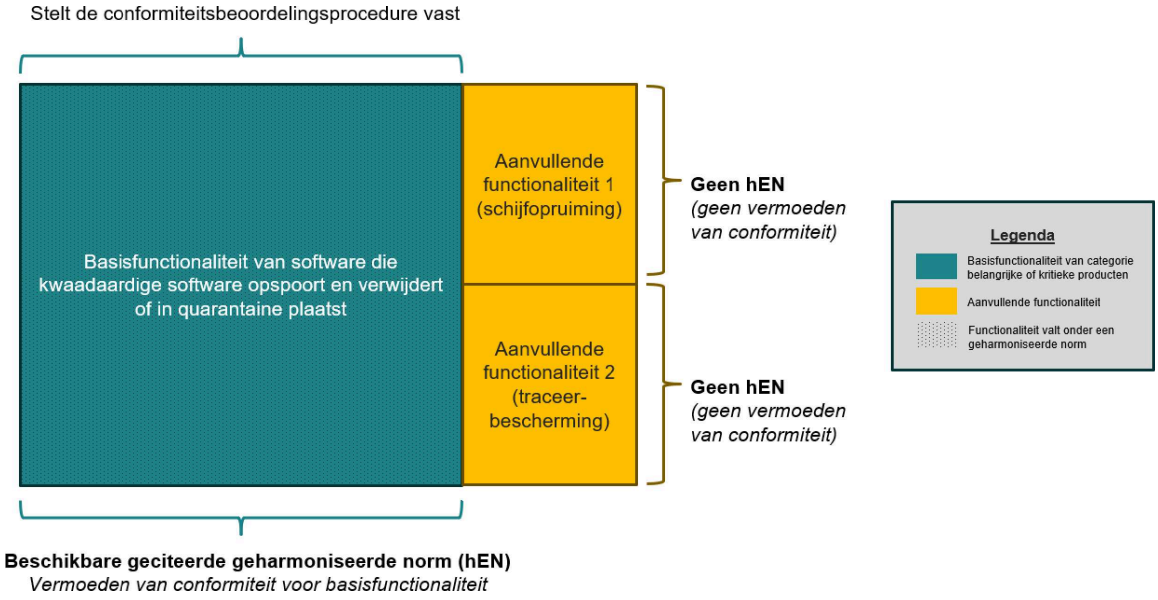
155. In de in de punten 151 en 152 besproken gevallen mag de fabrikant de internecontroleprocedure gebruiken omdat de geharmoniseerde norm de risico's dekt die verbonden zijn aan de basisfunctionaliteit van het product met digitale elementen. De in die voorbeelden beschreven producten met digitale elementen kunnen echter breder zijn dan het toepassingsgebied van de geharmoniseerde normen, en aanvullende functionaliteiten kunnen cyberbeveiligingsrisico's inhouden die niet door een dergelijke geharmoniseerde norm worden gedekt. Voor die producten met digitale elementen kan derhalve geen vermoeden van conformiteit gelden voor die aanvullende functionaliteiten.

Voorbeeld 64: antivirussoftware heeft de basisfunctionaliteit van software waarmee kwaadaardige software wordt opgespoord en verwijderd of in quarantaine geplaatst, en de risico's die met die basisfunctionaliteit gepaard gaan, worden gedekt door de geharmoniseerde norm. Dat product met digitale elementen bevat ook aanvullende functionaliteiten, namelijk een functie voor schijfopruiming en traceerbescherming die de gebruiker beschermt wanneer deze op het internet aan het surfen is, waarvan de risico's niet onder de geharmoniseerde norm vallen. Indien de geharmoniseerde norm wordt toegepast, mag de fabrikant voor zijn conformiteitsbeoordeling gebruikmaken van de internecontroleprocedure. De fabrikant kan profiteren van het vermoeden van conformiteit voor de risico's die verband houden met de basisfunctionaliteit van dat product, maar niet voor de risico's die verband houden met aanvullende functionaliteiten.

([27]) Zoals hierboven vermeld, wordt in de rest van dit punt kortheidshalve alleen verwezen naar geharmoniseerde normen waarvan de referenties in het *Publicatieblad van de Europese Unie* zijn bekendgemaakt. Dezelfde richtsnoeren gelden echter ook voor gemeenschappelijke specificaties en voor Europese regelingen voor cyberbeveiligingscertificering.

Figuur 7:

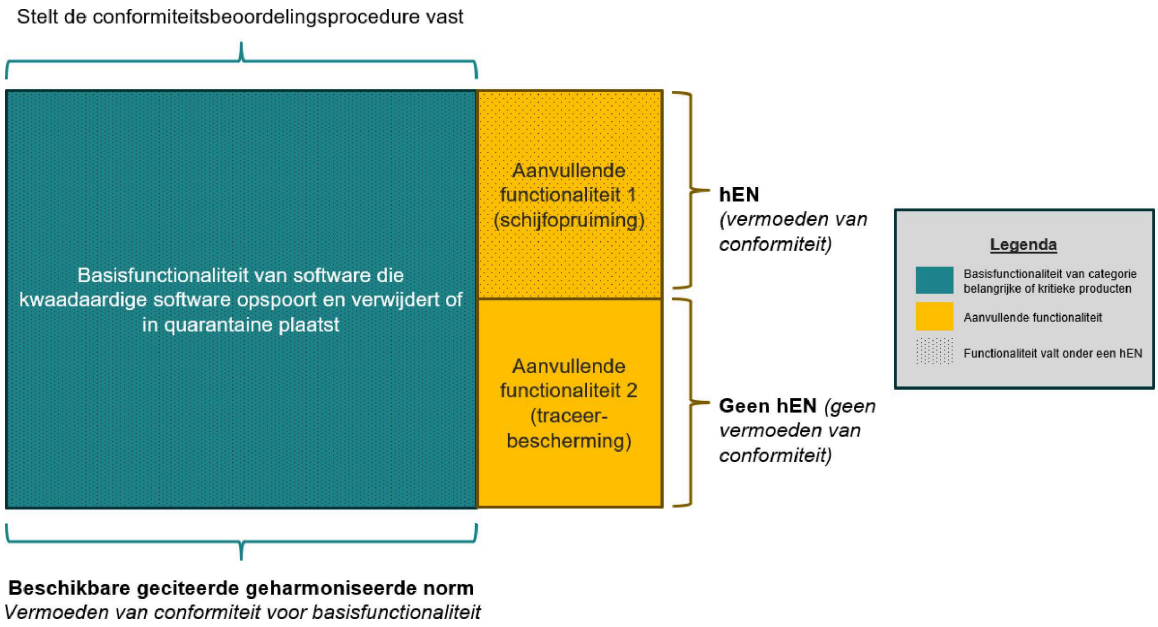
geharmoniseerde norm verleent een vermoeden van conformiteit voor de basisfunctionaliteit, aangezien deze betrekking heeft op alle risico's die verband houden met die basisfunctionaliteit, maar niet voor aanvullende functionaliteiten



Voorbeeld 65: in hetzelfde scenario als het vorige voorbeeld is de geharmoniseerde norm nu bijgewerkt om ook risico's te dekken die verband houden met een van de aanvullende functionaliteiten, namelijk schijfopruiming, maar niet de andere (d.w.z. traceerbescherming). Indien de geharmoniseerde norm wordt toegepast, mag de fabrikant voor zijn conformiteitsbeoordeling gebruikmaken van de internecontroleprocedure. Er geldt een vermoeden van conformiteit voor de risico's in verband met de basisfunctionaliteit van dat product en voor de functionaliteit schijfopruiming, maar niet voor de risico's in verband met de functionaliteit traceerbescherming

Figuur 8:

geharmoniseerde norm verleent het vermoeden van conformiteit voor de basisfunctionaliteit en aanvullende functionaliteit 1, aangezien hiermee alle risico's in verband met die twee functionaliteiten worden gedekt, maar niet voor aanvullende functionaliteit 2



7. **BEOORDELING VAN CYBERBEVEILIGINGSRISICO'S EN INTEGRATIE VAN PRODUCTEN MET DIGITALE ELEMENTEN EN COMPONENTEN**

7.1. **Over de evaluatie en behandeling van cyberbeveiligingsrisico's**

156. De in artikel 13, lid 2, van de verordening cyberweerbaarheid bedoelde beoordeling van cyberbeveiligingsrisico's vereist dat fabrikanten relevante risico's in kaart brengen en de mogelijke gevolgen ervan voor het product met digitale elementen beoordelen. Fabrikanten moeten ook passende maatregelen nemen om die risico's aan te pakken, overeenkomstig de essentiële vereisten van bijlage I.

157. Bij organisatorisch risicobeheer worden risico's doorgaans beoordeeld aan de hand van acceptatiecriteria die zijn afgeleid van de interne doelstellingen of risicobereidheid van de organisatie. In het kader van de verordening cyberweerbaarheid moeten eventueel resterende cyberbeveiligingsrisico's daarentegen worden beoordeeld in het licht van het vereiste dat het in de handel gebrachte product met digitale elementen een passend niveau van cyberbeveiliging waarborgt op basis van de risico's, rekening houdend met het beoogde doel en het redelijkerwijs voorzienbare gebruik ervan.

158. Bijgevolg zijn de interne risicotolerantie, de handelsstrategie of louter kostenoverwegingen van de fabrikant niet relevant bij de bepaling of de risico's zijn aangepakt. Voor de toepassing van artikel 13, leden 2 en 3, moeten fabrikanten in staat zijn te bepalen of de vastgestelde cyberbeveiligingsrisico's voldoende zijn aangepakt door de uitvoering van de essentiële eisen van deel I van bijlage I, in het licht van het beoogde doel, het redelijkerwijs te voorziene gebruik en de gebruiksomstandigheden, met inbegrip van, in voorkomend geval, de operationele omgeving (bv. de beoogde gebruikers van het product met digitale elementen) en de te beschermen activa, rekening houdend met de verwachte gebruiksduur van het product met digitale elementen.

159. Resterende cyberbeveiligingsrisico's zijn een inherent resultaat van risicobeoordeling en -behandeling. Erkend wordt dat cyberbeveiligingsrisico's in de praktijk niet volledig kunnen worden weggenomen. Het bestaan van restrisico's betekent echter niet dat de fabrikant naar eigen goeddunken elk risico mag aanvaarden. Een product met digitale elementen mag alleen in de handel worden gebracht wanneer de restrisico's, zodra passende maatregelen zijn genomen, voldoende zijn aangepakt door de uitvoering van de essentiële vereisten, rekening houdend met het beoogde doel en het redelijkerwijs te voorziene gebruik van het product met digitale elementen.

160. Overeenkomstig artikel 13, lid 3, moeten fabrikanten, wanneer cyberbeveiligingsrisico's worden vastgesteld, deze aanpakken door middel van passende maatregelen, onder meer op productniveau. Afhankelijk van de omstandigheden kan dit bijvoorbeeld inhouden dat het aanvalsoppervlak wordt verkleind, technische waarborgen worden toegepast, de functionaliteit wordt beperkt of aangepast, of het beoogde doel van het product met digitale elementen nauwkeuriger wordt gedefinieerd. Fabrikanten kunnen ook stappen ondernemen om het redelijkerwijs te verwachten gebruik van het product met digitale elementen vorm te geven, bijvoorbeeld door middel van risicocommunicatie, gebruikershandleidingen of het ontwerp van de gebruikersinterface, teneinde het gedrag van gebruikers in de richting van veilige gebruikspatronen te sturen.

161. De verordening cyberweerbaarheid voorziet niet in de overdracht van cyberbeveiligingsrisico's of verantwoordelijkheden aan gebruikers of derden om tekortkomingen in het productontwerp te compenseren of om te rechtvaardigen dat cyberbeveiligingsrisico's niet worden aangepakt. De verplichting om een veilig product met digitale elementen in de handel te brengen en conformiteit met de essentiële vereisten aan te tonen, blijft berusten bij de fabrikant.

162. Aan gebruikers verstrekte informatie en instructies kunnen worden gebruikt om de veilige inzet en werking van het product met digitale elementen te ondersteunen, ook wanneer de fabrikant ervoor heeft gekozen het beoogde doel van dat product te beperken tot betrouwbare omgevingen, en om gebruikers te informeren over restrisico's, op een wijze die passend is voor de aard van het product met digitale elementen en de beoogde gebruikers ervan.

Voorbeeld 66: een fabrikant ontwikkelt een industriële sensor voor gebruik in betrouwbare omgevingen. Om de sensor correct te laten functioneren, voert de fabrikant geen maatregelen uit ter bescherming tegen fysieke aanvallen op de sensor zelf. Om de in de risicobeoordeling vastgestelde risico's te beperken, beperkt de fabrikant het beoogde doel van de sensor tot gebruik in betrouwbare omgevingen waar ongeoorloofde fysieke toegang tot het product met digitale elementen wordt voorkomen. Informatie en instructies voor de gebruikers bieden duidelijke informatie over deze beperkingen op het gebruik van de sensor, op een wijze die passend is voor de aard van het product met digitale elementen en de beoogde gebruikers ervan.

Voorbeeld 67: een fabrikant ontwikkelt een softwaretoepassing voor professioneel gebruik op beheerde desktop- en mobiele apparaten. De toepassing verwerkt lokaal opgeslagen gevoelige gegevens en door gebruikers gegenereerde inhoud. Tijdens de risicobeoordeling identificeert de fabrikant het risico van ongeoorloofde toegang tot dergelijke gegevens indien deze in leesbare tekst op het apparaat worden opgeslagen. In plaats van binnen de toepassing zelf een eigen versleutelingsmechanisme te ontwerpen en toe te passen, kiest de fabrikant ervoor gebruik te maken van de versleutelings- en sleutelbeheersfuncties die reeds worden geleverd door het besturingssysteem waarop de toepassing moet draaien, aangezien de ingebouwde cryptografische diensten van het besturingssysteem gebruiksklaar zijn en regelmatig worden onderhouden.

163. Wanneer bij de cyberbeveiligingsrisicobeoordeling risico's worden vastgesteld die niet adequaat kunnen worden aangepakt door middel van passende maatregelen, kan de naleving van de verordening cyberweerbaarheid wijzigingen vereisen van het ontwerp, de functionaliteit of het beoogde doel van het product met digitale elementen. Overwegingen die uitsluitend verband houden met de kosten of de commerciële haalbaarheid zijn onvoldoende redenen om dergelijke risico's onbehandeld te laten wanneer dit zou verhinderen dat het product met digitale elementen aan de essentiële vereisten voldoet.

7.2. Over het zodanig ontwerpen, ontwikkelen en produceren van producten met digitale elementen dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen

164. Met het in deel I, punt 1), van bijlage I bij de verordening cyberweerbaarheid bedoelde essentiële cyberbeveiligingsvereiste is bepaald dat producten met digitale elementen zodanig worden ontworpen, ontwikkeld en geproduceerd dat zij een passend niveau van cyberbeveiliging waarborgen op basis van de risico's.

165. Dit essentiële vereiste is bedoeld om alle cyberbeveiligingsrisico's aan te pakken die in het kader van de cyberbeveiligingsrisicobeoordeling zijn vastgesteld. Dit omvat met name cyberbeveiligingsrisico's die anders niet adequaat worden aangepakt in het kader van de uitvoering van de essentiële vereisten van deel I van bijlage I, met uitzondering van punt 1). Dit essentiële vereiste verschilt van de wettelijke verplichting om een cyberbeveiligingsrisicobeoordeling uit te voeren, die moet worden uitgevoerd op grond van artikel 13, lid 2.

166. Wanneer alle relevante cyberbeveiligingsrisico's in verband met een product met digitale elementen worden behandeld door passende maatregelen uit te voeren om aan de andere toepasselijke essentiële vereisten dan punt 1) te voldoen, wordt aan het in deel I, punt 1), van bijlage I bedoelde essentiële vereiste geacht te zijn voldaan. Omgekeerd moeten fabrikanten, wanneer bij de beoordeling van cyberbeveiligingsrisico's aanvullende risico's worden vastgesteld die niet volledig met dergelijke maatregelen worden aangepakt, passende maatregelen nemen op het product met digitale elementen om die risico's aan te pakken, zodat zij voldoen aan het essentiële vereiste van deel I, punt 1), van bijlage I. In de praktijk wordt in de meeste gevallen verwacht dat naleving van de andere essentiële vereisten zal leiden tot conformiteit met dit vereiste.

7.3. Risicobeoordeling en passende zorgvuldigheid met betrekking tot externe afhankelijkheden en geïntegreerde componenten

167. De verordening cyberweerbaarheid voorziet in twee afzonderlijke maar complementaire verplichtingen voor fabrikanten met betrekking tot het beheer van cyberbeveiligingsrisico's. Ten eerste worden fabrikanten in artikel 13, lid 2, verplicht om een cyberbeveiligingsrisicobeoordeling uit te voeren voor het product met digitale elementen zelf. Ten tweede bevat artikel 13, lid 5, de verplichting om passende zorgvuldigheid te betrachten met betrekking tot geïntegreerde componenten. Samen zijn deze twee verplichtingen bedoeld om ervoor te zorgen dat het product met digitale elementen veilig blijft, ook wanneer het afhankelijk is van oplossingen voor gegevensverwerking op afstand, diensten op afstand of software- of hardwarecomponenten van derden.

168. De cyberbeveiligingsrisicobeoordeling heeft betrekking op de identificatie en het beheer van relevante risico's die van invloed kunnen zijn op het product met digitale elementen, met inbegrip van risico's die niet van het product zelf afkomstig zijn, zoals externe netwerken, milieufactoren of andere externe aspecten die van invloed kunnen zijn op het product met digitale elementen of waar het product van afhankelijk is. Voor dergelijke externe risico's vereist de verordening cyberweerbaarheid niet dat fabrikanten de externe omgeving controleren of regelen. In plaats daarvan zijn fabrikanten verplicht dergelijke risico's in kaart te brengen en te beperken door middel van het ontwerp en de ontwikkeling van het product met digitale elementen zelf. Dit omvat de uitvoering van de toepasselijke essentiële vereisten van deel I van bijlage I en, indien nodig, het verstrekken van informatie en instructies aan gebruikers over de integratie- of gebruiksrisico's.

169. Een fabrikant kan bijvoorbeeld een risico vaststellen dat onbevoegden tijdens de werking van het product toegang krijgen tot back-endsystemen die geen deel uitmaken van het product met digitale elementen zelf, en kan proberen kwaadwillige opdrachten naar het product met digitale elementen te sturen. Indien zij niet door de fabrikant of onder zijn verantwoordelijkheid zijn ontworpen en ontwikkeld, of indien zij geen van de functies van het product met digitale elementen ondersteunen, vormen dergelijke back-endsystemen geen oplossingen voor gegevensverwerking op afstand en zij vallen derhalve buiten het toepassingsgebied van het product met digitale elementen voor de toepassing van de verordening cyberweerbaarheid. Niettemin wordt in de verordening cyberweerbaarheid vereist dat de fabrikant het risico dat zij kunnen vormen, aanpakt door middel van maatregelen op productniveau, zoals het vereisen van cryptografische authenticatie van opdrachten op afstand, het verifiëren van de integriteit van configuratiewijzigingen of het genereren van voor de veiligheid relevante logbestanden of waarschuwingen wanneer abnormaal gedrag wordt gedetecteerd. Evenzo kan in de verordening cyberweerbaarheid, wanneer een fabrikant een risico vaststelt dat voortvloeit uit het feit dat een dergelijke externe dienst niet beschikbaar is, bijvoorbeeld als gevolg van stroomonderbrekingen of storingen in de infrastructuur, op productniveau risicobeperkende maatregelen worden vereist tegen dergelijke cyberbeveiligingsrisico's, bijvoorbeeld door ervoor te zorgen dat de niet-beschikbaarheid er niet toe leidt dat het gebruik van het product met digitale elementen onveilig wordt. In dergelijke gevallen bevat de verordening cyberweerbaarheid bepalingen over hoe het product met digitale elementen op die externe risico's reageert; de verordening legt geen verplichtingen op over de wijze waarop de back-endinfrastructuur wordt georganiseerd of bemand of moet functioneren, en behandelt die infrastructuur evenmin als onderdeel van het product met digitale elementen.

170. Passende zorgvuldigheid heeft betrekking op elementen die deel uitmaken van het product met digitale elementen zelf, met name geïntegreerde software- of hardwarecomponenten die door een derde worden geleverd. Fabrikanten moeten passende maatregelen nemen om ervoor te zorgen dat dergelijke componenten de conformiteit van het product met digitale elementen met de essentiële vereisten niet ondermijnen. Dit kan alleen worden bereikt door te bepalen wat het product met digitale elementen van zijn componenten nodig heeft om zijn cyberbeveiligingsdoelstellingen te verwezenlijken, en door op risicogebaseerde wijze na te gaan of die componenten in overeenstemming zijn met de behoeften van het product, zoals ook aangegeven in overweging 34.

171. In overeenstemming met zijn cyberbeveiligingsrisicobeoordeling moet de fabrikant vaststellen aan welke vereisten de geïntegreerde component moet voldoen. Indien het product met digitale elementen bijvoorbeeld afhankelijk is van cryptografische functies, updatemechanismen of beveiligde communicatie die door een component worden verstrekt, moet de fabrikant in het kader van zijn passende zorgvuldigheid die behoeften vaststellen en controleren of de component daaraan voldoet. Het bewijs hiervoor kan bestaan uit documentatie die is verkregen van de fabrikant van de component, zoals technische specificaties, veiligheidsdocumentatie of relevante conformiteits- of zekerheidsdocumentatie. In voorkomend geval kan de fabrikant ook tests uitvoeren om te controleren of die componenten de betreffende functies naar behoren vervullen. Hoewel passende zorgvuldigheid een afzonderlijke wettelijke verplichting is, wordt hiermee het vermogen van de fabrikant om aan te tonen dat hij voldoet aan de essentiële vereisten voor het product met digitale elementen als geheel, ondersteund en benadrukt.

172. Bij de beoordeling van de risico's voor het product met digitale elementen als geheel moeten elementen buiten het product, zoals milieuelementen, externe infrastructuur, andere systemen of netwerken, in aanmerking worden genomen bij de cyberbeveiligingsrisicobeoordeling en, in voorkomend geval, worden aangepakt door middel van maatregelen op productniveau om de conformiteit van het product met digitale elementen met de essentiële vereisten te waarborgen. Componenten die fysiek of logisch in het product met digitale elementen zijn geïntegreerd, maar afkomstig zijn van derden, moeten ook als onderdeel van de risicobeoordeling worden beschouwd. Met het oog op de naleving moet de fabrikant deze echter behandelen als extern geleverde componenten waarvan de eigenschappen na integratie door middel van passende zorgvuldigheid worden geverifieerd, aangezien de fabrikant deze mogelijk niet opnieuw heeft ontworpen of ontwikkeld.

173. Dezelfde logica geldt tijdens de ontwikkeling en integratie van componenten. Wanneer de fabrikant zelf functionaliteiten ontwikkelt, moet hij de essentiële vereisten rechtstreeks implementeren. Wanneer de fabrikant door derden ontwikkelde componenten integreert, moet hij er door middel van passende zorgvuldigheid voor zorgen dat die componenten zodanig kunnen worden gebruikt dat het product met digitale elementen als geheel aan de vereisten kan voldoen. In beide gevallen blijft het doel hetzelfde: dat het product met digitale elementen, zoals het in de handel wordt gebracht, een passend niveau van cyberbeveiliging bereikt, zoals vereist door het verordening cyberweerbaarheid, rekening houdend met de risico's die in de cyberbeveiligingsrisicobeoordeling zijn vastgesteld.

7.4. **Hergebruik van risicobeoordelingen en conformiteitsdocumentatie voor families van producten met digitale elementen**

174. Fabrikanten kunnen producten met digitale elementen in de handel brengen die vergelijkbaar zijn, bijvoorbeeld verschillende varianten, modellen of configuraties van dezelfde productfamilie. Wanneer dergelijke producten met digitale elementen dezelfde architectuur, hetzelfde beveiligingsrelevante ontwerp en hetzelfde beoogde doel hebben en aan dezelfde cyberbeveiligingsrisico's worden blootgesteld, wordt in de verordening cyberweerbaarheid niet vereist dat fabrikanten elke variant met het oog op risicobeoordeling en conformiteitsbeoordeling als een volledig afzonderlijk product met digitale elementen behandelen.

175. In dergelijke gevallen kunnen fabrikanten, mits alle betrokken varianten afdoende worden gedekt wat betreft relevante risico's en essentiële vereisten, zich baseren op: i) één enkele overeenkomstig artikel 13, lid 2, van de verordening cyberweerbaarheid uitgevoerde cyberbeveiligingsrisicobeoordeling; ii) één enkele set technische documenten, en iii) één conformiteitsbeoordelingsprocedure. Dit maakt het ook mogelijk één EU-conformiteitsverklaring af te geven voor de groep producten met digitale elementen, mits de productvarianten waarop deze van toepassing is, duidelijk worden geïdentificeerd.

176. Doorslaggevend is of de verschillen tussen de varianten relevant zijn voor cyberbeveiliging. Variaties die geen invloed hebben op de cyberbeveiligingseigenschappen van het product met digitale elementen, zoals verschillen in kleur, vorm, opslagcapaciteit of andere voor de veiligheid niet relevante kenmerken, vereisen geen afzonderlijke risicobeoordelingen of conformiteitsbeoordelingen. Omgekeerd kunnen varianten in sommige gevallen verschillen op manieren die wel van invloed zijn op de uitvoering van essentiële vereisten, bijvoorbeeld as ze werken met verschillende communicatie-interfaces, softwarestacks, updatemechanismen of connectiviteit op afstand. In dergelijke gevallen moeten die verschillen tot uiting komen in de risicobeoordeling en, indien nodig, in de conformiteitsbeoordeling en de technische documentatie.

177. Fabrikanten blijven verantwoordelijk voor het waarborgen dat de risicobeoordeling en de bijbehorende documentatie een nauwkeurige afspiegeling vormen van de producten met digitale elementen die in de handel zijn gebracht. Wanneer een nieuwe variant nieuwe cyberbeveiligingsrisico's met zich meebrengt of wanneer de manier waarop essentiële vereisten worden uitgevoerd hierdoor wordt gewijzigd, moet de bestaande risicobeoordelings- en conformiteitsdocumentatie dienovereenkomstig worden bijgewerkt. Het gebruik van één enkele conformiteitsbeoordeling is alleen mogelijk voor zover de producten met digitale elementen geen verschillen vertonen met betrekking tot hun cyberbeveiligingseigenschappen.

8. **GEGEVENSVERWERKING OP AFSTAND**

178. In artikel 3, punt 1), van de verordening cyberweerbaarheid wordt een product met digitale elementen gedefinieerd als "een software- of hardwareproduct en zijn oplossingen voor gegevensverwerking op afstand, met inbegrip van software- of hardwarecomponenten die afzonderlijk in de handel worden gebracht". In dit licht moet de fabrikant het product met digitale elementen als geheel beschouwen, met inbegrip van zijn oplossingen voor gegevensverwerking op afstand (RDPS). Wanneer bijvoorbeeld wordt aangetoond dat het product met digitale elementen voldoet aan de essentiële vereisten van bijlage I, moet rekening worden gehouden met RDPS, te beginnen met de risicobeoordeling (artikel 13, lid 2). Hetzelfde geldt voor levenscyclusverplichtingen, zoals het melden van actief uitgebuite kwetsbaarheden en ernstige incidenten (artikel 14).

179. Het doel van deze richtsnoeren is fabrikanten verder te ondersteunen bij het bepalen of er bij hun product met digitale elementen sprake is van RDPS zoals gedefinieerd in de verordening cyberweerbaarheid en hoe zij in dit verband aan hun nalevingsverplichtingen kunnen voldoen. Na een eerste analyse van de definities en overwegingen in de verordening cyberweerbaarheid bevatten deze richtsnoeren vragen om fabrikanten te helpen verduidelijken of er bij hun product met digitale elementen sprake is van RDPS (zie punt *8.1*, "Wat wordt beschouwd als een oplossing voor gegevensverwerking op afstand voor een product met digitale elementen?"). Vervolgens wordt ingegaan op de technische gevolgen van RDPS en op de wijze waarop de naleving van de verordening cyberweerbaarheid moet worden beoordeeld (zie punt *8.2*, "Praktische en technische gevolgen van oplossingen voor gegevensverwerking op afstand en afhankelijkheid van oplossingen van derden").

180. In artikel 3, punt 2), wordt "gegevensverwerking op afstand" zelfs gedefinieerd als "gegevensverwerking vanop een afstand waarvoor de software is ontworpen en ontwikkeld door de fabrikant of onder de verantwoordelijkheid van de fabrikant, en bij gebreke waarvan het product met digitale elementen een van zijn functies niet zou kunnen vervullen". RDPS worden daarom gedefinieerd als de software-elementen ("het deel van een elektronisch informatiesysteem dat uit computercode bestaat", zoals gedefinieerd in artikel 3, punt 4), van gegevensverwerking op afstand. Het is niet de bedoeling om, als onderdeel van het toepassingsgebied van het product met digitale elementen, de hardware op te nemen waar gegevensverwerking op afstand van afhankelijk kan zijn.

181. In de overwegingen 11 en 12 wordt nader toegelicht hoe dit begrip moet worden uitgelegd. In overweging 11 wordt verduidelijkt dat het doel van het opnemen van oplossingen voor gegevensverwerking op afstand is dat "dergelijke producten volledig en op passende wijze [worden] beveiligd door de fabrikanten, ongeacht of de gegevens worden verwerkt of lokaal worden opgeslagen op het apparaat van de gebruiker dan wel op afstand door de fabrikant". Ook wordt hier gesteld dat de "vereisten met betrekking tot oplossingen voor gegevensverwerking op afstand die binnen het toepassingsgebied van deze verordening vallen, […] derhalve geen technische, operationele of organisatorische maatregelen [omvatten] om de risico's voor de beveiliging van de netwerk- en informatiesystemen van een fabrikant als geheel te beheren".

182. Daarom volgt uit overweging 11 dat het niet de bedoeling is dat de vereisten van de verordening cyberweerbaarheid betrekking hebben op de volledige IT-infrastructuur van een organisatie, maar alleen op softwarecomponenten die de uitvoering van de oplossing voor gegevensverwerking mogelijk maken. Interne systemen met betrekking tot de eigen personele middelen van de fabrikant, loonadministratie, klantrelatiebeheer, pijpleidingen voor continue integratie/continue levering en de verspreiding van beveiligingsupdates naar perifere locaties mogen bijvoorbeeld niet als RDPS worden beschouwd. Evenzo vallen systemen die verband houden met controle- en testactiviteiten, zoals penetratietests, "threat hunting" (het opspeuren van bedreigingen) en "red teaming" (het opsporen van kwetsbaarheden), buiten het toepassingsgebied van een product met digitale elementen dat onder de verordening cyberweerbaarheid valt. Het is belangrijk op te merken dat het toepassen van doeltreffende en regelmatige tests en evaluaties van de beveiliging van het product met digitale elementen weliswaar een essentieel vereiste is dat is vastgelegd in deel II, punt 3), van bijlage I bij de verordening cyberweerbaarheid, maar dat dit niet betekent dat dergelijke activiteiten voor het product met digitale elementen als RDPS moeten worden beschouwd.

183. In overweging 12 ligt de nadruk op clouddiensten en wordt nader ingegaan op de omstandigheden waaronder clouddiensten als RDPS kunnen worden beschouwd. Tot slot wordt er in de overweging aan herinnerd dat cloudcomputingdiensten en cloudmodellen binnen het toepassingsgebied vallen van Richtlijn (EU) 2022/2555 (NIS 2-richtlijn) ([28]), waarin de voorschriften inzake het beheer van cyberbeveiligingsrisico's voor aanbieders van cloudcomputingdiensten zijn vastgesteld. Die voorschriften zijn nader gespecificeerd in Uitvoeringsverordening (EU) 2024/2690 van de Commissie ([29]).

8.1. **Wat wordt beschouwd als een oplossing voor gegevensverwerking op afstand voor een product met digitale elementen?**

184. De definitie van gegevensverwerking op afstand in artikel 3, punt 2), berust dus op drie elementen: i) of de gegevensverwerking "op afstand" plaatsvindt; ii) of het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen zou beletten een van zijn functies uit te voeren, en iii) of de software door de fabrikant zelf of onder zijn verantwoordelijkheid is ontworpen en ontwikkeld. In de volgende drie punten wordt nader ingegaan op elk van deze elementen.

([28]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (PB L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Het begrip "op afstand"*

185. Het begrip "op afstand" als bedoeld in artikel 3, punt 2), is relevant, maar niet voldoende om te bepalen of een product met digitale elementen RDPS omvat. Bovendien is het, gezien de verscheidenheid aan oplossingen die onder dit begrip kunnen vallen, niet mogelijk om een uitputtende definitie van "op afstand" te geven. Een beoordeling per geval door de fabrikant is noodzakelijk.

186. In overweging 11 van de verordening cyberweerbaarheid wordt verwezen naar gegevens die "op afstand door de fabrikant" worden verwerkt of opgeslagen, in tegenstelling tot gegevens die "worden verwerkt of lokaal worden opgeslagen op het apparaat van de gebruiker". Gegevensverwerking op afstand vindt doorgaans plaats buiten de gebruikersomgeving van een product met digitale elementen of de operationele omgeving van een organisatie (voor een professionele gebruiker). Dit belet echter niet dat de verwerking ook dicht bij het apparaat (langs de "edge") plaatsvindt. De overdracht van gegevens kan bedraad (bv. via een ethernetkabel) of draadloos (bv. via wifi, bluetooth) plaatsvinden. Cloudcomputing, met inbegrip van edgecomputing, is een typisch voorbeeld van gegevensverwerking "op afstand". In het geval van een cloudgebaseerde functie waartoe de gebruiker toegang heeft via een mobiele applicatie, vindt een deel van de gegevensverwerking bijvoorbeeld plaats in de cloud, buiten de omgeving van de gebruiker.

187. Het is belangrijk op te merken dat RDPS niet noodzakelijkerwijs hoeft plaats te vinden op cloudinfrastructuur van derden. Gegevensverwerking op afstand op lokale servers op een bedrijfslocatie van de fabrikant kan ook als RDPS worden aangemerkt. Met andere woorden, een oplossing die op locatie en in een particuliere cloud wordt uitgevoerd, kan net zo waarschijnlijk als RDPS worden aangemerkt als een oplossing die op een openbare cloud en op een locatie elders wordt uitgevoerd.

188. De twee beslissende en cumulatieve vragen die bepalen of gegevensverwerking als oplossing voor gegevensverwerking op afstand onder de verordening cyberweerbaarheid valt, worden hieronder uiteengezet, in de punten *8.1.2* en *8.2*. Indien beide vragen bevestigend worden beantwoord, kan de gegevensverwerking op afstand als RDPS worden aangemerkt.

8.1.2. *Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren?*

189. Zoals bepaald in de definitie van "gegevensverwerking op afstand" in artikel 3, punt 2), zou, om gegevensverwerking op afstand als RDPS te kunnen aanmerken, het ontbreken ervan het product met digitale elementen moeten beletten een van zijn functies uit te voeren. Het begrip "functies" in deze definitie is niet beperkt tot de "basisfunctionaliteit" of het "beoogde doel" van het product met digitale elementen, aangezien de verordening cyberweerbaarheid een dergelijke beperking niet oplegt. De functies binnen het toepassingsgebied van de verordening cyberweerbaarheid zijn zowel functies die rechtstreeks beantwoorden aan het beoogde doel van het product met digitale elementen zoals ervaren door gebruikers, als functies die de algemene prestaties van het product ondersteunen.

190. Voorbeelden van functies waarbij gegevensverwerking op afstand kan plaatsvinden en die een product met digitale elementen zouden beletten een van zijn functies uit te voeren, zijn: i) het verzenden van opdrachten naar een apparaat; ii) het synchroniseren van bestanden; iii) het onboarden van de gebruiker; iv) configuratie (personalisering van het product met digitale elementen); v) de geautomatiseerde verspreiding van updates, met inbegrip van updates van functies en beveiligingspatches; vi) identiteits- en toegangsbeheer.

191. In sommige gevallen kan de gebruiker zowel op afstand als handmatig een functie gebruiken (bv. een lamp met een app inschakelen of handmatig). Deze optie sluit niet uit dat de gegevensverwerking in verband met de uitvoering van de functie op afstand als RDPS wordt aangemerkt. Het op afstand uitvoeren van deze functie wordt ook beschouwd als onderdeel van de functies die het product met digitale elementen aanbiedt.

192. Wanneer daarentegen het ontbreken van een bepaalde gegevensverwerking het product met digitale elementen niet belet een van zijn functies uit te voeren, wordt een dergelijke verwerking niet beschouwd als RDPS in de zin van de verordening cyberweerbaarheid. Dit omvat bijvoorbeeld de analyse op afstand van telemetriegegevens die uitsluitend voor statistische doeleinden of voor toekomstige productontwikkeling worden verzameld.

193. Niettemin moeten fabrikanten, zelfs wanneer de gegevensverwerking een functie van een product met digitale elementen niet ondersteunt, in het kader van hun cyberbeveiligingsrisicobeoordeling (bv. in het licht van de operationele omgeving van het product) mogelijk overwegen of die componenten op afstand risico's met zich meebrengen voor het product met digitale elementen, en dergelijke risico's dienovereenkomstig beperken (bv. door middel van risicobeperkende maatregelen op productniveau).

194. Websites zijn een specifiek geval dat nadere verduidelijking behoeft, zoals ook is toegelicht in punt *2.1*, "In de handel brengen". Websites vallen niet binnen het toepassingsgebied van RDPS indien zij geen functie van een product met digitale elementen ondersteunen, zoals toegelicht in overweging 11 van de verordening cyberweerbaarheid. Het volstaat niet dat een website informatie bevat over een product met digitale elementen om te worden geacht binnen het toepassingsgebied van RDPS te vallen, zelfs als het product de gebruiker naar een dergelijke website stuurt. Zo is het doorsturen van gebruikers naar een externe webpagina met informatie en instructies voor gebruikers geen RDPS. Een website kan daarentegen binnen het toepassingsgebied van RDPS vallen als hij een functie van een product met digitale elementen mogelijk maakt of ondersteunt. Zo zou een authenticatieportaal dat inloggegevens of tokens afgeeft die nodig zijn voor de werking van het product met digitale elementen, als RDPS worden beschouwd (mits ook aan de andere criteria van de definitie is voldaan).

8.1.3. *Is de software ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant?*

195. In de definitie van "gegevensverwerking op afstand" van artikel 3, punt 2), van de verordening cyberweerbaarheid wordt verder gespecificeerd dat de software voor dergelijke gegevensverwerking op afstand door de fabrikant zelf of onder zijn verantwoordelijkheid moet worden ontworpen en ontwikkeld. Gegevensverwerking op afstand die volledig door de fabrikant is ontwikkeld en ontworpen (intern), zou uiteraard als RDPS worden aangemerkt. Dit zou ook het geval zijn als fabrikanten een beroep doen op een externe dienstverlener voor de ontwikkeling en het ontwerp van een oplossing (d.w.z. "onder zijn verantwoordelijkheid"). De zinsnede "onder de verantwoordelijkheid van de fabrikant" verwijst naar oplossingen voor verwerking op afstand die zijn toegesneden op de fabrikant. Dit zijn gevallen waarin de fabrikant niet louter een licentie verleent voor een bestaand product met digitale elementen of een bestaande dienst die een dienstverlener aan zijn klanten aanbiedt of enigszins gewijzigde versies daarvan. "Onder de verantwoordelijkheid van de fabrikant" houdt in dat de software uitsluitend door of namens de fabrikant wordt gebouwd op basis van door hem verstrekte ontwerpen en specificaties.

196. Voor een goed begrip van RDPS is "wie de oplossing exploiteert" geen doorslaggevende factor, aangezien de definitie van de verordening cyberweerbaarheid alleen verwijst naar het ontwerp en de ontwikkeling van RDPS. Dit is in overeenstemming met de aanpak volgens de verordening cyberweerbaarheid waarbij er vereisten en verplichtingen gelden voor fabrikanten, en niet voor de werking van het product met digitale elementen. Indien fabrikanten oplossingen ontwerpen en ontwikkelen die vervolgens door een derde worden geëxploiteerd, blijven zij verantwoordelijk voor de naleving van de essentiële vereisten van de verordening cyberweerbaarheid voor het product met digitale elementen dat zij in de handel brengen.

197. Er moet een onderscheid worden gemaakt tussen de gevallen waarin het ontwerp en de ontwikkeling worden uitgevoerd door fabrikanten (of onder hun verantwoordelijkheid) en gevallen waarin wordt vertrouwd op oplossingen van derden die niet door fabrikanten (of onder hun verantwoordelijkheid) zijn ontworpen en ontwikkeld. Het is bijvoorbeeld nuttig om rekening te houden met de meest voorkomende cloudmodellen waarover gebruikers in verschillende mate zeggenschap hebben en die ook worden genoemd in overweging 12 van de verordening cyberweerbaarheid, namelijk software als dienst ("software as a service", SaaS), platform als dienst ("platform as a service", PaaS) en infrastructuur als dienst ("infrastructure as a service", IaaS).

198. In het geval van een IaaS-oplossing van derden beheert of controleert de fabrikant de onderliggende fysieke en virtuele middelen (zoals de onderliggende hardware en de hypervisor van de aanbieder van clouddiensten) niet, maar is hij in staat willekeurige software uit te rollen en te gebruiken met behulp van dergelijke middelen, zoals besturingssystemen en applicaties. Dergelijke software wordt door de fabrikant zelf of onder zijn verantwoordelijkheid ontworpen en ontwikkeld en kan daarom als RDPS worden aangemerkt (indien deze aan de andere elementen van de definitie voldoet).

199. In het geval van een PaaS-oplossing van derden gebruikt de fabrikant zijn eigen (gebouwde of gekochte) applicatie met behulp van programmeertalen en uitvoeringsomgevingen die door de aanbieder van clouddiensten worden aangeboden, en integreert hij de applicatie in zijn product met digitale elementen. De fabrikant heeft zeggenschap over de applicatie en eventueel over de configuratie-instellingen voor de uitvoeringsomgeving. De applicatie is daarom ontworpen en ontwikkeld door de fabrikant zelf of onder zijn verantwoordelijkheid en kan daarom als RDPS worden aangemerkt (indien zij aan de andere elementen van de definitie voldoet).

200. In het geval van een SaaS-oplossing van derden biedt de SaaS-aanbieder de fabrikant een volledig ontwikkelde applicatie aan die in het product met digitale elementen van de fabrikant moet worden geïntegreerd. De fabrikant heeft beperkte mogelijkheden om gebruikersspecifieke configuratie-instellingen voor de applicatie te beheren. De applicatie is derhalve niet door de fabrikant zelf of onder zijn verantwoordelijkheid ontworpen en ontwikkeld.

201. Wanneer bepaalde elementen echter niet als RDPS kunnen worden aangemerkt (bv. de hypervisor in het geval van een IaaS-infrastructuur van derden, het besturingssysteem in het geval van een PaaS-oplossing van derden, of de SaaS-applicatie van derden), maar in het product met digitale elementen zijn geïntegreerd op een wijze die gevolgen heeft voor de beveiliging ervan, moeten dergelijke oplossingen als vergelijkbaar met componenten van derden worden beschouwd. De fabrikant is verplicht de risico's in verband met de integratie van die elementen vast te stellen en te beoordelen en deze aan te pakken door de essentiële vereisten op het product met digitale elementen zelf toe te passen. Dit kan in voorkomend geval worden ondersteund door de beveiligingsfuncties die de aanbieder van clouddiensten beschikbaar stelt via zijn model voor gedeelde verantwoordelijkheid, wanneer de fabrikant deze functies gebruikt of configureert om de vastgestelde risico's aan te pakken. Daarnaast wordt van de fabrikant verwacht dat hij een soortgelijke verplichting nakomt als de in artikel 13, lid 5, bedoelde verplichting om passende zorgvuldigheid te betrachten met betrekking tot de beveiliging van deze componenten, op een wijze die in verhouding staat tot het risico dat de oplossing op afstand vormt voor de beveiliging van het product met digitale elementen.

202. Derhalve kan dit als volgt worden samengevat:

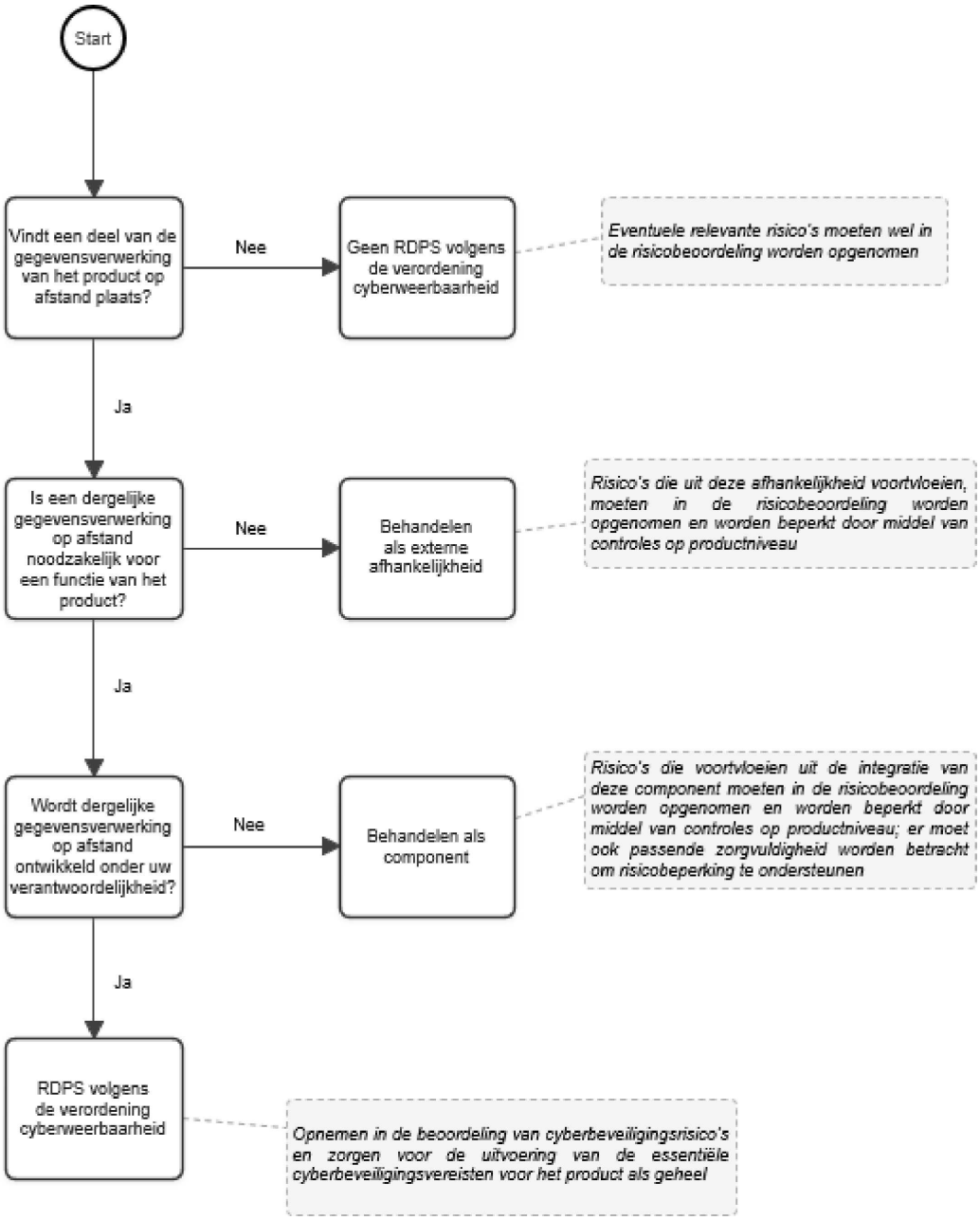
a) wil gegevensverwerking als RDPS kunnen worden aangemerkt, dan moet het antwoord op beide vragen in de punten *8.1.2*, "Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren?", en *8.1.3*, "Is de software ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant?", bevestigend zijn;

b) als het antwoord op de vraag in punt *8.1.2*, "Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren?", ontkennend is, moeten fabrikanten in het kader van hun risicobeoordeling de risico's beoordelen die voortvloeien uit het bestaan van een dergelijke gegevensverwerking;

c) als het antwoord op de vraag in punt *8.1.2*, "Zou het ontbreken van een dergelijke gegevensverwerking het product met digitale elementen beletten een van zijn functies uit te voeren?", bevestigend is, maar het antwoord op de vraag in punt *8.1.3*, "Is de software ontworpen en ontwikkeld door of onder de verantwoordelijkheid van de fabrikant?", ontkennend, dan moeten fabrikanten de oplossing van derden als een component behandelen. In het kader van de risicobeoordeling moeten fabrikanten de risico's beoordelen die voortvloeien uit de integratie van een dergelijke oplossing en deze dienovereenkomstig beperken. Daarnaast moeten fabrikanten passende zorgvuldigheid betrachten.

Figuur 9:

gestileerd stroomschema om te bepalen of een product met digitale elementen RDPS omvat



8.2. Praktische en technische gevolgen van oplossingen voor gegevensverwerking op afstand en afhankelijkheid van oplossingen van derden

203. De verordening cyberweerbaarheid volgt een risicogebaseerde aanpak, die is verankerd in artikel 13, leden 2 en 3, alsook in het eerste essentiële vereiste van deel I van bijlage I, waarin is bepaald dat "producten met digitale elementen […] zodanig [worden] ontworpen, ontwikkeld en geproduceerd dat zij een passend cyberbeveiligingsniveau op basis van de risico's waarborgen". Bijgevolg moet een risicogebaseerde aanpak worden overwogen bij de toepassing van de vereisten van de verordening cyberweerbaarheid op de RDPS en de behandeling van risico's die voortvloeien uit diensten van derden die in het product met digitale elementen zijn geïntegreerd.

204. Ten eerste moeten fabrikanten i) in de technische documentatie aangeven dat er bij hun product met digitale elementen sprake is van RDPS of het product afhankelijk is van oplossingen op afstand van derden, en ii) dergelijke oplossingen beschrijven. Als dezelfde RDPS meerdere producten met digitale elementen ondersteunt, moet de RDPS in de technische documentatie van elk product worden vermeld. De documentatie over RDPS die meerdere producten met digitale elementen bedient, kan zowel in diverse productconformiteitsbeoordelingen worden hergebruikt.

205. Zoals aangegeven in overweging 11, moet RDPS die deel uitmaakt van het product met digitale elementen en derhalve aan de conformiteitsbeoordeling van het product wordt onderworpen, worden beperkt tot de softwaremodules die verantwoordelijk zijn voor de functionaliteit van het product met digitale elementen, en tot de interfaces die deze modules gebruiken met externe diensten. Overige back-endsystemen die verdere verwerkingen uitvoeren en waarmee geen directe interactie is met het product met digitale elementen, worden niet als RDPS beschouwd.

206. Niettemin blijven die back-endsystemen externe afhankelijkheden die in het kader van de cyberbeveiligingsrisicobeoordeling moeten worden beoordeeld en door middel van maatregelen op productniveau moeten worden beperkt. Bij de door de fabrikant uitgevoerde risicobeoordeling moet in feite rekening worden gehouden met: i) risico's in verband met RDPS; ii) risico's in verband met het gebruik van oplossingen op afstand van derden (vergelijkbaar met componenten van derden), en iii) risico's in verband met de productomgeving (bv. onderliggende hardware). Fabrikanten moeten zelf beveiligingscontroles op het product met digitale elementen uitvoeren om die risico's te beperken.

207. Bovendien kan, als onderdeel van de conformiteitsbeoordeling en/of de naleving van de zorgvuldigheidsverplichtingen met betrekking tot diensten op afstand van derden, de volgende niet-uitputtende lijst van zekerheidsartefacten worden hergebruikt ter ondersteuning van de beoordeling van de fabrikant:

a) bewijs van nakoming van de verplichtingen uit hoofde van Uitvoeringsverordening (EU) 2024/2690 van de Commissie;

b) bewijs van nakoming van de verplichtingen uit hoofde van Verordening (EU) 2022/2554 (DORA-verordening);

c) conformiteitsverklaring of certificaat verkregen in het kader van een Europese regeling voor cyberbeveiligingscertificering (vastgesteld op grond van Verordening (EU) 2019/881, de cyberbeveiligingsverordening);

d) bewijs van conformiteit met ISO/IEC 27017:2015 of ISO/IEC 27001:2022.

208. Tot slot moeten fabrikanten in hun interacties met externe aanbieders van diensten op afstand de meest geschikte beveiligingsmaatregelen nemen op basis van hun risicobeoordeling (en, in voorkomend geval, ondersteund door het model van gedeelde verantwoordelijkheid van de aanbieder). Die risicobeperkende maatregelen moeten onder meer bestaan uit beveiligingscontroles voor hun producten met digitale elementen en de verificatie van beveiligingsmaatregelen die door de externe aanbieders zelf worden genomen (passende zorgvuldigheid). Een instrument om dergelijke risico's te beperken, kan erin bestaan veiligheidsgaranties op te nemen in dienstenniveauovereenkomsten (SLA's) met externe aanbieders, met inbegrip van garanties dat aanbieders kwetsbaarheden adequaat aanpakken. Een ingrijpende wijziging van de door de externe aanbieders van diensten op afstand aangeboden oplossingen mag niet worden aangemerkt als een ingrijpende wijziging van het product met digitale elementen, aangezien deze elementen niet onder de verantwoordelijkheid van de fabrikant vallen. In het kader van hun zorgvuldigheidsverplichtingen en om de risico's die voortvloeien uit het inschakelen van externe aanbieders correct te beperken, worden fabrikanten echter aangemoedigd ervoor te zorgen dat externe aanbieders van clouddiensten hen naar behoren op de hoogte houden van wijzigingen die zij in hun oplossingen aanbrengen. Op basis van dergelijke informatie kan het nodig zijn dat fabrikanten hun risicobeoordeling herzien. Bij de geactualiseerde risicobeoordeling moet worden nagegaan of de externe dienstverleners nog steeds voldoende garanties bieden op het gebied van cyberbeveiliging en of de beveiligingscontroles op productniveau nog steeds toereikend zijn. In sommige gevallen is het mogelijk dat fabrikanten dergelijke controles moeten aanpassen of naar een andere externe dienstverlener moeten overstappen.

8.3. **Praktijkvoorbeelden van oplossingen voor gegevensverwerking op afstand**

Om fabrikanten aanvullende praktische richtsnoeren te bieden, wordt in dit punt een reeks fictieve praktijkvoorbeelden gegeven, waarin typische producten met digitale elementen worden beschreven die afhankelijk zijn van gegevensverwerking op afstand en die laten zien of een dergelijke verwerking kan worden aangemerkt als oplossingen voor gegevensverwerking op afstand in de zin van de verordening cyberweerbaarheid.

8.3.1. *Mobiele bankapplicatie*

Een financiële entiteit brengt een mobiele bankapplicatie op de markt. De back-endsystemen van de app ondersteunen onder meer authenticatie, autorisatie, rekeningbeheer en betaalverkeer. De financiële entiteit gebruikt een hybride strategie op basis van interne infrastructuur en oplossingen op afstand van derden om de functionaliteiten van de app te ondersteunen. Het gaat onder meer om de volgende functionaliteiten:

Zelf gehoste infrastructuur die door de financiële entiteit is ontwikkeld:

— de klant opent de mobiele bankapplicatie en wordt geauthenticeerd via de bankinterface, een zelf gehoste oplossing die is ontwikkeld door de financiële entiteit die de verzoeken van de app ontvangt en de respectieve antwoorden terugstuurt. De bankinterface verifieert de identiteit van de klant door het rekeningbeheersysteem te doorzoeken en verleent toegang tot de applicatie;

— de klant initieert een overschrijving via de app. De app stuurt de opdracht door naar de bankinterface, die een overeenkomstig verzoek indient bij het grootboeksysteem;

— het rekeningbeheersysteem en het grootboeksysteem, beide zelf gehost maar logisch gescheiden van de bankinterface, registreren de transactie;

— het grootboeksysteem stuurt de transactiestatus terug naar de bankinterface, die het resultaat aan de klant laat zien.

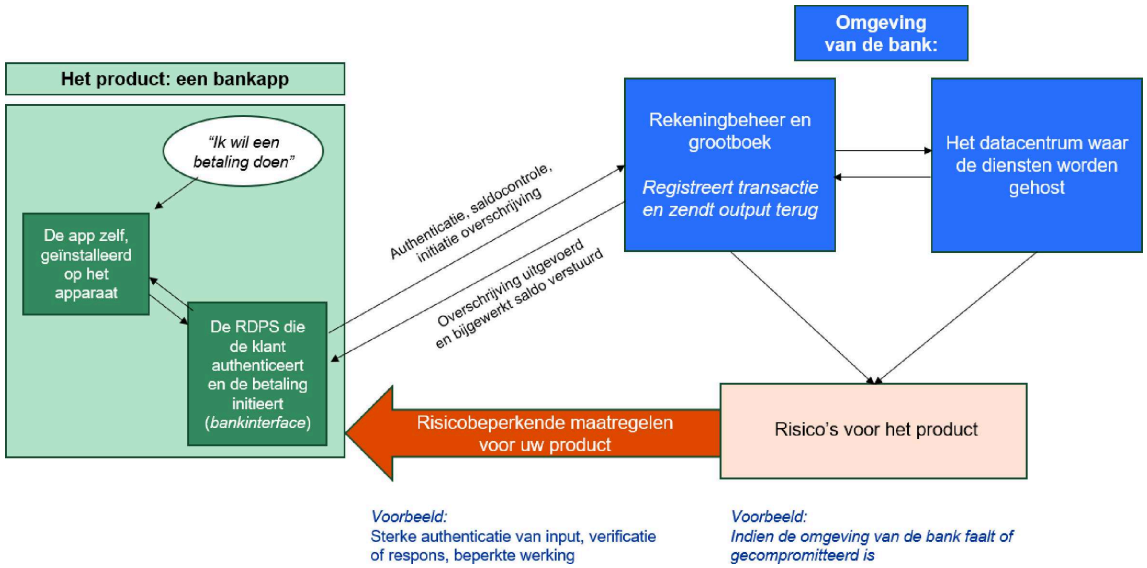
Gevolgen voor RDPS:

— de bankinterface is noodzakelijk voor de uitvoering van de functies van de app, namelijk het authenticeren van de klant, het versturen van de opdrachten van de klant, met inbegrip van opdrachten voor het uitvoeren van betalingen en het doen van overschrijvingen, en het teruggeven van de daaruit voortvloeiende status. De bankinterface wordt ontworpen en ontwikkeld onder de verantwoordelijkheid van de fabrikant. Aangezien het antwoord op beide vragen in de vorige punten bevestigend is, moet de bankinterface als RDPS worden beschouwd. Daarom moet het worden opgenomen in de cyberbeveiligingsrisicobeoordeling en in de uitvoering van de essentiële vereisten voor het product met digitale elementen als geheel. De daaropvolgende verwerking van een eenmaal ingediende opdracht, met name de registratie van de transactie in de systemen voor het beheer van rekeningen en grootboeken, afwikkeling en clearing, wordt uitgevoerd door systemen waarmee de app niet rechtstreeks contact heeft en wordt op die basis niet aangemerkt als RDPS;

— het rekeningbeheersysteem en het grootboeksysteem kwalificeren niet als RDPS voor de bankapplicatie. Er is geen sprake van rechtstreekse interactie met de app (in plaats daarvan is er interactie tussen de app en de bankinterface, die op zijn beurt op de systemen vertrouwt). Hoewel de beschikbaarheid van de systemen noodzakelijk kan zijn om een functie te voltooien, heeft de verordening cyberweerbaarheid alleen betrekking op die delen van het systeem waarbij er sprake is van directe interactie met het product met digitale elementen. Zij vallen derhalve buiten de definitie van RDPS voor de toepassing van de verordening cyberweerbaarheid. De systemen blijven echter externe afhankelijkheden die kunnen leiden tot aanzienlijke cyberbeveiligingsrisico's voor het product met digitale elementen. Zo kan het compromitteren van het grootboeksysteem een aanvaller in staat stellen de transactieresultaten te beïnvloeden die vervolgens in de applicatie worden weergegeven. De fabrikant moet die risico's daarom identificeren en beoordelen in het kader van de cyberbeveiligingsrisicobeoordeling en ze beperken door middel van maatregelen op productniveau, zoals een sterke authenticatie van de back-endinterfaces, bescherming van de integriteit van transactiegegevens, beveiligde communicatiekanalen en verificatie van de door de app ontvangen antwoorden.

Figuur 10:

gestileerde weergave van een bankapp op basis van RDPS



Door derden ontwikkelde SaaS voor klantenservice:

— de financiële entiteit integreert in de app een door een externe aanbieder ontwikkelde en beheerde chatoplossing voor klantenservice; de externe aanbieder heeft de chatservercode geschreven, heeft de gebruikersinterface gebouwd en beheert de infrastructuur waar de chat wordt gevoerd (d.w.z. het SaaS-model);

— wanneer de klant een vraag stelt, verbindt de app de klant met de dienst van de derde om een chatsessie tot stand te brengen en de berichtenstroom te beheren, zonder de derde toegang te verlenen tot centrale banksystemen.

Gevolgen voor RDPS:

— de ondersteunende chatoplossing is noodzakelijk opdat het product met digitale elementen een van zijn functies kan vervullen, maar is niet ontworpen en ontwikkeld door de financiële entiteit zelf of onder haar verantwoordelijkheid; het is derhalve geen RDPS. De oplossing moet echter worden behandeld als een component van derden. De afhankelijkheid van die dienst van derden kan cyberbeveiligingsrisico's voor de bankapplicatie met zich meebrengen, bijvoorbeeld als een aanvaller het chatkanaal zou gebruiken om zich als de bank voor te doen of om kwaadwillige inhoud aan gebruikers te geven. De financiële entiteit moet bij de cyberbeveiligingsrisicobeoordeling rekening houden met die risico's en deze beperken door middel van maatregelen op productniveau, zoals het isoleren van de chatfunctie van centrale bankfuncties, het controleren van gegevensstromen en het valideren van inhoud. Er moet ook passende zorgvuldigheid met betrekking tot de SaaS worden betracht.

8.3.2. *Slimme thermostaat*

Een slimme thermostaat stelt gebruikers in staat via een mobiele applicatie de temperatuur in huis te regelen. De mobiele applicatie en de slimme thermostaat maken gebruik van gegevensverwerking op afstand om gegevens uit te wisselen (bv. verzoek om de temperatuur te verhogen) en gegevens op te slaan (bv. gebruikersvoorkeuren). Deze functies werden ontwikkeld en ontworpen onder de verantwoordelijkheid van de fabrikant, maar worden geëxploiteerd op een onderliggende fysieke en virtuele infrastructuur die door een derde (IaaS van derden) ter beschikking wordt gesteld.

Aangezien de slimme thermostaat zonder deze gegevensverwerking op afstand niet in staat zou zijn de slimme functionaliteiten uit te voeren, zou het ontbreken ervan het product met digitale elementen beletten een of meer van zijn functies uit te voeren. Daarnaast is de software ontwikkeld en ontworpen onder de verantwoordelijkheid van de fabrikant van de slimme thermostaat. Daarom kan de gegevensverwerking op afstand worden aangemerkt als RDPS zoals gedefinieerd in de verordening cyberweerbaarheid.

Met het oog op de naleving van de verordening cyberweerbaarheid moet de fabrikant van de slimme thermostaat de RDPS en de afhankelijkheid van de IaaS van derden documenteren in de technische documentatie van het product met digitale elementen, met inbegrip van details over de gecontracteerde dienst. De fabrikant moet die elementen in aanmerking nemen bij de risicobeoordeling, die het beoogde doel en het redelijkerwijs te voorziene gebruik van het product met digitale elementen omvat. De fabrikant voert de essentiële vereisten van de verordening cyberweerbaarheid uit op basis van de risico's van de RDPS. Wat de IaaS van derden betreft, moet de fabrikant ervoor zorgen dat de beveiligingsmaatregelen van de externe aanbieder passend zijn en/of relevante maatregelen nemen ten aanzien van de infrastructuur. In het eerste geval zou de fabrikant bijvoorbeeld kunnen vragen om bewijs dat aan de NIS 2-verplichtingen is voldaan.

8.3.3. *E-reader*

De fabrikant van software voor e-readers maakt gebruik van een SaaS-opslagdienst van derden om door klanten gekochte elektronische boeken op te slaan en hen in staat te stellen toegang te krijgen tot hun boeken. Het ontbreken van deze opslagdienst zou het product met digitale elementen beletten een van zijn functies uit te voeren, maar de externe SaaS-opslagdienst is niet ontwikkeld door of onder de verantwoordelijkheid van de fabrikant; de SaaS-aanbieder stelt het voor alle gebruiksscenario's ter beschikking van de klanten.

De SaaS-opslagdienst voldoet niet aan de definitie van RDPS. De fabrikant van e-lezers vertrouwt echter op die externe dienst voor de werking van zijn product met digitale elementen en moet daarom bij de cyberbeveiligingsrisicobeoordeling rekening houden met de daaraan verbonden risico's. De fabrikant van de e-reader moet de SaaS als een component behandelen. De fabrikant moet passende beveiligingsmaatregelen op productniveau treffen, zoals beveiligde authenticatie, versleuteling en bescherming van de integriteit van de communicatie met de opslagdienst. Passende zorgvuldigheid bij de selectie en integratie van de SaaS-aanbieder dient ook ter ondersteuning van de verplichtingen van de fabrikant, zodat het product met digitale elementen als geheel aan de essentiële vereisten kan voldoen.

8.3.4. *Industriële robot*

Een industriële robot heeft tot taak onderdelen te verzamelen. De robot stuurt via camera's verzamelde informatie naar een dienst op afstand die door de fabrikant zelf is ontworpen en ontwikkeld. Deze dienst draait op een onderliggende fysieke en virtuele infrastructuur die wordt aangeboden door een externe dienstverlener (IaaS van derden). De clouddienst berekent de positie van een onderdeel op basis van de camerabeelden en stuurt opdrachten terug naar de robot om de onderdelen te verzamelen.

Zonder deze gegevensverwerking zou de industriële robot geen onderdelen kunnen verzamelen en dus een van zijn functies niet kunnen uitoefenen. Bovendien is de software die op de infrastructuur draait, ontworpen en ontwikkeld door de fabrikant zelf. De door de fabrikant zelf ontworpen en ontwikkelde software voldoet aan de definitie van RDPS.

De fabrikant van de industriële robot moet de RDPS en de afhankelijkheid van de IaaS van derden documenteren in de technische documentatie van het product met digitale elementen (met inbegrip van details over de gecontracteerde dienst). De fabrikant moet die elementen ook in aanmerking nemen bij de risicobeoordeling, die het beoogde doel en het redelijkerwijs te voorziene gebruik van het product met digitale elementen omvat. De fabrikant past de essentiële vereisten van het verordening cyberweerbaarheid toe op het product met digitale elementen, met inbegrip van RDPS, op basis van de risico's. Passende zorgvuldigheid bij de selectie van de IaaS-aanbieder dient ook ter ondersteuning van de verplichtingen van de fabrikant. De fabrikant zou bijvoorbeeld kunnen vragen om bewijs dat aan de NIS 2-verplichtingen is voldaan.

8.3.5. *Cellulair netwerk*

Een smartphone is afhankelijk van een 5G-netwerk om gebruikers een internetverbinding, telefoongesprekken en berichten te bieden (mobiele connectiviteit). Het cellulaire netwerk is ontwikkeld en ontworpen door exploitanten van telecommunicatiesystemen. Het netwerk bestaat uit kleine cellen en telefoonmasten en andere netwerkapparatuur.

Het product met digitale elementen moet correct verbinding kunnen maken met een netwerk; dit is een van de functies ervan. Of dat netwerk al dan niet operationeel is, is echter niet relevant om na te gaan of het product met digitale elementen correct werkt. Het netwerk is slechts een communicatiekanaal en is niet noodzakelijk voor het product met digitale elementen om zijn functie van "correct verbinding maken met een netwerk" te vervullen. Evenzo wordt een ethernetkabel, een router of een wifi-signaal niet beschouwd als gegevensverwerking waarvan de afwezigheid het product met digitale elementen zou beletten een van zijn functies uit te voeren, maar eerder als een katalysator van communicatie/connectiviteit.

Bijgevolg voldoet het cellulaire netwerk niet aan de definitie van RDPS. Het netwerk mag niet als een component van derden worden beschouwd, aangezien er in het product geen software met digitale elementen is geïntegreerd en het product in plaats daarvan louter op dit netwerk vertrouwt. Als zodanig hoeft de fabrikant geen zorgvuldigheidsverplichtingen ten aanzien van de netwerkaanbieder na te komen.

9. **AANVULLENDE ELEMENTEN**

9.1. **Meldingsplicht**

209. Op grond van artikel 14, leden 1 en 3, van de verordening cyberweerbaarheid moet een fabrikant tegelijkertijd het als coördinator aangewezen CSIRT en Enisa in kennis stellen van i) elke actief uitgebuite kwetsbaarheid in zijn product met digitale elementen waarvan hij kennis krijgt en ii) elk ernstig incident dat gevolgen heeft voor de beveiliging van het product met digitale elementen waarvan het kennis krijgt.

210. Overeenkomstig artikel 69, lid 3, en artikel 71, lid 2, tweede volzin, is de verplichting om aan artikel 14 te voldoen met ingang van 11 september 2026 van toepassing op alle producten met digitale elementen die binnen het toepassingsgebied van de verordening cyberweerbaarheid vallen, met inbegrip van producten met digitale elementen die vóór 11 december 2027 in de handel zijn gebracht. Bovendien blijft de meldingsplicht, in tegenstelling tot de verplichtingen inzake de respons op kwetsbaarheden, die alleen gelden voor de duur van de ondersteuningsperiode van een product, van toepassing nadat een product met digitale elementen niet langer wordt ondersteund. Indien een product met digitale elementen vóór 11 december 2027 in de handel is gebracht of indien de ondersteuningsperiode ervan is verstreken, is de fabrikant niet verplicht te voldoen aan de verplichtingen inzake de respons op kwetsbaarheden van deel II van bijlage I.

211. Er zij aan herinnerd dat de verplichting om dergelijke gebeurtenissen te melden van toepassing is zodra de fabrikant zich ervan bewust wordt dat een kwetsbaarheid actief wordt uitgebuit of dat zich een ernstig incident heeft voorgedaan dat ertoe heeft geleid dat de beveiliging van zijn product met digitale elementen in gevaar is gebracht. Daarom moeten richtsnoeren over wanneer een fabrikant geacht wordt daarvan kennis te hebben gekregen, fabrikanten helpen bepalen op welk moment de toepasselijke meldingstermijnen ingaan.

212. Fabrikanten kunnen onderworpen zijn aan een vergelijkbare meldingsplicht uit hoofde van verschillende EU-handelingen. Om ervoor te zorgen dat het begrip "er kennis van heeft gekregen" consequent wordt uitgelegd en om de naleving van die verplichtingen door fabrikanten te vergemakkelijken, zijn deze richtsnoeren afgestemd op overweging 31 van Uitvoeringsverordening (EU) 2024/2690 van de Commissie en afdeling II, punt A, van Richtsnoer 9/2022 inzake de melding van inbreuken in verband met persoonsgegevens uit hoofde van de AVG.

213. In sommige gevallen zal een fabrikant een verdacht voorval opmerken, of zal een derde, zoals een persoon, een klant, een entiteit, een autoriteit, een mediaorganisatie of een andere bron, een potentieel incident of kwetsbaarheid onder zijn aandacht brengen. In dergelijke gevallen moet de fabrikant het verdachte voorval onmiddellijk beoordelen om te bepalen of het een actief uitgebuite kwetsbaarheid of een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen vormt. De fabrikant moet derhalve worden geacht kennis te hebben gekregen van het feit dat hij na een dergelijke eerste beoordeling een redelijke mate van zekerheid heeft dat: i) een kwetsbaarheid in zijn product met digitale elementen actief wordt uitgebuit of ii) zich een ernstig incident heeft voorgedaan dat ertoe heeft geleid dat de beveiliging van zijn product met digitale elementen in gevaar is gebracht.

214. Daarom zal het tijdstip waarop een fabrikant kan worden geacht er kennis van te hebben gekregen, afhangen van de omstandigheden van de specifieke actief uitgebuite kwetsbaarheid of het ernstige incident. In sommige gevallen zal het van meet af aan relatief duidelijk zijn dat een kwetsbaarheid actief wordt uitgebuit of dat een ernstig incident gevolgen heeft voor de beveiliging van een product met digitale elementen. In andere gevallen kan het enige tijd duren om vast te stellen of een product met digitale elementen is getroffen door een kwetsbaarheid en of die kwetsbaarheid wordt uitgebuit door een kwaadwillige actor, dan wel of een incident gevolgen heeft voor de beveiliging van een product met digitale elementen. De nadruk moet echter liggen op onmiddellijk handelen om een eerste beoordeling uit te voeren om te bepalen of inderdaad aan dergelijke voorwaarden is voldaan, met name wanneer de kwetsbaarheid een aanzienlijk risico kan vormen, en in dat geval om corrigerende maatregelen te nemen en een melding te doen overeenkomstig de verordening cyberweerbaarheid.

215. Bovendien vereist de structuur van de meldingsplicht dat fabrikanten hun melding actualiseren naarmate het interne onderzoek vordert en zij meer te weten komen over de actief uitgebuite kwetsbaarheid of het incident. Fabrikanten moeten met name onverwijld en in elk geval binnen 24 uur nadat zij er kennis van hebben gekregen, een vroegtijdige waarschuwing met beperkte informatie indienen. In het kader van de melding moet vervolgens onverwijld en in elk geval binnen 72 uur na kennisneming aanvullende informatie worden verstrekt ("72-uursmelding"). De volledige melding moet zijn ingediend binnen 14 dagen nadat een corrigerende of risicobeperkende maatregel beschikbaar is voor actief uitgebuite kwetsbaarheden, of binnen één maand na de 72-uursmelding voor ernstige incidenten.

216. Zoals ook in herinnering is gebracht in punt *3.3.1*, "Langdurige ondersteuning en waarborging van de levensvatbaarheid van FOSS", zijn opensourcesoftwarestewards ook verplicht actief uitgebuite kwetsbaarheden te melden overeenkomstig artikel 24, lid 3 ([30]). Deze verplichting geldt zodra zij kennis krijgen van een actief uitgebuite kwetsbaarheid, en niet alleen wanneer er sprake is van een kwetsbaarheid in de codebase van FOSS waarvan die entiteit de steward is. In de praktijk zal een steward, omdat FOSS-componenten doorgaans downstream worden geïntegreerd in andere producten met digitale elementen, waarschijnlijk kennis krijgen van actieve uitbuiting via een melding van derden, waarin wordt vastgesteld dat de uitbuiting in FOSS-componenten is geïntegreerd in andere producten met digitale elementen. Dit kan bijvoorbeeld het geval zijn wanneer een fabrikant van een product met digitale elementen actieve uitbuiting in een in zijn eigen product geïntegreerde FOSS-component detecteert en meldt aan de steward van die component; of wanneer een gebruiker of een beveiligingsonderzoeker bewijs vindt van uitbuiting van een FOSS-component die is geïntegreerd in een product met digitale elementen en die actieve uitbuiting meldt aan de steward van de component.

217. Ook moet worden verduidelijkt dat, aangezien de verplichting om actief uitgebuite kwetsbaarheden te melden van toepassing is wanneer de fabrikant kennis krijgt van actieve uitbuiting, de fabrikant niet verplicht is kwetsbaarheden te melden waarvan hij reeds vóór 11 september 2026 (de datum waarop de meldplicht van toepassing wordt) kennis had gekregen. De verordening cyberweerbaarheid vereist derhalve niet dat dergelijke kwetsbaarheden met terugwerkende kracht worden gemeld. De verplichting is daarentegen wel van toepassing wanneer de fabrikant vóór 11 september 2026 op de hoogte was van een kwetsbaarheid, maar op dat moment niet op de hoogte was van een actieve uitbuiting ervan (hetzij omdat die nog niet had plaatsgevonden, hetzij omdat de fabrikant er geen kennis van had). Indien na 11 september 2026 vervolgens actieve uitbuiting plaatsvindt of de fabrikant er kennis van krijgt, wordt de kwetsbaarheid beschouwd als een actief uitgebuite kwetsbaarheid waarvoor de meldplicht geldt.

218. Evenzo is een fabrikant alleen verplicht actief uitgebuite kwetsbaarheden in zijn product met digitale elementen te melden. Wanneer een product met digitale elementen een actief uitgebuite kwetsbaarheid bevat die afkomstig is van een component van derden, moet de fabrikant van het product met digitale elementen die actief uitgebuite kwetsbaarheid melden. Indien een fabrikant zich er echter van bewust is dat een component van derden een kwetsbaarheid bevat, maar die kwetsbaarheid i) niet kan worden uitgebuit in zijn product met digitale elementen (bv. omdat de kwetsbare code niet bereikbaar is) of ii) niet is uitgebuit in zijn product met digitale elementen, kan die kwetsbaarheid niet worden aangemerkt als een actief uitgebuite kwetsbaarheid in zijn product met digitale elementen, en is die fabrikant derhalve niet onderworpen aan de meldplicht. Die fabrikant kan die kwetsbaarheid nog steeds op vrijwillige basis melden overeenkomstig artikel 15 van de verordening cyberweerbaarheid. Ook moet de fabrikant voldoen aan de vereisten inzake de respons op kwetsbaarheden van deel II van bijlage I bij de verordening cyberweerbaarheid, en de kwetsbaarheid melden aan de persoon of entiteit die de component vervaardigt of onderhoudt, overeenkomstig artikel 13, lid 6, en zoals nader toegelicht in punt *9.2.1*, "Upstream melden en beveiligingsoplossingen delen".

([30]) Voor zover de steward betrokken is bij de ontwikkeling van een product met digitale elementen.

219. Nadat fabrikanten kennis hebben gekregen van een actief uitgebuite kwetsbaarheid of een ernstig incident, moeten zij overeenkomstig artikel 14, lid 8, ook de getroffen gebruikers, en in voorkomend geval alle gebruikers, informeren. Indien zij dit niet tijdig doen, kunnen de CSIRT's die de melding hebben ontvangen, dergelijke informatie aan gebruikers verstrekken wanneer dit evenredig en noodzakelijk wordt geacht om de gevolgen van die kwetsbaarheid of dat incident te voorkomen of te beperken.

220. In overeenstemming met de risicogebaseerde aanpak van de verordening cyberweerbaarheid moet de in artikel 14, lid 8, vastgestelde verplichting om gebruikers te informeren op risicogebaseerde en evenredige wijze worden toegepast. Met name houdt het verstrekken van informatie over een actief uitgebuite kwetsbaarheid of een ernstig incident niet in dat dergelijke informatie openbaar moet worden gemaakt of ongedifferentieerd openbaar moet worden gemaakt. In voorkomend geval, en in het licht van de aard van het product met digitale elementen, de getroffen gebruikers en de mogelijke gevolgen van de kwetsbaarheid of het incident, kunnen fabrikanten de bekendmaking van gedetailleerde informatie beperken tot de betrokken relevante gebruikers of klanten. Dit is met name het geval voor producten met digitale elementen die worden gebruikt in gevoelige of essentiële omgevingen, waar de openbaarmaking van technische details zelf de cyberbeveiligingsrisico's kan vergroten of verdere uitbuiting kan vergemakkelijken.

221. Zodra de kwetsbaarheid adequaat is aangepakt of beperkt, kan bredere openbaarmaking passend zijn. Dit zou bijvoorbeeld het geval zijn wanneer openbaarmaking bijdraagt tot een groter algemeen bewustzijn of gebruikers in staat stelt na te gaan of hun producten met digitale elementen niet langer in gevaar zijn. In dergelijke gevallen moeten de mate van detail en het moment van een bredere openbaarmaking evenredig blijven en rekening houden met de restrisico's van uitbuiting, de aard van het product met digitale elementen en de belangen van de betrokken gebruikers. Bovendien moeten fabrikanten op grond van deel II, punt 4), van bijlage I informatie over verholpen kwetsbaarheden openbaar maken zodra een beveiligingsupdate beschikbaar wordt gesteld.

9.2. **Respons op kwetsbaarheden**

9.2.1. *Upstream melden en beveiligingsoplossingen delen*

222. Op grond van artikel 13, lid 6, van de verordening cyberweerbaarheid moeten fabrikanten kwetsbaarheden in geïntegreerde componenten melden aan de persoon of entiteit die die component vervaardigt of onderhoudt ("upstream melden").

223. Fabrikanten zijn alleen verplicht om upstream een melding te doen met betrekking tot de versie van de component die zij integreren. Indien de persoon of entiteit die de component vervaardigt of onderhoudt beveiligingsbeleid, gecoördineerde procedures voor de openbaarmaking van kwetsbaarheden of aangewezen kanalen voor het melden van kwetsbaarheden heeft vastgesteld, moeten fabrikanten in overeenstemming daarmee hun melding indienen, met name wanneer vroegtijdige openbaarmaking van niet-gepatchte kwetsbaarheden de cyberbeveiligingsrisico's zou kunnen vergroten. Om de belasting van upstream-onderhoudsbedrijven te verminderen, met name bij opensourceprojecten, zijn fabrikanten bovendien niet verplicht om upstream een melding te doen wanneer zij kunnen bevestigen dat de persoon of entiteit die een component vervaardigt of onderhoudt, zich al bewust is van het bestaan van een kwetsbaarheid. Fabrikanten worden aangemoedigd redelijke maatregelen te nemen om te voorkomen dat dubbele meldingen worden ingediend, bijvoorbeeld door openbaar toegankelijke kwetsbaarheidsdatabanken, projectspecifieke veiligheidsadviezen of gevestigde probleemtrackers te controleren voordat zij upstream een melding doen.

224. Fabrikanten zijn alleen verplicht om upstream een melding te doen van de kwetsbaarheden die in de geïntegreerde component zelf bestaan, en niet van kwetsbaarheden die bestaan als gevolg van de integratie tussen de component en een andere door de fabrikant ontwikkelde code of door de integratie van andere componenten. Niettemin kunnen er situaties zijn waarin de integratie van een component in een specifiek product met digitale elementen bepaalde gedragingen, interacties of veiligheidsrelevante kenmerken van die component blootlegt die afzonderlijk van elkaar niet duidelijk of niet gemakkelijk identificeerbaar waren. In dergelijke gevallen worden fabrikanten aangemoedigd deze informatie te delen met de persoon of entiteit die het onderdeel vervaardigt of onderhoudt, teneinde goede praktijken voor de respons op kwetsbaarheden te bevorderen die gericht zijn op het vergemakkelijken van doeltreffend herstel en het verbeteren van de algemene veiligheid van het ecosysteem van componenten.

225. Tot slot zijn fabrikanten ook niet verplicht de kwetsbaarheid upstream te melden wanneer de component niet langer een onderhouder heeft of wanneer de fabrikant niet langer afhankelijk is van de oorspronkelijke onderhouder voor nieuwe versies of beveiligingsoplossingen. In dergelijke gevallen wordt de fabrikant niettemin aangemoedigd om gebruikers van die component te informeren via redelijke alternatieve maatregelen, bv. via bestaande "community"-mechanismen (zoals mailinglijsten of het verspreiden van tickets) of via openbare kwetsbaarheidsregisters.

226. Bovendien moeten fabrikanten die een softwarewijziging hebben ontwikkeld om een kwetsbaarheid in een geïntegreerde component aan te pakken, op grond van artikel 13, lid 6, die softwarewijziging ("beveiligingsoplossing") delen met de persoon of entiteit die de component vervaardigt of onderhoudt ("upstream delen").

227. Wanneer fabrikanten krachtens artikel 13, lid 6, verplicht zijn een beveiligingsoplossing te delen, moet deze oplossing in voorkomend geval in een machineleesbaar formaat worden verstrekt, op een wijze die gemakkelijk kan worden geverifieerd en, in voorkomend geval, kan worden geïntegreerd door de persoon of entiteit die de component vervaardigt of onderhoudt. Wanneer de component een vrije en opensourcecomponent is, moet de beveiligingsoplossing worden gedeeld op een wijze die verenigbaar is met de licentie van die component, bijvoorbeeld door het te delen onder dezelfde licentie of onder een licentie die de onderhouder in staat stelt de component onder zijn eigen licentie te distribueren. Indien de onderhouder van die component richtsnoeren heeft over de wijze waarop beveiligingsoplossingen moeten worden gedeeld, moet de fabrikant die richtsnoeren volgen.

228. Fabrikanten worden er in de verordening cyberweerbaarheid echter niet toe verplicht ervoor te zorgen dat hun beveiligingsoplossingen noodzakelijkerwijs worden aanvaard door de persoon of entiteit die de component vervaardigt of onderhoudt. Zij zijn evenmin verplicht ervoor te zorgen dat deze oplossingen noodzakelijkerwijs worden geïntegreerd in het coderegister van de component, bijvoorbeeld wanneer de onderhouder de voorkeur kan geven aan een andere optie om het probleem op te lossen. Evenzo zijn fabrikanten niet verplicht een voorgestelde oplossing te aanvaarden die door de onderhouder van de component is ontwikkeld, en kunnen zij er de voorkeur aan geven het probleem op andere geschikte manieren te verhelpen.

229. In sommige gevallen kan de persoon of entiteit die de component vervaardigt of onderhoudt, reeds een beveiligingsoplossing hebben verstrekt om de kwetsbaarheid aan te pakken, maar besluit een fabrikant een andere risicobeperkingsstrategie te volgen (bv. door een andere configuratie te wijzigen). In dergelijke gevallen vereist de verordening cyberweerbaarheid niet dat de fabrikant de wijziging van een ander deel van het systeem upstream deelt. De fabrikant wordt niettemin aangemoedigd dit wel te doen wanneer dit de persoon of entiteit die de component onderhoudt, kan ondersteunen.

9.2.2. *Bekende uitbuitbare kwetsbaarheden*

230. In een van de essentiële vereisten van deel I van bijlage I bij de verordening cyberweerbaarheid is bepaald dat, op basis van de in artikel 13, lid 2, bedoelde cyberbeveiligingsrisicobeoordeling, en in voorkomend geval, producten met digitale elementen op de markt moeten worden aangeboden zonder bekende kwetsbaarheden die kunnen worden uitgebuit.

231. In artikel 3, punt 41), wordt "uitbuitbare kwetsbaarheid" gedefinieerd als "een kwetsbaarheid die onder praktische operationele omstandigheden effectief door een tegenstander zou kunnen worden gebruikt". Niet alle kwetsbaarheden kunnen worden uitgebuit onder praktische operationele omstandigheden, en sommige kwetsbaarheden kunnen alleen worden uitgebuit onder theoretische omstandigheden (bv. in een lab of in een simulatie) en/of niet onder omstandigheden die zich zouden voordoen in de operationele omgeving van een product met digitale elementen.

232. In de verordening cyberweerbaarheid wordt vereist dat fabrikanten over passende beleidslijnen en procedures beschikken om potentiële kwetsbaarheden die door interne of externe bronnen zijn gemeld, aan te pakken en te verhelpen (artikel 13, lid 8). Er wordt echter niet uitdrukkelijk gespecificeerd wanneer een uitbuitbare kwetsbaarheid moet worden geacht bekend te zijn bij de fabrikant, waardoor de verplichting ontstaat om aan dit essentiële vereiste te voldoen op het moment van het in de handel brengen.

233. Een kwetsbaarheid moet als bekend worden beschouwd wanneer deze is opgenomen in toepasselijke openbaar toegankelijke kwetsbaarheidsdatabanken, zoals de bij artikel 12, lid 2, van Richtlijn (EU) 2022/2555 opgezette Europese kwetsbaarheidsdatabank of andere prominente kwetsbaarheidsdatabanken.

234. Daarnaast kan een kwetsbaarheid ook bekend zijn wanneer de fabrikant hiervan op de hoogte is gebracht via niet-openbare informatie, bijvoorbeeld via gecoördineerde openbaarmaking door een veiligheidsonderzoeker of via de eigen interne tests en analyses van de fabrikant, bijvoorbeeld wanneer gebruik wordt gemaakt van door AI aangedreven diensten. Evenzo kan een kwetsbaarheid bekend zijn wanneer er publiekelijk en prominent melding van is gemaakt in betrouwbare mediakanalen, waaronder gespecialiseerde publicaties op het gebied van cyberbeveiliging of de algemene massamedia.

235. Het enkele feit dat een kwetsbaarheid wordt gemeld of gevonden, betekent op zich echter niet dat deze in de praktijk kan worden uitgebuit of van toepassing is op het specifieke product met digitale elementen in kwestie. De fabrikant moet dit onderzoeken en de controleren of dergelijke informatie klopt en van toepassing is op zijn eigen product met digitale elementen. Bijgevolg kan er een beperkte periode verstrijken tussen de eerste melding van de kwetsbaarheid en de bevestiging ervan. Zoals aangegeven in punt *9.1*, "Meldingsplicht", moet de nadruk liggen op snelle maatregelen om de zaak te onderzoeken en actie te ondernemen.

236. Bovendien is de verplichting voor fabrikanten om te voldoen aan de essentiële vereisten van deel I van bijlage I van toepassing op het moment van het in de handel brengen, overeenkomstig artikel 13, lid 1. In de praktijk kan het gebeuren dat nieuwe mogelijk uitbuitbare kwetsbaarheden worden ontdekt in de laatste fasen van de ontwikkelingscyclus van het product met digitale elementen, kort voordat het in de distributieketen terechtkomt (en dus in de handel wordt gebracht).

237. Aangezien de verplichting om producten met digitale elementen in de handel te brengen zonder bekende uitbuitbare kwetsbaarheden, een risicogebaseerde verplichting is, is het aan de fabrikant om op basis van de cyberbeveiligingsrisicobeoordeling te bepalen of het product met digitale elementen veilig in de handel kan worden gebracht, in overeenstemming met de verordening cyberweerbaarheid. Als alternatief kan de fabrikant bepalen dat een nieuwe kwetsbaarheid die mogelijk bekend is geworden, moet worden verholpen voordat het product met digitale elementen in de handel kan worden gebracht. Bij die vaststelling moeten fabrikanten rekening houden met de ernst, de uitbuitbaarheid en de mogelijke gevolgen van de kwetsbaarheid, alsook met de risico's die zich voordoen voor het product met digitale elementen zelf zodra het in gebruik is genomen. Zij kunnen ook rekening houden met het risico dat de release van het product wordt uitgesteld totdat de kwetsbaarheid is verholpen, bijvoorbeeld omdat de nieuwe release ook andere kwetsbaarheden aanpakt die kunnen worden uitgebuit, of noodzakelijk is voor de continue werking van kritieke systemen. Hoe dan ook blijft de fabrikant, zodra een product met digitale elementen in de handel is gebracht, verplicht om kwetsbaarheden doeltreffend en in overeenstemming met de vereisten inzake de respons op kwetsbaarheden van deel II van bijlage I aan te pakken.

9.2.3. *Doeltreffende en regelmatige tests en evaluaties*

238. Op grond van deel II, punt 3), van bijlage I moeten fabrikanten gedurende de hele ondersteuningsperiode doeltreffende en regelmatige tests en beoordelingen van het product met digitale elementen uitvoeren. Het uitvoeren van regelmatige tests vereist niet de automatische herhaling, met vaste tussenpozen, van een verder ongewijzigd testprogramma. Het houdt in dat er regelmatig wordt geëvalueerd of nieuwe informatie, over bijvoorbeeld nieuw vastgestelde dreigingen of nieuw ontdekte kwetsbaarheden, vereist dat de bestaande tests worden geactualiseerd, en dat dienovereenkomstig tests worden uitgevoerd.

239. De frequentie, diepgang en inhoud van de evaluatie moeten in verhouding staan tot het cyberbeveiligingsrisicoprofiel van het product met digitale elementen, de evolutie ervan in de loop van de tijd en de stand van het dreigingslandschap. Wanneer uit de evaluatie blijkt dat er relevante nieuwe informatie is die van invloed is op de testset, moeten er nieuwe of gewijzigde tests voor het product worden ontwikkeld en uitgevoerd om ervoor te zorgen dat kwetsbaarheden worden aangepakt. Dit kan het opnieuw uitvoeren van bestaande tests omvatten wanneer door een wijziging van het product met digitale elementen dergelijke soorten tests passend zijn, zoals regressietests.

240. Indien uit de evaluatie niet blijkt dat er sprake is van dergelijke informatie, hoeven er geen aanvullende tests te worden ontwikkeld. Andere verplichtingen inzake de respons op kwetsbaarheden, waaronder de verplichting om kwetsbaarheden in verband met de risico's aan te pakken en te verhelpen, blijven eveneens toepassing.

9.3. **Raakvlakken met andere wetgeving**

9.3.1. *Verordening (EU) 2019/2144 en Verordening (EU) nr. 168/2013*

241. In artikel 2, lid 2, punt c), van de verordening cyberweerbaarheid is bepaald dat de verordening niet van toepassing is op producten met digitale elementen waarop Verordening (EU) 2019/2144 van toepassing is. Verordening (EU) 2019/2144 is van toepassing op "voertuigen van de categorieën M, N en O, zoals gedefinieerd in artikel 4 van Verordening (EU) 2018/858, en op systemen, onderdelen en technische eenheden die voor dergelijke voertuigen worden ontworpen en gebouwd".

242. Evenzo zijn producten met digitale elementen die binnen het toepassingsgebied van Verordening (EU) nr. 168/2013 vallen, bij Gedelegeerde Verordening (EU) 2025/1535 van de Commissie uitgesloten van het toepassingsgebied van de verordening cyberweerbaarheid. Verordening (EU) nr. 168/2013 is van toepassing op voertuigen van categorie L en "op voor dergelijke voertuigen ontworpen en gebouwde systemen, onderdelen en technische eenheden, alsook voertuigdelen en uitrustingsstukken" (artikel 2, lid 1).

243. Voertuigen waarop deze verordeningen van toepassing zijn, vallen niet onder de verordening cyberweerbaarheid. Voorts zijn aanvullende verduidelijkingen nodig met betrekking tot het toepassingsgebied van de vrijstelling voor systemen, onderdelen, technische eenheden, voertuigdelen en uitrustingsstukken (voor de toepassing van dit punt "componenten") die voor dergelijke voertuigen zijn ontworpen en gebouwd en die worden beschouwd als producten met digitale elementen in de zin van de verordening cyberweerbaarheid.

244. Dergelijke componenten worden geacht niet onder de verordening cyberweerbaarheid te vallen, mits zij uitsluitend zijn ontworpen en gebouwd voor integratie in voertuigen die onder de Verordeningen (EU) 2019/2144 en (EU) nr. 168/2013 vallen. Dit is het geval ongeacht of de fabrikant van die component deze rechtstreeks aan de voertuigfabrikant of aan een andere marktdeelnemer in de toeleveringsketen van de automobielsector verkoopt, zolang de component duidelijk bedoeld en alleen geschikt is voor uiteindelijke integratie in die voertuigen.

245. Een fabrikant die generieke componenten verkoopt die producten met digitale elementen zijn die in verschillende soorten producten kunnen worden geïntegreerd, en niet uitsluitend in voertuigen die onder die verordeningen vallen, is daarentegen onderworpen aan de verordening cyberweerbaarheid.

246. De beoordeling of een component in de zin van de verordening cyberweerbaarheid in de handel wordt gebracht, moet gebaseerd zijn op de objectieve voorwaarden waaronder de component op de markt wordt aangeboden. Wanneer een fabrikant een component aanbiedt die niet uitsluitend geschikt is voor uiteindelijke integratie in die voertuigen via distributiekanalen die openstaan voor klanten buiten de toeleveringsketen van de automobielsector, zoals algemene verkooppunten of onlineverkoopkanalen die bestellingen van het grote publiek aanvaarden, valt de component binnen het toepassingsgebied van de verordening cyberweerbaarheid, ongeacht eventuele verklaringen over het beoogde gebruik ervan. In dergelijke omstandigheden kan de component niet worden geacht uitsluitend te zijn ontworpen en gebouwd voor integratie in voertuigen die onder de Verordening (EU) 2019/2144 en Verordening (EU) nr. 168/2013 vallen, en moet de fabrikant voldoen aan de verordening cyberweerbaarheid. Daarentegen kan het gebruik van beperkte, business-to-business distributiekanalen die beperkt zijn tot de toeleveringsketen van de automobielsector erop wijzen dat deze uitsluitend voor een dergelijke integratie is ontworpen en gebouwd.

9.3.2. *Geldigheid van EU-typeonderzoekscertificaten (artikel 69, lid 1)*

247. Volgens artikel 69, lid 1, van de verordening cyberweerbaarheid blijven "[c]ertificaten van EU-typeonderzoek en goedkeuringsbesluiten die zijn afgegeven met betrekking tot cyberbeveiligingsvereisten voor onder andere harmonisatiewetgeving van de Unie dan deze verordening vallende producten met digitale elementen, {…] geldig tot en met 11 juni 2028, tenzij zij vóór die datum vervallen, of tenzij anders bepaald in dergelijke andere harmonisatiewetgeving van de Unie, in welk geval zij geldig blijven als bedoeld in die wetgeving".

248. De blijvende geldigheid van dergelijke certificaten en goedkeuringsbesluiten moet worden opgevat als beperkt tot de cyberbeveiligingsrisico's en de overeenkomstige eisen die vallen onder de respectieve harmonisatiewetgeving van de Unie op basis waarvan zij zijn afgegeven. Voor die risico's hoeven fabrikanten de naleving niet uitsluitend voor de toepassing van de verordening cyberweerbaarheid opnieuw te beoordelen of aan te tonen tijdens de in artikel 69, lid 1, bedoelde geldigheidsduur voor producten met digitale elementen die zij voornemens zijn op of na 11 december 2027 en tot en met 11 juni 2028 in de handel te brengen ([31]). Dit is het geval voor certificaten en goedkeuringsbesluiten die worden afgegeven wanneer de toepasselijke harmonisatiewetgeving van de Unie vereist dat de fabrikant de conformiteitsbeoordelingsprocedure via een aangemelde instantie uitvoert, of wanneer de fabrikant er vrijwillig voor heeft gekozen dit te doen.

249. Bijgevolg ontslaat het bestaan van een geldig certificaat of goedkeuringsbesluit uit hoofde van andere harmonisatiewetgeving van de Unie fabrikanten niet van de verplichting om een uitgebreide cyberbeveiligingsrisicobeoordeling uit te voeren in het kader van de verordening cyberweerbaarheid (of van andere verplichtingen uit hoofde daarvan). In plaats daarvan kunnen zij voor hun conformiteitsbeoordelingsprocedure vertrouwen op bestaande certificeringen als bewijs van conformiteit, voor zover de overeenkomstige cyberbeveiligingsrisico's reeds zijn gedekt. Indien het certificaat of goedkeuringsbesluit op grond van andere harmonisatiewetgeving van de Unie geldig is tot na 11 juni 2028, mag de fabrikant zich voor de toepassing van de verordening cyberweerbaarheid niettemin slechts tot en met 11 juni 2028 op dat certificaat of besluit beroepen.

250. Indien bij de overeenkomstig artikel 13, lid 2, uitgevoerde cyberbeveiligingsrisicobeoordeling aanvullende risico's worden vastgesteld die niet vallen onder de cyberbeveiligingsvereisten die ten grondslag liggen aan het bestaande certificaat of goedkeuringsbesluit, blijven de fabrikanten verantwoordelijk voor het aanpakken van die risico's overeenkomstig de verordening cyberweerbaarheid. In dergelijke gevallen vereist conformiteit dat de vastgestelde problemen worden beoordeeld en beperkt, ongeacht of het bestaande certificaat of goedkeuringsbesluit nog geldig is.

251. Dit kan worden geïllustreerd met het volgende voorbeeld waarin een product met digitale elementen onderworpen is aan de cyberbeveiligingsvereisten van Gedelegeerde Verordening (EU) 2022/30 van de Commissie tot aanvulling van Richtlijn 2014/53/EU (gedelegeerde handeling bij de richtlijn radioapparatuur), en waarin op basis van die vereisten een EU-typeonderzoekscertificaat of een goedkeuringsbesluit is afgegeven. In dat geval blijft het certificaat of besluit overeenkomstig artikel 69, lid 1, geldig voor de cyberbeveiligingsrisico's die onder dat certificaat vallen en verband houden met de essentiële eisen inzake cyberbeveiliging van Richtlijn 2014/53/EU (de richtlijn radioapparatuur).

252. In dergelijke gevallen zijn fabrikanten voor de toepassing van de verordening cyberweerbaarheid niet verplicht de conformiteit opnieuw te beoordelen of aan te tonen met betrekking tot de risico's die reeds door die certificaten worden aangepakt, zolang het desbetreffende certificaat of goedkeuringsbesluit geldig blijft en in elk geval niet na 11 juni 2028. Dit omvat bijvoorbeeld cyberbeveiligingsrisico's in verband met netwerkbescherming, bescherming van persoonsgegevens en privacy of preventie van fraude (voor zover die risico's onder dat certificaat vallen) in verband met de cyberbeveiligingsvereisten van de richtlijn radioapparatuur en zoals weergegeven in de conformiteitsbeoordeling.

253. Wanneer bij de overeenkomstig artikel 13, lid 2, van de verordening cyberweerbaarheid uitgevoerde cyberbeveiligingsrisicobeoordeling echter aanvullende cyberbeveiligingsrisico's worden vastgesteld die niet door die certificaten worden gedekt, blijven de fabrikanten verantwoordelijk voor het aanpakken van die risico's overeenkomstig de verordening cyberweerbaarheid. Hierbij kan het bijvoorbeeld gaan om risico's in verband met procedures voor de respons op kwetsbaarheden, minimale gegevensverwerking en vermindering van het aanvalsoppervlak, of andere productspecifieke cyberbeveiligingsaspecten die niet in die certificaten aan bod komen of in elk geval niet onder de essentiële eisen inzake cyberbeveiliging van de richtlijn radioapparatuur vallen.

254. Het bestaan van een geldig certificaat van EU-typeonderzoek of goedkeuringsbesluit op grond van de richtlijn radioapparatuur voor de essentiële eisen ervan met betrekking tot cyberbeveiliging toont op zich dus niet aan dat de verordening cyberweerbaarheid volledig wordt nageleefd. In plaats daarvan kunnen fabrikanten dat certificaat of besluit gebruiken als bewijs van conformiteit voor de overeenkomstige risico's, waarbij ervoor wordt gezorgd dat alle resterende of nieuw vastgestelde risico's worden beoordeeld en beperkt in overeenstemming met de verordening cyberweerbaarheid.

([31]) Producten met digitale elementen die vóór 11 december 2027 in de handel zijn gebracht, zijn onderworpen aan de wetgeving van de Unie die van toepassing is op het moment dat zij in de handel worden gebracht en, indien zij conform waren, kunnen zij worden verkocht en in gebruik worden genomen, tenzij zij op of na 11 december 2027 ingrijpende wijzigingen ondergaan. Zie voor de begrippen "in de handel brengen" en "op de markt aanbieden" ook punt *2.1*, "In de handel brengen", van dit document en hoofdstuk 2 van de Blauwe Gids.

255. Evenzo blijft, wanneer een product met digitale elementen onderworpen is aan de essentiële gezondheids- en veiligheidseisen met betrekking tot cyberbeveiliging van Verordening (EU) 2023/1230 (de machineverordening), die volledig van toepassing zijn met ingang van 20 januari 2027, en wanneer op basis van die eisen een EU-typeonderzoekscertificaat of een goedkeuringsbesluit is afgegeven, dat certificaat of dat goedkeuringsbesluit overeenkomstig artikel 69, lid 1, van de verordening cyberweerbaarheid geldig voor de cyberbeveiligingsrisico's die onder de machineverordening vallen.

256. Dit betreft met name cyberbeveiligingsaspecten in verband met de bescherming tegen corruptie en de veiligheid en betrouwbaarheid van controlesystemen, zoals uiteengezet in de punten 1.1.9 en 1.2.1 van bijlage III bij de machineverordening. Voor die risico's hoeven fabrikanten voor de toepassing van de verordening cyberweerbaarheid de conformiteit niet opnieuw te beoordelen of aan te tonen zolang het desbetreffende certificaat of goedkeuringsbesluit geldig blijft, en in elk geval niet na 11 juni 2028. Dit geldt voor zover die risico's zijn aangepakt in het kader van de conformiteitsbeoordeling uit hoofde van de machineverordening.

257. Net als bij de bovengenoemde essentiële eisen inzake cyberbeveiliging van de richtlijn radioapparatuur blijven fabrikanten, wanneer bij de overeenkomstig artikel 13, lid 2, van de verordening cyberweerbaarheid uitgevoerde cyberbeveiligingsrisicobeoordeling aanvullende cyberbeveiligingsrisico's worden vastgesteld die niet onder het desbetreffende op grond van de machineverordening afgegeven certificaat vallen en die verband houden met de cyberbeveiligingsvereisten van die verordening, verantwoordelijk voor het aanpakken van die risico's overeenkomstig de verordening cyberweerbaarheid.