Europeiska unionens officiella tidning

SV
C-serien

C/2026/6013

17.11.2026

MEDDELANDE FRÅN KOMMISSIONEN

Kommissionens vägledning om tillämpningen av förordning (EU) 2024/2847 (cyberresiliensförordningen)

(C/2026/6013)

Innehåll

Sida

1. INLEDNING ... 3
   - 1.1 Cyberresiliensförordningen ... 3
   - 1.2 Syftet med denna vägledning ... 3
2. TILLÄMPNINGSOMRÅDE ... 4
   - 2.1 Utsläppande på marknaden ... 4
   - 2.2 Programvara som produkt med digitala element ... 5
   - 2.3 Datorkod ... 6
   - 2.4 Hårdvara och programvara som tillsammans utgör en produkt med digitala element ... 7
   - 2.5 Dataanslutning ... 8
   - 2.6 Komplexa system ... 8
   - 2.7 Produkter med digitala element som utformats innan cyberresiliensförordningen började tillämpas ... 9
3. FRI PROGRAMVARA MED ÖPPEN KÄLLKOD ... 11
   - 3.1 Fastställande av vem som ansvarar för programvara med fri och öppen källkod ... 12
   - 3.2 Fastställande av om programvara med fri och öppen källkod har släppts ut på EU-marknaden ... 13
     - 3.2.1 Uttagande av avgift ... 13
     - 3.2.2 Monetarisering av andra tjänster eller krav på behandling av personuppgifter ... 13
     - 3.2.3 Stödtjänster ... 14
     - 3.2.4 Donationer ... 15
     - 3.2.5 Finansiering av programvara med fri och öppen källkod ... 15
     - 3.2.6 Ideella enheter som inrättats för att uppnå icke-vinstdrivande mål ... 16
     - 3.2.7 Andra tillverkares integrering av programvaran ... 16
   - 3.3 Förvaltare av programvara med fri och öppen källkod ... 16
     - 3.3.1 Bibehållet stöd och säkerställande av bärkraften hos en programvara med fri och öppen källkod 17
   - 3.4 Bidragsgivare och användning i senare led ... 18
   - 3.5 Vägledande scenarier ... 19
4. VÄSENTLIGA ÄNDRINGAR OCH RESERVDELAR ... 21
   - 4.1 Fysiska reparationer ... 22
   - 4.2 Reservdelar ... 23
   - 4.3 Programuppdateringar som väsentliga ändringar ... 24

4.4 Följderna av en väsentlig ändring 27
4.4.1 Väsentliga ändringar utförda av en annan person än den ursprungliga tillverkaren 28
4.4.2 Väsentliga ändringar utförda av den ursprungliga tillverkaren 29
5. STÖDPERIOD 29
5.1 Väsentliga ändringar och stödperioden 31
6. VIKTIGA OCH KRITISKA PRODUKTER MED DIGITALA ELEMENT 32
6.1 Vad är en kärnfunktion? 33
6.2 Bedömning av överensstämmelse för viktiga och kritiska produkter med digitala element 36
6.3 Följderna för en presumtion om överensstämmelse 38
7. BEDÖMNING AV CYBERSÄKERHETSRISKER OCH INTEGRERING AV PRODUKTER MED DIGITALA ELEMENT OCH KOMPONENTER 41
7.1 Om utvärdering och behandling av cybersäkerhetsrisker 41
7.2 Om utformning, utveckling och produktion av produkter med digitala element på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna 42
7.3 Riskbedömning och tillbörlig aktsamhet med avseende på externa beroenden och integrerade komponenter 42
7.4 Återanvändning av riskbedömningar och dokumentation om överensstämmelse för produktfamiljer med digitala element 44
8. FJÄRRBEHANDLING AV DATA 44
8.1 Vad betraktas som en lösning för fjärrbehandling av data för en produkt med digitala element? 45
8.1.1 Begreppet ”på distans” 46
8.1.2 Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner? 46
8.1.3 Har programvaran utformats och utvecklats av tillverkaren eller under dennes ansvar? 47
8.2 Praktiska och tekniska konsekvenser av lösningar för fjärrbehandling av data och beroende av lösningar från tredje part 49
8.3 Användningsfall för lösningar för fjärrbehandling av data 50
8.3.1 Mobil bankapplikation 51
8.3.2 Smart termostat 52
8.3.3 Läsplatta 53
8.3.4 Industrirobot 53
8.3.5 Mobilnät 53
9. YTTERLIGARE ELEMENT 54
9.1 Rapporteringsskyldigheter 54
9.2 Sårbarhetshantering 56
9.2.1 Rapportering till tidigare led och delning av säkerhetsåtgärder 56
9.2.2 Kända sårbarheter som kan utnyttjas 57
9.2.3 Effektiva och regelbundna provningar och granskningar 58
9.3 Samspel med annan lagstiftning 59
9.3.1 Förordning (EU) 2019/2144 och förordning (EU) nr 168/2013 59
9.3.2 EU-typkontrollintygens giltighet (artikel 69.1) 59

1. **INLEDNING**

1.1 **Cyberresiliensförordningen**

1. Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen) ([1]) trädde i kraft den 10 december 2024. Förordningen syftar till att stärka EU:s strategi när det gällercybersäkerhet, ta upp frågan om cyberresiliens på EU-nivå och förbättra den inre marknadens funktionssätt genom att fastställa en enhetlig rättslig ram för väsentliga cybersäkerhetskrav för utsläppande av produkter med digitala element på EU-marknaden samt under en produkt med digitala elements livscykel.

2. Cyberresiliensförordningen bygger på EU:s nya lagstiftningsram, som fastställs i Europaparlamentets och rådets förordning (EG) nr 765/2008 av den 9 juli 2008 om krav för ackreditering och marknadskontroll i samband med saluföring av produkter och upphävande av förordning (EEG) nr 339/93 och i Europaparlamentets och rådets beslut nr 768/2008/EG av den 9 juli 2008 om en gemensam ram för saluföring av produkter och upphävande av rådets beslut 93/465/EEG ([2]).

3. Marknadskontroll och kontroll av efterlevnaden utförs av de nationella marknadskontrollmyndigheterna. Produkter med digitala element som omfattas av cyberresiliensförordningen tillämpningsområde omfattas också av Europaparlamentets och rådets förordning (EU) 2019/1020 av den 20 juni 2019 om marknadskontroll och överensstämmelse för produkter och om ändring av direktiv 2004/42/EG och förordningarna (EG) nr 765/2008 och (EU) nr 305/2011. Kommissionen och Europeiska unionens cybersäkerhetsbyrå (Enisa) stöder de ekonomiska aktörerna och medlemsstaterna vid tillämpningen av cyberresiliensförordningen.

1.2 **Syftet med denna vägledning**

4. Enligt artikel 26.1 i cyberresiliensförordningen ska kommissionen offentliggöra vägledning som ska vara till hjälp för ekonomiska aktörer vid tillämpningen av förordningen, med särskilt fokus på att underlätta efterlevnaden för mikroföretag samt små och medelstora företag. I artikel 26.2 fastställs de aspekter som bör tas upp i vägledningen. Dessa inbegriper bland annat i) cyberresiliensförordningens tillämpningsområde (i synnerhet lösningar för fjärrbehandling av data och programvara med fri och öppen källkod), ii) begreppet ”stödperioder”, iii) samspelet mellan cyberresiliensförordningen och den övriga EU-lagstiftningen, och iv) begreppet ”väsentlig ändring”.

5. Den 3 december 2025 offentliggjorde kommissionen en rad vanliga frågor som är avsedda att hjälpa ekonomiska aktörer att förbereda sig inför genomförandet av cyberresiliensförordningen ([3]).

6. Denna vägledning är avsedd att hjälpa ekonomiska aktörer att uppfylla kraven i cyberresiliensförordningen och att stödja verksamheten inom marknadskontrollmyndigheter, anmälande myndigheter och anmälda organ i syfte att säkerställa en harmoniserad tillämpning av cyberresiliensförordningen i hela unionen. Tanken är inte att vägledningen ska omfatta hela cyberresiliensförordningens tillämpningsområde, utan den ska snarare förtydliga vissa centrala bestämmelser och hur de kan genomföras i praktiken. Vägledningen gäller cyberresiliensförordningen och är inte tillämplig på annan EU-lagstiftning.

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

([2]) I kommissionens arbetsprogram för 2026 planeras en ”europeisk produktlagstiftning” som uppdaterar den nya lagstiftningsramen och reglerna för marknadskontroll och standardisering: https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:52025DC0870.

([3]) De vanliga frågorna kan laddas ned via kommissionens webbplats för genomförande av cyberresiliensförordningen från den särskilda webbsidan för vanliga frågor.

7. Berörda parter rådfrågades i omfattande grad vid utarbetandet av denna vägledning, inbegripet expertgruppen för cybersäkerhet för produkter med digitala element ([4]), och genom ett offentligt samråd som hölls mellan den 3 mars och den 13 april 2026 ([5]).

8. Denna vägledning är inte bindande för ekonomiska aktörer eller andra aktörer som omfattas av cyberresiliensförordningen. En officiell tolkning av cyberresiliensförordningen får endast göras av Europeiska unionens domstol. I denna vägledning anges dock kommissionens tolkning av cyberresiliensförordningen i syfte att stödja efterlevnaden och bidra till ett effektivt genomförande av förordningen. Vägledningen innehåller även ett antal exempel för att illustrera tillämpningen av särskilda bestämmelser. Dessa exempel är dock inte avsedda att ersätta bedömning från fall till fall. Sådana bedömningar krävs alltid för att ta hänsyn till varje enskilt fall och omständigheter.

9. I enlighet med artikel 26 i cyberresiliensförordningen kan kommissionen överväga att utfärda ytterligare vägledning, inklusive vägledning riktad till de tillverkare som omfattas av cyberresiliensförordningen och annan harmoniserad unionslagstiftning eller av andra närliggande unionsrättsakter. Denna vägledning kan till exempel ta upp frågor om samspelet mellan cyberresiliensförordningen och förordning (EU) 2024/1689 om harmoniserade regler för artificiell intelligens (*AI-förordningen*) och förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn.

2. **TILLÄMPNINGSOMRÅDE**

2.1 **Utsläppande på marknaden**

10. Cyberresiliensförordningen gäller för produkter med digitala element som tillhandahålls på EU-marknaden. Begreppet ”tillhandahållande på marknaden” definieras i artikel 3.22 i cyberresiliensförordningen som ”leverans av en produkt med digitala element för distribution eller användning på unionsmarknaden i samband med kommersiell verksamhet, antingen mot betalning eller kostnadsfritt”. I enlighet med artikel 3.21 släpps en produkt med digitala element ut på EU-marknaden när den tillhandahålls för första gången.

11. Den senaste utgåvan av *blåboken om genomförandet av EU:s produktbestämmelser*, som offentliggjordes 2022 (*blåboken*) ([6]), ger vägledning som främjar förståelsen av EU:s produktbestämmelser och deras enhetliga tillämpning inom de olika sektorsspecifika rättsliga ramar som är anpassade till den nya lagstiftningsramen, såsom cyberresiliensförordningen. I blåboken anges att begreppen ”utsläppande på marknaden” och ”tillhandahållande” ska förstås som att de avser ”varje individuell produkt, inte typer av produkter, och det spelar ingen roll om produkten tillverkades som en individuell enhet eller i serie” (avsnitt 2.3).

12. För mer ”traditionella” produkter med digitala element som omfattas av den nya lagstiftningsramen, såsom hårdvara i form av maskiner eller radioutrustningsprodukter med digitala element, är begreppet ”utsläppande på marknaden” väletablerat, och blåboken ger ytterligare vägledning som klargör när sådana produkter anses ha släppts ut på marknaden. De ”sammanfattande exempel” som anges i avsnitt 2.12 i blåboken innehåller ytterligare exempel på begreppet ”utsläppande på marknaden”.

13. Med tanke på hur immateriella produkter med digitala element (t.ex. fristående programvara) fungerar behövs dock ytterligare vägledning rörande när sådana produkter med digitala element ska anses ha släppts ut på marknaden. När en programvaras tillverkningsfas har slutförts och en produkt med digitala element bjuds ut till potentiella användare på EU-marknaden kan tillverkaren anses ha tillverkat flera kopior av samma programvaruprodukt med digitala element och tillhandahållit dem för distribution eller användning. Till skillnad från materiella produkter med digitala element är fristående programvara rent faktiskt inte föremål för några fysiska produktions- eller

([4]) Expertgruppen för cybersäkerhet för produkter med digitala element (Expert Group on Cybersecurity of Products with Digital Elements) i registret över kommissionens expertgrupper och liknande organ.
([5]) Offentligt samråd om utkastet till kommissionsvägledning om cyberresiliensförordningen.
([6]) Meddelande från kommissionen,*2022 års blåbok om genomförandet av EU:s produktbestämmelser* 2022/C 247/01 (EUT C 247, 29.6.2022, s 1).

lagerbegränsningar: Varje åtgärd som gör programvaran tillgänglig för nedladdning eller distribution leder till att en ny identisk kopia skapas för användaren. Så länge som denna version av programvaran inte ändras på ett sätt som påverkar efterlevnaden av cyberresiliensförordningen ska utsläppandet på EU-marknaden anses ha ägt rum vid tidpunkten för det första erbjudandet om distribution eller användning. Möjligheten att senare ladda ned eller distribuera denna version av programvaruprodukten med digitala element ska därför betraktas som ett fall där denna programvaruprodukt med digitala element tillhandahålls ([7]).

14. En fristående programvaruprodukt med digitala element bör därför anses ha släppts ut på marknaden när dess tillverkningsfas är slutförd och programvaran för första gången tillhandahålls för distribution eller användning på EU-marknaden i samband med kommersiell verksamhet. Tillverkaren bör anses ha släppt ut flera exemplar av samma programvaruprodukt med digitala element på marknaden samtidigt. Även om flera exemplar av samma programvara fortsatt utgör enskilda produkter med digitala element anses de därför släppas ut på marknaden samtidigt, oavsett när innehavet eller användningen av varje enskilt exemplar överförs till en annan fysisk eller juridisk person. Om tillverkaren samtidigt tillhandahåller programvaran i olika varianter som skiljer sig åt på grund av de komponenter som ingår, konfigurationerna eller de aktiverade funktionerna (t.ex. versioner för olika operativsystem eller paket med olika uppsättningar funktioner) kan dessa varianter inte betraktas som flera exemplar av samma programvaruprodukt med digitala element. De bör därför behandlas som separata produkter med digitala element när de släpps ut på marknaden.

Exempel 1: Den 1 januari 2028 tillhandahåller företag A för första gången version 1.0.0 av sin programvara X via sin webbplats för distribution. Samma dag köper kund 1 ett exemplar av version 1.0.0 av programvaran X. Den 15 januari 2028 köper kund 2 ett exemplar av version 1.0.0 av programvaran X. Båda exemplaren av version 1.0.0 av programvaran X släpps ut på marknaden den 1 januari 2028.

15. Med tanke på programvaruutvecklingens iterativa natur bör det dessutom klargöras att senare versioner av en programvaruprodukt med digitala element anses vara nyutsläppta på marknaden om dessa versioner betraktas som en ”väsentlig ändring” av en programvaruprodukt med digitala element som redan släppts ut på marknaden, såsom anges i skäl 41 i cyberresiliensförordningen. Versioner som inte kan betecknas som väsentliga ändringar kräver inte att tillverkaren genomför ett nytt förfarande för bedömning av överensstämmelse, och ändrar därför inte den programvarans datum för utsläppande på marknaden. Mer vägledning om begreppet ”väsentliga ändringar” finns i avsnitt *4 Väsentliga ändringar*.

Exempel 2: Den 1 januari 2028 tillhandahåller företag A för första gången version 1.0.0 av programvaran X via sin webbplats för distribution. Samma dag köper kund 1 ett exemplar av version 1.0.0 av programvaran X. Den 15 januari 2028 släpper företag A en uppdaterad version 1.0.1 av programvaran X som inte utgör en väsentlig ändring. Den 30 januari 2028 köper kund 2 ett exemplar av version 1.0.1 av programvaran X. Båda exemplaren av version 1.0.0 och 1.0.1 av programvara X anses ha släppts ut på marknaden den 1 januari 2028.

16. Vägledningen i punkterna 13, 14 och 15 gäller uteslutande i den mån som produkten med digitala element är en fristående programvara. Så är till exempel inte fallet när programvaran kombineras med hårdvara, vilket beskrivs i avsnitt *2.4 Hårdvara och programvara som tillsammans utgör en produkt*.

2.2 **Programvara som produkt med digitala element**

17. I artikel 3.1 i cyberresiliensförordningen definieras ”produkt med digitala element” som en ”programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat”. Sådana produkter med digitala element omfattas av cyberresiliensförordningen om deras avsedda ändamål eller rimligen förutsebara användning inbegriper en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nätverk.

([7]) I enlighet med artikel 13.11 får tillverkarna upprätthålla offentliga programvaruarkiv som förbättrar användarnas tillgång till äldre versioner. I dessa fall ska användarna på ett tydligt och lättillgängligt sätt få information om riskerna med att använda programvara som inte stöds.

18. Cyberresiliensförordningen kan därför omfatta en rad olika produkter med digitala element, däribland i) fristående programvara, såsom appar och datorprogram, oavsett om de distribueras digitalt eller fysiskt, ii) maskinvara med inbyggd programvara (t.ex. enheter för sakernas internet, bärbara datorer, surfplattor), iii) fristående hårdvara (t.ex. integrerade kretsar, moderkort), och iv) varje kombination av maskinvara och programvara som levereras separat men som är avsedd att fungera tillsammans.

19. Fristående programvaror omfattas därför av cyberresiliensförordningen om de släpps ut på marknaden som produkter med digitala element. Det är lämpligt att skilja mellan programvaruprodukter med digitala element som omfattas av cyberresiliensförordningen och ett fjärrtillhandahållande av tjänster som inte omfattas av cyberresiliensförordningen.

20. För att programvara ska omfattas av cyberresiliensförordningen måste en programvaruprodukt med digitala element tillhandahållas till en användare, erhållas av den användaren och användas inom, eller som en del av, ett elektroniskt informationssystem på användarens sida. Programvara som laddas ned, installeras eller på annat sätt tillhandahålls till användaren och körs på användarens elektroniska informationssystem uppfyller dessa kriterier, till exempel när den tar formen av ett webbläsartillägg eller en applikation som utvecklats med hjälp av webbteknik men som tillhandahålls för lokal körning.

21. Programvara som fjärrkörs och som användaren endast har åtkomst till utgör däremot inte en produkt med digitala element enbart på denna grund. Skälen 11 och 12 i cyberresiliensförordningen gör denna särskillnad genom att förklara att fjärrbehandling eller fjärrlagring endast omfattas av cyberresiliensförordningen i den mån som krävs för att en produkt med digitala element ska kunna utföra sina funktioner (dvs. genom begreppet fjärrbehandling av data enligt definitionen i artikel 3.2) och inte i sig som produkter med digitala element. Detta är vanligtvis fallet för webbapplikationer, inklusive progressiva webbappar, om de uteslutande nås genom en webbläsare. Detsamma gäller webbplatser: även om webbplatser tekniskt sett kan köras och exekveras på användarens enhet i begränsad omfattning följer det av skäl 12 i cyberresiliensförordningen att webbplatserna inte i sig ska betraktas som produkter med digitala element och enbart omfattas av cyberresiliensförordningens tillämpningsområde om de stöder funktionen hos en produkt med digitala element, dvs. i den mån de kan betraktas som fjärrbehandling av data (vilket förklaras närmare i avsnitt *8* och i synnerhet i *8.1.2 Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner?*).

Exempel 3: En mobilapplikation som en användare laddar ner från en appbutik och installerar på sin smarttelefon tillhandahålls till användaren och körs på användarens enhet och utgör därför en produkt med digitala element. Om applikationen släpps ut på marknaden i samband med kommersiell verksamhet kan den omfattas av cyberresiliensförordningen.

Exempel 4: En skrivbordsapplikation som är byggd med hjälp av webbteknik men paketerad för lokal installation tillhandahålls till användaren och körs på användarens enhet, och utgör därför en produkt med digitala element. Om applikationen släpps ut på marknaden i samband med kommersiell verksamhet kan den omfattas av cyberresiliensförordningen.

Exempel 5: En webbapplikation som användaren har åtkomst till uteslutande via en webbläsare är inte en produkt med digitala element. Såvida den inte stöder funktionaliteten hos en produkt med digitala element omfattas den inte av cyberresiliensförordningen. En applikation som tillhandahålls till användaren som en lokalt installerad klient som körs på användarens enhet är däremot en produkt med digitala element. Om applikationen släpps ut på marknaden i samband med kommersiell verksamhet kan den omfattas av cyberresiliensförordningen.

Om klienten använder databehandling på distans som motsvarar definitionen av fjärrbehandling av data för att utföra en eller flera av sina funktioner utgör den databehandlingen på distans också en del av produkten med digitala element.

Exempel 6: En webbplats som endast presenterar information för sina besökare och inte stöder funktionerna hos en produkt med digitala element är inte i sig en produkt med digitala element. Den omfattas därför inte av cyberresiliensförordningen.

2.3 **Datorkod**

22. Det är också lämpligt att klargöra huruvida källkod kan utgöra en programvaruprodukt med digitala element. I cyberresiliensförordningen definieras programvara som ”den del av ett elektroniskt informationssystem som utgörs av datorkod” (artikel 3.4). Datorkod kan ta formen av i) maskinkod, som är en uppsättning instruktioner som utförs direkt av en dators processor och är skriven i binärt format, eller ii) källkod, dvs. en uppsättning instruktioner och förklaringar som skrivs på ett programmeringsspråk och som måste sammanställas eller tolkas för att utföras av en dator. Definitionen av programvara i cyberresiliensförordningen omfattar båda dessa typer.

23. En separat fråga är om ett visst tillhandahållande av datorkod motsvarar ett utsläppande av en produkt med digitala element på EU-marknaden, vilket kräver tillhandahållande i samband med kommersiell verksamhet. Detta är ofta inte fallet när det gäller källkod. En fysisk eller juridisk person som delar datakod med fri och öppen källkod på allmänt tillgängliga databaser anses i allmänhet inte släppa ut den koden på EU-marknaden enligt cyberresiliensförordningen (vilket diskuteras närmare i avsnitt *3 Fri programvara med öppen* källkod). Ofärdig kod som delas under utformnings- och utvecklingsfasen för en produkt med digitala element (t.ex. för provning eller granskning) anses inte heller släppas ut på marknaden enligt cyberresiliensförordningen, eftersom dess tillverkningsfas inte är slutförd. På samma sätt anses inte heller prov- eller demokod som tillhandahålls som en del av handlednings- eller utbildningsmaterial ha släppts ut på marknaden enligt cyberresiliensförordningen ([8]).

24. Om en tillverkare däremot förser sina kunder med datorkod som en produkt med digitala element betraktas koden som utsläppt på marknaden, oavsett om den är maskinkod eller källkod ([9]).

Exempel 7: Företag A licensierar källkod till företag B för en anpassningsbar intern plattform och tillhandahåller den källkoden i en textfil. Även om denna källkod kräver ytterligare anpassning och kompilering av företag B innan den används släpper företag A ut den källkoden på marknaden och omfattas därför av cyberresiliensförordningen. Företag A ansvarar inte för att företag B:s därpå följande anpassningar och kompilering av koden är förenliga med cyberresiliensförordningen.

2.4 **Hårdvara och programvara som tillsammans utgör en produkt med digitala element**

25. Huruvida programvaran utgör en del av en produkt med digitala element bör inte avgöras av hur eller när programvaran tillhandahålls till användaren, utan av huruvida programvaran, mot bakgrund av produktens avsedda ändamål och rimligen förutsebara användning, är nödvändig för att produkten med digitala element ska kunna utföra sina avsedda funktioner. Om en hårdvaruprodukt med digitala element är utformad för att fungera tillsammans med en specifik programvara som tillhandahålls av samma tillverkare för att utföra produktens funktioner, utgör hårdvaran och programvaran tillsammans produkten med digitala element. Den programvara som är nödvändig för att driva, konfigurera, styra eller använda en produkt med digitala element i enlighet med dess avsedda ändamål är därför en del av produkten med digitala element, även om den erhålls via en separat kanal (t.ex. en appbutik, en nedladdningslänk eller annan digital kanal efter det att hårdvaruprodukten med digitala element har släppts ut på marknaden). Programvaran släpps således ut på marknaden samtidigt som enheterna av hårdvaruprodukten med digitala element släpps ut på marknaden.

Exempel 8: En nätverksskrivare släpps ut på marknaden som en hårdvaruprodukt med digitala element, medan de drivrutiner som krävs för att skicka utskriftsjobb, konfigurera enheten och hantera dess drift görs tillgängliga för nedladdning från tillverkarens webbplats. Även om skrivaren och drivrutinerna levereras via olika kanaler utgör de tillsammans en enda produkt med digitala element, eftersom skrivaren inte kan uppfylla sitt avsedda syfte utan drivrutinerna.

Exempel 9: En kroppsburen träningsenhet släpps ut på marknaden för att mäta en användarens hjärtfrekvens och aktivitetsnivå, tillverkaren tillhandahåller även den smarttelefonapplikation som krävs för att visa mätningarna, visa historiken och möjliggöra konfiguration av enheten. Även om applikationen laddas ned separat via en appbutik utgör den bärbara enheten och programmet tillsammans en enda produkt med digitala element, eftersom de är utformade och avsedda att fungera tillsammans i syfte att leverera de funktioner som tillhandahålls av produkten med digitala element.

([8]) Man bör också komma ihåg att artikel 4.3 gör det möjligt för tillverkare att på marknaden tillhandahålla ofärdig programvara som inte är förenlig med förordningen, t.ex. alfaversioner, betaversioner eller lanseringskandidater, förutsatt att den inte färdigställda programvaran endast görs tillgänglig under så lång tid som behövs för att testa den och få återkoppling.

([9]) Å andra sidan bör det noteras att själva datorkoden enligt lagstiftningen om produktansvar inte utgör en produkt, och att tillverkare som släpper ut sådan kod på marknaden därför inte kan hållas ansvariga enligt direktiv (EU) 2024/2853 (produktansvarsdirektivet). I skäl 13 i det direktivet anges att ”information [...] dock inte [bör] betraktas som en produkt, och reglerna om skadeståndsansvar för produkter bör därför inte tillämpas på innehållet i digitala filer, såsom mediefiler eller e-böcker eller enbart källkoden för programvara”. Detta utesluter inte att tillverkare kan vara ansvariga enligt nationell skadeståndsrätt.

2.5 **Dataanslutning**

26. Enligt artikel 2.1 i cyberresiliensförordningen är förordningen ”tillämplig på alla produkter med digitala element som tillhandahålls på marknaden och vars avsedda ändamål eller rimligen förutsebara användning omfattar en direkt eller indirekt logisk eller fysisk dataanslutning till en enhet eller ett nät”. Cyberresiliensförordningens tillämpningsområde är därför förankrat inte enbart i förekomsten av elektronik, utan i kapaciteten hos en produkt med digitala element att utbyta digital information.

27. Termerna ”logisk anslutning” och ”fysisk anslutning” definieras i artikel 3, men ”dataanslutning” eller ”digitala data” definieras inte i cyberresiliensförordningen. Det är därför lämpligt att fastställa en tolkning av vad en dataanslutning är i syfte att klargöra gränsen för cyberresiliensförordningens tillämpningsområde. Denna gräns är särskilt viktig för att skilja mellan produkter med digitala element som endast använder elektriska signaler och produkter som är en del av digital kommunikation och därmed utsätts för cybersäkerhetsrisker.

28. På den mest grundläggande nivån innebär en dataanslutning överföring av information i binär form, dvs. som en sekvens av nollor och ettor. Att enbart slå på och av en utgång (dvs. 0/1) utgör inte i sig en dataanslutning om dessa tillstånd inte är avsedda att representera data eller inte läses av en digital ingång. För att något ska utgöra en dataanslutning måste de binära tillstånden avsiktligt kodas som information av en källa och måste kunna avkodas som information vid destinationen. Med andra ord måste det finnas en avsändare som avsiktligt genererar digitala symboler enligt ett definierat system och en mottagare som kan tolka dessa symboler som data. Om elektriska eller elektroniska signaler enbart används för att utlösa eller driva en funktion, utan att överföra någon digitalt kodad information, finns det enligt cyberresiliensförordningen ingen dataanslutning, och därför omfattas produkten med digitala element inte av artikel 2.1.

2.6 **Komplexa system**

29. Produkter med digitala element som omfattas av cyberresiliensförordningen behöver inte bestå enbart av enskilda enheter eller programvarukomponenter utan kan även bestå av komplexa system, däribland system som består av flera hård- och programvarukomponenter som fungerar tillsammans för att utföra en viss funktion. Om ett sådant system släpps ut på marknaden som en enda produkt med digitala element utgör det en produkt med digitala element i den mening som avses i cyberresiliensförordningen.

30. Sådana komplexa system kännetecknas ofta av långa utformnings- och utvecklingscykler, med avtal som kan ha undertecknats innan cyberresiliensförordningen börjar tillämpas, förlängd driftsmässig livslängd och stor teknisk och organisatorisk komplexitet. System som ska släppas ut på marknaden efter det att cyberresiliensförordningen börjar tillämpas får förlita sig på komponenter som släppts ut på marknaden innan cyberresiliensförordningen började tillämpas, på etablerade arkitekturer eller på allmänt använda interoperabilitetsstandarder, däribland standarder som avses i annan EU-lagstiftning eller sektorsspecifika ramar. Till följd av detta kan vissa tekniska egenskaper hos dessa system vara svåra eller oproportionerliga att ändra utan att påverka deras avsedda syfte, säkerhet, tillförlitlighet eller interoperabilitet med befintlig infrastruktur.

31. I sig utesluter dessa egenskaper inte komplexa system från cyberresiliensförordningens tillämpningsområde. De illustrerar snarare tillämpningen av cyberresiliensförordningens riskbaserade metod, som gör det möjligt att påvisa efterlevnaden på olika sätt beroende på egenskaperna och begränsningarna hos produkten med digitala element, i enlighet med artikel 13.3 i cyberresiliensförordningen. Dessa egenskaper utgör en del av produktens avsedda syfte och driftssammanhang och är därför relevanta vid bedömningen av överensstämmelse med de väsentliga cybersäkerhetskraven (*de väsentliga kraven*). I skäl 55 anges uttryckligen att vissa väsentliga krav kanske inte är helt förenliga med beskaffenheten hos en produkt med digitala element. Detta kan till exempel vara fallet om överensstämmelse skulle undergräva de obligatoriska interoperabilitetskraven eller medföra att systemet inte fungerar som det ska.

32. Tillverkarna måste hantera cybersäkerhetsrisker på grundval av den bedömning av cybersäkerhetsrisker som avses i artikel 13.2. Som också förklaras i skäl 55 finns vissa fall där specifika väsentliga krav inte är tillämpliga eller inte kan uppfyllas genom tillämpning av de senaste säkerhetsåtgärderna, till exempel på grund av att systemets avsedda

ändamål kräver att en produkt med digitala element interagerar med befintliga beroenden eller uppfyller vissa interoperabilitetskrav. I sådana fall bör tillverkarna fastställa och dokumentera dessa särskilda begränsningar, bedöma de därtill hörande riskerna och genomföra lämpliga alternativa eller kompenserande riskreducerande åtgärder för att inte undergräva säkerheten för produkten med digitala element. I detta syfte spelar både den tekniska dokumentation som avses i artikel 31 och den information och de instruktioner till användaren som avses i bilaga II en avgörande roll för att på ett öppet sätt beskriva de fastställda begränsningarna, de därtill hörande cybersäkerhetsriskerna och de riskreducerande åtgärder som vidtagits. I enlighet med skyldigheten att hålla riskbedömningen uppdaterad under stödperioden bör tillverkarna också regelbundet ompröva huruvida sådana begränsningar kvarstår. Om dessa begränsningar kan hävas eller minskas med tiden bör tillverkarna uppdatera produkten med digitala element i enlighet med detta, så att den gradvis kan övergå till en lämplig cybersäkerhetsnivå ([10]).

Exempel 10: En tillverkare släpper ut en produkt med digitala element på marknaden som kommunicerar med externa system med hjälp av ett nätverksprotokoll. Som en del av tillämpningen av de väsentliga kraven fastställer tillverkaren, på grundval av bedömningen av cybersäkerhetsrisker, att ett säkert kommunikationsprotokoll måste användas för att säkerställa konfidentialiteten och integriteten för de uppgifter som utbyts av produkten med digitala element.

Det avsedda syftet inbegriper dock interoperabilitet med befintliga system som endast stöder ett äldre eller mindre säkert protokoll. I sådana fall får tillverkaren tillämpa det protokollet om så är nödvändigt för att uppnå interoperabilitet, förutsatt att de därtill hörande cybersäkerhetsriskerna fastställs och minskas på andra sätt.

Om det är tekniskt möjligt för produkten med digitala element att stödja både det säkra och det mindre säkra protokollet förväntas tillverkaren tillämpa det säkra protokollet och möjliggöra dess användning som standard. Det mindre säkra protokollet skulle endast tillåtas när det krävs för interoperabilitetens skull.

Exempel 11: En tillverkare av ett industriellt automatiseringssystem köper in att antal mikrokontroller innan cyberresiliensförordningen träder i kraft. Tillverkaren genomför bedömningen av cybersäkerhetsrisker med avsikt att släppa ut sitt industriella automatiseringssystem på marknaden efter det att cyberresiliensförordningen har trätt i kraft. På grundval av denna bedömning av cybersäkerhetsrisker fastställer tillverkaren att det inte finns några särskilda cybersäkerhetsrisker kopplade till användningen av en av dessa mikrokontroller. Tillverkaren integrerar mikrokontrollern i sitt industriella automatiseringssystem och säkerställer att produkten med digitala element som helhet (det industriella automatiseringssystemet) uppfyller de väsentliga kraven.

2.7 **Produkter med digitala element som utformats innan cyberresiliensförordningen började tillämpas**

33. I vissa fall kommer tillverkare, efter det att cyberresiliensförordningen börjar tillämpas den 11 december 2027, att släppa ut enheter av en produkt med digitala element som är tillverkad i enlighet med en typ eller modell som har utformats och utvecklats före den dag då cyberresiliensförordningen börjar tillämpas. I sådana fall kräver efterlevnaden av denna förordning inte nödvändigtvis att utformningen av dessa enheter av produkten med digitala element ska ändras. Tillverkaren ska utföra en bedömning av cybersäkerhetsrisker i enlighet med artikel 13.2 i cyberresiliensförordningen för att, på grundval av det avsedda syftet med och den rimligen förutsebara användningen av produkten med digitala element, fastställa vilka av de väsentliga kraven i del I i bilaga I som är tillämpliga på den produkten med digitala element och hur dessa krav uppfylls.

34. Om resultatet av riskbedömningen visar att produkten med digitala element redan innehåller lämpliga och effektiva säkerhetsåtgärder som åtgärdar de relevanta riskerna får tillverkaren förlita sig på dessa befintliga åtgärder för att visa att kraven i cyberresiliensförordningen är uppfyllda. Cyberresiliensförordningen i sig påför inte någon skyldighet att införa nya säkerhetsfunktioner eller att ändra utformningen av produkten med digitala element om detta inte är nödvändigt för att åtgärda de fastställda riskerna.

([10]) Det bör noteras att de överväganden som fastställs i denna punkt kan vara tillämpliga, beroende på vad som är lämpligt, på alla produkter med digitala element som omfattas av cyberresiliensförordningen, och inte bara på ”komplexa system”.

35. Tillverkaren omfattas dock fortfarande av de skyldigheter som fastställs i cyberresiliensförordningen. Dessa skyldigheter inbegriper att innan produkten med digitala element släpps ut på marknaden säkerställa att det tillämpliga förfarandet för bedömning av överensstämmelse har genomförts, att EU-försäkran om överensstämmelse har upprättats och att den har försetts med CE-märkning. Uppfyllandet av dessa krav är inte beroende av huruvida utformningen av produkten med digitala element krävde några ändringar till följd av riskbedömningen. När det gäller produkter med digitala element som har utformats före den dag då cyberresiliensförordningen börjar tillämpas men som släpptes ut på marknaden efter den dagen, bör skyldigheten i artikel 13.2, om det inte är möjligt för tillverkaren att visa på vilket sätt riskbedömningen har beaktats under utformnings- och utvecklingsfasen av produkten med digitala element, förstås som att den kräver att tillverkarna utför en bedömning av cybersäkerhetsrisker och med denna som underlag visar att produkten med digitala element innehåller lämpliga säkerhetsåtgärder i syfte att minimera cybersäkerhetsriskerna, förebygga incidenter och minimera deras inverkan, även när det gäller användarnas hälsa och säkerhet.

36. Produkter med digitala element som utformats innan cyberresiliensförordningen började tillämpas kan därför släppas ut på marknaden enligt cyberresiliensförordningen utan att deras utformning ändras, förutsatt att tillverkaren genom bedömningen av cybersäkerhetsrisker och den tekniska dokumentationen kan visa att produkten med digitala element uppnår en lämplig cybersäkerhetsnivå mot bakgrund av sitt avsedda syfte och rimligen förutsebara användning, och att den uppfyller de väsentliga kraven för cybersäkerhet.

37. Det är dessutom lämpligt att klargöra tillämpningen av skyldigheterna avseende bedömningen av överensstämmelse för tillverkare av produkter med digitala element som släpps ut på marknaden efter den dag då cyberresiliensförordningen börjar tillämpas, men som har tillverkats i enlighet med en typ eller modell som utformades och utvecklades före denna dag. I enlighet med artikel 13.12 ska tillverkaren genom det relevanta förfarandet för bedömning av överensstämmelse visa att dennes produkt med digitala element uppfyller de tillämpliga väsentliga kraven och inkludera bevis för detta i produktens tekniska dokumentation (punkt 6 i bilaga VII).

38. Tillämpningen av dessa krav måste dock tolkas mot bakgrund av bedömningen av cybersäkerhetsrisker och riskprofilen för cybersäkerhet avseende produkten med digitala element. Om riskbedömningen visar, med avseende i synnerhet på produkter med digitala element som utformats redan innan cyberresiliensförordningen började tillämpas (men som släppts ut på marknaden efter detta datum) och som omfattas av förfarandet för bedömning av överensstämmelse enligt artikel 32.1, att produkten med digitala element redan innehåller lämpliga och effektiva säkerhetsåtgärder som åtgärdar riskerna med den produkten bör skyldigheten att tillhandahålla bevis som en del av förfarandet för bedömning av överensstämmelse inte tolkas som att tillverkaren måste tillhandahålla provningsresultat som omfattar de ursprungliga utformnings- och utvecklingsfaserna för sådana produkter med digitala element. Detta skulle inte vara nödvändigt, eftersom det inte skulle bidra till att öka säkerheten för själva produkten med digitala element. I fall då provningar ändå är nödvändiga förväntas tillverkarna inte tillhandahålla bevis på att alla produktvarianter har provats, utan kan gruppera sådana provningar för produktfamiljer med digitala element, enligt vad som diskuteras närmare i avsnitt *7.4 Återanvändning av riskbedömningar och dokumentation om överensstämmelse för produktfamiljer med digitala element*.

39. Tillverkaren bör dock tillhandahålla bevis för hur denne efterlever de processer för sårbarhetshantering som fastställs i del II i bilaga I, hålla sin riskbedömning uppdaterad i enlighet med artikel 13.3 samt fullgöra alla andra skyldigheter som fastställs i cyberresiliensförordningen, bland annat genom att förse användare med information och instruktioner i enlighet med artikel 13.18.

Exempel 12: En tillverkare släpper ut en mikrokontroller på marknaden. Mikrokontrollern har utformats och utvecklats före den dag då cyberresiliensförordningen börjar tillämpas. Mikrokontrollern är avsedd att integreras i en rad olika elektroniska produkter med digitala element, däribland produkter med digitala element med konnektivitetsfunktioner.

Innan tillverkaren släpper ut nya enheter av mikrokontrollern på marknaden efter det att cyberresiliensförordningen har börjat tillämpas, utför denne en bedömning av cybersäkerhetsrisker i enlighet med artikel 13.2. På grundval av mikrokontrollerns avsedda ändamål och rimligen förutsebara användning fastställer tillverkaren de relevanta cybersäkerhetsriskerna, såsom obehörig åtkomst, manipulering av programvara eller data och missbruk av tillgängliga gränssnitt.

Resultatet av riskbedömningen visar att mikrokontrollern, såsom den ursprungligen utformades, redan innehåller lämpliga och effektiva säkerhetsåtgärder som åtgärdar de fastställda riskerna. Tillverkaren drar därför slutsatsen att produkten med digitala element uppfyller de relevanta väsentliga kraven i del I i bilaga I och att det inte är nödvändigt att ändra utformningen eller införa ytterligare säkerhetsfunktioner.

Om det inte är möjligt att visa hur en bedömning av cybersäkerhetsriskerna beaktades under den ursprungliga utformnings- och utvecklingsfasen, dokumenterar tillverkaren en aktuell bedömning av cybersäkerhetsriskerna och förklarar hur den befintliga utformningen och åtgärderna minskar de fastställda riskerna. Tillverkaren behöver inte återskapa den tidigare utformningen eller provningsdokumentationen, eftersom detta inte skulle bidra till att förbättra cybersäkerheten för produkten med digitala element. Om flera varianter av mikrokontrollern bygger på samma utformning och har samma cybersäkerhetsriskprofil får tillverkaren även förlita sig på representativa bevis som omfattar den relevanta produktfamiljen.

Tillverkaren säkerställer också uppfyllandet av de krav på sårbarhetshantering som anges i del II i bilaga I, bland annat genom att upprätthålla processer för åtgärdande och avhjälpande av sårbarheter och genom att ha översyn över bedömningen av cybersäkerhetsriskerna i enlighet med artikel 13.3.

Under dessa omständigheter får den mikrokontroller som utformats före den dag då cyberresiliensförordningen börjar tillämpas släppas ut på marknaden utan att dess utformning ändras, förutsatt att tillverkaren genom bedömningen av cybersäkerhetsrisker och den tekniska dokumentationen kan visa att den uppnår en lämplig cybersäkerhetsnivå mot bakgrund av sitt avsedda syfte och rimligen förutsebara användning, och att den uppfyller de tillämpliga väsentliga kraven.

3. **FRI PROGRAMVARA MED ÖPPEN KÄLLKOD**

40. Som nämndes i avsnitt *2.1 Utsläppande på marknaden* är cyberresiliensförordningen tillämplig på produkter med digitala element som tillhandahålls på EU-marknaden för första gången i samband med kommersiell verksamhet (dvs. som släpps ut på marknaden) samt på alla efterföljande fall som innebär att samma produkt med digitala element görs tillgänglig på marknaden. I blåboken (avsnitt 2.2) klargörs att ”kommersiell verksamhet” ska förstås som ett tillhandahållande av varor, mot betalning eller kostnadsfritt, i ett affärssammanhang och att detta endast kan bedömas från fall till fall, med hänsyn tagen till leveransernas frekvens, produktens egenskaper, leverantörens avsikter osv.

41. Tillhandahållande i samband med kommersiell verksamhet kännetecknas av en rad olika omständigheter, som utförligt dokumenteras i blåboken och anges i skäl 15 i cyberresiliensförordningen. Dessa kan inbegripa att direkt ta ut en avgift, samt att ”en avgift tas ut för tekniska stödtjänster när detta inte enbart tjänar till att täcka faktiska kostnader, när syftet är att monetarisera, till exempel genom att tillhandahålla en programvaruplattform som tillverkaren använder för att monetarisera andra tjänster, genom att som ett villkor för användning kräva behandling av personuppgifter för andra syften än uteslutande för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet, eller genom att ta emot donationer som överstiger kostnaderna för utformning, utveckling och tillhandahållande av en produkt med digitala element” (skäl 15) ([11]).

42. I cyberresiliensförordningen erkänns dock särdragen hos de olika sätten att utveckla och publicera ”programvara med fri och öppen källkod”, och viss vägledning ges för att fastställa om en programvara med fri och öppen källkod är en produkt med digitala element som släpps ut på marknaden (dvs. i samband med kommersiell verksamhet) i den mening som avses i cyberresiliensförordningen. Såsom förklaras i skäl 18 bör ”de omständigheter under vilka produkten med digitala element har utvecklats, eller hur utvecklingen har finansierats, [...] inte beaktas vid fastställandet av huruvida denna verksamhet är av kommersiell eller icke-kommersiell karaktär”. Mer specifikt ”bör tillhandahållandet av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte monetariseras av deras tillverkare inte betraktas vara en kommersiell verksamhet [...], för att säkerställa en tydlig åtskillnad mellan utvecklings- och leveransfaserna”.

([11]) Man bör också komma ihåg att även om produkter med digitala element ofta monetariseras (även) genom behandling av personuppgifter, är skydd av personuppgifter en grundläggande rättighet, och därför kan personuppgifter inte betraktas som en vara, såsom anges i skäl 24 i Europaparlamentets och rådets direktiv 2019/770 av den 20 maj 2019 om vissa aspekter på avtal om tillhandahållande av digitalt innehåll och digitala tjänster (EUT L 136, 22.5.2019, s. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj/swe).

43. Det är därför lämpligt att i) klargöra vad programvara med fri och öppen källkod är, ii) när denna anses falla under en fysisk eller juridisk persons ansvar, och iii) ge exempel för att hjälpa berörda parter förstå när distributionen av programvara med fri och öppen källkod utgör ett utsläppande på marknaden. Om programvara med fri och öppen källkod inte släpps ut på marknaden faller den utanför cyberresiliensförordningens tillämpningsområde, såvida inte den enhet som publicerar den är en juridisk person som uppfyller definitionen av ”förvaltare av programvara med fri och öppen källkod” (*förvaltare*) enligt artikel 3.14. I det fallet omfattas den endast av de skyldigheter som anges i artikel 24.

44. I artikel 3.48 definieras programvara med fri och öppen källkod som ”programvara vars källkod delas öppet och som tillhandahålls inom ramen för en licens med fri och öppen källkod som ger alla rättigheter att göra den fritt tillgänglig att användas, modifieras och vidaredistribueras”. Även om denna vägledning inte identifierar särskilda licenser med fri och öppen källkod som är förenliga med definitionen i artikel 3.48, följer det av ordalydelsen i den bestämmelsen att endast programvara som kumulativt uppfyller två villkor kan betraktas som fri programvara med öppen källkod enligt cyberresiliensförordningen: i) programvaran måste göras tillgänglig genom en licens med fri och öppen källkod som ger hela den uppsättning rättigheter som avses i artikel 3.48, och ii) dess källkod måste delas öppet.

45. Kravet på att licensen föreskriver att programvaran ska vara ”fritt tillgänglig att användas, modifieras och vidaredistribueras” återspeglar den traditionella förståelsen av programvara med fri och öppen källkod, nämligen att användarna måste ha tillgång till källkoden och kunna använda den utan onödiga begränsningar, ändra den och vidaredistribuera originalversioner eller modifierade versioner. Tillgång till källkoden är därför en nödvändig förutsättning för att de andra rättigheterna ska kunna utövas: utan tillgång till källkoden är det inte praktiskt möjligt att ändra eller på ett meningsfullt sätt återanvända programvaran.

46. Artikel 3.48 går dock längre än att enbart hänvisa till licensvillkoren, eftersom det uttryckligen krävs att källkoden ”delas öppet”. Begreppet ”delas öppet” innebär att källkoden måste göras tillgänglig för allmänheten (antingen i tidigare eller senare led) och inte bara tillhandahållas på begränsad eller villkorlig grund. Programvara som distribueras inom ramen för en licens med fri och öppen källkod men vars källkod endast delas (eller tillåts att delas) med betalande kunder eller en begränsad grupp användare ska därför inte betraktas som programvara med fri och öppen källkod i den mening som avses i artikel 3.48. Enligt cyberresiliensförordningen bör därför endast programvara vars källkod är allmänt tillgänglig och licensierad inom ramen för en licens för fri och öppen källkod som ger alla de rättigheter som avses i artikel 3.48 betraktas som programvara med fri och öppen källkod.

3.1 **Fastställande av vem som ansvarar för programvara med fri och öppen källkod**

47. Cyberresiliensförordningen lägger ett stort ansvar på ekonomiska aktörer som tillhandahåller produkter med digitala element på EU-marknaden. I förordningen definieras en tillverkare som en fysisk eller juridisk person som tillhandahåller en produkt med digitala element under eget namn eller varumärke, och som gör detta i samband med kommersiell verksamhet (vilket innebär att produkten släpps ut på marknaden). På samma sätt är en importör en fysisk eller juridisk person som är etablerad i EU och som tillhandahåller en produkt med digitala element som tillhör en person som är etablerad utanför EU och som gör detta i samband med kommersiell verksamhet (vilket innebär att produkten släpps ut på marknaden). Förvaltarnas skyldigheter är tillämpliga på den juridiska person som tillhandahåller en programvara med fri och öppen källkod avsedd för kommersiell verksamhet ([12]), men som inte släpper ut den på marknaden i den mening som avses i cyberresiliensförordningen.

48. För att avgöra om en fysisk eller juridisk person släpper ut programvara med fri och öppen källkod på EU-marknaden måste det därför först klargöras om den fysiska eller juridiska personen faktiskt tillhandahåller programvaran med fri och öppen källkod. För att korrekt fastställa de tillämpliga skyldigheterna enligt cyberresiliensförordningen är det viktigt att fastställa om den fysiska eller juridiska personen verkligen utför handlingen att tillhandahålla en programvara med fri och öppen källkod. I skäl 18 påminns om att cyberresiliensförordningen inte är tillämplig på fysiska eller juridiska personer som bidrar med källkod till produkter med digitala element som betraktas som programvara med fri och öppen källkod men som inte faller under deras ansvar.

([12]) Detta är ett nödvändigt men inte tillräckligt villkor för att en juridisk person ska kunna betraktas som en förvaltare av programvara med fri och öppen källkod, eftersom definitionen i artikel 3.14 fastställer ytterligare villkor för att en juridisk person ska betraktas som en förvaltare.

49. Med tanke på särdragen i utvecklingen av programvaror med fri och öppen källkod, vilken ofta inbegriper bidragsgivare, decentraliserade samarbetsmodeller och en särskillnad mellan bidrag och beslutsfattande, är det lämpligt att klargöra att programvara med fri och öppen källkod anses vara ”under ansvar av” fysiska eller juridiska personer som publicerar den och utövar primär kontroll över besluten rörande dess utveckling, lanseringar och distribution (ofta kallade *den som underhåller programvaran*). Personer som bidrar med källkod men inte kontrollerar lanseringar, färdplaner eller styrningsbeslut betraktas som ”bidragsgivare” – i sådana fall är programvaran med fri och öppen källkod inte under deras ansvar, även om de har bidragit med kod till den. Enbart förekomsten av tekniska tillstånd, t.ex. som ger åtkomst, är inte tillräckligt för att fastställa att programvaran med fri och öppen källkod är under den personens ansvar. Ansvaret ligger hos dem som publicerar och kontrollerar programvaran med fri och öppen källkod.

Exempel 13: En enskild utvecklare eller anställd i ett företag skickar in en ”pull”- eller en ”merge”-begäran som innehåller en säkerhetsprogramfix eller en ny funktion för ett projekt med programvara med fri och öppen källkod. Den som ansvarar för projektet granskar, godkänner och införlivar koden i huvuddatabasen, och inkluderar den därefter i en ny version. I detta scenario är den person som lämnade in pull-begäran en ”bidragsgivare” och omfattas inte av cyberresiliensförordningen. Även om denna person bidrog med källkod utövar hen inte primärkontroll över utvecklings-, lanserings- eller distributionsbesluten.

3.2 **Fastställande av om programvara med fri och öppen källkod har släppts ut på EU-marknaden**

50. När det väl har fastställts att en programvara med fri och öppen källkod faller under en fysisk eller juridisk persons ansvar måste det fastställas om den personen tillhandahåller den i samband med kommersiell verksamhet, vilket därmed utgör ett utsläppande på marknaden.

3.2.1 *Uttagande av avgift*

51. Om den fysiska eller juridiska person som tillhandahåller en programvara med fri och öppen källkod tar ut en avgift för själva programvaran (t.ex. genom att ta ut en avgift för de förkompilerade binärfilerna) släpper personen ut en produkt med digitala element på marknaden. Den person som släpper ut en programvara med fri och öppen källkod på marknaden är därför en tillverkare enligt cyberresiliensförordningen.

52. Tillverkare av programvara med fri och öppen källkod tillhandahåller ofta kostnadsfria versioner av den programvaran (som ofta kallas ”versioner för en nätgemenskap för öppen källkod”) vars kodbas är (nästan) identisk med den betalda versionen. Dessa produkter med digitala element är dock olika produkter: den betalda versionen är monetariserad på något sätt (t.ex. genom att en avgift tas ut eller på något annat sätt som diskuteras i detta avsnitt) och anses därför ha släppts ut på marknaden, vilket utlöser tillverkarens skyldigheter. Den version som tillhandahålls kostnadsfritt (eller den versionen som tillhandahålls inom en gemenskap för öppen källkod) är inte monetariserad och betraktas därför enligt cyberresiliensförordningen inte som utsläppt på marknaden. Detta är också fallet när den betalda versionen är en ”förbättrad” kommersiell version, som utökar kodbasen i den version som tillhandahålls kostnadsfritt, eller införlivar den versionen i en bredare produkt med digitala element (t.ex. som i modellen med ”öppen kärna”).

53. Om den person som tillhandahåller community-versionen är en juridisk person omfattas den juridiska personen också av förvaltarens skyldigheter för den version som denne tillhandahåller kostnadsfritt (version för en nätgemenskap för öppen källkod). Om enheten är en fysisk person omfattas den version som tillhandahålls kostnadsfritt (en version för en nätgemenskap för öppen källkod) inte av cyberresiliensförordningen.

3.2.2 *Monetarisering av andra tjänster eller krav på behandling av personuppgifter*

54. En fysisk eller juridisk person som offentliggör en programvara med fri och öppen källkod kan också släppa ut denna på marknaden (dvs. tillhandahålla den i samband med kommersiell verksamhet) om den tillhandahåller den programvara genom vilken den monetariserar andra produkter med digitala element eller tjänster, eller om den som villkor för användningen kräver att få behandla personuppgifter av andra skäl än enbart för att förbättra programvarans säkerhet, kompatibilitet eller interoperabilitet.

Exempel 14: En fysisk eller juridisk person offentliggör en marknadsplatsapplikation med fri och öppen källkod. Applikationen är tillgänglig kostnadsfritt och gör det möjligt för användare att köpa varor eller tjänster genom den. Appen gör det möjligt för den person som publicerade den att monetarisera andra produkter med digitala element och tjänster som erbjuds genom appen (t.ex. genom annonser, kommissionsavgifter eller abonnemangsavgifter). Appen anses därför ha släppts ut på marknaden i samband med kommersiell verksamhet.

Exempel 15: En fysisk eller juridisk person publicerar ett virtuellt privat nätverk (VPN) med fri och öppen källkod. Appen är tillgänglig kostnadsfritt, men gör det möjligt för användare att betala för att få tillgång till ytterligare servrar eller dedikerade IP-adresser. Applikationen gör det möjligt för den personen att monetarisera andra tjänster som erbjuds genom den, och den anses därför ha släppts ut på marknaden i samband med kommersiell verksamhet.

Exempel 16: En fysisk eller juridisk person publicerar en fitnessapp med fri och öppen källkod. Appen är tillgänglig kostnadsfritt, men dess användning villkoras med behandling av användarnas personuppgifter för ändamål såsom riktad reklam eller analysverksamhet som inte har något samband med programvarans säkerhet, kompatibilitet eller interoperabilitet. Genom att kräva en sådan uppgiftsbehandling som ett villkor för användning anses applikationen därför ha släppts ut på marknaden i samband med kommersiell verksamhet.

3.2.3 *Stödtjänster*

55. Enbart det faktum att en fysisk eller juridisk person som publicerar en programvara med fri och öppen källkod också erbjuder betalda stödtjänster kopplade till programvaran innebär inte i sig att produkten med digitala element tillhandahålls i samband med kommersiell verksamhet. Stödtjänster kan inbegripa verksamhet såsom konsulttjänster, utbildning eller yrkesmässiga tjänster kopplade till kundens användning, dokumentation, konfiguration och spridning av programvaran.

56. Den avgörande faktorn är huruvida tillgången till själva programvaran med fri och öppen källkod (dvs. tillhandahållandet av produkten med digitala element), inklusive dess underhåll, är villkorad mot ersättning snarare än enbart erbjudandet av yrkesmässiga tjänster kring en fritt tillgänglig produkt med digitala element, såsom anges i skäl 18 i cyberresiliensförordningen (”tillhandahållandet av produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte monetariseras av deras tillverkare [bör] inte betraktas vara en kommersiell verksamhet”). Om programvaran med fri och öppen källkod kan laddas ner och installeras fritt, och användarna kan välja att köpa yrkesmässiga tjänster separat, betraktas inte den programvaran med fri och öppen källkod som utsläppt på marknaden.

57. I vissa fall är däremot tillgången till en viss version av en produkt med digitala element (t.ex. vissa fördelar såsom tekniskt stöd eller prestandaoptimering) villkorad mot ersättning. I sådana fall utgör detta tillhandahållande ett monetariserat tillhandahållande av en produkt med digitala element i samband med kommersiell verksamhet och anses därför ha släppts ut på marknaden. Detta omfattar fall där en betald utgåva eller en företagsversion görs tillgänglig inom ramen för ett kommersiellt avtal, oavsett om en funktionellt likvärdig programvara också är tillgänglig kostnadsfritt inom ramen för en licens med fri och öppen källkod.

Exempel 17: En fysisk eller juridisk person publicerar ett operativsystem med fri och öppen källkod och erbjuder en betald version av samma operativsystem där stödtjänster ingår, t.ex. tekniskt stöd eller prestandaoptimering. Den betalda versionen av operativsystemet anses därför ha släppts ut på marknaden i samband med kommersiell verksamhet.

Exempel 18: En fysisk eller juridisk person publicerar ett kommandoradverktyg med fri och öppen källkod. Verktyget är fritt tillgängligt och vem som helst kan ladda ner det och installera det. Den fysiska eller juridiska personen erbjuder yrkesmässiga tjänster separat, såsom valfria konsulttjänster för att utbilda användare och hjälpa dem installera och använda verktyget. Denna programvara med fri och öppen källkod anses inte ha släppts ut på marknaden i den mening som avses i cyberresiliens-förordningen.

58. Särskilt när det gäller fysiska personer som publicerar programvara med fri och öppen källkod skulle det faktum att de erbjuder tekniskt stöd direkt i kombination med tillgång till produkten med digitala element ändå inte betraktas som en kommersiell verksamhet om, såsom anges i skäl 15 i cyberresiliensförordningen, den kostnad som tas ut endast tjänar till att täcka de faktiska kostnaderna. Sådana faktiska kostnader omfattar en rad olika kostnader för programvarans utformning, utveckling och underhåll, inklusive personens rimliga levnadsomkostnader. En fysisk person som publicerar en programvara med fri och öppen källkod och erbjuder tekniskt stöd för att täcka sina kostnader och erhålla skälig ersättning ska därför inte, enbart på denna grund, anses släppa ut programvaran på EU-marknaden.

59. En fysisk eller juridisk person som erbjuder tekniskt stöd i förbindelse med en programvara med fri och öppen källkod som inte faller under dennes ansvar anses inte släppa ut programvaran på marknaden, såvida inte den personen i väsentlig grad ändrar programvaran med fri och öppen källkod, i enlighet med artikel 22, som en del av tillhandahållandet av detta stöd.

Exempel 19: En tjänsteleverantör publicerar inte en programvara med fri och öppen källkod, men hjälper en kund att installera den på kundens lokala server. Tjänsteleverantören gör detta utan att göra en väsentlig ändring av denna programvara med fri och öppen källkod. Tjänsteleverantören anses därför inte släppa ut programvaran med fri och öppen källkod på marknaden.

3.2.4 *Donationer*

60. Fysiska eller juridiska personer som publicerar projekt med programvara med fri och öppen källkod inkluderar rutinmässigt sätt för användare av den programvaran att frivilligt donera pengar för att tacka projektets utgivare och även för att säkerställa att projektet fortsätter att underhållas aktivt.

61. Att som anges i skäl 15 i cyberresiliensförordningen ”ta emot donationer utan avsikt att göra vinst bör inte betraktas som en kommersiell verksamhet”. Enbart det faktum att det finns en länk till en donationsplattform eller liknande verktyg för att samla in donationer bör inte ses som en avsikt att gå med vinst, inte ens om det belopp som samlas in via donationer överstiger de kostnader som är förknippade med utformning, utveckling och tillhandahållande av en produkt med digitala element. Detta inbegriper rimlig ersättning till de medarbetare som anställs av en juridisk person och/eller en fysisk persons rimliga levnadskostnader. Det är naturligt för donationer att variera över tid, och därför krävs en viss flexibilitet vid bedömningen av huruvida en programvara med fri och öppen källkod som uteslutande monetariseras genom donationer anses ha släppts ut på marknaden. En programvara med fri och öppen källkod som endast stöds genom donationer kommer därför sannolikt inte att betraktas som utsläppt på marknaden i den mening som avses i cyberresiliensförordningen.

Exempel 20: En fysisk eller juridisk person publicerar ett programvaruverktyg med fri och öppen källkod i en offentlig onlinedatabas som gör det möjligt för vem som helst att ladda ned, använda, modifiera och vidaredistribuera det inom ramen för en licens för fri och öppen källkod. Utgivaren uppmanar användarna att göra frivilliga donationer via en donationsplattform för att stödja projektets fortsatta utveckling och underhåll. Tillgången till programvaran, dess källkod och uppdateringar är inte villkorad av att en donation görs. Denna programvara med fri och öppen källkod anses inte ha tillhandahållits i samband med kommersiell verksamhet och anses inte ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen.

62. Det finns dock fall där en programvara med fri och öppen källkod som stöds genom donationer kan anses ha släppts ut på marknaden. Detta är fallet om donationerna, baserat på en övergripande bedömning av omständigheterna, i praktiken motsvarar debiteringen av en avgift för att få tillgång till produkten med digitala element eller vissa av dess funktioner. Detta kan särskilt vara fallet när tillgången till programvaran med fri och öppen källkod, till väsentliga funktioner eller till uppdateringar i praktiken är villkorad med att göra en donation, eller när donationerna är förknippade med avtalsmässiga fördelar eller exklusiva fördelar som går utöver förmåner inom en nätgemenskap för öppen källkod.

Exempel 21: En fysisk eller juridisk person publicerar en programvaruprodukt med digitala element inom ramen för en licens med fri och öppen källkod, men tillhandahåller nedladdningsbara versioner och säkerhetsuppdateringar enbart till användare som gör en donation. Användare som inte donerar får inte tillgång till den aktuella versionen av programvaran.

I detta fall är donationerna i praktiken ett villkor för tillgång till produkten med digitala element och är därför liktydigt med att en avgift tas ut. Den programvaran med fri och öppen källkod anses därför ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen.

Exempel 22: En fysisk eller juridisk person gör källkoden för en programvara med fri och öppen källkod allmänt tillgänglig, men tillhandahåller förkompilerade binärfiler, regelbundna uppdateringar och garanterade säkerhetskorrigeringar endast till personer som gör donationer. I detta fall är donationerna kopplade till tillgången till väsentliga aspekter av produkten med digitala element och utgör en ersättning för tillhandahållandet av den produkten. Denna programvara med fri och öppen källkod anses därför ha släppts ut på marknaden i samband med kommersiell verksamhet.

3.2.5 *Finansiering av programvara med fri och öppen källkod*

63. Enbart det faktum att en tredje part har betalat för, sponsrat eller på annat sätt finansierat utvecklingen av en programvara med fri och öppen källkod avgör inte i sig om programvaran med fri och öppen källkod har släppts ut på marknaden. Det är allmän praxis i ekosystemet för programvaror med fri och öppen källkod att en enskild utvecklare, stiftelse eller nätgemenskap för öppen källkod erhåller finansiering från företag, offentliga organ eller andra sponsorer för att arbeta med specifika funktioner, åtgärda buggar eller underhålla kritiska komponenter. Denna finansiering kan ta många former, bland annat bidrag, buggbelöningsprogram, sponsring, tjänstekontrakt eller betalt utvecklingsarbete.

64. Såsom redan påpekats tydliggörs i skäl 18 i cyberresiliensförordningen att ”de omständigheter under vilka produkten med digitala element har utvecklats, eller hur utvecklingen har finansierats, [...] inte [bör] beaktas vid fastställandet av huruvida denna verksamhet är av kommersiell eller icke-kommersiell karaktär”.

65. Om programvaran med fri och öppen källkod delas öppet och görs fritt tillgänglig så att alla kan få tillgång till, använda, modifiera och vidaredistribuera den bör det faktum att en kommersiell enhet kan ha betalat för projektet därför inte bidra till att fastställa huruvida programvaran har släppts ut på marknaden. Om den programvaran med fri och öppen källkod inte har monetariserats på annat sätt ska den inte anses ha släppts ut på marknaden. Om det företag som finansierade utvecklingen av programvaran med fri och öppen källkod (samt eventuella andra företag) integrerar den i sin produkt med digitala element ska det företaget tillämpa tillbörlig aktsamhet i enlighet med artikel 13.5 i cyberresiliensförordningen.

Exempel 23: En enskild utvecklare publicerar ett projekt med programvara med fri och öppen källkod och underhåller det aktivt. Tillverkare A begär att den enskilda utvecklaren lägger till en särskild funktion i den programvaran med fri och öppen källkod och finansierar den utvecklingen. Utvecklaren lägger till funktionen i kodbasen för programvaran med fri och öppen källkod, delar den öppet och gör den tillgänglig så att alla kan få tillgång till, använda, modifiera och vidaredistribuera den. Den enskilda utvecklaren anses inte ha släppt ut den programvaran med fri och öppen källkod på marknaden. Om tillverkaren integrerar programvaran med fri och öppen källkod i sin produkt med digitala element måste den iaktta tillbörlig aktsamhet i enlighet med artikel 13.5.

3.2.6 *Ideella enheter som inrättats för att uppnå icke-vinstdrivande mål*

66. Om den juridiska person som offentliggör en programvara med fri och öppen källkod är en ideell organisation ”inrättad på ett sätt som säkerställer att alla intäkter efter kostnader används för att uppnå icke-vinstdrivande mål” (skäl 18 i cyberresiliensförordningen), anses den programvara med fri och öppen källkod som den juridiska personen publicerar inte ha släppts ut på marknaden. Om den juridiska personen uppfyller definitionen av ”förvaltare” omfattas den av de motsvarande skyldigheterna (artikel 24 i cyberresiliensförordningen).

Exempel 24: En juridisk person publicerar en webbläsare med fri och öppen källkod som direkt monetariseras genom sökmotorpartnerskap, men alla dess intäkter efter kostnader används för icke-vinstdrivande ändamål. Webbläsaren anses inte ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen. Den juridiska person som publicerar webbläsaren omfattas av de skyldigheter som gäller för förvaltare.

3.2.7 *Andra tillverkares integrering av programvaran*

67. I vissa fall publiceras en programvara med fri och öppen källkod av en klart identifierbar fysisk eller juridisk person, men den programvaran med fri och öppen källkod ”är [avsedd] att integreras av andra tillverkare i deras egna produkter med digitala element”. I sådana fall anses inte programvaran med fri och öppen källkod ha släppts ut på EU-marknaden, såvida den inte också monetariseras av den person som publicerar den (dvs. den ursprungliga tillverkaren), i linje med tidigare avsnitt i denna vägledning.

68. Om denna programvara med fri och öppen källkod inte släpps ut på marknaden skulle den juridiska person som publicerar den omfattas av en förvaltares skyldigheter, om den tillhandahåller stöd på varaktig basis, i linje med definitionen av ”förvaltare”.

Exempel 25: En juridisk person publicerar ett bibliotek för programvara med fri och öppen källkod avsett för att bygga användargränssnitt. Den monetariserar inte tillhandahållandet av detta bibliotek, utan integrerar det i en av sina produkter med digitala element (som i sin tur släpps ut på marknaden). Biblioteket anses inte ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen, men det är avsett att integreras i produkter med digitala element. Den juridiska person som publicerar det är dess förvaltare.

Exempel 26: En juridisk person släpper ut ett operativsystem på marknaden och publicerar även bibliotek för programvara med fri och öppen källkod (FOSS-bibliotek) som ska fungera som referenstillämpningar för dem som använder operativsystemet. Den juridiska personen monetariserar inte FOSS-biblioteken, vilka är avsedda att integreras i andra produkter med digitala element. Den juridiska person som publicerar dem är en förvaltare av dessa FOSS-bibliotek.

3.3 **Förvaltare av programvara med fri och öppen källkod**

69. I cyberresiliensförordningen införs den nya rättsliga kategorin ”förvaltare av programvara med fri och öppen källkod” mot bakgrund av ”hur viktigt det är för cybersäkerheten hos många produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som offentliggörs men inte tillhandahålls på marknaden i den mening som avses i [cyberresiliensförordningen]” (skäl 19 i cyberresiliensförordningen).

70. I vissa fall offentliggörs en programvara med fri och öppen källkod men tillhandahålls inte på marknaden i den mening som avses i cyberresiliensförordningen av en juridisk person som ”har till syfte eller som mål att systematiskt och varaktigt tillhandahålla stöd för utvecklingen av [programvara med fri och öppen källkod] [...] [avsedd] för kommersiell verksamhet, och som säkerställer dessa produkters bärkraft.” (artikel 3.14 i cyberresiliensförordningen). I sådana fall omfattas den juridiska personen av en förvaltares skyldigheter.

71. En förvaltare definieras som ”en juridisk person, annan än en tillverkare”, eftersom en tillverkare per definition är den fysiska eller juridiska person som släpper ut produkter med digitala element på marknaden (”saluför dessa”) under eget namn eller varumärke. En juridisk person kan endast vara en förvaltare av produkter med digitala element som betraktas som programvara med fri och öppen källkod och som har publicerats, men som inte tillhandahålls på marknaden i den mening som avses i cyberresiliensförordningen. Begreppet förvaltare gäller därför för specifika fall av programvaror med fri och öppen källkod som ”i slutändan är avsedda för kommersiell verksamhet, såsom integrering i kommersiella tjänster eller i monetariserade produkter med digitala element” (skäl 19 i cyberresiliensförordningen ([13])) men som inte tillhandahålls på marknaden i den mening som avses i cyberresiliensförordningen, och för vilka den juridiska person som publicerar den programvaran med fri och öppen källkod säkerställer ett systematiskt stöd.

72. Att vara förvaltare för en viss programvara med fri och öppen källkod innebär inte att den juridiska personen nödvändigtvis också är en förvaltare för andra programvaror med fri och öppen källkod som den publicerar. Att vara tillverkare för en viss programvara med fri och öppen källkod innebär likaså inte att den juridiska personen kanske inte är en förvaltare för andra programvaror med fri och öppen källkod. Detta inbegriper att tillhandahålla ”versioner för en nätgemenskap för öppen källkod” av samma programvara med fri och öppen källkod, såsom beskrivs i avsnitt *3.2.1 Uttagande av avgift*.

73. En juridisk person kan därför samtidigt vara förvaltare för en viss programvara med fri och öppen källkod (där förvaltaren systematiskt tillhandahåller stöd på varaktig basis och säkerställer programvarans bärkraft) och tillverkare för en annan specifik programvara med fri och öppen källkod (där den släpper ut denna programvara på marknaden). Med andra ord kan samma juridiska person behöva fullgöra olika roller för olika programvaruprojekt med fri och öppen källkod.

74. För varje specifik programvara med fri och öppen källkod som den juridiska personen publicerar måste denne förvissa sig om att programvaran med fri och öppen källkod anses ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen. I så fall blir den juridiska personen programvarans tillverkare. Om programvara med fri och öppen källkod inte anses ha släppts ut på marknaden kan den juridiska personen vara dess förvaltare, om programvaran är avsedd för kommersiell verksamhet och om den juridiska personen underhåller den i linje med definitionen av förvaltare ([14]).

3.3.1 *Bibehållet stöd och säkerställande av bärkraften hos en programvara med fri och öppen källkod*

75. I skäl 19 förklaras att tillhandahållandet av varaktigt stöd till utvecklingen av en produkt med digitala element kan omfatta (men inte är begränsat till) i) hysande och förvaltning av samarbetsplattformar, ii) hysande av källkod eller programvara, iii) styrning eller förvaltning av produkter med digitala element som betraktas som programvara med fri och öppen källkod, och iv) styrning av utvecklingen av sådana produkter med digitala element.

76. Detta kan till exempel vara fallet för en juridisk person som utvecklar programvara med fri och öppen källkod för integrering i sina egna produkter med digitala element och sedan publicerar den utan att släppa ut den på marknaden. Detta diskuteras också i avsnitt *3.2.7 Andra tillverkares integrering av* programvaran. I detta fall är den juridiska personen inte en tillverkare av programvaran, men kan vara en förvaltare av den. Såsom även förklaras i tidigare avsnitt anses dessutom en juridisk person som publicerar både en kostnadsfri version (eller en version för nätgemenskapen för öppen källkod) och en monetariserad version av samma programvara med fri och öppen källkod vara en förvaltare av den kostnadsfria versionen (eller en version för en nätgemenskap för öppen källkod) och en tillverkare av den monetariserade versionen.

77. På samma sätt är en juridisk person som monetariserar en programvara med fri och öppen källkod men som är en ideell enhet vars vinst efter kostnader används för att uppnå icke-vinstdrivande mål (och vars programvara med fri och öppen källkod därför inte anses ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen, såsom diskuteras i avsnitt *3.2.6 Ideella enheter*) en förvaltare av den programvara med fri och öppen källkod som den publicerar.

78. Dessutom erbjuder vissa stiftelser samarbetsplattformar med olika styrningsformer som gör det möjligt för tillverkare att regelbundet bidra till utvecklingen av programvara med fri och öppen källkod och/eller som regelbundet finansieras av tillverkare. Sådana stiftelser ska betraktas som förvaltare i förhållande till specifika programvaror med fri och öppen källkod som är avsedda för kommersiell verksamhet och för vilka stiftelsen erbjuder varaktigt stöd. Såsom förklaras i avsnitt *3.3 Förvaltare av programvara* med fri och öppen källkod omfattas dock en sådan stiftelse eventuellt inte av några skyldigheter enligt cyberresiliensförordningen för andra specifika programvaror med fri och öppen källkod som den hyser, i de fall den inte tillhandahåller systematiskt stöd till en specifik programvara med fri och öppen källkod, inte säkerställer dess bärkraft, och/eller den specifika programvaran inte är avsedd för kommersiell verksamhet.

([13]) Denna föreställning ingår också i formuleringen ”avsedda för kommersiell verksamhet” som ingår i definitionen av ”förvaltare av programvara med fri och öppen källkod” i artikel 3.14 i cyberresiliensförordningen.

([14]) Den juridiska personen får inte heller omfattas av några skyldigheter enligt cyberresiliensförordningen, i fall då i) en viss programvara med fri och öppen källkod inte släppts ut på marknaden i den mening som avses i cyberresiliensförordningen, och ii) den juridiska personen inte uppfyller definitionen av förvaltare i förhållande till den specifika programvaran med fri och öppen källkod.

79. Den typ av ”varaktigt stöd” som stiftelser och liknande organisationer tillhandahåller för specifika programvaruprojekt med fri och öppen källkod kan variera kraftigt. Vissa juridiska personer tillhandahåller t.ex. endast icke-tekniskt stöd, såsom hantering av varumärkena för projekt, fastställande av styrningsregler, anordnande av evenemang inom en nätgemenskap för öppen källkod eller insamling av donationer. Andra enheter tillhandahåller också den underliggande it-infrastruktur som krävs för att driva projektet, såsom att hysa källkodsdatabaser, tillhandahålla versionskontrollsystem eller skapa signeringsnycklar. Andra går längre med avseende på den typ av stöd de tillhandahåller genom att aktivt bidra med tekniska resurser till projektet, till exempel genom att anställa utvecklare, samordna utvecklingsarbete, granska eller slå samman kod, hantera lanseringsversioner eller hantera sårbarhetsrapporter och säkerhetsprogramfixar. Alla juridiska personer som betraktas som förvaltare enligt cyberresiliensförordningen är skyldiga att fullgöra skyldigheterna i artikel 24.1 och 24.2, men i vilken utsträckning de skyldigheter som fastställs i artikel 14.1, 14.3 och 14.8 är tillämpliga på dessa juridiska personer varierar beroende på vilken typ av stöd de tillhandahåller, i enlighet med artikel 24.3.

80. Till exempel deltar en förvaltare som endast tillhandahåller icke-tekniskt stöd per definition inte i utvecklingen av produkten med digitala element och behöver därför inte rapportera aktivt utnyttjade sårbarheter. Denna förvaltare tillhandahåller inte heller några nätverks- eller informationssystem för utveckling av sådana produkter med digitala element, och är därför inte skyldig att rapportera allvarliga incidenter till Enisa och CSIRT-enheterna eller till berörda användare. Om förvaltaren blir medveten om en aktivt utnyttjad sårbarhet (t.ex. genom en rapport från externa källor, såsom forskare inom informationssäkerhet), bör den dock dela informationen med de som underhåller produkten med digitala element, i enlighet med sin cybersäkerhetspolicy. De som underhåller produkterna med digitala element och/eller förvaltarna bör också överväga att rapportera sårbarheten på frivillig basis i enlighet med artikel 15.

81. Om en förvaltare däremot tillhandahåller den underliggande it-infrastrukturen för vissa produkter med digitala element måste den underrätta Enisa och CSIRT-enheterna i enlighet med artikel 14.3 om alla allvarliga incidenter med koppling till denna infrastruktur som har en inverkan på säkerheten för produkter med digitala element. De måste också i lämpliga fall informera alla användare (t.ex. genom ett allmänt tillkännagivande). Även om förvaltaren inte är skyldig att rapportera de aktivt utnyttjade sårbarheter som den blir medveten om bör den främja en korrekt hantering av sårbarheter och överväga frivillig rapportering i enlighet med artikel 15, såsom anges i föregående punkt.

82. Slutligen, om en förvaltare även tillhandahåller ingenjörsresurser till specifika produkter med digitala element måste den i) i enlighet med artikel 14.1 anmäla aktivt utnyttjade sårbarheter som den får kännedom om, och ii) i lämpliga fall informera alla användare. I den mån som förvaltaren också har ett direkt förhållande till de berörda användarna måste den också informera dessa direkt, i enlighet med artikel 14.8.

83. Om en enhet upphör att tillhandahålla systematiskt stöd på varaktig basis för en specifik programvara med fri och öppen källkod kanske den inte längre uppfyller definitionen av förvaltare och omfattas kanske därför inte längre av de motsvarande skyldigheterna. I sådana fall uppmuntras denna enhet att tydligt meddela ändringen i sin status för den specifika programvaran med fri och öppen källkod.

84. I vissa situationer kan en enhet som var förvaltare för ett specifikt projekt besluta att monetarisera projektet direkt och därigenom släppa ut produkten med digitala element på marknaden, vilket innebär att tillverkarens skyldigheter enligt cyberresiliensförordningen blir tillämpliga. Under sådana omständigheter betraktas denna enhet som tillverkare av produkten med digitala element från och med den dag då den släppte ut produkten på marknaden (men inte av tidigare versioner för vilka den agerade som förvaltare).

3.4 **Bidragsgivare och användning i senare led**

85. Som redan nämnts i avsnitt *3.1 Fastställande av vem som ansvarar för programvara* med fri och öppen källkod klargörs i cyberresiliensförordningen att den inte är tillämplig ”på fysiska eller juridiska personer som bidrar med källkod till produkter med digitala element som klassificeras som programvara med fri och öppen källkod och som inte omfattas av deras ansvar” (skäl 18).

86. Tillverkare av produkter med digitala element som integrerar komponenter för programvara med fri och öppen källkod i sina egna produkter med digitala element blir inte heller ansvariga för dessa enskilda komponenters förenlighet med cyberresiliensförordningen, inte ens om tillverkarna bidrar med källkod till deras underhåll.

87. Likaså har enbart det faktum att tillverkarna integrerar komponenter för programvara med fri och öppen källkod i sina egna (monetariserade) produkter med digitala element inte någon inverkan på statusen för denna komponent för programvara med fri och öppen källkod enligt cyberresiliensförordningen. De som underhåller komponenter för en programvara med fri och öppen källkod som inte släpps ut på marknaden har inga skyldigheter gentemot andra enheter som kanske integrerar sådana komponenter i sina produkter med digitala element. Huruvida cyberresiliensförordningen gäller för en viss komponent för programvara med fri och öppen källkod beror enbart på om den fysiska eller juridiska person som publicerar den släpper ut den på marknaden.

88. Tillverkare av produkter med digitala element som integrerar komponenter för programvara med fri och öppen källkod måste dock uppfylla kraven i cyberresiliensförordningen när det gäller sina egna produkter med digitala element. De är också skyldiga att visa tillbörlig aktsamhet i enlighet med artikel 13.5 gentemot de komponenter för programvara med fri och öppen källkod som de integrerar. Dessutom måste de rapportera sårbarheter i integrerade komponenter och dela säkerhetskorrigeringar i enlighet med artikel 13.6. För mer vägledning i det här ämnet, se avsnitt *9.2.1 Rapportering till tidigare led och delning* av säkerhetsåtgärder.

3.5 **Vägledande scenarier**

89. Exemplen nedan är helt hypotetiska och endast avsedda att illustrera olika fall som förklaras i avsnitten ovan.

Exempel 27: Enskild utvecklare A har utvecklat en programvara med fri och öppen källkod. Utvecklare A publicerar den programvaran med fri och öppen källkod under sitt eget namn eller varumärke, men tar inte ut någon avgift för dess användning. Programvaran delas öppet och är fritt tillgänglig för alla för tillgång, användning, modifiering och vidaredistribuering. Utvecklare A lägger också till en länk till en plattform för insamling av frivilliga donationer.

Företagen B, C och D integrerar denna programvara med fri och öppen källkod i sina egna produkter med digitala element. För att stödja det löpande underhållet gör företag B, C och D frivilliga donationer till utvecklare A. Dessa donationer gör det möjligt för utvecklare A att aktivt underhålla projektet.

Denna programvara med fri och öppen källkod har inte släppts ut på marknaden i den mening som avses i cyberresiliensförordningen. Utvecklare A har inga skyldigheter enligt cyberresiliensförordningen. Företagen B, C och D ska visa tillbörlig aktsamhet i enlighet med artikel 13.5 när de integrerar denna programvara med fri och öppen källkod i sina egna produkter med digitala element.

Exempel 28: Den ideella stiftelsen F publicerar en komponent för programvara med fri och öppen källkod för integrering i andra kommersiella produkter med digitala element. Stiftelse F åtar sig att ge varaktigt stöd till denna programvara med fri och öppen källkod för att säkerställa dess bärkraft och användning. Företagen A, B och C integrerar denna programvara med fri och öppen källkod i sina egna produkter med digitala element. Företagen A och B bidrar frivilligt med en del av sina utvecklares tid till att utveckla och underhålla projekt med programvara med fri och öppen källkod inom stiftelse F, även för den berörda programvaran med fri och öppen källkod.

Eftersom stiftelse F är en ideell enhet som inrättats på ett sådant sätt att dess vinst efter kostnader används för att uppnå ickevinstdrivande mål anses programvaran med fri och öppen källkod inte ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen. Stiftelse F är förvaltare för programvaran med fri och öppen källkod och omfattas av de motsvarande skyldigheterna enligt artikel 24. Företagen A, B och C ska visa tillbörlig aktsamhet i enlighet med artikel 13.5 när de integrerar denna programvara med fri och öppen källkod i sina egna produkter med digitala element.

Exempel 29: Företaget A har utvecklat en komponent för programvara med fri och öppen källkod för integrering i sina egna produkter med digitala element. Företaget publicerar också den programvaran med fri och öppen källkod separat under sitt eget namn eller varumärke och underhåller den aktivt. Det tar dock inte ut någon avgift för programvarans användning eller monetariserar den på andra sätt. Företagen B, C och D integrerar den programvaran med fri och öppen källkod i sina egna produkter med digitala element och bidrar frivilligt med en del av sina utvecklares tid till att underhålla den.

Denna programvara med fri och öppen källkod anses inte ha släppts ut på marknaden i den mening som avses i cyberresiliensförordningen. Företag A är inte dess tillverkare, utan dess förvaltare. Företagen B, C och D ska visa tillbörlig aktsamhet i enlighet med artikel 13.5 när de integrerar programvaran med fri och öppen källkod i sina egna produkter med digitala element.

Exempel 30: Företaget A publicerar en programvara med fri och öppen källkod under sitt eget namn eller varumärke och erbjuder den som betald version, vilket inbegriper vissa fördelar såsom tekniskt stöd eller prestandaoptimering. Utvecklare från företagen B, C och D bidrar till underhållet av programvaran med fri och öppen källkod, men den står fortfarande under företag A:s kontroll.

Företag A betraktas som tillverkare av denna programvara med fri och öppen källkod ([15]). Företagen B, C och D omfattas inte av skyldigheterna enligt cyberresiliensförordningen för denna specifika programvara med fri och öppen källkod. Om de integrerar den programvaran med fri och öppen källkod i sina egna produkter med digitala element måste de iaktta tillbörlig aktsamhet i enlighet med artikel 13.5.

Exempel 31: Företaget A publicerar en programvara med fri och öppen källkod under sitt eget namn eller varumärke och tillhandahåller löpande underhåll för att säkerställa dess långsiktiga bärkraft, så att programvaran kan integreras i andra företags produkter med digitala element. Företaget A tar inte ut någon avgift för dess användning, behandlar inte några personuppgifter som det samlar in via produkten med digitala element eller säljer några stödtjänster som är kopplade till publiceringen av programvaran med fri och öppen källkod.

Företag B bidrar med kod och utvecklares tid till underhållet av programvaran med fri och öppen källkod, men distribuerar den inte kommersiellt. Företag B erbjuder tekniska stödtjänster oberoende av distributionen av programvaran med fri och öppen källkod. Företag A anses vara förvaltare av denna programvara med fri och öppen källkod, medan företag B inte har några skyldigheter enligt cyberresiliensförordningen för denna programvara med fri och öppen källkod.

Exempel 32: En komponent för programvara med fri och öppen källkod publiceras av en ideell enhet som inrättats på ett sådant sätt att alla intäkter efter kostnaderna används för att uppnå icke-vinstdrivande mål. Enheten tillhandahåller varaktigt stöd för att säkerställa projektets långsiktiga bärkraft. Underhållet finansieras genom offentlig finansiering, såsom forskningsbidrag. Ytterligare utveckling, inklusive nya funktioner, finansieras genom donationer och särskilda projekt som genomförs i partnerskap med tillverkare som integrerar denna programvara med fri och öppen källkod i sina produkter med digitala element. Sådana funktioner införlivas i kodbasen för programvaran med fri och öppen källkod.

Den ideella enhet som offentliggör programvaran med fri och öppen källkod betraktas som förvaltare av denna komponent för programvara med fri och öppen källkod. En tillverkare som har bidragit till utvecklingen av vissa funktioner betraktas inte som tillverkare av denna komponent för programvara med fri och öppen källkod. Om tillverkaren integrerar den komponenten för programvara med fri och öppen källkod i sin egen produkt med digitala element måste den iaktta tillbörlig aktsamhet i enlighet med artikel 13.5.

Exempel 33: En ideell enhet som inrättats på ett sådant sätt att alla intäkter efter kostnader används för att uppnå icke-vinstdrivande mål publicerar ett kit för utveckling av programvara med fri och öppen källkod och säkerställer ett löpande underhåll för kittet. Kittet för utveckling av programvaran delas öppet och är fritt tillgängligt för alla för tillgång, användning, modifiering och vidaredistribuering. Finansieringen tillhandahålls genom medlemsavgifter som betalas till den ideella enheten, och utvecklare som är anställda av medlemsorganisationer bidrar med kod och andra resurser till utvecklingen av kittet. Tillverkarna använder kittet för utveckling av programvaror som en komponent för att bygga andra produkter med digitala element.

Den ideella enhet som offentliggör kittet för utveckling av programvaror är kittets förvaltare. Stiftelsens medlemmar är inte ansvariga för kittets förenlighet med cyberresiliensförordningen. Om tillverkarna använder kittet för utveckling av programvaror för att bygga sina egna produkter med digitala element måste de iaktta tillbörlig aktsamhet i enlighet med artikel 13.5.

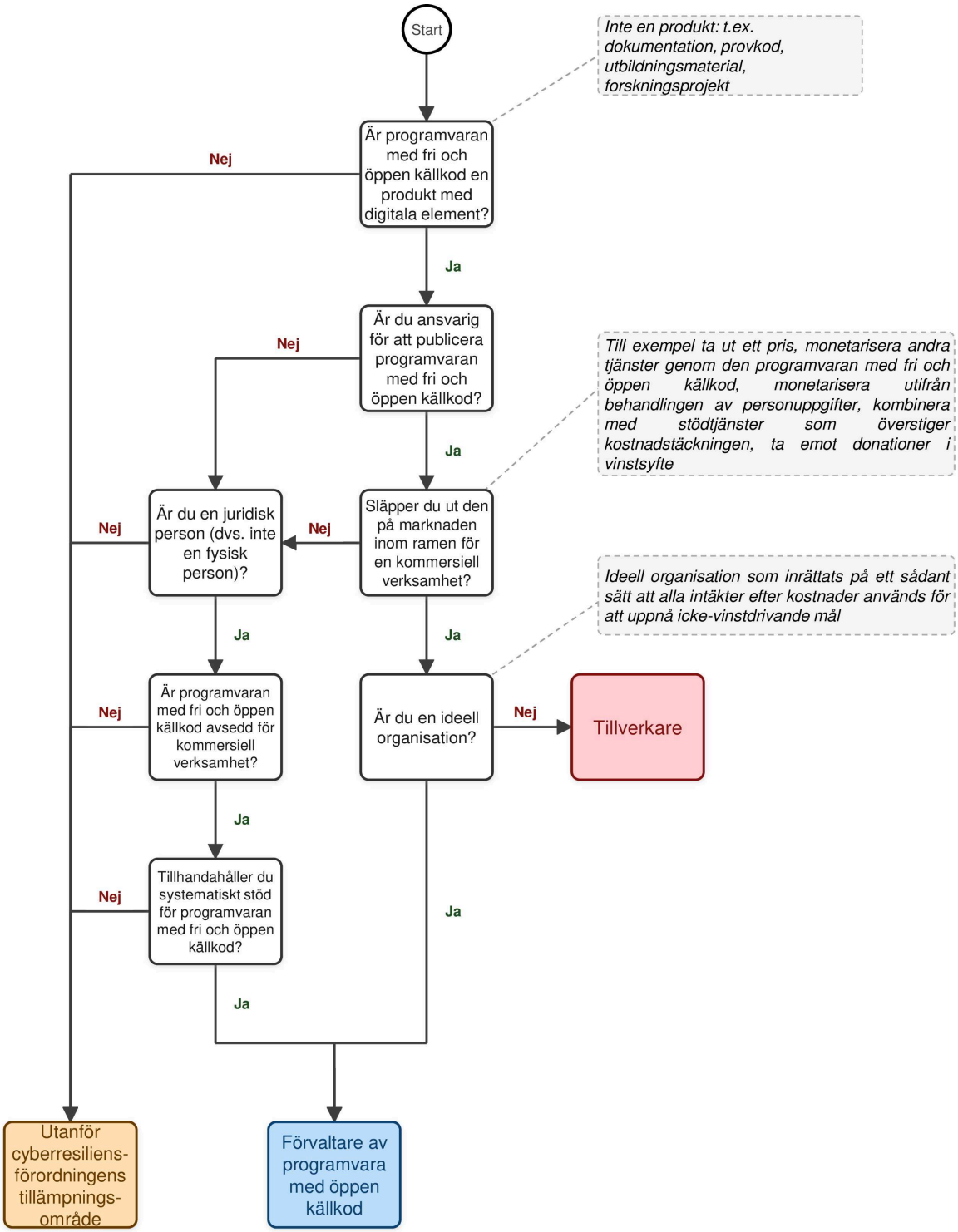
Exempel 34: En enskild utvecklare publicerar ett bibliotek för programvara med fri och öppen källkod i en offentlig paketdatabas för ett visst programmeringsspråk och underhåller det aktivt. I paketdokumentationen lägger utvecklaren till en länk för att samla in donationer. En tillverkare laddar ner biblioteket kostnadsfritt från databasen och integrerar det i sin egen produkt med digitala element.

Den enskilda utvecklaren och paketdatabasen har inga skyldigheter enligt cyberresiliensförordningen. Den tillverkare som integrerar biblioteket måste visa tillbörlig aktsamhet i enlighet med artikel 13.5.

([15]) Såvida inte företag A är en ideell enhet som inrättats på ett sådant sätt att alla vinster efter kostnader används för att uppnå icke-vinstdrivande mål – i detta fall skulle företaget vara förvaltare av denna programvara med fri och öppen källkod.

Figur 1

Stiliserat flödesschema för cyberresiliensförordningens omfattning av fri programvara med öppen källkod



4. VÄSENTLIGA ÄNDRINGAR OCH RESERVDELAR

90. I artikel 3.30 i cyberresiliensförordningen definieras en ”väsentlig ändring” som en ändring av produkten med digitala element efter dess utsläppande på marknaden, vilket i) påverkar överensstämmelsen för produkten med digitala element med de väsentliga cybersäkerhetskraven i del I i bilaga I, eller ii) leder till en ändring av det avsedda ändamål för vilket produkten med digitala element har bedömts.

91. Begreppet väsentlig ändring är relevant för att fastställa skyldigheterna enligt cyberresiliensförordningen i ett antal fall, däribland följande:

a) I enlighet med artikel 21 betraktas en importör eller distributör som genomför en väsentlig ändring av en produkt med digitala element som redan släppts ut på marknaden som dess tillverkare.

b) I enlighet med artikel 22 betraktas varje fysisk eller juridisk person som utför en väsentlig ändring av en produkt med digitala element och tillhandahåller den på marknaden som dess tillverkare.

c) I enlighet med artikel 69.2 ska varje fysisk eller juridisk person som efter den 11 december 2027 genomför en väsentlig ändring av en produkt med digitala element som släppts ut på marknaden före den 11 december 2027 och släpper ut den på marknaden betraktas som dess tillverkare.

d) För tillverkare av produkter med digitala element som släpps ut på marknaden efter den 11 december 2027, för att avgöra om en produkt med digitala element måste genomgå ett nytt förfarande för bedömning av överensstämmelse på grund av de ändringar som gjorts efter detta datum, i synnerhet mot bakgrund av programvaruutvecklingens iterativa karaktär.

92. Därför är det viktigt att ge vägledning för att hjälpa ekonomiska aktörer att förstå när ändringar av hårdvara eller programvara räknas som väsentliga ändringar.

4.1 **Fysiska reparationer**

93. I skäl 42 i cyberresiliensförordningen anges att ”om en produkt med digitala element är föremål för renovering, underhåll och reparation av en produkt med digitala element, enligt definitionen i artikel 2.18, 2.19 och 2.20 i Europaparlamentets och rådets förordning (EU) 2024/1781, medför detta inte nödvändigtvis en väsentlig ändring av produkten, exempelvis om det avsedda ändamålet och de avsedda funktionerna inte ändras och risknivån inte påverkas. Tillverkarens uppgradering av en produkt med digitala element kan dock medföra ändringar av produktens utformning och utveckling och skulle därför kunna påverka dess avsedda ändamål och uppfyllande av de krav som fastställs i den här förordningen”. Detta är förenligt med avsnitt 2.1 i blåboken, där man påminner om att ”en produkt som har genomgått större förändringar efter att den tagits i bruk måste anses vara en ny produkt om i) dess ursprungliga prestanda, ändamål eller typ ändras utan att detta förutses i den ursprungliga riskbedömningen, ii) farans art har förändrats eller risknivån har ökat i förhållande till relevant harmoniseringslagstiftning, och iii) produkten tillhandahålls (eller tas i bruk, om den tillämpliga lagstiftningen även omfattar ibruktagande). Bedömningen måste göras från fall till fall och med hänsyn till den berörda lagstiftningens syfte och den typ av produkter som omfattas”.

94. Renoverings-, underhålls- eller reparationsverksamhet som leder till fysiska ändringar av produkter med digitala element som redan släppts ut på marknaden innebär inte nödvändigtvis att väsentliga ändringar görs. En bedömning från fall till fall bör därför göras för att fastställa om en sådan fysisk ändring påverkar överensstämmelsen med de väsentliga kraven i del I i bilaga I för produkten med digitala element, eller om den leder till en ändring av produktens avsedda ändamål som omfattas av bedömningen av cybersäkerhetsrisker.

95. En ersättning av defekta eller slitna delar med delar som presterar bättre (t.ex. på grund av tekniska framsteg eller på grund av att den gamla delen inte längre tillverkas) utgör inte i sig en väsentlig ändring av den reparerade produkten med digitala element. Den utgör endast en väsentlig ändring om ändringen i prestanda eller det sätt på vilket den reparerade produkten med digitala element fungerar i) påverkar produktens uppfyllande av de väsentliga kraven eller ii) leder till en ändring av det avsedda ändamål som inte omfattades av riskbedömningen.

Exempel 35: En tillverkare av en server utför en reparation under vilken ett defekt RAM-minne byts ut mot ett nytt minne med bättre prestanda. Serverns uppfyllande av de väsentliga kraven påverkas inte. Servern presterar bättre, men den nya prestandan omfattas fortsatt av serverns avsedda användning enligt vad som beaktas i bedömningen av cybersäkerhetsrisker. Servern betraktas inte som väsentligen ändrad.

4.2 **Reservdelar**

96. I artikel 2.6 i cyberresiliensförordningen fastställs att reservdelar som är avsedda att ersätta identiska komponenter och som tillverkas enligt samma specifikationer som dessa komponenter inte omfattas av cyberresiliensförordningen. I skäl 29 anges vidare att undantaget omfattar både reservdelar för produkter med digitala element som gjorts tillgängliga innan cyberresiliensförordningen började tillämpas, och reservdelar som redan har genomgått ett förfarande för bedömning av överensstämmelse i enlighet med förordningen.

97. Undantaget i artikel 2.6 i cyberresiliensförordningen bör tolkas som att det endast är tillämpligt om reservdelen specifikt tillhandahålls för att reparera eller förlänga hållbarheten hos en produkt med digitala element som redan släppts ut på marknaden (före eller efter den 11 december 2027). Om en produkt med digitala element tillhandahålls som en fristående produkt, utan någon koppling till underhåll eller reparation av en befintlig produkt med digitala element, släpps den ut på marknaden i den mening som avses i cyberresiliensförordningen och bör inte betraktas som en reservdel som omfattas av artikel 2.6. Syftet med underhållet eller reparationen bör framgå tydligt av sammanhanget för tillhandahållandet, till exempel genom identifiering av produkten med digitala element eller produktfamiljen i beställningen eller det kommersiella erbjudandet, eller genom tillhandahållande via eftermarknadsförsäljnings- eller servicekanaler. Stödjande bevis för detta bör också finnas tillgängliga för marknadskontrollmyndigheterna. Det faktum att en produkt med digitala element tekniskt sett skulle kunna användas för att ersätta en komponent är inte i sig tillräckligt för att den ska omfattas av undantaget i frånvaro av sådana aspekter.

98. Om en reservdel är identisk med en komponent som redan ingår i en produkt med digitala element som antingen har släppts ut på marknaden före den dag då cyberresiliensförordningen börjar tillämpas eller som har släppts ut på marknaden i enlighet med cyberresiliensförordningen, omfattas den reservdelen i sig inte av cyberresiliensförordningen.

99. Bedömningen av huruvida en reservdel bör betraktas som identisk med en komponent bör inriktas på dess funktionella roll i produkten med digitala element och de egenskaper som kan vara relevanta för cybersäkerheten. Även om det alltid behövs en bedömning från fall till fall, hindrar skillnader som inte påverkar komponentens säkerhetsegenskaper eller cybersäkerhetsriskprofil inte i sig den reservdelen från att omfattas av artikel 2.6 i cyberresiliensförordningen.

100. De skillnader i egenskaper som är relevanta för komponentens cybersäkerhet, såsom algoritmer, protokoll, kryptografiska mekanismer, åtkomstkontrollfunktioner eller andra säkerhetsrelevanta egenskaper, kan däremot innebära att den nya delen inte kan betraktas som identisk med den komponent som den är avsedd att ersätta.

101. Om en reservdel inte är identisk med den ursprungliga komponenten utgör denna reservdel en produkt med digitala element i sig och omfattas därför av cyberresiliensförordningen. I sådana fall ska uppfyllandet av de väsentliga kraven bedömas mot bakgrund av ersättningskomponentens avsedda ändamål. Av särskild betydelse är ersättningskomponentens funktion att säkerställa kompatibilitet eller interoperabilitet med en befintlig produkt med digitala element, inbegripet om produkten är en produkt med digitala element som släppts ut på marknaden innan cyberresiliensförordningen började tillämpas. Om vissa väsentliga krav rimligen inte kan uppfyllas på grund av detta avsedda ändamål eller på grund av tekniska begränsningar, måste tillverkaren avspegla detta i bedömningen av cybersäkerhetsrisker och genomföra lämpliga alternativa eller kompenserande riskreducerande åtgärder för att inte undergräva säkerheten hos produkten med digitala element. Som också diskuteras i avsnitt *2.6 Komplexa system*, spelar både den tekniska dokumentationen och informationen och instruktionerna till användaren en viktig roll när det gäller att öppet beskriva de fastställda begränsningarna, de därtill hörande cybersäkerhetsriskerna och de riskreducerande åtgärder som har vidtagits. Som förklaras i avsnitt *4.1 Fysiska reparationer* leder en ersättning av defekta eller slitna delar med delar som presterar bättre inte i sig till att en väsentlig ändring anses har gjorts av den reparerade produkten med digitala element.

Exempel 36: En tillverkare har släppt ut anslutna styrenheter på EU-marknaden. I ett fall släpptes styrenheten ut på marknaden under 2026, före den dag då cyberresiliensförordningen började tillämpas. I ett annat fall släpptes styrenheten ut på marknaden under 2028, i enlighet med cyberresiliensförordningen. Under 2028 slutar en digital kommunikationsmodul i båda typerna av styrenheter att fungera. Som reservdel tillhandahåller tillverkaren en ersättningsmodul som är identisk och tillverkad enligt samma specifikationer som originalet.

I båda fallen omfattas ersättningsmodulen av undantaget i artikel 2.6. Reservdelen omfattas inte i sig av cyberresiliensförordningen, trots att den är en produkt med digitala element, eftersom den ersätter en identisk komponent i en produkt med digitala element. Reparationen utgör inte någon väsentlig ändring av produkten med digitala element.

Exempel 37: En tillverkare släppte ut en ansluten industriell styrenhet på EU-marknaden under 2026 före den dag då cyberresiliensförordningen började tillämpas. Under 2028 slutar ett kommunikationschip i den styrenheten att fungera. Eftersom tillverkaren inte längre tillverkar chippet tillhandahåller den i stället en reservdel i form av ett nyare chip med motsvarande funktionalitet, men med ett annat kryptografiskt genomförande och en uppdaterad säker startmekanism, för att på så vis bibehålla kompatibiliteten och den fortsatta driften.

I detta fall kan inte ersättningschippet anses vara identiskt, eftersom skillnaderna i det kryptografiska genomförandet och den säkra startmekanismen påverkar chippets cybersäkerhetsegenskaper. Det omfattas därför inte av undantaget i artikel 2.6 och utgör en produkt med digitala element som omfattas av cyberresiliensförordningen. Ersättningsdelens överensstämmelse måste bedömas mot bakgrund av dess avsedda syfte, däribland dess roll när det gäller att säkerställa interoperabiliteten hos produkten med digitala element som släppts ut på marknaden innan cyberresiliensförordningen började tillämpas.

Exempel 38: En tillverkare släpper under 2028 ut en styrenhet för smarta byggnader på marknaden i enlighet med cyberresiliensförordningen. Under 2029 slutar den trådlösa modulen i styrenheten att fungera. Eftersom tillverkaren inte längre tillverkar modulen levererar den som reservdel en ny modul som har samma funktion och använder samma kommunikationsprotokoll och säkerhetsmekanismer, men som baseras på en annan chippsats och har en uppdaterad fast programvara som inte ändrar egenskaper som kan vara relevanta för cybersäkerheten.

I detta fall kan ersättningsmodulen anses vara identisk. Modulen omfattas därför av undantaget i artikel 2.6 och omfattas inte av cyberresiliensförordningen.

102. Undantaget för reservdelar gäller oavsett om reservdelen ersätter en komponent inom en produkt med digitala element eller om den ersätter en komplett produkt med digitala element som i sig utgör en del av en större produkt, inbegripet när denna större produkt med digitala element består av flera integrerade komponenter, under förutsättning att ersättningsdelen specifikt tillhandahålls som en reservdel, såsom förklaras i föregående punkter.

Exempel 39: År 2027 släpper en tillverkare ut ett industriellt automatiseringssystem på marknaden som innehåller en programmerbar styrlogikenhet som en av systemets komponenter. År 2031 slutar styrlogikenhetens centralprocessor (CPU) att fungera. Tillverkaren erbjuder två reparationsalternativ: i) leverans av en ersättningscentralprocessor som kan betraktas som identisk med den centralprocessor som ursprungligen installerades, eller ii) leverans av en komplett ersättningsstyrlogikenhet, som kan anses vara identisk med den styrlogikenhet som ursprungligen installerades. I båda fallen tillhandahålls ersättningsenheten genom tillverkarens kanal för eftermarknadsservice som en reservdel, och det industriella automatiseringssystem för vilket reservdelen är avsedd är tydligt angivet. I båda fallen omfattas ersättningsenheten av undantaget i artikel 2.6, oavsett om ersättningsenheten är en komponent inom styrlogikenheten eller styrlogikenheten som helhet.

4.3 **Programuppdateringar som väsentliga ändringar**

103. Programvaruutveckling är iterativ av naturen, och programvaruprodukter med digitala element som redan släppts ut på marknaden uppdateras ofta och kontinuerligt. I detta sammanhang är det lämpligt att ge mer vägledning för att fastställa när programvaran ska anses vara väsentligt ändrad. Denna vägledning är särskilt avsedd att hjälpa tillverkare av programvaruprodukter med digitala element som gör ändringar i sina egna produkter att avgöra om dessa ändringar betraktas som väsentliga ändringar.

104. I skäl 39 anges att en produkt med digitala element ändras väsentligt om ändringen ändrar nivån på cybersäkerhetsrisken och tillverkaren inte har tagit hänsyn till en sådan ändrad eller ytterligare risk i sin riskbedömning, och följaktligen i sitt uppfyllande av de väsentliga kraven. En tillverkare bör därför från fall till fall bedöma om en programvaruuppdatering medför nya eller ökade cybersäkerhetsrisker, och om dessa risker redan har tagits upp i riskbedömningen.

105. Om en tillverkare inför nya funktioner i en produkt med digitala element som leder till en ändring av produktens avsedda ändamål som helhet är det sannolikt att tillverkaren inte beaktade dessa ändringar i sin riskbedömning. Under sådana omständigheter skulle ändringen i allmänhet betraktas som en väsentlig ändring.

Exempel 40: En tillverkare släpper ut en instrumentpanel på marknaden som samlar in data från maskiner och visar trender och varningar, utan att erbjuda någon möjlighet att styra dessa maskiner. Tillverkaren utvecklar därefter en ny version av instrumentpanelen, och inför då funktioner som gör att man kan styra maskinerna, bland annat genom att justera driftsparametrarna och starta om maskinerna efter feltillstånd. Som en följd av dessa förändringar har instrumentpanelens avsedda syfte utvecklats utöver vad som förutsågs i riskbedömningen, och instrumentpanelen har ändrats från ett verktyg för situationsmedvetenhet till en produkt med digitala element avsedd att utöva operativ kontroll över andra enheter. Instrumentpanelen har därför ändrats väsentligt.

Exempel 41: En tillverkare släpper ut en programvaruapplikation för konsumenter på marknaden som är avsedd att organisera och visa personuppgifter, såsom e-postmeddelanden, meddelanden eller dokument, och att stödja grundläggande sök- och filtreringsfunktioner. Tillverkaren inför därefter en uppdatering som gör det möjligt för appen att automatiskt analysera användarinnehållet för att skapa beteendeprofiler och fatta automatiserade beslut som påverkar prioriteringen, undertryckandet eller rekommendationen av innehåll utan användarens ingripande. Till följd av denna ändring övergår programvarans avsedda syfte från ett användarstyrt informationshanteringsverktyg till ett automatiserat system för beslutsfattande, vilket inte förutsågs i riskbedömningen. Appen har därför ändrats väsentligt.

106. Samtidigt är det dock möjligt att en tillverkare gradvis inför nya funktioner som redan ingår i dennes riskbedömning eller som i sig inte ändrar cybersäkerhetsriskprofilen för produkten med digitala element. Detta kan exempelvis vara fallet om tillverkaren har förväntat sig att dessa funktioner ska utvecklas, redan har beskrivit och bedömt de därtill hörande riskerna och har vidtagit lämpliga riskreducerande åtgärder för att säkerställa en fortsatt uppfyllande av de väsentliga kraven. Detta kan också vara fallet om de nya funktionerna inte medför ändringar som introducerar nya eller ökade risker. Uppdateringar av detta slag bör därför inte betraktas som väsentliga ändringar, eftersom de inte ökar cybersäkerhetsrisken och följaktligen inte ändrar uppfyllandet av de väsentliga kraven.

Exempel 42: Ett meddelandeprogram släpps ursprungligen med funktioner som är begränsade till meddelanden mellan enskilda användare (one-to-one-messaging). Tillverkarens riskbedömning omfattar ett senare införande av gruppmeddelanden, däribland en ökad komplexitet i dirigeringen av meddelanden. I en därpå följande uppdatering lägger tillverkaren till en gruppchattfunktion jämte administratörskontroller och modereringsverktyg som redan förutsågs och bedömdes i den ursprungliga utformningen. Uppdateringen inför funktioner som omfattas av det ursprungliga avsedda ändamålet och den ursprungliga riskbedömningen. Meddelandeapplikationen har därför inte ändrats väsentligt.

Exempel 43: Ett produktionsövervakningssystem släpps ut på marknaden med aktiverade skrivskyddade instrumentpaneler, och med automatiska kontrollfunktioner som är närvarande i systemarkitekturen men förblir inaktiverade. Tillverkarens riskbedömning omfattar uttryckligen en framtida aktivering av automatiska reglerkretsar, däribland de cybersäkerhetsrisker som är förenade med styrning av slutna kretsar, samt skyddsåtgärder såsom åsidosättningsmekanismer för operatören och felsäkra tillstånd. I en senare uppdatering aktiverar tillverkaren de automatiska styrfunktionerna och aktiverar skyddsåtgärderna enligt den ursprungliga bedömningen. Produktionsövervakningssystemet har därför inte ändrats väsentligt.

107. Omvänt kan även begränsade eller till synes små nya funktioner införa betydande cybersäkerhetsrisker som påverkar överensstämmelsen med de väsentliga kraven. Bedömningen av väsentliga ändringar bör därför inte baseras på ändringens omfattning eller komplexitet, utan på dess potentiella negativa inverkan på cybersäkerhetsriskprofilen för produkten med digitala element och följaktligen på uppfyllandet av de väsentliga kraven.

Exempel 44: En tillverkare uppdaterar ett program och lägger till en "kom-ihåg-mig-funktion" eller en permanent inloggningsfunktion som lagrar autentiseringstoken lokalt för att förbättra användarvänligheten. Även om funktionens omfattning är begränsad, medför den nya risker kopplade till stölder av token, obehörig åtkomst och sessionskapning som inte beaktades i riskbedömningen. Uppdateringen påverkar därför överensstämmelsen med de väsentliga kraven. Programvaruapplikationen har ändrats väsentligt.

Exempel 45: En tillverkare lägger till en ny loggnings- och diagnostikfunktion till en befintlig programvaruprodukt med digitala element, som gör det möjligt att exportera detaljerade systemloggar för felsökning. Även om funktionen förefaller vara liten leder den till insamling och lagring av känsliga operativa data i ett okrypterat format, vilket inför risker för dataexponering som inte tidigare har bedömts eller begränsats. Ändringen kan därför ha en betydande inverkan på cybersäkerhetsriskprofilen för produkten med digitala element. Programvaruprodukten med digitala element har därmed ändrats väsentligt.

108. I enlighet med skäl 39 i cyberresiliensförordningen ska säkerhetsuppdateringar i allmänhet inte betraktas som väsentliga ändringar, eftersom deras främsta syfte är att minska den cybersäkerhetsrisk som är förknippad med produkten med digitala element. En säkerhetsuppdatering som inte ändrar produktens avsedda syfte och inte medför nya cybersäkerhetsrisker bör därför inte betraktas som en väsentlig ändring, även om uppdateringen kan införa betydande tekniska ändringar. Detta inbegriper om vissa funktioner ändras eller begränsas enbart i syfte att minska de identifierade sårbarheterna och säkerställa ett fortsatt uppfyllande av de väsentliga kraven.

Exempel 46: En tillverkare genomför en säkerhetsuppdatering för att åtgärda ett säkerhetsproblem i kodbasen för en produkt med digitala element genom att korrigera ett inmatningsvalideringsfel (input validation error) som kan leda till buffertöverfyllning, eller genom att åtgärda ett logiskt fel som gör det möjligt att kringgå autentiseringen genom en felaktig sessionstokenvalidering. Uppdateringen modifierar den interna i användningen av programvaran utan att påverka produktens avsedda syfte eller införa någon ny exponering. En sådan uppdatering är uteslutande avsedd att minska cybersäkerhetsrisken. Säkerhetsuppdateringen bör inte betraktas som en väsentlig ändring.

Exempel 47: En tillverkare genomför en säkerhetsuppdatering som stärker de befintliga säkerhetskonfigurationerna, till exempel genom att skärpa brandväggsreglerna, inaktivera oanvända nätverksportar, ändra standardprinciperna för administratörslösenord eller göra multifaktorautentisering obligatorisk i de fall dessa funktioner redan var tillgängliga eller planerade. Även om uppdateringen kan påverka hur användarna konfigurerar eller får tillgång till produkten med digitala element, ändrar den inte produktens avsedda syfte och syftar enbart till att förbättra dess säkerhet. Säkerhetsuppdateringen bör inte betraktas som en väsentlig ändring.

Exempel 48: En tillverkare släpper ut en programvaruprodukt med digitala element på marknaden som säkrar kommunikationen med hjälp av en konfigurerbar krypteringsram som stöder flera olika krypteringsalgoritmer och nyckelstorlekar, enligt beskrivningen i produktens tekniska dokumentation och riskbedömning. Riskbedömningen omfattar alla kryptografiska alternativ som tillhandahålls i produkten med digitala element och förutspår att vissa algoritmer i framtiden kommer att bli förlegade. Riskbedömningen inbegriper även begränsningsåtgärder, såsom kryptografisk flexibilitet, intern nyckelhantering och kompatibilitetstester. Som svar på den framväxande kryptografiska vägledningen genomför tillverkaren en säkerhetsuppdatering som inaktiverar en förlegad algoritm och aktiverar ett starkare alternativ som redan stöds, utan att införa några nya externa beroenden eller ändra dataflödena. Eftersom uppdateringen tillämpar en säkerhetsåtgärd som förutsågs och bedömdes som en del av den ursprungliga utformningen, och den inte medför några nya cybersäkerhetsrisker, bör säkerhetsuppdateringen inte betraktas som en väsentlig ändring.

109. En säkerhetsuppdatering kan däremot betraktas som en väsentlig ändring om uppdateringen, trots sitt säkerhetsmål, leder till att produktens avsedda ändamål ändras utöver vad som ursprungligen förutsågs eller medför nya eller ökade cybersäkerhetsrisker. Detta kan exempelvis vara fallet om en uppdatering väsentligt ändrar produktens gränser eller beroendestruktur på ett sätt som inte förutsågs i riskbedömningen, t.ex. genom att väsentligt ändra dataflödena, eller genom att lägga till nya externt åtkomliga gränssnitt.

Exempel 49: En tillverkare släpper ut en programvaruprodukt med digitala element på marknaden som är avsedd att tillhandahålla lokal filkryptering för data som lagras på en användares enhet, vilket gör det möjligt för användaren att kryptera och dekryptera filer på begäran. Efter upptäckten av ett säkerhetsproblem i krypteringsarbetsflödet tillhandahåller tillverkaren en säkerhetsuppdatering som tar bort de lokala krypteringsfunktionerna och i stället kräver att alla filer laddas upp till, lagras i och behandlas av en fjärrkrypteringstjänst som drivs av tillverkaren. Till följd av denna ändring utför produkten med digitala element inte längre någon lokal kryptering såsom ursprungligen var avsett, utan fungerar i stället som en fjärrkrypterings- och databehandlingstjänst. Även om uppdateringen införs av säkerhetsskäl förändrar den i grunden produktens avsedda ändamål på ett sätt som inte anges i riskbedömningen, och betraktas därför som en väsentlig ändring.

Exempel 50: En tillverkare släpper ut en programvaruprodukt med digitala element på marknaden som förlitar sig på ett etablerat krypteringsprotokoll och en internt hanterad nyckellivscykel för att säkra kommunikationen mellan komponenterna i produkten med digitala element. Som svar på nyligen identifierade kryptografiska svagheter genomför tillverkaren en säkerhetsuppdatering som ersätter den befintliga krypteringsmekanismen med ett annat protokoll som kräver användning av en extern nyckelhanteringstjänst som drivs av en tredje part. Till följd av denna förändring ändras beroendena och dataflödena i produkten med digitala element väsentligt, så att nya externa gränssnitt införs jämte ett beroende av tredjepartstjänster som inte beaktades i riskbedömningen. Även om uppdateringen är säkerhetsdriven introducerar den nya cybersäkerhetsrisker, och kan därför betraktas som en väsentlig ändring.

110. Såsom anges i punkt 104 ovan bör bedömningen av huruvida en programvaruuppdatering utgör en väsentlig ändring göras från fall till fall. Vid utförandet av denna bedömning kan tillverkarna, på ett icke uttömmande sätt, överväga om programvaruuppdateringen

a) inför nya hotvektorer, såsom ytterligare gränssnitt, kommunikationskanaler, exekveringsmiljöer eller externa beroenden genom vilka hot kan uppstå,

b) möjliggör nya attackscenarier, t.ex. nya sätt på vilka otillåten åtkomst, manipulation, störning eller missbruk av produkten med digitala element, eller av de data som behandlas av den, rimligen skulle kunna förekomma,

c) ändrar sannolikheten för tidigare identifierade attackscenarier, till exempel genom att minska den insats eller expertis som krävs för att utnyttja dem, öka exponeringen för icke-betrodda aktörer eller försvaga de befintliga skyddsåtgärderna,

d) ändrar den potentiella effekten av tidigare identifierade attackscenarier, t.ex. omfattningen av berörda data eller funktioner, de operativa, säkerhetsmässiga eller ekonomiska konsekvensernas svårighetsgrad, eller förmågan att upptäcka, begränsa eller återhämta sig från en incident.

111. I vissa fall introducerar en programuppdatering inte några nya hotvektorer, möjliggör inte några nya attackscenarier och ändrar inte i någon större utsträckning sannolikheten för eller effekten av tidigare identifierade attackscenarier. Detta kan tyda på att uppdateringen inte introducerar några nya eller ökade cybersäkerhetsrisker, under förutsättning att de antaganden och begränsningsåtgärder som riskbedömningen bygger på förblir giltiga och effektiva. Det är därför troligt att uppdateringen inte kan betraktas som en väsentlig ändring.

112. Omvänt kan en programuppdatering introducera nya hotvektorer, möjliggöra nya attackscenarier eller väsentligt ändra sannolikheten för eller effekten av befintliga attackscenarier. I sådana fall bör tillverkaren åter bedöma cybersäkerhetsriskerna för produkten med digitala element och avgöra om de väsentliga kraven fortfarande uppfylls, inbegripet om uppdateringen medför nya eller ökade risker som inte förutsågs i riskbedömningen.

113. Huruvida en programvaruuppdatering kan betraktas som en väsentlig ändring är relevant för att fastställa om vissa skyldigheter enligt cyberresiliensförordningen är tillämpliga, enligt vad som anges i punkt 91. Oavsett om ändringarna betraktas som väsentliga förblir tillverkarna dock ansvariga för att säkerställa säkerheten för programvaruuppdateringar och för deras produkt med digitala element under stödperioden, i enlighet med de krav på sårbarhetshantering som anges i del II i bilaga I till cyberresiliensförordningen. Oavsett om programvaruuppdateringar betraktas som väsentliga ändringar eller inte måste tillverkarna dessutom se till att riskbedömningen och den tekniska dokumentationen fortsatt är korrekta, fullständiga och kontinuerligt uppdaterade i enlighet med artiklarna 13.7 och 31.2.

4.4 **Följderna av en väsentlig ändring**

114. Följderna av en väsentlig ändring som utförs av en annan aktör än den ursprungliga tillverkaren av en produkt med digitala element som redan släppts ut på marknaden tas upp i artiklarna 21 och 22 i cyberresiliensförordningen. Artikel 21 handlar om importörer och distributörer, medan artikel 22 handlar om varje annan fysisk eller juridisk person än tillverkaren, importören eller distributören.

115. Om den väsentliga ändringen utförs av den ursprungliga tillverkaren av produkten med digitala element härrör följderna från det allmänt fastställda begreppet väsentlig ändring som avses i skäl 41 i cyberresiliensförordningen och beskrivs närmare i avsnitt 2.1 i blåboken. I det avsnittet anges att en produkt som har genomgått betydande förändringar eller en omarbetning efter utsläppandet på marknaden ska betraktas som en ny produkt om dess ursprungliga prestanda, syfte eller typ har modifierats, farans art har ändrats eller risknivån har höjts och produkten med digitala element görs tillgänglig på marknaden.

116. Den allmänt fastställda följden är därför att om en modifiering av en produkt med digitala element betraktas som en väsentlig ändring och den modifierade produkten med digitala element tillhandahålls på marknaden, ska den betraktas som en ny produkt med digitala element enligt cyberresiliensförordningen. Tillhandahållandet av den väsentligt ändrade produkten på marknaden utgör således ett nytt utsläppande på marknaden. Detta gäller oavsett om den väsentliga ändringen utförs av den ursprungliga tillverkaren eller av en annan person. För att säkerställa att cyberresiliensförordningen tillämpas på ett enhetligt och proportionerligt sätt för de olika kategorierna av aktörer som kan genomföra en väsentlig ändring, tar följande underavsnitt upp de därav följande skyldigheterna för den person som utför den väsentliga ändringen när den väsentligt ändrade produkten med digitala element släpps ut på marknaden. Följderna för stödperioden för produkten med digitala element tas upp i avsnitt *5 Stödperiod*.

4.4.1 *Väsentliga ändringar utförda av en annan person än den ursprungliga tillverkaren*

117. I enlighet med artiklarna 21 och 22 ska, om en väsentlig ändring av en produkt med digitala element som redan släppts ut på marknaden utförs av en annan fysisk eller juridisk person än tillverkaren av produkten med digitala element, den person som utför den väsentliga ändringen och gör den modifierade produkten med digitala element tillgänglig på marknaden betraktas som tillverkare av den modifierade produkten med digitala element, oavsett om den personen deltog i produktens ursprungliga utformning eller ursprungliga utsläppande på marknaden.

118. I artikel 22 klargörs vidare att den person som utför modifieringen endast omfattas av de skyldigheter som fastställs i artiklarna 13 och 14 när det gäller den del av produkten med digitala element som påverkas av den väsentliga ändringen, om ändringen inte påverkar cybersäkerheten hos produkten med digitala element som helhet.

119. Om en väsentlig ändring påverkar uppfyllandet av de väsentliga kraven men inte negativt påverkar cybersäkerheten hos produkten med digitala element som helhet, omfattas den person som utför modifieringen av artiklarna 13 (inklusive skyldigheten att säkerställa uppfyllandet av de väsentliga kraven och att genomföra ett förfarande för bedömning av överensstämmelse) och 14 (rapporteringsskyldigheter) endast med avseende på den del av produkten med digitala element som har ändrats väsentligt ([16]). Dessutom fortsätter den ursprungliga tillverkarens skyldigheter enligt cyberresiliensförordningen att gälla för den ursprungliga produkten med digitala element som släppts ut på marknaden, något som säkerställer kontinuiteten i sårbarhetshanteringen och överensstämmelsen för de oförändrade delarna.

120. Väsentliga ändringar bör inte förväxlas med integrering, där en person monterar komponenter (inbegripet, i förekommande fall, genom att modifiera dem) så att de bildar en ny produkt med digitala element som denne själv släpper ut på marknaden. I sådana fall ändrar inte integreraren en produkt med digitala element som redan släppts ut på marknaden av en annan tillverkare utan släpper snarare ut en egen ny produkt med digitala element på marknaden. Integreraren är tillverkare av den nya produkten med digitala element enligt cyberresiliensförordningen och måste följa förordningen i sin helhet när det gäller produkten med digitala element som helhet. Om tillverkaren integrerar komponenter som omfattas av cyberresiliensförordningen får tillverkaren förlita sig på de överensstämmelseåtgärder som vidtagits av komponenternas tillverkare för att främja sin egen efterlevnad av cyberresiliensförordningen.

Exempel 51: Ett företag köper standardiserade mikrokontrollermoduler och konnektivitetskomponenter från tredjepartsleverantörer, utvecklar sin egen fasta programvara och ett sensorpaket och monterar dessa i en ansluten jordbruksövervakningsprodukt med digitala element som det släpper ut på marknaden under sitt eget namn. Även om företaget har modifierat de underliggande mikrokontrollermodulerna och kombinerat dem med andra komponenter ändrar det inte väsentligt en produkt med digitala element som redan har släppts ut på marknaden – företaget släpper snarare ut en ny produkt med digitala element på marknaden. Enligt cyberresiliensförordningen betraktas företaget som tillverkare av jordbruksövervakningsenheten och är skyldigt att följa förordningen med avseende på jordbruksövervakningsenheten som helhet.

([16]) I enlighet med avsnitt 2.1 i blåboken är det ”inte nödvändigt att upprepa provningar och ta fram ny dokumentation om aspekter som inte påverkas av ändringen. Det är den fysiska eller juridiska person som utför eller låter utföra ändringarna av produkten som ska visa att det inte är nödvändigt att uppdatera alla delar i den tekniska dokumentationen. Den fysiska eller juridiska person som utför eller låter utföra ändringarna av produkten har ansvaret för den ändrade produktens överensstämmelse och för att utarbeta en försäkran om överensstämmelse, även om befintliga provningar och teknisk dokumentation används”.

121. Om en väsentlig ändring som utförs av en annan person än den ursprungliga tillverkaren inverkar negativt på cybersäkerheten hos produkten med digitala element som helhet, till exempel på grund av att modifieringen inte längre är inriktad på eller begränsad till en viss komponent eller ett visst delsystem, bör den modifierade produkten med digitala element som tillhandahålls på marknaden betraktas som en ny produkt med digitala element som omfattas av cyberresiliensförordningen i sin helhet. I sådana fall har produktens övergripande cybersäkerhetsriskprofil ändrats, och modifieringen kan inte bedömas utan att beakta produkten med digitala element i sin helhet. Den person som utför ändringen omfattas av en tillverkares skyldigheter enligt artiklarna 13 och 14 med avseende på den modifierade produkten med digitala element som helhet.

4.4.2 *Väsentliga ändringar utförda av den ursprungliga tillverkaren*

122. Om den väsentliga ändringen utförs av den ursprungliga tillverkaren, inbegripet i samband med iterativ utveckling av programvaruprodukter med digitala element, betraktas denne fortsatt som tillverkare enligt cyberresiliensförordningen. Den väsentligt modifierade produkten med digitala element ska dock anses vara nyutsläppt på marknaden.

123. I enlighet med avsnitt 2.1 i blåboken får den ursprungliga tillverkare som släpper ut den väsentligt ändrade produkten med digitala element på marknaden återanvända befintlig dokumentation och befintliga provningar för de aspekter av produkten med digitala element som inte påverkas av den väsentliga ändringen. Närmare bestämt bör förfarandet för bedömning av överensstämmelse inriktas på de väsentligt ändrade delarna av produkten med digitala element när tillverkaren släpper ut väsentligt ändrade versioner av samma produkt med digitala element på marknaden. Om en tredjepartsbedömning av överensstämmelse utförs bör organet för bedömning av överensstämmelse likaledes inrikta sin bedömning på de väsentligt ändrade delarna. För oförändrade delar av produkten med digitala element får tillverkaren återanvända befintlig dokumentation och befintliga provningsresultat.

124. De proportionalitetsöverväganden som anges i föregående underavsnitt gäller i lika hög grad för väsentliga ändringar som utförs av den ursprungliga tillverkaren av en produkt med digitala element som släpps ut på marknaden före den 11 december 2027. En sådan väsentlig ändring som utförs av den ursprungliga tillverkaren innebär inte i sig att tillverkaren måste se till att hela produkten med digitala element som släppts ut på marknaden före det datumet till fullo överensstämmer med cyberresiliensförordningen, såvida inte ändringen negativt påverkar cybersäkerheten hos produkten med digitala element som helhet. Om ändringen inte påverkar cybersäkerheten hos produkten med digitala element som helhet bör den ursprungliga tillverkarens skyldigheter med avseende på ändringen begränsas till de väsentligt ändrade delarna.

5. **STÖDPERIOD**

125. Enligt artikel 13.8 i cyberresiliensförordningen ska tillverkarna fastställa den stödperiod under vilken sårbarheterna hos produkten med digitala element, inklusive dess komponenter, hanteras effektivt och i enlighet med de grundläggande krav som anges i del II i bilaga I. Stödperioden avspeglar den tidsperiod under vilken produkten med digitala element förväntas vara i bruk (den förväntade användningstiden) och bör fastställas mot bakgrund av kriterierna i artikel 13.8, i synnerhet rimliga användarförväntningar, arten av produkt med digitala element, inbegripet dess avsedda ändamål, samt den relevanta unionslagstiftning som fastställer livslängden för produkter med digitala element ([17]). På det hela taget ska sådana kriterier beaktas på ett sätt som säkerställer proportionaliteten vid fastställandet av stödperioden.

([17]) Ytterligare kriterier som kan beaktas i enlighet med artikel 13.8 inbegriper stödperioderna för produkter med digitala element som erbjuder en liknande funktion och som släpps ut på marknaden av andra tillverkare, tillgången till driftsmiljön, stödperioderna för de integrerade komponenter som tillhandahåller kärnfunktioner och som kommer från tredje part samt relevant vägledning från cyberresiliensförordningens särskilda administrativa samarbetsgrupp (Adco-gruppen) och kommissionen.

126. Enligt artikel 13.8 ska stödperioden dessutom vara minst fem år, såvida inte produkten med digitala element förväntas vara i bruk i mindre än fem år, i vilket fall stödperioden ska motsvara den förväntade användningstiden. Den minsta stödperioden fungerar därför enbart som ett skydd som säkerställer att sårbarheter hanteras under en tillräckligt lång period, samtidigt som tillverkarna kan ta hänsyn till produkter med digitala element med genuint kortare förväntade användningstider. I skäl 60 ges mer vägledning i detta avseende, och det klargörs där att produkter med digitala element som rimligen förväntas vara i bruk längre än fem år därför bör ha längre stödperioder. En stödperiod på fem år ska därför inte betraktas som standard för alla produkter med digitala element. I stället bör tillverkaren fastställa en lämplig stödperiod mot bakgrund av de kriterier som avses i artikel 13.8.

127. Enligt artikel 13.19 ska tillverkarna vid tidpunkten för köpet ange stödperiodens slutdatum på ett tydligt och begripligt sätt (åtminstone månad och år). Denna artikel kräver också att tillverkarna visar ett meddelande till användarna när stödperioden har löpt ut, om så är tekniskt möjligt mot bakgrund av arten av produkt med digitala element. Denna skyldighet är avsedd att ge användarna insyn i hur länge de kan förvänta sig få säkerhetsstöd.

128. När det gäller programvaruprodukter med digitala element, som ofta utvecklas och släpps ut iterativt och där väsentligt ändrade versioner kan släppas ut på marknaden med korta mellanrum över tid, måste stödperioden förstås mot bakgrund av denna utvecklingsmodell. Varje väsentligt ändrade version av en programvaruprodukt med digitala element som släpps ut på marknaden måste ha en angiven stödperiod som stämmer överens med artikel 13.8. Detta inbegriper en minsta stödperiod på åtminstone fem år, såvida inte den förväntade användningstiden för den versionen bevisligen är kortare, vilket också klargörs i skäl 60. I avsnitt *5.1 Väsentliga ändringar och stödperioden* förtydligas vidare att om den väsentliga ändringen inte leder till ändringar av de faktorer som ursprungligen fastställde den förväntade användningstiden för produkten med digitala element påverkas inte den ursprungliga stödperioden (dvs. inklusive i fall där den återstående stödperioden är kortare än fem år).

129. Artikel 13.10 ger programvaruprodukter med digitala element flexibilitet genom att under vissa omständigheter tillåta tillverkarna att säkerställa uppfyllandet av kravet på sårbarhetshantering i del II punkt 2 i bilaga I (att åtgärda och avhjälpa sårbarheter) endast för den version av programvaruprodukten med digitala element som senast släpptes ut på marknaden. Detta är tillåtet om användarna av tidigare versioner som släppts ut på marknaden har tillgång till den version som senast släpptes ut på marknaden kostnadsfritt och inte ådrar sig ytterligare kostnader för att anpassa den hårdvaru- och programvarumiljö där de använder den ursprungliga versionen av produkten.

130. Vid tillämpning av artikel 13.10 bör begreppet ”ytterligare kostnader” tolkas på ett praktiskt och proportionellt sätt, med beaktande av normal och förväntad praxis för underhåll och drift av programvara. Det inbegriper inte de rimliga driftsansträngningar som ingår i genomförandet av programuppdateringar eller upprätthållandet av en säker driftsmiljö, såsom arbetstid, rutintestning, konfigurationsjusteringar eller uppgraderingar av underliggande programvaruberoenden som är nödvändiga för att åtgärda uttjänta komponenter eller kända säkerhetsproblem. Med ”ytterligare kostnader” avses däremot bördor som går utöver vad som normalt kan förväntas i samband med programvaruuppdateringar, såsom nödvändiga inköp av ny maskinvara, utbyte av infrastruktur eller grundläggande förändringar av driftsmiljön.

131. För programvaruprodukter med digitala element som ständigt utvecklas kan tillverkarna på marknaden släppa ut flera på varandra följande väsentligt ändrade versioner under relativt korta tidsintervall och förvänta sig att användarna regelbundet uppgraderar. I sådana fall måste den angivna stödperioden för varje väsentligt ändrade version uppfylla kraven i artikel 13.8 vid den tidpunkt då den släpps ut på marknaden. Med andra ord måste tillverkaren ange en ny stödperiod för den väsentligt ändrade versionen. Tillverkarna får dock stödja sig på artikel 13.10 för att upphöra med att åtgärda och avhjälpa sårbarheter för tidigare versioner när användarna väl

har haft möjlighet att kostnadsfritt uppgradera till en senare version enligt ovan, även om detta leder till en kortare effektiv stödperiod för dessa tidigare versioner ([18]). Tillverkaren fortsätter att omfattas av de andra sårbarhetshanteringskraven i del II i bilaga I, samt av rapporteringsskyldigheterna enligt artikel 14. Såsom också förklaras i skäl 40 omfattar dessa krav bland annat, för alla efterföljande väsentligt ändrade versioner av programvaruprodukten med digitala element som släpps ut på marknaden, i) upprätthållandet av en policy för samordnad delgivning av information om sårbarhet, och ii) åtgärder för att underlätta utbyte av information om potentiella sårbarheter ([19]).

Exempel 52: En tillverkare släpper ut en smarttelefonmodell på EU-marknaden och anger en stödperiod på X år från och med dagen för utsläppandet på marknaden, under vilken tillverkaren kommer att tillhandahålla säkerhetsuppdateringar för åtgärdande av sårbarheter. Under den perioden släpper tillverkaren regelbundna programuppdateringar och väsentligt ändrade versioner av operativsystemet, som användarna kan installera kostnadsfritt utan att behöva någon ny hårdvara.

Tillverkaren får i enlighet med artikel 13.10 åtgärda och avhjälpa sårbarheter för den senaste version av operativsystemet som gjorts tillgänglig för den smarttelefonmodellen, under förutsättning att tidigare versioner kan uppgraderas kostnadsfritt och utan ytterligare kostnad. Under loppet av stödperioden omfattas tillverkaren fortfarande av andra sårbarhetshanteringskrav, såsom samordnad delgivning av information om sårbarhet och åtgärder för informationsutbyte.

Exempel 53: En tillverkare släpper ut en programvaruprodukt med digitala element på marknaden och ger ut väsentligt ändrade versioner med några månaders mellanrum, vilka avspeglar säkerhetsförbättringar, nya funktioner och kompatibilitet med uppdaterade operativsystem och plattformar. Varje version släpps ut på marknaden med en angiven stödperiod i enlighet med artikel 13.8. Tillverkaren förväntar sig att användarna gör regelbundna uppgraderingar som en del av den normala driften och ger tillgång till den senaste versionen kostnadsfritt. Att genomföra uppgraderingar kan medföra vissa operativa insatser, t.ex. provning eller justeringar av konfigurationen, men medför inga ytterligare kostnader, såsom inköp av ny hårdvara eller grundläggande infrastrukturförändringar. I detta sammanhang kan tillverkaren med stöd av artikel 13.10 sluta att åtgärda och avhjälpa sårbarheter för tidigare versioner när användarna kan uppgradera till den senaste versionen, samtidigt som denne fortsätter att uppfylla övriga krav avseende sårbarhetshantering för alla efterföljande väsentligt ändrade versioner.

5.1 **Väsentliga ändringar och stödperioden**

132. Såsom anges i avsnitt 4.4 *Följderna av en väsentlig ändring* ska en produkt med digitala element, om en modifiering av denna betraktas som en väsentlig ändring och den modifierade produkten med digitala element tillhandahålls på marknaden, betraktas som en ny produkt enligt cyberresiliensförordningen, och tillgängliggörandet av den väsentligt ändrade produkten med digitala element på marknaden utgör ett nytt utsläppande på marknaden. Det är därför lämpligt att klargöra vilken effekt detta nya utsläppande på marknaden har på stödperioden för den väsentligt ändrade produkten med digitala element.

133. Stödperioden för en väsentligt ändrad produkt med digitala element bör fastställas på grundval av produktens förväntade användningstid, mot bakgrund av kriterierna i artikel 13.8 i cyberresiliensförordningen. En väsentlig ändring bör därför kräva en ny bedömning gentemot dessa kriterier, men leder inte automatiskt till att stödperioden återställs eller ens förlängs. Den relevanta frågan är huruvida den väsentliga ändringen påverkar de faktorer som ursprungligen fastställde produktens förväntade användningstid och därmed den ursprungliga stödperioden.

([18]) Man bör komma ihåg att artikel 13.19 kräver att tillverkarna, när så är tekniskt möjligt mot bakgrund av arten av produkten med digitala element, visar ett meddelande till användarna om att deras produkt med digitala element har nått slutet av sin stödperiod. Därför förväntas användare som inte har uppgraderat till den senaste versionen informeras, om så är tekniskt möjligt, när åtgärdandet och avhjälpandet av sårbarheter för tidigare versioner upphör.

([19]) Det bör noteras att även om användarna kan uppgradera till den senaste versionen av programvaran utan extra kostnader kan tillverkarna ändå välja att fortsätta åtgärda och avhjälpa sårbarheter i tidigare versioner av programvaran, däribland på betald basis eller inom ramen för andra kommersiella arrangemang. Cyberresiliensförordningen kräver inte att tillverkarna tillhandahåller säkerhetsuppdateringar för sådana tidigare versioner utan kostnad.

134. Om den väsentliga ändringen inte påverkar dessa faktorer fortsätter de kriterier som anges i artikel 13.8 att tyda på samma förväntade användningstid som ursprungligen fastställdes, och stödperioden för den modifierade produkten med digitala element bör anpassas till den återstående förväntade användningstiden för den produkt som ursprungligen släpptes ut på marknaden. Detta är vanligtvis fallet om den förväntade användningstiden främst bestämdes av faktorer som inte ändras på grund av ändringen, t.ex. hårdvarukomponenternas fysiska hållbarhet om den väsentliga ändringen endast gäller programvarufunktioner eller backend-tjänster.

Exempel 54: En tillverkare släpper ut en robotdammsugare på marknaden med en förväntad användningstid på X år, fastställd på grundval av arten av produkt med digitala element, däribland hårdvarukomponenternas fysiska hållbarhet och egenskaper rörande slitage, och med beaktande av rimliga användarförväntningar rörande produktens livslängd. Tillverkaren anger en stödperiod på X år. Efter Y år släpper tillverkaren en programvaruuppdatering som räknas som en väsentlig ändring, vilken lägger till nya rengöringslägen och navigeringsfunktioner. Programuppdateringen påverkar inte hårdvarans fysiska hållbarhet och ändrar inte de rimliga användarförväntningarna på produktens livslängd. Kriterierna i artikel 13.8 fortsätter därför att tyda på samma förväntade användningstid. Stödperioden för den modifierade produkten med digitala element överensstämmer med den återstående förväntade användningstiden enligt vad som ursprungligen fastställdes.

Exempel 55: En tillverkare släpper ut en komplex industrimaskinprodukt med digitala element på marknaden, med ett molnbaserat backend-system som utgör en lösning för fjärrbehandling av data. Den förväntade användningstiden är X år, fastställd mot bakgrund av rimliga användarförväntningar och arten av produkt med digitala element, såsom maskinhårdvarans fysiska hållbarhet och förväntade slitage. Stödperioden ska anpassas till den förväntade användningstiden på X år. Efter Y år omskapar tillverkaren det molnbaserade backend-systemet (lösningen för fjärrdatabehandling) och introducerar då nya applikationsprogrammeringsgränssnitt (API) och dataflöden på ett sätt som räknas som en väsentlig ändring av produkten med digitala element men som inte ändrar arten av produkt eller påverkar användarnas förväntningar. Kriterierna i artikel 13.8 fortsätter därför att tyda på samma förväntade användningstid. Stödperioden för den modifierade produkten med digitala element överensstämmer med den återstående förväntade användningstiden enligt vad som ursprungligen fastställdes.

135. Om den väsentliga ändringen påverkar de faktorer som ursprungligen fastställde den förväntade användningstiden för produkten med digitala element, bör tillverkaren på nytt beräkna stödperioden för att återspegla den nya förväntade användningstiden, och då tillämpa kriterierna i artikel 13.8 i enlighet med detta. Detta kan t.ex. vara fallet med vitaliserande hårdvarumodifieringar som förlänger produktens driftsmässiga livslängd, eller med en betydande omprogrammering eller omskrivning av produktens kärnprogramvara som väsentligen ändrar dess förväntade användningstid ([20]).

Exempel 56: En tillverkare släpper ut en programmerbar styrlogikenhet (PLC) på marknaden med en förväntad användningstid på X år, vilken främst bestäms på grundval av arten av produkt med digitala element och hållbarheten hos den underliggande hårdvaran. Stödperioden fastställs i enlighet med detta. Flera år efter det att produkten först släpptes ut på marknaden genomför tillverkaren en väsentlig ändring som består i en ersättning av den programmerbara styrlogikenhetens inbyggda datorplattform, inbegripet processorn, minnet och exekveringsmiljön, med en ny generation komponenter som är utformade för en betydligt längre driftsmässig livstid. Till följd av modifieringen förändras de rimliga användarförväntningarna och arten av produkt med digitala element: användaren av den programmerbara styrlogikenheten kan nu rimligen förvänta sig att den programmerbara styrlogikenheten förblir i produktiv användning efter den ursprungligen angivna förväntade användningstiden, med stöd av den nya datorplattformen. Kriterierna i artikel 13.8 tyder därför på en längre förväntad användningstid, och tillverkaren beräknar stödperioden på nytt för den specifika programmerbara styrlogikenheten i enlighet med detta.

6. **VIKTIGA OCH KRITISKA PRODUKTER MED DIGITALA ELEMENT**

136. I artikel 7.1 i cyberresiliensförordningen fastställs att produkter med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga III till den förordningen anses vara ”viktiga produkter med digitala element”. I bilaga III delas viktiga produkter med digitala element upp ytterligare i klass I och klass II. På samma sätt fastställs i artikel 8.1 att produkter med digitala element som har kärnfunktionen hos en produktkategori som anges i bilaga IV till cyberresiliensförordningen anses vara ”kritiska produkter med digitala element” ([21]).

([20]) Man bör komma ihåg att renoverings-, underhålls- eller reparationsverksamhet i allmänhet inte anses utgöra väsentliga ändringar, såsom anges i avsnitt 4.1 *Physical repairs*.

([21]) I kommissionens genomförandeförordning (EU) 2025/2392 fastställs den tekniska beskrivningen av kategorierna viktiga och kritiska produkter.

137. Klassificeringen av en produkt med digitala element som viktig eller kritisk eller som tvärtom tillhörande ”standard”-kategorin ([22]) är relevant vid fastställandet av det förfarande för bedömning av överensstämmelse som tillverkaren måste följa, i enlighet med artikel 32, innan denne kan släppa ut den produkten med digitala element på marknaden. I synnerhet kan produkter med digitala element i standardkategorin alltid förlita sig på förfarandet för intern kontroll baserat på modul A (”självbedömning”) ([23]). Viktiga produkter med digitala element av klass I eller II och kritiska produkter med digitala element omfattas av strängare förfaranden för bedömning av överensstämmelse. Detta omfattar inte viktiga produkter med digitala element av klass I eller II som betraktas som programvara med fri och öppen källkod som släpps ut på marknaden, för vilka tillverkarna i enlighet med artikel 32.5 får följa förfarandena för standardkategorin.

138. Begreppet *kärnfunktion* är därför viktigt för att tillverkaren ska kunna fastställa det tillämpliga systemet för bedömning av överensstämmelse. Detta begrepp definieras dock inte uttryckligen i cyberresiliensförordningen. Produkter med digitala element kan utföra en rad olika funktioner, varav vissa kan komplettera den produktens kärnfunktioner, och bör inte påverka produktens klassificering som standard/viktig av klass I/viktig av klass II/kritisk. Det är därför lämpligt att tillhandahålla mer vägledning för att hjälpa tillverkare att utföra de relevanta förfarandena för bedömning av överensstämmelse på ett korrekt sätt, och för att hjälpa marknadskontrollmyndigheterna att säkerställa en harmoniserad verkställighet av cyberresiliensförordningen i hela EU.

6.1 **Vad är en kärnfunktion?**

139. Kärnfunktionen hos en produkt med digitala element avser produktens viktigaste funktioner och tekniska kapacitet som produkten inte fungerar utan. Detta kan bedömas mot bakgrund av produktens specifika sammanhang och användningförhållanden, med beaktande bland annat av den information som tillverkaren tillhandahåller i instruktionerna till användaren, reklam- eller försäljningsmaterial och uttalanden samt i den tekniska dokumentationen.

Exempel 57: En programvaruprodukt med digitala element tillhandahåller ett abstraktionslager för den underliggande hårdvaran och styr körning av programvarukomponenter. Dess huvudfunktioner inbegriper initialisering av hårdvara och kringutrustning, process- och minneshantering, input-outputkontroll, schemaläggning, resursfördelning och exponering av systemtjänster och applikationsprogrammeringsgränssnitt (API) genom vilka applikationer interagerar med enhetens hårdvaru- och programvaruresurser. Den tekniska dokumentationen visar att produkten med digitala element orkestrerar datorresurser, verkställer systemkonfigurationer och tillhandahåller standardiserade gränssnitt för programvarumoduler och ansluten kringutrustning. Tillverkaren betonar att dessa funktioner gör det möjligt för plattformen att fungera som en central programvarumiljö där applikationer kan köras på ett tillförlitligt sätt. Produkten med digitala element har kärnfunktionen hos ett operativsystem, såsom beskrivs i punkt 11 i bilaga I till genomförandeförordning (EU) 2025/2392.

140. Funktionen hos en produkt med digitala element begränsas sällan uteslutande till dess kärnfunktion, eftersom produkter med digitala element ofta – om inte alltid – utför ytterligare funktioner som inte bidrar till produktens kärnfunktion. Detta kan även inbegripa att införliva komponenter som i sig har samma funktion som en annan viktig eller kritisk produkt med digitala element. Det faktum att en produkt med digitala element utför andra funktioner än eller utöver dem som beskrivs i de tekniska beskrivningarna av viktiga eller kritiska produkter med digitala element hindrar dock inte i sig produkten från att ha en sådan kärnfunktion.

([22]) Termen *standardkategori* är inte en term som definieras i cyberresiliensförordningen. Användningen av termen i detta dokument avser produkter med digitala element som inte har kärnfunktionerna hos en produktkategori som anges i bilagorna III eller IV till cyberresiliensförordningen och som följaktligen omfattas av det system för bedömning av överensstämmelse som anges i artikel 32.1.

([23]) Tillverkaren kan dock alltid välja att tillämpa ett strängare förfarande för bedömning av överensstämmelse i enlighet med artikel 32.1.

Figur 2

Illustration av hur kärnfunktionen, och inte de kompletterande funktionerna, fastställer det tillämpliga förfarandet för bedömning av överensstämmelse



141. En produkt med digitala element kan ha förmågan att utföra funktionerna hos en viktig eller kritisk produktkategori, men ändå ha en annan kärnfunktion än denna produktkategori. I sådana fall skulle den produkten med digitala element inte betraktas som en viktig eller kritisk produkt med digitala element. Såsom uttryckligen anges i artikel 7.1 i cyberresiliensförordningen för viktiga produkter med digitala element (och med tillämpning av samma logik för kritiska produkter med digitala element), innebär enbart integreringen av en viktig eller kritisk produkt med digitala element inte i sig att produkten med digitala element blir en viktig eller kritisk produkt med digitala element.

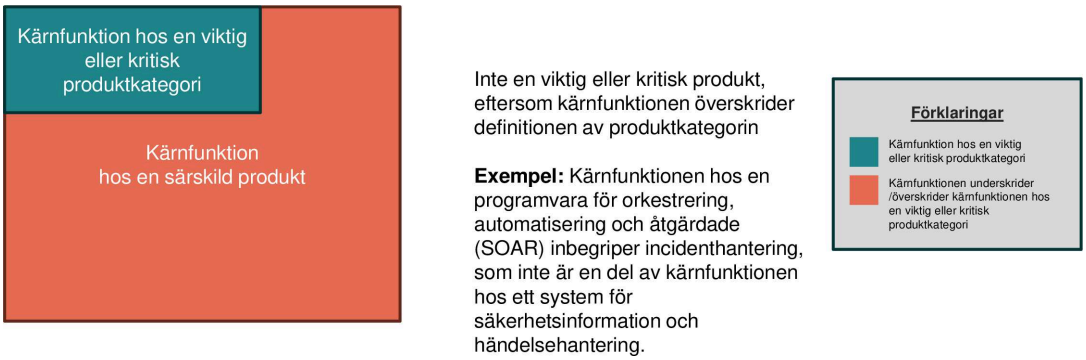
Exempel 58: En smarttelefon integrerar ett operativsystem som tillhandahåller de funktioner som beskrivs i punkt 11 i bilaga I till genomförandeförordning (EU) 2025/2392. Även om operativsystemet gör det möjligt att hantera hårdvaruresurser och köra programvaruapplikationer har smarttelefonen som helhet en annan kärnfunktion (t.ex. att göra det möjligt för användare att kommunicera och få tillgång till information och tjänster). Enbart integreringen av ett operativsystem innebär inte att smarttelefonen har ett operativsystems kärnfunktion.

142. Vissa produkter med digitala element kan likna en viktig eller kritisk produktkategori eller tillhöra samma allmänna produktfamilj, men deras kärnfunktion kan betydligt överstiga eller betydligt understiga kärnfunktionen hos den kategorin. Detta är inte fallet om en produkt med digitala element innehåller ytterligare funktioner som endast kompletterar eller förbättrar kärnfunktionen, vilken i sig motsvarar kärnfunktionen hos en viktig eller kritisk produktkategori – i sådana fall behåller produkten med digitala element den kategorins kärnfunktion och klassificeras i enlighet med detta. Denna bedömning bör grunda sig på produktens huvudsakliga funktioner och tekniska kapacitet, objektivt betraktade mot bakgrund av dess avsedda syfte, och inte på det sätt på vilket produkten med digitala element beskrivs eller marknadsförs, i de fall den beskrivningen inte avspeglar produktens faktiska tekniska egenskaper.

Exempel 59: En programvara för orkestrering, automatisering och åtgärdande (SOAR) har ofta kapacitet att utföra funktionerna hos produkter med digitala element i kategorin ”system för säkerhetsinformation och händelsehantering (SIEM)”, dvs. att samla in, analysera och korrelera data från flera olika källor och presentera dem som handlingsbar information för säkerhetsändamål. Programvarans kärnfunktion är dock betydligt mer omfattande än kärnfunktionen hos ett system för säkerhetsinformation och händelsehantering, och inbegriper tjänster såsom incidenthantering som kärnelement hos dess tekniska kapacitet. Därför anses programvara för orkestrering, automatisering och åtgärdande i allmänhet inte ha samma kärnfunktion som ett system för säkerhetsinformation och händelsehantering.

Figur 3

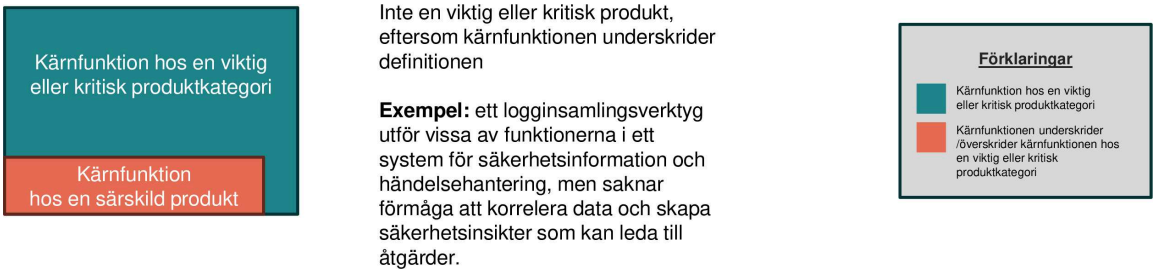
Illustration av kärnfunktionen hos en produkt med digitala element som betydligt överstiger definitionen av en viktig eller kritisk produktkategori



Exempel 60: Vissa verktyg för logginsamling och visualisering kan mata in loggdata och presentera grundläggande instrumentpaneler som visar systemhändelser. Dessa verktyg kan visserligen stödja säkerhetsövervakningsaktiviteter, men deras kärnfunktion motsvarar inte kärnfunktionen hos systemen för säkerhetsinformation och händelsehantering, eftersom de inte utför några datakorrelationer och inte heller tillhandahåller några säkerhetsinsikter som kan leda till åtgärder. Därför ska sådana verktyg i allmänhet inte anses ha samma kärnfunktion som systemen för säkerhetsinformation och händelsehantering.

Figur 4

Illustration av kärnfunktionen hos en produkt med digitala element som betydligt understiger definitionen av en viktig eller kritisk produktkategori

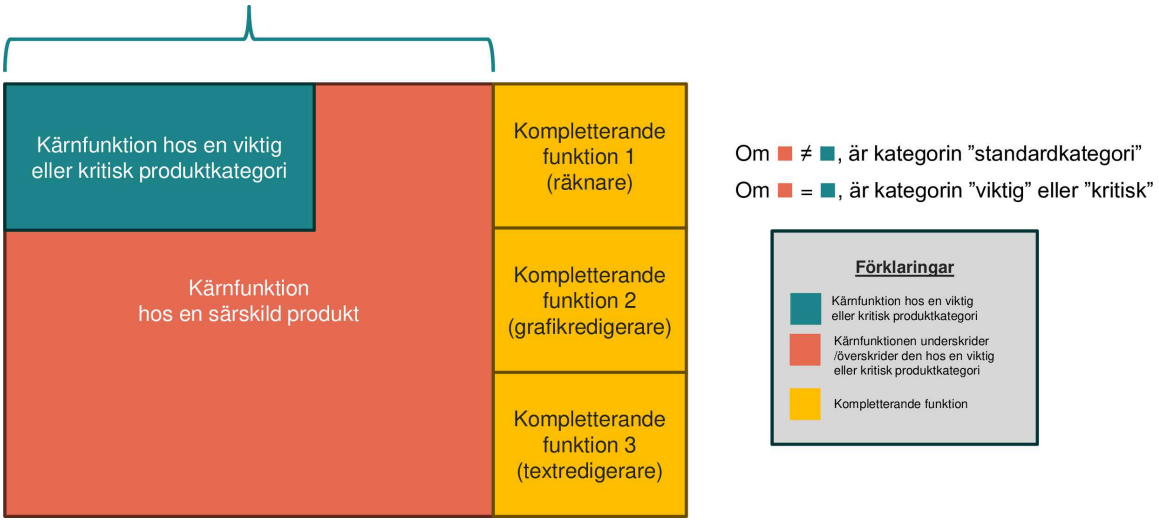


143. En tillverkare får inte ge en felaktig bild av kärnfunktionerna hos sin produkt med digitala element på ett sådant sätt att denne kan undvika det system för bedömning av överensstämmelse som är tillämpligt på viktiga eller kritiska produkter med digitala element, t.ex. genom att i alltför hög grad betona eller tona ner den roll som vissa funktioner spelar, så att produkten betydligt överskrider eller understiger en viss kärnfunktion. Detta skulle exempelvis vara fallet om det finns en tydlig oförenlighet mellan reklammaterialet, bruksanvisningarna och den tekniska dokumentationen.

144. En produkt med digitala element får inte ha mer än en kärnfunktion för fastställandet av det tillämpliga systemet för bedömning av överensstämmelse. I enlighet med bilaga VII till cyberresiliensförordningen ska tillverkarna, som en del av en produkts tekniska dokumentation, beskriva det avsedda syftet med produkten med digitala element och det förfarande för bedömning av överensstämmelse som de har följt. Produktens kärnfunktion bör därför tydligt anges. Detta gör det möjligt att korrekt identifiera det tillämpliga systemet för bedömning av överensstämmelse, och gör det möjligt för marknadskontrollmyndigheterna att övervaka och kontrollera att förordningen tillämpas korrekt.

Figur 5

Illustration av hur kärnfunktionen hos en viss produkt med digitala element avgör produktklassen och därmed det tillämpliga förfarandet för bedömning av överensstämmelse



145. Vissa produkter med digitala element släpps ut på marknaden som enskilda produkter med digitala element men består av olika moduler med separata funktioner. Om en tillverkare även tillhandahåller dessa moduler separat på marknaden, t.ex. om de erbjuds för separat inköp, licensiering eller abonnemang, utgör dessa moduler i sig fristående produkter med digitala element. De ska därför klassificeras på grundval av sin respektive kärnfunktion (och därför omfattas av ett lämpligt system för bedömning av överensstämmelse på grundval av varje moduls kärnfunktion). Detta påverkar inte de moduler som endast tillhandahålls som komponenter i en integrerad produkt med digitala element och inte görs tillgängliga separat. I sådana fall bestäms kärnfunktionen på nivån för den integrerade produkten med digitala element.

Exempel 61: En tillverkare släpper ut en enhetlig säkerhetssvit på marknaden som kombinerar flera moduler, inklusive ett system för säkerhetsinformation och händelsehantering, ett intrångsdetektionssystem och en analysmodul. Tillverkaren erbjuder också dessa moduler för separata prenumerationer. I detta scenario är varje modul en separat produkt med digitala element och klassificeras på grundval av sin egen kärnfunktion. Systemmodulen för säkerhetsinformation och händelsehantering omfattas av systemet för bedömning av överensstämmelse för viktiga produkter med digitala element som tillhör klass I eftersom dess kärnfunktion är den hos ”system för säkerhetsinformation och händelsehantering (SIEM)”. Intrångsdetektionssystemet omfattas av systemet för bedömning av överensstämmelse för viktiga produkter med digitala element som tillhör klass II eftersom dess kärnfunktion är den hos ”brandväggar, intrångsdetektions- och intrångsskyddssystem”. Analysmodulen omfattas av systemet för bedömning av överensstämmelse för ”standardprodukter” med digitala element eftersom dess kärnfunktion inte är den hos en viktig eller kritisk produktkategori.

146. Bristande efterlevnad av de skyldigheter som anges i artikel 32 i cyberresiliensförordningen kan leda till administrativa sanktionsavgifter i enlighet med artikel 64.3.

6.2 Bedömning av överensstämmelse för viktiga och kritiska produkter med digitala element

147. När tillverkaren har fastställt kärnfunktionen hos produkten med digitala element måste den utföra ett av de tillämpliga förfarandena för bedömning av överensstämmelse. Tillverkaren måste säkerställa att produkten med digitala element som helhet uppfyller de väsentliga kraven, med beaktande, i förekommande fall, av säkerheten hos de komponenter eller funktioner som är integrerade i produkten.

148. Ett strängare förfarande för bedömning av överensstämmelse, med deltagande av en tredje part (baserat på modul B +C, modul H eller ordningar för cybersäkerhetscertifiering), är obligatoriskt för viktiga produkter med digitala element av klass II (med undantag för dem som kan betraktas som programvara med fri och öppen källkod i enlighet med artikel 32.5) och för kritiska produkter med digitala element ([24]). Viktiga produkter med digitala element av klass I (med undantag för produkter som uppfyller kraven för programvara med fri och öppen källkod, i enlighet med artikel 32.5) behöver däremot endast genomgå ett tredjepartsförfarande för bedömning av överensstämmelse om tillverkaren inte har tillämpat eller endast delvis har tillämpat relevanta harmoniserade standarder som har offentliggjorts i *Europeiska unionens officiella tidning* (*harmoniserade standarder*), gemensamma specifikationer eller europeiska ordningar för cybersäkerhetscertifiering med minst assuransnivån ”väsentlig” ([25]).

149. För att en viktig produkt med digitala element av klass I ska kunna omfattas av förfarandet för intern kontroll måste därför i) alla tillämpliga krav i en relevant harmoniserad standard tillämpas, och ii) standardens tillämpningsområde måste omfatta åtminstone alla de cybersäkerhetsrisker som är förknippade med produktens kärnfunktion.

150. Omfattningen av produkten med digitala element kan vara bredare än vad som föreskrivs i den relevanta harmoniserade standarden, och sådana ytterligare funktioner kan medföra andra eller ytterligare cybersäkerhetsrisker. Tillverkaren är alltid skyldig att göra en riskbedömning i enlighet med artikel 13.2 och bör följaktligen kontrollera om tillämpningen av en harmoniserad standard omfattar alla de risker som är förknippade med produkten med digitala element. Om tillämpningen av standarden inte omfattar alla risker bör tillverkaren på andra sätt säkerställa att dennes produkt med digitala element uppfyller de väsentliga kraven.

151. Om tillverkaren av en viktig produkt med digitala element av klass I har tillämpat en relevant harmoniserad standard som omfattar de risker som är förknippade med produktens kärnfunktion, kan denne därför besluta att använda förfarandet för intern kontroll för att visa på produktens överensstämmelse. Som ett led i sin bedömning av överensstämmelse kommer tillverkaren fortfarande att behöva visa att alla de risker som är tillämpliga på dennes produkt med digitala element har åtgärdats. Om det finns ett glapp mellan den harmoniserade standardens tillämpningsområde och omfattningen av produkten med digitala element som helhet måste tillverkaren därför ändå dokumentera vilka ytterligare åtgärder denne har vidtagit för att hantera dessa risker.

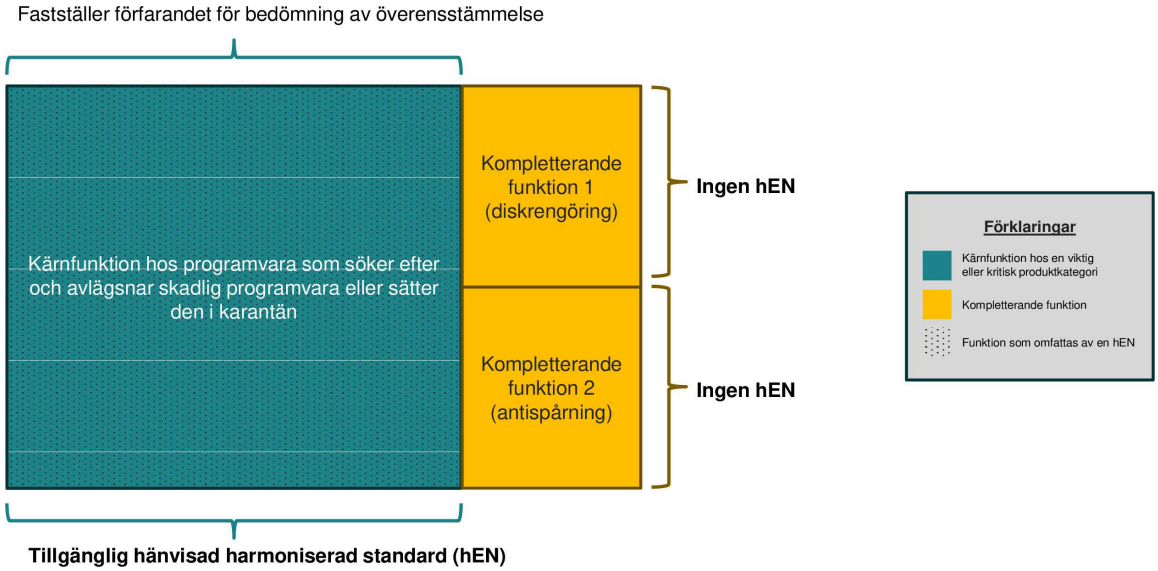
Exempel 62: Ett antivirusprogram har kärnfunktionen hos programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän enligt beskrivningen i punkt 4 i bilaga I till genomförandeförordning (EU) 2025/2392. Produkten med digitala element innehåller också ytterligare funktioner, närmare bestämt en diskrengöringsfunktion och en antispårningsfunktion som skyddar användaren när denne surfar på webben. Tillverkaren utför en riskbedömning som omfattar produkten med digitala element i sin helhet, inklusive antivirusprogrammets kärnfunktion samt diskrengörings- och antispårningsfunktionerna. Tillverkaren tillämpar en harmoniserad standard som omfattar de risker som är förknippade med antivirusprogrammets kärnfunktion och ytterligare åtgärder för att hantera de risker som härrör från de ytterligare funktionerna. Tillverkaren får använda förfarandet för intern kontroll för sin bedömning av överensstämmelse, vilket omfattar produkten med digitala element som helhet, inklusive diskrengörings- och antispårningsfunktionerna.

([24]) Detta är också fallet när man använder en europeisk ordning för cybersäkerhetscertifiering med minst assuransnivån ”väsentlig”, eftersom det finns krav på deltagande av ett tredjepartscertifieringsorgan.

([25]) För enkelhetens skull hänvisar återstoden av detta avsnitt endast till harmoniserade standarder som har offentliggjorts i *Europeiska unionens officiella tidning*. Samma vägledning gäller dock även för gemensamma specifikationer som antagits i enlighet med artikel 27.2 och för europeiska ordningar för cybersäkerhetscertifiering när så anges av kommissionen genom delegerade akter i enlighet med artikel 27.9.

Figur 6

Illustration av hur användningen av en angiven harmoniserad standard som endast omfattar kärnfunktionen avgör det tillämpliga förfarandet för bedömningen av överensstämmelse



152. Detta är också fallet om produkten med digitala element integrerar en ytterligare funktion som i sig är funktionen hos en annan viktig eller kritisk produkt med digitala element. Det är i själva verket kärnfunktionen hos produkten med digitala element som helhet, och inte de integrerade komponenternas separata funktioner, som avgör huruvida produkten med digitala element tillhör den viktiga eller kritiska produktkategorin (och därmed det tillämpliga systemet för bedömning av överensstämmelse). Om en produkt med digitala element till exempel har kärnfunktionen hos en viktig produkt med digitala element av klass I omfattas produkten som helhet av det system för bedömning av överensstämmelse som gäller för viktiga produkter med digitala element av klass I, även om den integrerar en komponent som i sig är en kritisk produkt med digitala element. I sådana fall, om tillverkaren tillämpar en harmoniserad standard som omfattar de risker som är förknippade med den produktens kärnfunktion, är det tillåtet att använda förfarandet för intern kontroll.

Exempel 63: Hårdvaruprodukten med digitala element har kärnfunktionen hos en router, såsom beskrivs i punkt 12 i bilaga I till genomförandeförordning (EU) 2025/2392. Produkten med digitala element inbegriper också ytterligare funktioner, däribland brandväggskapacitet, eftersom den integrerar en brandväggskomponent. Tillverkaren utför en riskbedömning som omfattar produkten med digitala element i sin helhet, inklusive routerns kärnfunktion och brandväggens funktion. Tillverkaren tillämpar en harmoniserad standard som omfattar de risker som är förknippade med routerns kärnfunktion och ytterligare åtgärder för att hantera de risker som härrör från de ytterligare funktionerna. Tillverkaren får till exempel tillämpa den harmoniserade standarden för brandväggar för att täcka de risker som är förknippade med brandväggens funktion. Tillverkaren får använda förfarandet för intern kontroll för sin bedömning av överensstämmelse, vilket omfattar produkten med digitala element som helhet, inklusive brandväggens funktion.

6.3 Följderna för en presumtion om överensstämmelse

153. I artikel 27.1 i cyberresiliensförordningen fastställs att produkter med digitala element och processer som införts av tillverkaren som överensstämmer med harmoniserade standarder, eller delar av sådana, vilka har offentliggjorts i *Europeiska unionens officiella tidning*, presumeras överensstämma med de väsentliga kraven i cyberresiliensförordningen som omfattas av dessa standarder eller delar av dem ([26]). I artikel 27.5 utökas denna presumtion om

([26]) Såsom tydligt anges i avsnitt 4.1.2.2 i blåboken förblir tillverkarna ”i riskrelaterad harmoniseringslagstiftning [...] alltid, även om de använder harmoniserade standarder till vilka en hänvisning offentliggjorts i *Europeiska unionens officiella tidning*, [...] fullt ansvariga för att bedöma alla risker med sina produkter så att de kan fastställa vilka väsentliga (eller andra) krav som är relevanta. När denna bedömning har gjorts kan tillverkarna välja att tillämpa tekniska specifikationer i harmoniserade standarder till vilka en hänvisning offentliggjorts i *Europeiska unionens officiella tidning* för att vidta riskbegränsande åtgärder som anges i harmoniserade standarder”.

överensstämmelse till att omfatta produkter med digitala element och processer som har införts av tillverkaren vilka överensstämmer med de gemensamma specifikationer som antagits av kommissionen genom genomförandeakter, och i artikel 27.8 fastställs presumtionen om överensstämmelse för produkter med digitala element och processer som har införts av tillverkaren för vilka en EU-försäkran om överensstämmelse eller ett certifikat har utfärdats inom ramen för en europeisk ordning för cybersäkerhetscertifiering som har antagits i enlighet med förordning (EU) 2019/881, om detta har specificerats genom delegerade akter i enlighet med artikel 27.9 ([27]).

154. Om tillverkaren har tillämpat en harmoniserad standard vars hänvisningar har offentliggjorts i EUT gynnas denne därför av en presumtion om överensstämmelse för de risker som omfattas av den standarden. Detta skulle till exempel kunna vara fallet om den offentliggjorda harmoniserade standarden hanterar alla risker som är förknippade med kärnfunktionen hos en produkt med digitala element och det inte finns några ytterligare funktioner som medför cybersäkerhetsrisker. Till exempel förväntas den harmoniserade standarden för routrar åtminstone hantera de risker som är förknippade med kärnfunktionen hos dessa produkter med digitala element. Om en sådan produkt inte innehåller några ytterligare funktioner eller om dessa ytterligare funktioner inte medför risker som inte hanteras i standarden, kan produkten med digitala element omfattas av en presumtion om överensstämmelse.

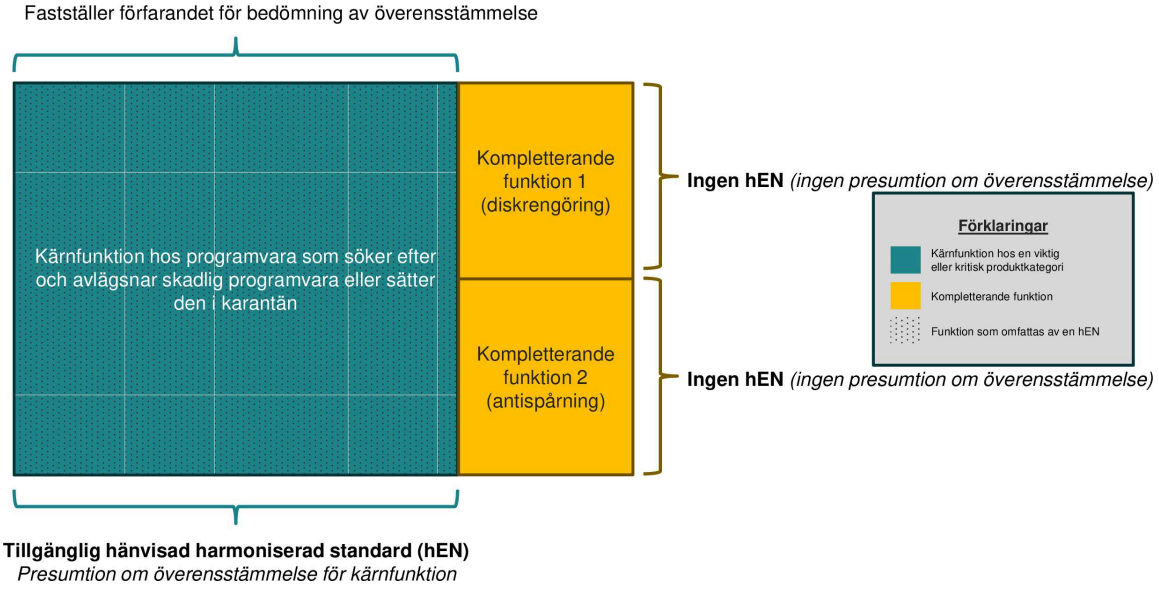
155. I de fall som diskuteras i punkterna 151 och 152 får tillverkaren använda förfarandet för intern kontroll eftersom den harmoniserade standarden täcker de risker som är förknippade med kärnfunktionen hos produkten med digitala element. De produkter med digitala element som beskrivs i dessa exempel kan dock vara mer omfattande än tillämpningsområdet för de harmoniserade standarderna, och ytterligare funktioner kan utgöra cybersäkerhetsrisker som inte tas upp i en sådan harmoniserad standard. Dessa produkter med digitala element kan därför inte komma i fråga för en presumtion om överensstämmelse för dessa ytterligare funktioner.

Exempel 64: Ett antivirusprogram har kärnfunktionen hos programvara som söker efter och avlägsnar skadlig programvara eller sätter den i karantän, och de risker som är förknippade med den kärnfunktionen omfattas av den harmoniserade standarden. Produkten med digitala element innehåller också ytterligare funktioner, närmare bestämt en diskrengöringsfunktion och en antispårningsfunktion som skyddar användaren när denne surfar på webben, vars risker inte omfattas av den harmoniserade standarden. Om den harmoniserade standarden tillämpas får tillverkaren använda förfarandet för intern kontroll för sin bedömning av överensstämmelse. Tillverkaren kommer att gynnas av presumtionen om överensstämmelse för de risker som är förknippade med produktens kärnfunktion, men inte för de risker som är förknippade med de ytterligare funktionerna.

([27]) Som angavs ovan hänvisar för enkelhetens skull återstoden av detta avsnitt endast till harmoniserade standarder som har offentliggjorts i *Europeiska unionens officiella tidning*. Samma vägledning gäller dock även för gemensamma specifikationer och europeiska ordningar för cybersäkerhetscertifiering.

Figur 7

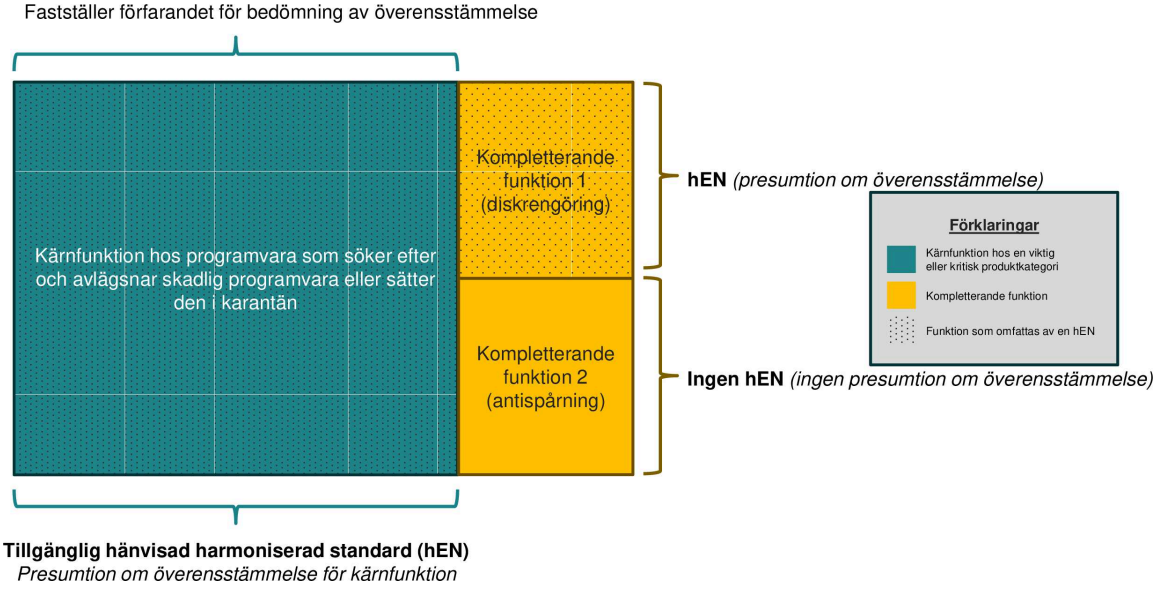
Den harmoniserade standarden medger en presumtion om överensstämmelse för kärnfunktionen, eftersom den behandlar alla risker som är förknippade med denna kärnfunktion, men inte för de kompletterande funktionerna



Exempel 65: I samma scenario som i det föregående exemplet har den harmoniserade standarden nu uppdaterats för att även omfatta risker förknippade med en av de ytterligare funktionerna, nämligen diskrengöringsfunktionen, men inte den andra (dvs. antispårningsfunktionen). Om den harmoniserade standarden tillämpas får tillverkaren använda förfarandet för intern kontroll för sin bedömning av överensstämmelse. Tillverkaren kommer att gynnas av en presumtion om överensstämmelse för de risker som är förknippade med produktens kärnfunktion och för diskrengöringsfunktionen, men inte för de risker som är förknippade med antispårningsfunktionen.

Figur 8

Den harmoniserade standarden medger en presumtion om överensstämmelse för kärnfunktionen och kompletterande funktion 1, eftersom den behandlar alla risker som är förknippade med dessa två funktioner, men inte för kompletterande funktion 2



7. **BEDÖMNING AV CYBERSÄKERHETSRISKER OCH INTEGRERING AV PRODUKTER MED DIGITALA ELEMENT OCH KOMPONENTER**

7.1 **Om utvärdering och behandling av cybersäkerhetsrisker**

156. Den bedömning av cybersäkerhetsrisker som föreskrivs i artikel 13.2 i cyberresiliensförordningen kräver att tillverkarna identifierar de relevanta riskerna och bedömer deras potentiella inverkan på produkten med digitala element. Tillverkarna måste också vidta lämpliga åtgärder för att hantera dessa risker, i enlighet med de väsentliga kraven i bilaga I.

157. Vid organisatorisk riskhantering utvärderas riskerna vanligen mot bakgrund av acceptanskriterier som härrör från organisationens interna mål eller riskbenägenhet. Enligt cyberresiliensförordningen bör den kvarstående cybersäkerhetsrisken däremot bedömas mot bakgrund av kravet att den produkt med digitala element som släpps ut på marknaden garanterar en lämplig cybersäkerhetsnivå baserat på riskerna, med beaktande av dess avsedda ändamål och rimligen förutsebara användning.

158. Tillverkarens interna risktolerans, affärsstrategi eller kostnadsöverväganden är därför inte relevanta för att avgöra om riskerna har åtgärdats. Vid tillämpningen av artikel 13.2 och 13.3 måste tillverkarna kunna avgöra huruvida de identifierade cybersäkerhetsriskerna har hanterats i tillräcklig utsträckning genom uppfyllandet av de väsentliga kraven i del I i bilaga I, mot bakgrund av det avsedda ändamålet, rimligen förutsebara användningen och användningsvillkoren, inbegripet, i förekommande fall, den operativa miljön (t.ex. de avsedda användarna av produkten med digitala element) och de tillgångar som ska skyddas, med beaktande av den tid under vilken produkten med digitala element förväntas vara i bruk.

159. Den kvarstående cybersäkerhetsrisken är ett naturligt resultat av riskbedömning och riskhantering. Man måste erkänna att cybersäkerhetsrisker i praktiken inte kan elimineras helt och hållet. Förekomsten av en kvarstående risk innebär dock inte att vilken risk som helst kan godtas efter tillverkarens gottfinnande. En produkt med digitala element får endast släppas ut på marknaden om de kvarstående riskerna, när lämpliga åtgärder väl har vidtagits, har hanterats i tillräcklig utsträckning genom uppfyllande av de väsentliga kraven, med beaktande av det avsedda syftet och rimligen förutsebara användningen av produkten med digitala element.

160. I enlighet med artikel 13.3 ska tillverkarna, i de fall cybersäkerhetsrisker identifieras, åtgärda dessa genom lämpliga åtgärder, inbegripet på produktnivå. Beroende på omständigheterna kan detta till exempel innebära att man minskar attackytan, genomför tekniska skyddsåtgärder, begränsar eller anpassar funktioner eller mer exakt definierar det avsedda ändamålet med produkten med digitala element. Tillverkarna får också vidta åtgärder för att forma den rimligen förutsebara användningen av produkten med digitala element, till exempel genom riskkommunikation, användarvägledning eller utformning av användargränssnittet, för att styra användarnas beteende i riktning mot säkra användningsmönster.

161. Cyberresiliensförordningen tillåter inte att cybersäkerhetsrisker eller cybersäkerhetsansvar överförs till användare eller tredje part för att kompensera för brister i produktutformningen eller för att motivera att cybersäkerhetsrisker lämnas oåtgärdade. Skyldigheten att släppa ut en säker produkt med digitala element på marknaden och att visa på uppfyllandet av de väsentliga kraven ligger fortsatt hos tillverkaren.

162. Den information och de instruktioner som tillhandahålls till användarna får användas för att stödja en säker distribution och drift av produkten med digitala element, inbegripet när tillverkaren har valt att begränsa produktens avsedda ändamål till betrodda miljöer, och för att informera användarna om kvarstående risker, på ett sätt som är lämpligt med tanke på arten av produkten med digitala element och dess avsedda användare.

Exempel 66: En tillverkare utvecklar en industriell sensor för användning i betrodda miljöer. För att sensorn ska fungera korrekt vidtar tillverkaren inga åtgärder för att skydda mot fysiska angrepp på sensorn i sig. För att minska de därtill hörande risker som identifieras i riskbedömningen begränsar tillverkaren sensorns avsedda ändamål till att endast användas i betrodda miljöer där obehörig fysisk tillgång till produkten med digitala element förhindras. Information och instruktioner till användarna ska ge tydlig information om dessa begränsningar av sensorns användning, på ett sätt som är lämpligt med tanke på arten av produkt med digitala element och dess avsedda användare.

Exempel 67: En tillverkare utvecklar en programvaruapplikation för yrkesmässig användning på hanterade skrivbordsenheter och mobila enheter. Applikationen behandlar lokalt lagrade känsliga data och användargenererat innehåll. Under riskbedömningen identifierar tillverkaren en risk för obehörig tillgång till sådana uppgifter om de lagras i klartextformat på enheten. I stället för att utforma och tillämpa en märkesskyddad krypteringsmekanism i själva applikationen väljer tillverkaren att använda de krypterings- och nyckelhanteringsfunktioner som tillhandahålls internt av det operativsystem som applikationen är avsett att köras på, eftersom operativsystemets inbyggda krypteringstjänster är mogna och underhålls regelbundet.

163. Om bedömningen av cybersäkerhetsrisker identifierar risker som inte kan hanteras på lämpligt sätt genom lämpliga åtgärder, kan överensstämmelse med cyberresiliensförordningen kräva ändringar av utformningen av, funktionen hos eller det avsedda ändamålet med produkten med digitala element. Överväganden som enbart avser kostnader eller kommersiell genomförbarhet utgör inte tillräckliga skäl för att lämna sådana risker oåtgärdade om detta skulle hindra produkten med digitala element från att uppfylla de väsentliga kraven.

7.2 Om utformning, utveckling och produktion av produkter med digitala element på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna

164. Det väsentliga cybersäkerhetskrav som avses i del I punkt 1 i bilaga I till cyberresiliensförordningen föreskriver att produkter med digitala element utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna.

165. Detta väsentliga krav syftar till att hantera alla cybersäkerhetsrisker som har identifierats som en del av bedömningen av cybersäkerhetsrisker. Detta omfattar i synnerhet de cybersäkerhetsrisker som annars inte hanteras på lämpligt sätt som en del av tillämpningen av de andra väsentliga kraven i del I i bilaga I än kravet i punkt 1. Detta väsentliga krav skiljer sig från den rättsliga skyldigheten att genomföra en bedömning av cybersäkerhetsrisker, som ska utföras i enlighet med artikel 13.2.

166. Om alla relevanta cybersäkerhetsrisker som är förknippade med en produkt med digitala element behandlas genom vidtagandet av lämpliga åtgärder för att åtgärda de andra tillämpliga väsentliga kraven än det i punkt 1, ska det väsentliga krav som avses i del I punkt 1 i bilaga I anses vara uppfyllt. Om det i bedömningen av cybersäkerhetsrisker fastställs ytterligare risker som inte helt och hållet hanteras av dessa åtgärder måste tillverkarna däremot vidta lämpliga åtgärder för produkten med digitala element för att hantera dessa risker, så att tillverkarna uppfyller det väsentliga krav som avses i del I punkt 1 i bilaga I. I de flesta fall förväntas överensstämmelsen med de andra väsentliga kraven i praktiken leda till att detta krav uppfylls.

7.3 Riskbedömning och tillbörlig aktsamhet med avseende på externa beroenden och integrerade komponenter

167. I cyberresiliensförordningen fastställs två separata men kompletterande skyldigheter för tillverkare med avseende på hanteringen av cybersäkerhetsrisker. För det första krävs enligt artikel 13.2 att tillverkarna genomför en bedömning av cybersäkerhetsrisker för själva produkten med digitala element. För det andra innebär artikel 13.5 en skyldighet att iaktta tillbörlig aktsamhet med avseende på integrerade komponenter. Tillsammans är dessa två skyldigheter utformade för att säkerställa att produkten med digitala element förblir säker, inbegripet när den är beroende av lösningar för fjärrbehandling av data, fjärrtjänster eller programvara eller hårdvarukomponenter från tredje part.

168. Bedömningen av cybersäkerhetsrisker rör identifiering och hantering av relevanta risker som kan påverka produkten med digitala element, däribland risker som kommer från utanför själva produkten, såsom externa nätverk, miljöfaktorer eller andra externa aspekter som kan påverka produkten med digitala element eller som produkten är beroende av. För sådana externa risker kräver inte cyberresiliensförordningen att tillverkarna kontrollerar eller styr den yttre miljön. Tillverkarna måste snarare identifiera dessa risker och minska dem genom att utforma och utveckla själva produkten med digitala element. Detta kommer att inbegripa ett uppfyllande av de lämpliga väsentliga kraven i del I i bilaga I och, vid behov, ett tillhandahållande av information och instruktioner till användarna om integrerings- eller spridningsrisker.

169. Till exempel kan en tillverkare identifiera en risk för att obehöriga kan få tillgång till backend-system som inte är en del av själva produkten med digitala element medan produkten är i drift, och försöka skicka skadliga kommandon till produkten med digitala element. Om sådana backend-system inte har utformats och utvecklats av tillverkaren eller ligger under dennes ansvar, eller om de inte stöder en av funktionerna hos produkten med digitala element, utgör de inte lösningar för fjärrbehandling av data och faller därför utanför omfattningen av produkten med digitala element enligt cyberresiliensförordningen. Cyberresiliensförordningen kräver dock att tillverkaren hanterar den risk som de kan utgöra genom åtgärder på produktnivå, t.ex. genom att kräva kryptografisk autentisering av fjärrkommandon, verifiering av integriteten hos konfigurationsändringar eller generering av säkerhetsrelevanta loggar eller varningar när onormalt beteende upptäcks. Om en tillverkare identifierar en risk som följer av att en sådan extern tjänst blir otillgänglig, till exempel på grund av strömavbrott eller fel i infrastrukturen, kan cyberresiliensförordningen kräva begränsande åtgärder på produktnivå mot sådana cybersäkerhetsrisker, t.ex. att säkerställa att avbrottet inte leder till att produkten med digitala element går in i osäkra tillstånd. I sådana fall reglerar cyberresiliensförordningen hur produkten med digitala element reagerar på dessa externa risker – den påför inte några skyldigheter för hur backend-infrastrukturen organiseras, bemannas eller drivs, och den betraktar inte heller denna infrastruktur som en del av produkten med digitala element.

170. Tillbörlig aktsamhet har att göra med delar som utgör en del av själva produkten med digitala element, i synnerhet integrerad programvara eller hårdvarukomponenter som tillhandahålls av en tredje part. Tillverkarna är skyldiga att vidta lämpliga åtgärder för att säkerställa att sådana komponenter inte undergräver överensstämmelsen med de väsentliga kraven hos produkten med digitala element. Detta kan endast uppnås genom att fastställa vad produkten med digitala element kräver av sina komponenter för att uppnå sina cybersäkerhetsmål, och genom att på ett riskbaserat sätt kontrollera att dessa komponenter är förenliga med produktens behov, vilket också anges i skäl 34.

171. I linje med sin bedömning av cybersäkerhetsrisker måste tillverkaren identifiera de krav som den integrerade komponenten bör uppfylla. Om till exempel produkten med digitala element är beroende av kryptografiska funktioner, uppdateringsmekanismer eller säker kommunikation som tillhandahålls av en komponent måste tillverkaren, som en del av den tillbörliga aktsamheten, identifiera dessa behov och verifiera att komponenten uppfyller dem. Bevis i detta syfte kan bestå av dokumentation som erhållits av komponentens tillverkare, såsom tekniska specifikationer, säkerhetsdokumentation eller relevant dokumentation om överensstämmelse eller assurans. I förekommande fall får tillverkaren också genomföra provningar för att kontrollera att dessa komponenter utför de relevanta funktionerna på ett tillfredsställande sätt. Även om tillbörlig aktsamhet är en separat rättslig skyldighet stöder den och utgör grunden för tillverkarens förmåga att påvisa överensstämmelsen med de väsentliga kraven för produkten med digitala element som helhet.

172. Vid bedömning av riskerna för produkten med digitala element som helhet måste delar utanför produkten, såsom miljöaspekter, extern infrastruktur, andra system eller nätverk, beaktas i bedömningen av cybersäkerhetsrisker och, i förekommande fall, hanteras genom åtgärder på produktnivå för att säkerställa att produkten överensstämmer med de väsentliga kraven. Komponenter som är fysiskt eller logiskt integrerade i produkten med digitala element men som kommer från en tredje part måste också övervägas som en del av riskbedömningen. Av överensstämmelseskäl bör dock tillverkaren behandla dessa som externt tillhandahållna komponenter vars egenskaper kontrolleras genom tillbörlig aktsamhet vid integrering, eftersom tillverkaren kanske inte har omformat eller omkonstruerat dem.

173. Samma logik gäller vid utveckling och integrering av komponenter. Om tillverkaren själv utvecklar funktioner måste denne direkt tillämpa de väsentliga kraven. Om tillverkaren integrerar komponenter som har utvecklats av andra måste den genom tillbörlig aktsamhet säkerställa att dessa komponenter kan användas på ett sätt som gör att produkten med digitala element som helhet överensstämmer med kraven. I båda fallen förblir målet detsamma: att den produkt med digitala element som släpps ut på marknaden ska uppnå en lämplig cybersäkerhetsnivå i enlighet med kraven i cyberresiliensförordningen, med beaktande av de risker som identifierats i bedömningen av cybersäkerhetsrisker.

7.4 Återanvändning av riskbedömningar och dokumentation om överensstämmelse för produktfamiljer med digitala element

174. Tillverkarna får släppa ut produkter med snarlika digitala element på marknaden, t.ex. olika varianter, modeller eller konfigurationer av samma produktfamilj. Om sådana produkter med digitala element har samma arkitektur, säkerhetsrelevanta utformning och avsedda ändamål och om de är utsatta för samma cybersäkerhetsrisker, kräver cyberresiliensförordningen inte att tillverkarna behandlar varje variant som en helt separat produkt med digitala element vid riskbedömningen och bedömningen av överensstämmelse.

175. I sådana fall får tillverkarna, under förutsättning att alla berörda varianter omfattas på lämpligt sätt när det gäller relevanta risker och väsentliga krav, förlita sig på i) en enda bedömning av cybersäkerhetsrisker som utförs i enlighet med artikel 13.2 i cyberresiliensförordningen, ii) en enda uppsättning teknisk dokumentation, och iii) ett enda förfarande för bedömning av överensstämmelse. Detta gör det också möjligt att utfärda en enda EU-försäkran om överensstämmelse för hela gruppen av produkter med digitala element, så länge den tydligt identifierar de produktvarianter på vilka den är tillämplig.

176. Den avgörande faktorn är huruvida skillnaderna mellan varianterna är relevanta för cybersäkerheten. Ändringar som inte påverkar cybersäkerhetsegenskaperna hos en produkt med digitala element, såsom skillnader i färg, formfaktor, minnesstorlek eller andra icke-säkerhetsrelevanta egenskaper, kräver inte separata riskbedömningar eller bedömningar av överensstämmelse. Omvänt kan varianter i vissa fall skilja sig åt på sätt som påverkar tillämpningen av de väsentliga kraven, till exempel genom olika kommunikationsgränssnitt, programvarustackar, uppdateringsmekanismer eller fjärranslutningar. I sådana fall måste dessa skillnader avspeglas i riskbedömningen och, vid behov, i bedömningen av överensstämmelse och den tekniska dokumentationen.

177. Tillverkarna är fortsatt ansvariga för att riskbedömningen och den därtill hörande dokumentationen korrekt avspeglar de produkter med digitala element som släpps ut på marknaden. Om en ny variant medför nya cybersäkerhetsrisker eller ändrar det sätt på vilket de väsentliga kraven tillämpas, måste den befintliga riskbedömningen och dokumentationen om överensstämmelse uppdateras i enlighet med detta. Det är endast möjligt att förlita sig på en enda bedömning av överensstämmelse om produkterna med digitala element inte uppvisar några skillnader med avseende på deras cybersäkerhetsegenskaper.

8. FJÄRRBEHANDLING AV DATA

178. I artikel 3.1 i cyberresiliensförordningen definieras ”produkt med digitala element” som en ”programvaru- eller hårdvaruprodukt och dess lösningar för fjärrbehandling av data, inbegripet programvaru- eller hårdvarukomponenter som släpps ut på marknaden separat”. Mot denna bakgrund måste tillverkaren beakta produkten med digitala element som en helhet, inbegripet dess lösningar för fjärrbehandling av data (RDPS). När man till exempel visar att produkten med digitala element uppfyller de väsentliga kraven i bilaga I måste man ta hänsyn till lösningarna för fjärrbehandling av data, med början i riskbedömningen (artikel 13.2). Detsamma gäller för skyldigheterna över hela livscykeln, såsom rapporteringen av aktivt utnyttjade sårbarheter och allvarliga incidenter (artikel 14).

179. Syftet med denna vägledning är att ge ytterligare stöd till tillverkarna så att de kan avgöra om deras produkt med digitala element har lösningar för fjärrbehandling av data i den mening som avses i cyberresiliensförordningen och hur de ska uppfylla sina skyldigheter i detta avseende. Efter en inledande analys av definitionerna och skälen i cyberresiliensförordningen kommer denna vägledning att ställa frågor som ska vägleda tillverkarna när de klargör om deras produkt med digitala element innehåller lösningar för fjärrbehandling av data (se avsnitt *8.1 Vad betraktas som en lösning för fjärrbehandling av data för en produkt med digitala* element?). Därefter kommer den att vidareutveckla de tekniska konsekvenserna av lösningarna för fjärrbehandling av data och hur efterlevnaden av cyberresiliensförordningen ska bedömas (se avsnitt *8.2 Praktiska och tekniska konsekvenser av lösningar för fjärrbehandling av data och beroende av lösningar* från tredje part).

180. I artikel 3.2 definieras faktiskt begreppet ”fjärrbehandling av data” som ”databehandling på distans för vilken programvaran utformats och utvecklats av tillverkaren eller under tillverkarens ansvar, och vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner”. En lösning för fjärrbehandling av data definieras därför som programvarudelen (”den del av ett elektroniskt informationssystem som utgörs av datorkod”, enligt definitionen i artikel 3.4) av fjärrbehandlingen av data. Den är inte avsedd att, som en del av omfattningen av produkten med digitala element, inkludera den hårdvara som fjärrbehandlingen av data kan vara beroende av.

181. Skälen 11 och 12 ger ytterligare förklaringar till hur detta begrepp bör tolkas. I skäl 11 klargörs att målet med att inbegripa lösningar för fjärrbehandling av data är att ”sådana produkter [säkras] i sin helhet, oavsett om uppgifterna behandlas eller lagras lokalt på användarens enhet eller på distans av tillverkaren”. Det anges också att ”kraven på lösningar för fjärrbehandling som omfattas av denna förordning innebär därför inte några tekniska, operativa eller organisatoriska åtgärder som syftar till att hantera riskerna för säkerheten i en tillverkares nätverks- och informationssystem som helhet”.

182. Av skäl 11 framgår därför att syftet inte är att kraven i cyberresiliensförordningen ska omfatta en organisations hela it-infrastruktur, utan endast de programvarukomponenter som gör det möjligt att använda lösningen för behandling av data. Exempelvis bör de interna system som avser tillverkarens egna personalresurser, lönelistor, hantering av kundrelationer, pipor för kontinuerlig integrering/kontinuerlig leverans (CI/CD) och distribution av säkerhetsuppdateringar till platser ute i kanten, inte betraktas som lösningar för fjärrbehandling av data. På samma sätt faller system som är kopplade till revisions- och provningsverksamhet, såsom penetrationstester, hotjakt och red teaming, utanför tillämpningsområdet för en produkt med digitala element som omfattas av cyberresiliensförordningen. Det är viktigt att notera att samtidigt som tillämpningen av effektiva och regelbundna provningar och granskningar av produktens säkerhet med digitala element är ett väsentligt krav som fastställs i del II punkt 3 i bilaga I till cyberresiliensförordningen, innebär detta inte att denna verksamhet ska betraktas som en lösning för fjärrbehandling av data för produkten med digitala element.

183. Skäl 12 är inriktat på molntjänster, och beskriver under vilka omständigheter som molntjänster kan betraktas som en lösning för fjärrbehandling av data. Avslutningsvis anges i skälet att molntjänster och molntjänstmodeller omfattas av direktiv (EU) 2022/2555 (NIS 2-direktivet) ([28]), som fastställer krav rörande riskhanteringsåtgärder för cybersäkerhet för leverantörer av molntjänster. Dessa krav specificeras närmare i kommissionens genomförandeförordning (EU) 2024/2690 ([29]).

8.1 **Vad betraktas som en lösning för fjärrbehandling av data för en produkt med digitala element?**

184. Definitionen av fjärrbehandling av data i artikel 3.2 bygger således på följande tre faktorer: i) huruvida databehandlingen sker ”på distans”, ii) huruvida avsaknaden av denna databehandling skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner, och iii) huruvida programvaran är utformad och utvecklad av tillverkaren eller under dennes ansvar. I de följande tre underavsnitten behandlas var och en av dessa aspekter mer ingående.

([28]) Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) (EUT L 333, 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Kommissionens genomförandeförordning (EU) 2024/2690 av den 17 oktober 2024 om fastställande av regler för tillämpningen av direktiv (EU) 2022/2555 vad gäller tekniska och metodologiska specifikationer för riskhanteringsåtgärder för cybersäkerhet och närmare angivelse av i vilka fall en incident ska anses vara betydande med avseende på leverantörer av DNS-tjänster, registreringsenheter för toppdomäner, leverantörer av molntjänster, leverantörer av datacentraltjänster, leverantörer av nätverk för leverans av innehåll, leverantörer av utlokaliserade driftstjänster, leverantörer av utlokaliserade säkerhetstjänster, leverantörer av marknadsplatser online, leverantörer av sökmotorer, leverantörer av plattformar för sociala nätverkstjänster och tillhandahållare av betrodda tjänster (EUT L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj/swe).

8.1.1 *Begreppet ”på distans”*

185. Begreppet ”på distans” som avses i artikel 3.2 är relevant men inte tillräckligt för att avgöra om en produkt med digitala element inkluderar en lösning för fjärrbehandling av data. Med tanke på den mångfald av lösningar som kan omfattas av detta begrepp är det dessutom inte möjligt att tillhandahålla en uttömmande definition av ”på distans”. Tillverkaren måste göra en bedömning från fall till fall.

186. I skäl 11 i cyberresiliensförordningen nämns data som behandlas eller lagras ”på distans av tillverkaren” i motsats till uppgifter som behandlas eller lagras ”lokalt på användarens enhet”. Fjärrbehandling av data sker vanligtvis utanför användarmiljön hos en produkt med digitala element eller en organisations driftsmiljö (för en yrkesmässig användare). Detta hindrar dock inte att bearbetningen även äger rum nära enheten (”ute i kanten”). Överföringen av data kan vara trådbunden (t.ex. en ethernetkabel) eller trådlös (t.ex. wifi, bluetooth). Molnbaserade datortjänster, inklusive kantdatorsystem, är ett typiskt exempel på fjärrbehandling av data. När det gäller molnbaserade funktioner som användaren får åtkomst till via en mobilapplikation sker till exempel en del av databehandlingen i molnet, alltså utanför användarens miljö.

187. Det är viktigt att notera att lösningar för fjärrbehandling av data inte nödvändigtvis körs på molninfrastruktur som tillhör en tredje part. Fjärrbehandling av data som körs på lokala servrar på plats i tillverkarens lokaler kan också utgöra en lösning för fjärrbehandling av data. Med andra ord är det lika sannolikt att en lösning som körs lokalt och i ett privat moln betraktas som en lösning för fjärrbehandling av data som en lösning som körs i ett offentligt moln och utanför tillverkarens lokaler.

188. De två avgörande och kumulativa frågor som fastställer om databehandling omfattas av cyberresiliensförordningen som en lösning för fjärrbehandling av data anges i avsnitten *8.1.2* och *8.2* nedan. Om båda frågorna besvaras jakande betraktas fjärrbehandlingen av data som en lösning för fjärrbehandling av data.

8.1.2 *Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner?*

189. Såsom fastställs i definitionen av ”fjärrbehandling av data” i artikel 3.2 skulle avsaknaden av fjärrbehandling av data behöva innebära att produkten med digitala element inte kan utföra en av sina funktioner för att denna fjärrbehandling av data skulle betraktas som en lösning för fjärrbehandling av data. Begreppet ”funktioner” som ingår i denna definition är inte begränsat till ”kärnfunktionen” eller det ”avsedda ändamålet” för produkten med digitala element, eftersom cyberresiliensförordningen inte föreskriver någon sådan begränsning. De funktioner som omfattas av cyberresiliensförordningen är både funktioner som direkt uppfyller det avsedda ändamålet för produkten med digitala element såsom detta upplevs av användarna och funktioner som stöder produktens övergripande prestanda.

190. Exempel på funktioner där fjärrdatabehandling kan ske och som skulle hindra en produkt med digitala element från att utföra en av sina funktioner skulle kunna inbegripa i) sändning av kommandon till en enhet, ii) synkronisering av filer, iii) introducering av användaren, iv) konfigurering (personalisering av produkten med digitala element), v) automatisk distribution av uppdateringar, inklusive uppdateringar av funktioner och säkerhetskorrigeringar, vi) identitets- och åtkomsthantering.

191. I vissa fall kan användaren använda en funktion både på distans och manuellt (t.ex. att tända en glödlampa med hjälp av en app eller manuellt). Att ha detta alternativ utesluter inte att den databehandling som är kopplad till funktionens fjärrbehandling betraktas som en lösning för fjärrdatabehandling. Att kunna utföra denna funktion på distans betraktas också som en del av de funktioner som produkten med digitala element erbjuder.

192. Om avsaknaden av en viss databehandling däremot inte hindrar produkten med digitala element från att utföra en av sina funktioner, betraktas denna behandling inte som en lösning för fjärrbehandling av data i den mening som avses i cyberresiliensförordningen. Detta inbegriper till exempel fjärranalys av telemetridata som samlats in enbart för statistiska ändamål eller för framtida produktutveckling.

193. Även om databehandlingen inte stöder en funktion hos en produkt med digitala element kan tillverkarna dock behöva överväga om dessa fjärrkomponenter medför risker för produkten med digitala element som en del av deras bedömning av cybersäkerhetsrisker (t.ex. mot bakgrund av produktens operativa miljö) och minska sådana risker i enlighet med detta (t.ex. genom begränsning på produktnivå).

194. Webbplatser är ett specifikt fall som förtjänar ytterligare förtydliganden, såsom också förklaras i *avsnitt 2.1 Utsläppande på marknaden*. Webbplatser betraktas inte som lösningar för fjärrbehandling av data om de inte stöder en funktion hos en produkt med digitala element, såsom förklaras i skäl 11 i cyberresiliensförordningen. Det räcker inte att en webbplats innehåller information om en produkt med digitala element för att den ska betraktas som en lösning för fjärrbehandling av data, även om produkten omdirigerar användaren till en sådan webbplats. Omdirigering av användare till en extern webbsida som ger information och instruktioner till användarna utgör till exempel inte en lösning för fjärrbehandling av data. En webbplats kan däremot betraktas som en lösning för fjärrbehandling av data om den möjliggör eller stöder en funktion hos en produkt med digitala element. En autentiseringsportal som utfärdar de autentiseringsuppgifter eller token som krävs för att produkten med digitala element ska kunna köras skulle till exempel betraktas som en lösning för fjärrbehandling av data (förutsatt att de andra kriterierna i definitionen också är uppfyllda).

8.1.3 *Har programvaran utformats och utvecklats av tillverkaren eller under dennes ansvar?*

195. I definitionen av ”fjärrbehandling av data” i artikel 3.2 i cyberresiliensförordningen anges vidare att programvaran för sådan databehandling på distans måste ha utformats och utvecklats av tillverkaren eller under dennes ansvar. Fjärrbehandling av data som helt och hållet har utvecklats och utformats av tillverkaren (internt) skulle helt naturligt betecknas som en lösning för fjärrbehandling av data. Detta skulle också vara fallet om tillverkarna förlitar sig på en extern tjänsteleverantör för utvecklingen och utformningen av en lösning (dvs. ”under dennes ansvar”). Frasen ”under tillverkarens ansvar” avser fjärrbehandlingslösningar som är skräddarsydda för tillverkaren. Dessa är fall där tillverkaren inte enbart licensierar en befintlig produkt med digitala element eller en tjänst som en tjänsteleverantör erbjuder sina kunder, eller något modifierade versioner av dessa. ”Under tillverkarens ansvar” innebär att programvaran byggs enbart av tillverkaren eller för tillverkarens räkning, på grundval av de konstruktioner och specifikationer som tillverkaren tillhandahåller.

196. För att förstå lösningar för fjärrbehandling av data är begreppet ”vem som använder lösningen” inte en avgörande faktor, eftersom definitionen i cyberresiliensförordningen endast avser utformningen och utvecklingen av lösningen för fjärrbehandling av data. Detta är förenligt med strategin i cyberresiliensförordningen, som innebär att kraven och skyldigheterna påförs tillverkarna och inte driften av produkten med digitala element. Om tillverkarna utformar och utvecklar lösningar som sedan används av en tredje part, förblir de ansvariga för uppfyllandet av cyberresiliensförordningens väsentliga krav för den produkt med digitala element som de släpper ut på marknaden.

197. Det är nödvändigt att särskilja mellan de fall där utformningen och utvecklingen utförs av tillverkare (eller under deras ansvar) och fall där programvaran är beroende av tredjepartslösningar som inte har utformats och utvecklats av tillverkare (eller under deras ansvar). Som exempel kan man tänka på de vanligaste molntjänstmodellerna, som tillhandahåller olika grader av användarkontroll och som också nämns i skäl 12 i cyberresiliensförordningen, nämligen Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) och Infrastructure-as-a-Service (IaaS).

198. När det gäller en IaaS-lösning från tredje part hanterar eller kontrollerar tillverkaren varken de underliggande fysiska eller virtuella resurserna (t.ex. den underliggande hårdvaran och molntjänstleverantörens hypervisor), men kan använda och köra valfri programvara med hjälp av dessa resurser, t.ex. operativsystem och applikationer. Denna programvara är utformad och utvecklad av tillverkaren eller under dennes ansvar, och kan därför betecknas som en lösning för fjärrbehandling av data (om den uppfyller övriga delar av definitionen).

199. När det gäller en PaaS-lösning från tredje part använder tillverkaren sin egen (skapade eller förvärvade) applikation med hjälp av programmeringsspråk och exekveringsmiljöer som tillhandahålls av molntjänstleverantören, och integrerar programmet i sin produkt med digitala element. Tillverkaren har kontroll över applikationen och eventuellt över konfigurationsinställningarna för exekveringsmiljön. Applikationen har därför utformats och utvecklats av tillverkaren, eller under dennes ansvar, och kan därför betecknas som en lösning för fjärrbehandling av data (om den uppfyller övriga delar av definitionen).

200. När det gäller en SaaS-lösning från tredje part erbjuder SaaS-leverantören tillverkaren en fullt utvecklad applikation som ska integreras i tillverkarens produkt med digitala element. Tillverkaren har begränsad möjlighet att hantera användarspecifika konfigurationsinställningar för applikationen. Applikationen är därför inte utformad och utvecklad av tillverkaren eller under dennes ansvar.

201. Om vissa element inte uppfyller kraven för att betecknas som en lösning för fjärrbehandling av data (t.ex. hypervisorn med avseende på en IaaS-infrastruktur från tredje part, operativsystemet med avseende på en PaaS-lösning från tredje part eller SaaS-applikationen från tredje part) men är integrerade i produkten med digitala element på ett sätt som påverkar dess säkerhet, bör sådana lösningar dock anses vara likvärdiga med komponenter från tredje part. Tillverkaren ska identifiera och bedöma de risker som är kopplade till integreringen av dessa delar och åtgärda dem genom att själv tillämpa de väsentliga kraven på produkten med digitala element. Detta kan i förekommande fall stödjas av de säkerhetsfunktioner som tillhandahålls av molntjänstleverantören genom dennes modell för delat ansvar, där tillverkaren använder eller konfigurerar dessa funktioner för att åtgärda de identifierade riskerna. Dessutom förväntas tillverkaren utöva en liknande skyldighet som den skyldighet att visa tillbörlig aktsamhet som avses i artikel 13.5 i fråga om dessa komponenters säkerhet, på ett sätt som är proportionellt till den risk som fjärrlösningen utgör för produkten med digitala elements säkerhet.

202. Detta kan därför sammanfattas på följande sätt:

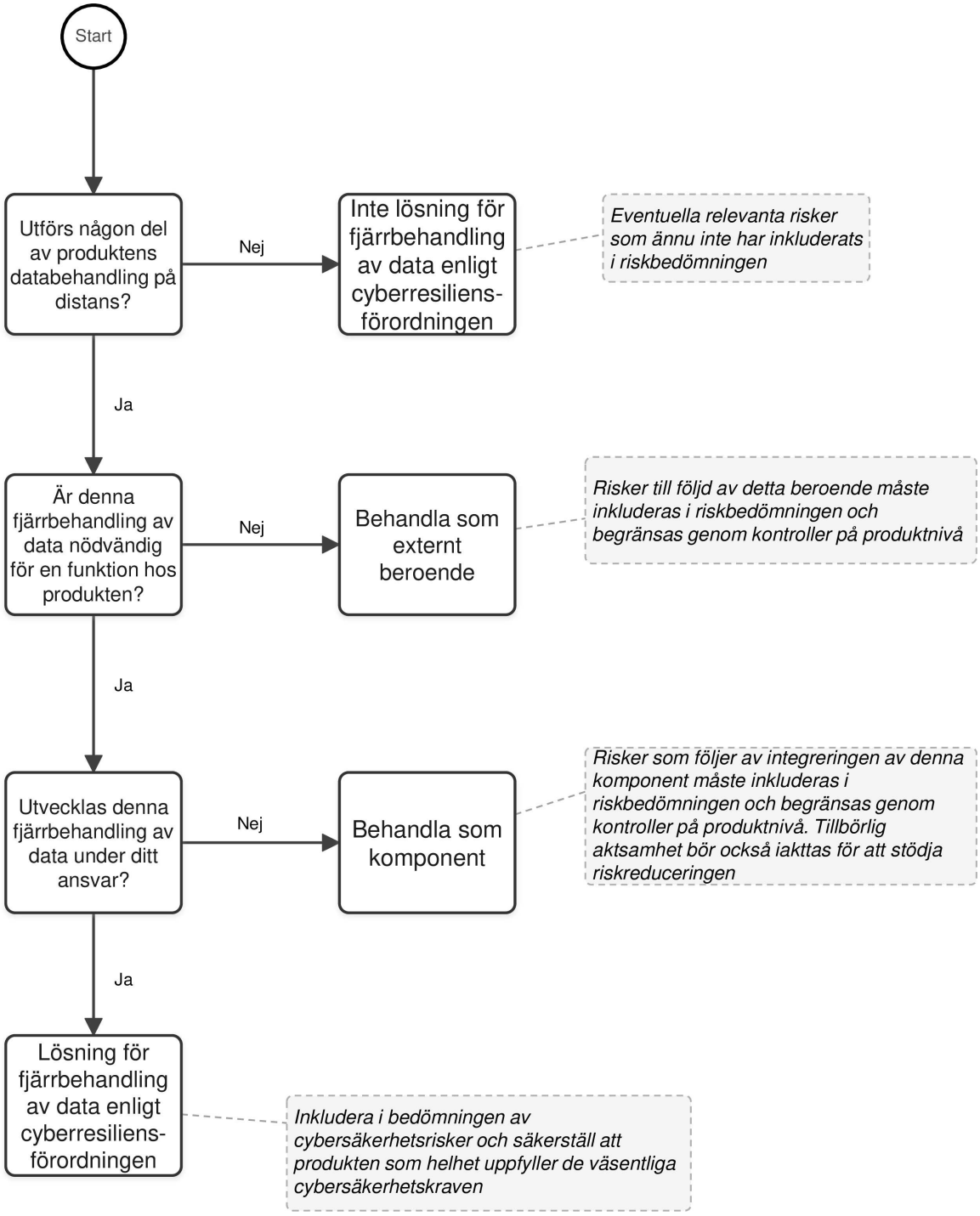
a) För att databehandling ska betraktas som en lösning för fjärrbehandling av data måste båda de frågor som ställs i avsnitten *8.1.2 Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner?* och *8.1.3 Har programvaran utformats och utvecklats av tillverkaren eller under dennes ansvar?* besvaras med ett ja.

b) Om svaret på frågan i avsnitt *8.1.2 Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner?* är nej bör tillverkare bedöma de risker som härrör från denna databehandling som en del av sin riskbedömning.

c) Om svaret på frågan i avsnitt *8.1.2 Kan avsaknad av databehandling innebära att en produkt med digitala element inte kan utföra en av sina funktioner?* är ja men svaret på frågan i *8.1.3 Har programvaran utformats och utvecklats av tillverkaren eller under dennes ansvar?* är nej, bör tillverkare behandla tredjepartslösningen som en komponent. Som en del av riskbedömningen bör tillverkare bedöma de risker som härrör från integreringen av en sådan lösning och begränsa dem i enlighet med detta. Tillverkarna bör dessutom iaktta tillbörlig aktsamhet.

Figur 9

Stiliserat flödesschema för hur man avgör om en produkt med digitala element innehåller lösningar för fjärrbehandling av data



8.2 Praktiska och tekniska konsekvenser av lösningar för fjärrbehandling av data och beroende av lösningar från tredje part

203. Cyberresiliensförordningen följer en riskbaserad metod som fastställs i artikel 13.2 och 13.3 samt i det första väsentliga kravet i del I i bilaga I, enligt vilket ”produkter med digitala element ska utformas, utvecklas och produceras på ett sådant sätt att de säkerställer en lämplig cybersäkerhetsnivå baserat på riskerna”. Följaktligen bör en riskbaserad metod övervägas vid tillämpningen av kraven i cyberresiliensförordningen på lösningen för fjärrbehandling av data och hanteringen av de risker som härrör från de tredjepartstjänster som har integrerats i produkten med digitala element.

204. För det första bör tillverkarna i) i den tekniska dokumentationen ange att deras produkter med digitala element har en lösning för fjärrbehandling av data eller är beroende av fjärrlösningar från tredje part och ii) beskriva dessa lösningar. Om samma lösning för fjärrbehandling av data stöder flera produkter med digitala element måste lösningen för fjärrbehandling av data anges i den tekniska dokumentationen för varje produkt. Dokumentationen rörande lösningar för fjärrbehandling av data som betjänar flera produkter med digitala element kan återanvändas från bedömningen av överensstämmelse för en produkt till en annan.

205. Såsom anges i skäl 11 bör en lösning för fjärrbehandling av data som ingår i produkten med digitala element och som därför omfattas av produktens bedömning av överensstämmelse begränsas till de programvarumoduler som ansvarar för funktionerna hos produkten med digitala element, och till de gränssnitt som dessa moduler använder för externa tjänster. Ytterligare backend-system som utför därpå följande behandling och med vilka produkten med digitala element inte samverkar direkt anses inte vara lösningar för fjärrbehandling av data.

206. Dessa backend-system är dock fortfarande externa beroenden som måste bedömas som en del av bedömningen av cybersäkerhetsrisker och begränsas genom åtgärder på produktnivå. I den riskbedömning som utförs av tillverkaren bör följande beaktas: i) risker som rör lösningen för fjärrbehandling av data, ii) risker som rör tredjepartsfjärrlösningar (likvärdiga med komponenter från tredje part), och iii) risker som rör produktmiljön (t.ex. den underliggande hårdvaran). Tillverkarna bör själva genomföra säkerhetskontroller av produkten med digitala element för att minska dessa risker.

207. Som en del av bedömningen av överensstämmelse och/eller fullgörandet av skyldigheterna avseende tillbörlig aktsamhet med avseende på fjärrtjänster från tredje part kan följande icke uttömmande förteckning över assuransartefakter dessutom återanvändas som stöd för tillverkarens bedömning:

a) Bevis för fullgörande av skyldigheterna enligt kommissionens genomförandeförordning (EU) 2024/2690.

b) Bevis för fullgörande av skyldigheterna enligt förordning (EU) 2022/2554 (DORA).

c) Försäkran om överensstämmelse eller intyg som erhållits inom ramen för en europeisk ordning för cybersäkerhetscertifiering (som antagits enligt förordning (EU) 2019/881 – cybersäkerhetsförordningen).

d) Bevis på överensstämmelse med ISO/IEC 27017:2015 eller ISO/IEC 27001:2022.

208. Avslutningsvis måste tillverkarna i sin samverkan med tredjepartsleverantörer av fjärrtjänster genomföra de lämpligaste säkerhetsåtgärderna på grundval av sin riskbedömning (och, när så är lämpligt, med stöd av leverantörens modell för delat ansvar). Dessa begränsningsåtgärder bör inbegripa säkerhetskontroller av tillverkarnas produkter med digitala element och verifiering av de säkerhetsåtgärder som tillhandahålls av tredjepartsleverantörerna själva (tillbörlig aktsamhet). Ett verktyg för att minska dessa risker kan vara att införliva säkerhetsgarantier i tillverkarnas servicenivåavtal med tredjepartsleverantörer, inklusive försäkringar om att leverantörerna hanterar sårbarheter på lämpligt sätt. En betydande ändring av de lösningar som tillhandahålls av tredjepartsleverantörerna av fjärrtjänster bör inte betraktas som en väsentlig ändring av produkten med digitala element, eftersom dessa delar inte faller under tillverkarens ansvar. Som en del av sina skyldigheter med avseende på tillbörlig aktsamhet och för att på ett korrekt sätt minska de risker som härrör från användningen av tredjepartsleverantörer uppmuntras dock tillverkarna att säkerställa att deras tredjepartsleverantörer håller dem tillräckligt informerade om de ändringar de genomför i sina lösningar. På grundval av denna information kan tillverkarna behöva se över sin riskbedömning. I den uppdaterade riskbedömningen bör de överväga om leverantörerna av tredjepartstjänster fortfarande ger tillräckliga garantier när det gäller cybersäkerhet och om säkerhetskontrollerna på produktnivå fortfarande är tillräckliga. I vissa fall kan tillverkarna behöva ändra dessa kontroller eller byta leverantör av tredjepartstjänster.

8.3 **Användningsfall för lösningar för fjärrbehandling av data**

För att ge ytterligare praktisk vägledning till tillverkarna redovisas i detta avsnitt en rad fiktiva användningsfall som beskriver arketypiska produkter med digitala element som är beroende av fjärrbehandling av data och visar om denna behandling kan betraktas som en lösning för fjärrbehandling av data i den mening som avses i cyberresiliensförordningen.

8.3.1 *Mobil bankapplikation*

En finansiell enhet släpper ut en mobil bankapplikation på marknaden. Appens backend-system stöder bland annat autentisering, godkännande, kontohantering och betalningar. Den finansiella enheten använder en hybridstrategi som förlitar sig på intern infrastruktur samt fjärrlösningar från tredje part för att stödja appens funktioner. Dessa inbegriper bland annat

Infrastruktur som hyses på egen server och som utvecklats av den finansiella enheten:

— Kunden öppnar mobilbankapplikationen och autentiseras genom bankgränssnittet, en lösning på egen server som utvecklats av den finansiella enhet som tar emot appens begäranden och returnerar motsvarande svar. Bankgränssnittet verifierar kundens identitet genom att söka i kontohanteringssystemet och beviljar åtkomst till applikationen.

— Kunden initierar en överföring via appen. Appen skickar instruktionen till bankgränssnittet, som skickar motsvarande begäran till systemet med liggaren.

— Kontohanteringssystemet och systemet med liggaren, som båda hyses på egen server men som är logiskt segregerade från bankgränssnittet, registrerar transaktionen.

— Systemet med liggaren returnerar transaktionsstatusen till bankgränssnittet, som visar resultatet för kunden.

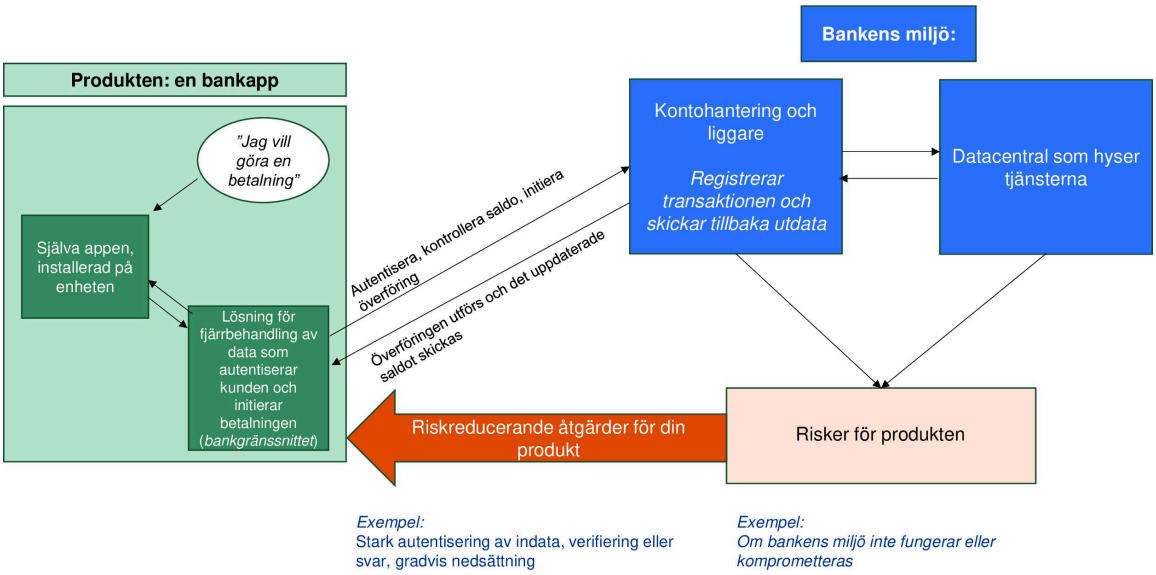
Konsekvenser för lösningen för fjärrbehandling av data:

— Bankgränssnittet är nödvändigt för att appen ska kunna utföra sina funktioner, dvs. autentisera kunden, skicka kundens instruktioner, inklusive betalnings- och överföringsinstruktioner, och returnera den därav följande statusen. Bankgränssnittet är utformat och utvecklat under tillverkarens ansvar. Eftersom svaret på båda de frågor som angavs i tidigare avsnitt är ja, ska bankgränssnittet betraktas som en lösning för fjärrbehandling av data. Den måste därför inkluderas i bedömningen av cybersäkerhetsrisker och i uppfyllandet av de väsentliga kraven för produkten med digitala element som helhet. Den därpå följande behandlingen av en instruktion när den väl har skickats, i synnerhet registreringen av transaktionen i kontohanteringssystemet och systemet med liggaren, betalningen och clearingen, utförs av system med vilka appen inte samverkar direkt och utgör därför inte en lösning för fjärrbehandling av data.

— Kontohanteringssystemet och systemet med liggaren betraktas inte som lösningar för fjärrbehandling av data i bankapplikationen. Appen samverkar inte direkt med dem (utan samverkar i stället med bankgränssnittet, som i sin tur är beroende av dessa system). Även om deras tillgänglighet kan vara nödvändig för att en funktion ska kunna slutföras, omfattar cyberresiliensförordningen endast de delar av systemet som samverkar direkt med produkten med digitala element. De faller därför utanför definitionen av lösning för fjärrbehandling av data enligt cyberresiliensförordningen. Dessa system är dock fortsatt externa beroenden som kan ge upphov till betydande cybersäkerhetsrisker för produkten med digitala element. Om systemet med liggaren komprometteras skulle en angripare till exempel kunna påverka de transaktionsresultat som senare visas i applikationen. Tillverkaren måste därför identifiera och bedöma dessa risker som en del av bedömningen av cybersäkerhetsrisker och minska dem genom åtgärder på produktnivå, såsom en stark autentisering av backend-gränssnitt, integritetsskydd för transaktionsdata, säkra kommunikationskanaler och verifiering av de svar som tas emot av appen.

Figur 10

Stiliserad representation av en bankapp som är beroende av lösningar för fjärrbehandling av data



SaaS-lösning från tredje part för kundsupport:

— Den finansiella enheten integrerar i sin app en chattlösning för kundsupport som har utvecklats av och drivs av en tredjepartsleverantör. Tredjepartsleverantören har skrivit chattserverkoden, byggt användargränssnittet och driver den infrastruktur där chatten körs (dvs. en SaaS-modell).

— När en kund initierar en supportbegäran ansluter appen kunden till tredjepartstjänsten, upprättar en chattsession och hanterar meddelandeflödet, utan att ge tredjeparten tillgång till de grundläggande banksystemen.

Konsekvenser för lösningen för fjärrbehandling av data:

— Chattlösningen för support är nödvändig för att produkten med digitala element ska kunna utföra en av sina funktioner, men den är inte utformad och utvecklad av den finansiella enheten eller under dess ansvar. Den utgör därför inte en lösning för fjärrbehandling av data. Den bör dock behandlas som en tredjeparts-komponent. Att förlita sig på en tredjepartstjänst kan medföra cybersäkerhetsrisker för bankapplikationen, till exempel skulle en angripare kunna använda chattkanalen och utge sig för att vara banken eller använda den för att ge användare skadligt innehåll. Den finansiella enheten måste beakta dessa risker i sin bedömning av cybersäkerhetsrisker och begränsa dem genom åtgärder på produktnivå, såsom att isolera chattfunktionen från bankapplikationens kärnfunktioner, kontrollera dataflödena och validera innehållet. Tillbörlig aktsamhet i fråga om SaaS-lösningen bör också iakttas.

8.3.2 *Smart termostat*

En smart termostat gör det möjligt för användare att kontrollera temperaturen i sina hem via en mobilapplikation. Mobilapplikationen och den smarta termostaten är beroende av fjärrbehandling av data för att utbyta data (t.ex. en begäran om att höja temperaturen) och lagra data (t.ex. användarinställningar). Dessa funktioner utvecklades och utformades under tillverkarens ansvar men kördes på en underliggande fysisk och virtuell infrastruktur som tillhandahölls av en tredje part (IaaS-lösning från tredje part).

Eftersom den smarta termostaten inte skulle kunna utföra sina smarta funktioner utan denna fjärrdatabehandling, skulle avsaknaden av denna hindra produkten med digitala element från att utföra en eller flera av sina funktioner. Dessutom utvecklades och utformades programvaran under ansvar av tillverkaren av den smarta termostaten. Fjärrbehandlingen av data räknas därför som en lösning för fjärrbehandling av data i den mening som avses i cyberresiliensförordningen.

För att kunna uppfylla kraven i cyberresiliensförordningen måste tillverkaren av den smarta termostaten dokumentera lösningen för fjärrbehandling av data såväl som beroendet av en IaaS-lösning från tredje part i den tekniska dokumentationen av produkten med digitala element, inklusive uppgifter om den avtalade tjänsten. Tillverkaren måste beakta dessa aspekter i riskbedömningen, som inbegriper det avsedda syftet och den rimligen förutsebara användningen av produkten med digitala element. Tillverkaren tillämpar de väsentliga kraven enligt cyberresiliensförordningen baserat på riskerna med lösningen för fjärrbehandling av data. För IaaS-lösningen från tredje part måste tillverkaren säkerställa att de säkerhetsåtgärder som tillhandahålls av tredjepartsleverantören är lämpliga, och/eller vidta relevanta åtgärder med avseende på infrastrukturen. När det gäller det förstnämnda kan tillverkaren t.ex. begära bevis för att skyldigheterna i NIS 2-direktivet har uppfyllts.

8.3.3 *Läsplatta*

Tillverkaren av en programvara för läsplattor använder en SaaS-lagringstjänst från tredje part för att lagra elektroniska böcker som köpts av kunder och göra det möjligt för dem att få tillgång till sina böcker. Avsaknaden av denna lagringstjänst skulle hindra produkten med digitala element från att utföra en av sina funktioner, men SaaS-lagringstjänsten från tredje part har inte utvecklats av eller under tillverkarens ansvar – leverantören av SaaS-lösningen gör den tillgänglig för kunder för alla användningsfall.

SaaS-lagringstjänsten uppfyller inte definitionen av en lösning för fjärrbehandling av data. Tillverkaren av programvaran för läsplattor är dock beroende av denna externa tjänst för att produkten med digitala element ska fungera, och måste därför ta hänsyn till de därtill hörande riskerna i sin bedömning av cybersäkerhetsrisker. Tillverkaren av programvaran för läsplattor bör behandla SaaS-lösningen som en komponent. Tillverkaren måste genomföra lämpliga säkerhetsåtgärder på produktnivå, såsom säker autentisering, kryptering och integritetsskydd för kommunikation med lagringstjänsten. Tillbörlig aktsamhet vid val och integrering av SaaS-leverantören kommer också att vara till stöd för tillverkarens skyldigheter, så att produkten med digitala element som helhet kan uppfylla de väsentliga kraven.

8.3.4 *Industrirobot*

En industrirobot har till uppgift att plocka upp delar. Roboten skickar information som samlats in via kameror till en fjärrtjänst som har utformats och utvecklats av tillverkaren. Denna tjänst körs på en underliggande fysisk och virtuell infrastruktur som tillhandahålls av en tredjepartsleverantör av tjänster (IaaS-lösning från tredje part). Molntjänsten beräknar positionen för en del baserat på sändningen från kameran och skickar kommandon tillbaka till roboten om att plocka upp delarna.

Avsaknaden av denna databehandling skulle hindra industriroboten från att plocka upp delar och därmed från att utföra en av sina funktioner. Dessutom har den programvara som körs på infrastrukturen utformats och utvecklats av tillverkaren. Den programvara som har utformats och utvecklats av tillverkaren uppfyller definitionen av en lösning för fjärrbehandling av data.

Tillverkaren av industriroboten måste dokumentera lösningen för fjärrbehandling av data såväl som beroendet av IaaS-lösningen från tredje part i den tekniska dokumentationen för produkten med digitala element (inklusive uppgifter om den avtalade tjänsten). Tillverkaren måste också beakta dessa aspekter i riskbedömningen, som inbegriper det avsedda syftet och den rimligen förutsebara användningen av produkten med digitala element. Tillverkaren tillämpar de väsentliga kraven enligt cyberresiliensförordningen på produkten med digitala element, inklusive dess lösning för fjärrbehandling av data, baserat på riskerna. Tillbörlig aktsamhet vid valet av IaaS-leverantör kommer också att vara till stöd för tillverkarens skyldigheter. Tillverkaren kan till exempel begära bevis för att skyldigheterna enligt NIS 2-direktivet har uppfyllts.

8.3.5 *Mobilnät*

En smarttelefon är beroende av ett 5G-nätverk för att tillhandahålla internetuppkoppling, telefonsamtal och meddelanden till sina användare (mobil uppkoppling). Mobilnätet utvecklas och utformas av teleoperatörer. Nätet består av små celler och basstationer samt annan nätutrustning.

Produkten med digitala element bör kunna ansluta till ett nät på rätt sätt – detta är en av dess funktioner. Huruvida nätverket är i drift eller inte är dock inte relevant för att fastställa om produkten med digitala element fungerar korrekt. Nätverket är endast en kommunikationskanal och är inte nödvändigt för att produkten med digitala element ska kunna utföra sin funktion att ”ansluta till ett nätverk på rätt sätt”. En ethernetkabel, router eller wifi-signal betraktas inte heller som databehandling vars avsaknad skulle innebära att produkten med digitala element inte kan utföra en av sina funktioner, utan snarare som en möjliggörande faktor för kommunikation/anslutning.

Följaktligen uppfyller mobilnätet inte definitionen av lösning för fjärrbehandling av data. Nätverket bör inte betraktas som en tredjepartskomponent, eftersom det inte finns någon programvara som är integrerad i produkten med digitala element, utan produkten i stället endast är beroende av detta nätverk. Det är därför inte nödvändigt för tillverkaren att utöva skyldigheten att visa tillbörlig aktsamhet gentemot nätleverantören.

9. **YTTERLIGARE ELEMENT**

9.1 **Rapporteringsskyldigheter**

209. Enligt artikel 14.1 och 14.3 i cyberresiliensförordningen ska en tillverkare samtidigt underrätta den CSIRT-enhet som utsetts till samordnare och Enisa om i) varje aktivt utnyttjad sårbarhet som ingår i dennes produkt med digitala element och som denne får kännedom om, och ii) varje allvarlig incident som påverkar säkerheten hos produkten med digitala element och som denne får kännedom om.

210. I enlighet med artiklarna 69.3 och 71.2 andra meningen tillämpas de skyldigheter som fastställs i artikel 14 från och med den 11 september 2026 på alla produkter med digitala element som omfattas av cyberresiliensförordningens tillämpningsområde, inbegripet de produkter med digitala element som släppts ut på marknaden före den 11 december 2027. Till skillnad från kraven på sårbarhetshantering, som endast gäller under stödperioden för en produkt, fortsätter rapporteringsskyldigheterna att gälla även efter det att en produkt med digitala element inte längre stöds. Om en produkt med digitala element släpptes ut på marknaden före den 11 december 2027, eller om dess stödperiod har löpt ut, behöver tillverkaren inte uppfylla de skyldigheter för sårbarhetshantering som anges i del II i bilaga I.

211. Man bör dock komma ihåg att skyldigheten att anmäla sådana händelser gäller när tillverkaren väl får kännedom om att en sårbarhet aktivt utnyttjas eller att en allvarlig incident har inträffat och har lett till att säkerheten för produkten med digitala element äventyras. Vägledning om när en tillverkare anses ha fått kännedom bör därför hjälpa tillverkarna att fastställa när de tillämpliga tidsfristerna för rapportering börjar.

212. Tillverkarna kan omfattas av jämförbara rapporteringsskyldigheter enligt olika EU-rättsakter. För att säkerställa att begreppet ”få kännedom” tolkas konsekvent och för att främja tillverkarnas efterlevnad av dessa skyldigheter, har denna vägledning anpassats till skäl 31 i kommissionens genomförandeförordning (EU) 2024/2690 och avsnitt II.A i riktlinjerna 9/2022 om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen.

213. I vissa fall kommer en tillverkare att upptäcka en misstänkt händelse, eller så kommer en tredje part, såsom en person, en kund, en enhet, en myndighet, en medieorganisation eller annan källa, att uppmärksamma tillverkaren på en potentiell incident eller sårbarhet. I sådana fall bör tillverkaren omedelbart bedöma den misstänkta händelsen för att avgöra om den utgör en aktivt utnyttjad sårbarhet eller en allvarlig incident som påverkar säkerheten för produkten med digitala element. Tillverkaren ska anses ha fått kännedom när den, efter en inledande bedömning, med rimlig grad av säkerhet kan fastställa att i) en sårbarhet som ingår i dennes produkt med digitala element utnyttjas aktivt, eller ii) en allvarlig incident har inträffat och har lett till att säkerheten för dennes produkt med digitala element äventyras.

214. Den tidpunkt då en tillverkare kan anses ha fått kännedom beror därför på omständigheterna kring den specifika aktivt utnyttjade sårbarheten eller allvarliga incidenten. I vissa fall kommer det redan från början att stå relativt klart att en sårbarhet håller på att utnyttjas aktivt eller att en allvarlig incident påverkar säkerheten för en produkt med digitala element. I andra fall kan det ta lite tid att fastställa om en produkt med digitala element påverkas av en sårbarhet och om denna sårbarhet håller på att utnyttjas av en illvillig aktör, eller om en incident påverkar säkerheten för en produkt med digitala element. Tonvikten bör dock ligga på snabba åtgärder för att genomföra den inledande bedömningen i syfte att avgöra om dessa villkor verkligen är uppfyllda, i synnerhet om sårbarheten kan utgöra en betydande risk, och att i så fall vidta korrigerande åtgärder och göra en anmälan i enlighet med cyberresiliensförordningen.

215. Dessutom kräver rapporteringsskyldigheternas struktur att tillverkarna steg för steg uppdaterar sina anmälningar, allteftersom deras interna utredningar går framåt och de får mer ingående kunskap om den aktivt utnyttjade sårbarheten eller incidenten. Tillverkarna är i synnerhet skyldiga att utan onödigt dröjsmål, och under alla omständigheter senast 24 timmar efter det att de har fått kännedom, lämna in en tidig varning som innehåller begränsad information. Ytterligare uppgifter behövs därefter som en del av den anmälan som ska lämnas in utan onödigt dröjsmål och under alla omständigheter inom 72 timmar efter det att de har fått kännedom (*72-timmarsanmälan*). Den fullständiga rapporten måste lämnas in inom 14 dagar efter det att en korrigerande eller begränsande åtgärd finns tillgänglig för aktivt utnyttjade sårbarheter, eller inom en månad efter det att 72-timmarsanmälan gjorts för allvarliga incidenter.

216. Såsom angavs i avsnitt *3.3.1 Bibehållet stöd och säkerställande av bärkraften hos* en programvara med fri och öppen källkod måste även förvaltare av programvara med öppen källkod rapportera om aktivt utnyttjade sårbarheter i enlighet med artikel 24.3 ([30]). Denna skyldighet gäller efter att ha fått kännedom om en aktivt utnyttjad sårbarhet och inte bara när det finns en sårbarhet i kodbasen hos en programvara med fri och öppen källkod för vilken den enheten är förvaltare. Eftersom komponenterna för programvaror med fri och öppen källkod vanligtvis integreras i senare led i andra produkter med digitala element, är det sannolikt att en förvaltare i praktiken kommer att få kännedom om ett aktivt utnyttjande via rapporter från tredje part, som identifierar utnyttjande i komponenter för programvaror med fri och öppen källkod som är integrerade i andra produkter med digitala element. Detta kan till exempel vara fallet om en tillverkare av en produkt med digitala element upptäcker ett aktivt utnyttjande av en komponent för programvara med fri och öppen källkod som är integrerad i den egna produkten och rapporterar detta till den komponentens förvaltare, eller när en användare eller en forskare inom informationssäkerhet hittar bevis för utnyttjande av en komponent för programvara med fri och öppen källkod som är integrerad i en produkt med digitala element och rapporterar detta aktiva utnyttjande till komponentens förvaltare.

217. Det bör också tydliggöras att eftersom skyldigheten att rapportera aktivt utnyttjade sårbarheter gäller när tillverkaren får kännedom om ett aktivt utnyttjande, behöver tillverkaren inte rapportera sårbarheter vars aktiva utnyttjande denne redan hade fått kännedom om före den 11 september 2026 (den dag då rapporteringsskyldigheten börjar gälla). Cyberresiliensförordningen kräver därmed inte någon retroaktiv rapportering av sådana sårbarheter. Skyldigheten gäller däremot om tillverkaren hade kännedom om en sårbarhet före den 11 september 2026 men inte kände till något aktivt utnyttjande av denna sårbarhet vid den tidpunkten (antingen på grund av att det ännu inte hade förekommit något utnyttjande, eller på grund av att tillverkaren inte hade fått kännedom om detta). Om det efter den 11 september 2026 sker ett aktivt utnyttjande eller om tillverkaren får kännedom om detta anses sårbarheten vara ett aktivt utnyttjande som omfattas av rapporteringsskyldigheten.

218. På samma sätt behöver en tillverkare endast rapportera om aktivt utnyttjade sårbarheter i sin produkt med digitala element. Om en produkt med digitala element innehåller en aktivt utnyttjad sårbarhet som härrör från en tredjepartskomponent ska tillverkaren av produkten med digitala element anmäla den aktivt utnyttjade sårbarheten. Om en tillverkare å andra sidan har kännedom om att en tredjepartskomponent innehåller en sårbarhet, men att den sårbarheten antingen i) inte kan utnyttjas i tillverkarens produkt med digitala element (t.ex. på grund av att den sårbara koden inte kan nås) eller ii) inte har utnyttjats i tillverkarens produkt med digitala element, kan den sårbarheten inte betraktas som en aktivt utnyttjad sårbarhet som ingår i tillverkarens produkt med digitala element, och därför omfattas den inte av obligatorisk rapportering för den tillverkaren. Den tillverkaren kan fortfarande anmäla sårbarheten på frivillig basis, i enlighet med artikel 15 i cyberresiliensförordningen. Tillverkaren ska också uppfylla kraven rörande sårbarhetshantering i del II i bilaga I till cyberresiliensförordningen, samt anmäla sårbarheten till den person eller enhet som tillverkar eller underhåller komponenten, i enlighet med artikel 13.6 och som förklaras närmare i avsnitt *9.2.1 Rapportering till tidigare led och delning* av säkerhetsåtgärder.

([30]) I den mån förvaltaren deltar i utvecklingen av en produkt med digitala element.

219. Efter att ha fått kännedom om en aktivt utnyttjad sårbarhet eller allvarlig incident måste tillverkarna också, i enlighet med artikel 14.8, informera de berörda användarna och, i förekommande fall, alla användare. Om tillverkarna underlåter att skyndsamt göra detta får de CSIRT-enheter som mottog anmälan förse användarna med denna information om detta anses vara proportionerligt och nödvändigt för att förhindra eller begränsa sårbarhetens eller incidentens inverkan.

220. I enlighet med den riskbaserade metoden enligt cyberresiliensförordningen ska skyldigheten att informera användare enligt artikel 14.8 tillämpas på ett riskbaserat och proportionellt sätt. I synnerhet innebär tillhandahållandet av information om en aktivt utnyttjad sårbarhet eller allvarlig incident inte att denna information måste offentliggöras eller utlämnas på ett urskillningslöst sätt. Om så är lämpligt, och mot bakgrund av arten av produkt med digitala element, de användare som påverkas och sårbarhetens eller incidentens potentiella inverkan, får tillverkarna begränsa utlämnandet av detaljerad information till de relevanta användarna eller berörda kunderna. Detta gäller i synnerhet för produkter med digitala element som används i känsliga eller väsentliga miljöer, där offentliggörandet av tekniska detaljer i sig skulle kunna öka cybersäkerhetsriskerna eller underlätta ett ytterligare utnyttjande.

221. När sårbarheten väl har åtgärdats eller avhjälpts på lämpligt sätt kan ett mer omfattande offentliggörande vara lämpligt. Detta skulle till exempel vara fallet om utlämnandet bidrar till att öka den allmänna medvetenheten eller gör det möjligt för användarna att kontrollera att deras produkter med digitala element inte längre påverkas. I sådana fall bör detaljnivån och tidpunkten för ett mer omfattande offentliggörande förbli proportionerlig och ta hänsyn till de kvarstående riskerna för utnyttjande, arten av produkt med digitala element och de berörda användarnas intressen. Dessutom krävs i del II punkt 4 i bilaga I att tillverkarna offentliggör information om åtgärdade sårbarheter när en säkerhetsuppdatering väl har gjorts tillgänglig.

9.2 **Sårbarhetshantering**

9.2.1 *Rapportering till tidigare led och delning av säkerhetsåtgärder*

222. Enligt artikel 13.6 i cyberresiliensförordningen ska tillverkare rapportera sårbarheter i en integrerad komponent till den person eller entitet som tillverkar eller underhåller den komponenten (”rapportering till tidigare led”).

223. Tillverkare behöver endast rapportera till tidigare led med avseende på den version av komponenten som de integrerar. Om den person eller entitet som tillverkar eller underhåller komponenten har inrättat säkerhetspolicyer, förfaranden för samordnad delgivning av information om sårbarheter eller särskilda kanaler för rapportering av sårbarheter, bör tillverkarna rapportera i enlighet med dessa, särskilt om ett förhastat offentliggörande av oåtgärdade sårbarheter skulle kunna medföra ökade cybersäkerhetsrisker. För att minska bördan för den som sköter underhållet i tidigare led, i synnerhet när det gäller projekt med öppen källkod, behöver tillverkarna inte rapportera till tidigare led om de kan bekräfta att den person eller entitet som tillverkar eller underhåller en komponent har kännedom om att det finns en sårbarhet. Tillverkarna uppmanas att vidta rimliga åtgärder för att undvika att dubbla rapporter lämnas in, till exempel genom att kontrollera allmänt tillgängliga sårbarhetsdatabaser, projektspecifika säkerhetsrådgivningar eller etablerade problemspårare innan de rapporterar till tidigare led.

224. Tillverkarna är endast skyldiga att rapportera till tidigare led om sårbarheter som finns i den integrerade komponenten i sig, och inte om sårbarheter som finns till följd av integreringen mellan komponenten och annan kod som utvecklats av tillverkaren eller integreringen av andra komponenter. Det kan dock finnas situationer där integreringen av en komponent för en särskild produkt med digitala element avslöjar vissa beteenden, interaktioner eller säkerhetsrelevanta egenskaper hos den komponenten som inte var uppenbara, eller inte lätt gick att identifiera, när denna betraktades separat. I sådana fall uppmuntras tillverkarna att vidarebefordra denna information till den person eller enhet som tillverkar eller underhåller komponenten, i syfte att främja god praxis för sårbarhetshantering som syftar till att underlätta ett effektivt åtgärdande och förbättra komponentekosystemets säkerhet totalt sett.

225. Avslutningsvis behöver tillverkarna inte heller rapportera sårbarheten till tidigare led om komponenten inte längre har någon som underhåller den eller om tillverkaren inte längre förlitar sig på den som ursprungligen underhöll komponenten för nya versioner eller säkerhetskorrigeringar. I sådana fall uppmuntras dock tillverkaren att informera användarna av den komponenten på rimliga alternativa sätt, t.ex. genom befintliga mekanismer inom en nätgemenskap för öppen källkod (t.ex. sändlistor eller utfärdande av serviceordrar) eller genom offentlig dokumentering av sårbarheter.

226. Enligt artikel 13.6 måste dessutom tillverkare som har utvecklat en ändring av programvara i syfte att åtgärda en sårbarhet hos en integrerad komponent dela denna programvaruändring (”säkerhetsåtgärd”) med den person eller enhet som tillverkar eller underhåller komponenten (”dela med tidigare led”).

227. Om tillverkarna är skyldiga att dela en säkerhetsåtgärd enligt artikel 13.6 bör denna säkerhetsåtgärd, när så är lämpligt, tillhandahållas i ett maskinläsbart format på ett sätt som lätt kan verifieras och, i förekommande fall, integreras av den person eller enhet som tillverkar eller underhåller komponenten. Om komponenten är en komponent med fri och öppen källkod bör säkerhetsåtgärden delas på ett sätt som är förenligt med komponentens licens, t.ex. genom att dela den inom ramen för samma licens eller inom ramen för en licens som gör det möjligt för den som underhåller komponenten att distribuera säkerhetsåtgärden inom ramen för sin egen licens. Om den som underhåller komponenten har riktlinjer för hur säkerhetsåtgärder ska delas bör tillverkaren följa dessa riktlinjer.

228. Enligt cyberresiliensförordningen är tillverkarna dock inte skyldiga att se till att deras säkerhetsåtgärder nödvändigtvis godtas av den person eller enhet som tillverkar eller underhåller komponenten. De är inte heller skyldiga att se till att dessa korrigeringar nödvändigtvis integreras i komponentens koddatabas, till exempel om den som underhåller eventuellt föredrar ett annat alternativ för att åtgärda problemet. På samma sätt behöver tillverkarna inte godta ett förslag till säkerhetsåtgärd som har utvecklats av den som underhåller komponenten, och de kan föredra att avhjälpa problemet på andra lämpliga sätt.

229. I vissa fall kan den person eller enhet som tillverkar eller underhåller komponenten redan ha tillhandahållit en säkerhetskorrigering som åtgärdar sårbarheten, men en tillverkare tillämpar en annan begränsningsstrategi (t.ex. genom att ändra en annan konfiguration). I sådana fall kräver inte cyberresiliensförordningen att tillverkaren delar ändringen av en annan del av systemet med tidigare led. Tillverkaren uppmanas dock att göra detta när det kan stödja den person eller enhet som underhåller komponenten.

9.2.2 *Kända sårbarheter som kan utnyttjas*

230. Ett av de väsentliga kraven i del I i bilaga I till cyberresiliensförordningen föreskriver att produkter med digitala element, på grundval av den bedömning av cybersäkerhetsrisker som avses i artikel 13.2 och i tillämpliga fall, måste tillhandahållas på marknaden utan kända sårbarheter som kan utnyttjas.

231. I artikel 3.41 definieras ”sårbarhet som kan utnyttjas” som ”en sårbarhet som kan utnyttjas effektivt av en motståndare under praktiska operativa förhållanden”. Alla sårbarheter kan inte utnyttjas under praktiska driftsförhållanden, och vissa sårbarheter kan endast utnyttjas under teoretiska förhållanden (t.ex. i ett labb eller i en simulering) och/eller inte under de förhållanden som skulle uppstå i driftsmiljön för en produkt med digitala element.

232. Cyberresiliensförordningen kräver att tillverkarna har lämpliga riktlinjer och förfaranden för att hantera och avhjälpa potentiella sårbarheter som rapporterats av interna eller externa källor (artikel 13.8). Det specificeras dock inte uttryckligen när tillverkaren bör anses ha kännedom om en sårbarhet som kan utnyttjas, något som därmed utlöser skyldigheten att uppfylla detta väsentliga krav vid tidpunkten för utsläppandet på marknaden.

233. En sårbarhet bör betraktas som känd när den förtecknas i relevanta allmänt tillgängliga sårbarhetsdatabaser, såsom den europeiska sårbarhetsdatabas som inrättats genom artikel 12.2 i direktiv (EU) 2022/2555 eller andra välkända sårbarhetsdatabaser.

234. Dessutom kan en sårbarhet också vara känd när tillverkaren har fått kännedom om den via icke-offentlig information, till exempel genom samordnad delgivning från en forskare inom informationssäkerhet eller genom tillverkarens egen interna provning och analys, inbegripet med användning av AI-drivna tjänster. På samma sätt kan en sårbarhet vara känd när den har rapporterats offentligt och på framträdande plats i tillförlitliga mediekanaler, inbegripet specialiserade cybersäkerhetspublikationer eller allmänna massmedier.

235. Enbart det faktum att en sårbarhet rapporteras eller upptäcks innebär dock inte i sig att den kan utnyttjas i praktiken eller tillämpas på den specifika produkten med digitala element. Tillverkaren behöver undersöka den och bekräfta sanningsenligheten hos denna information och tillämpligheten på den egna produkten med digitala element. En begränsad tidsperiod kan därför förflyta mellan den första rapporten om sårbarheten och bekräftelsen av den. Såsom anges i avsnitt *9.1 Rapporteringsskyldigheter*, bör tonvikten ligga på snabba åtgärder för att undersöka och vidta åtgärder.

236. Dessutom gäller skyldigheten för tillverkare att vid tidpunkten för utsläppandet på marknaden uppfylla de väsentliga krav som anges i del I i bilaga I, i enlighet med artikel 13.1. I praktiken kan det vara så att nya sårbarheter som potentiellt kan utnyttjas upptäcks under slutskedet av utvecklingslivscykeln för produkten med digitala element, däribland kort innan den kommer in i distributionskedjan (och därmed släpps ut på marknaden).

237. Eftersom skyldigheten att släppa ut produkter med digitala element på marknaden utan kända sårbarheter som kan utnyttjas är en riskbaserad skyldighet, åligger det tillverkaren att i enlighet med cyberresiliensförordningen fastställa huruvida produkten med digitala element, på grundval av bedömningen av cybersäkerhetsrisker, kan släppas ut på marknaden på ett säkert sätt. I andra fall kan tillverkaren fastställa att en ny sårbarhet som kan ha blivit känd måste åtgärdas innan produkten med digitala element kan släppas ut på marknaden. Vid detta fastställande bör tillverkare ta hänsyn till hur allvarlig sårbarheten är, i vilken grad den kan utnyttjas och dess potentiella konsekvenser, samt de risker som uppstår för produkten med digitala element när den väl används. De kan också ta hänsyn till riskerna med att skjuta upp utgivningen av produkten till dess att sårbarheten har åtgärdats, till exempel eftersom den nya versionen även åtgärdar andra sårbarheter som kan utnyttjas, eller är nödvändig för den fortsatta driften av kritiska system. När en produkt med digitala element väl har släppts ut på marknaden omfattas tillverkaren under alla omständigheter fortfarande av skyldigheten att hantera sårbarheter på ett effektivt sätt och i enlighet med de krav på sårbarhetshantering som anges i del II i bilaga I.

9.2.3 *Effektiva och regelbundna provningar och granskningar*

238. Enligt del II punkt 3 i bilaga I ska tillverkarna tillämpa effektiva och regelbundna provningar och granskningar av produkten med digitala element under hela stödperioden. En tillämpning av regelbundna provningar kräver inte mekanisk upprepning, med fasta intervall, av en oförändrad testkampanj. Det innebär att man regelbundet granskar huruvida ny information, såsom nyligen identifierade hot eller nyligen upptäckta sårbarheter, kräver att de befintliga provningarna uppdateras och att man utför provningar i enlighet med detta.

239. Granskningens frekvens, grundlighet och innehåll bör stå i proportion till cybersäkerhetsriskprofilen för produkten med digitala element, dess utveckling över tid och tillståndet för hotbilden. Om det vid granskningen upptäcks relevant ny information som påverkar provningsuppsättningen bör nya eller modifierade provningar utformas och utföras på produkten för att säkerställa att inga sårbarheter förblir oåtgärdade. Detta kan inbegripa att man på nytt utför befintliga provningar i de fall en ändring av produkten med digitala element gör att sådana typer av provningar är lämpliga, till exempel regressionstestning.

240. Om det vid granskningen inte framkommer någon sådan information behöver inga ytterligare provningar utformas. Andra skyldigheter när det gäller sårbarhetshantering, däribland åtgärdandet och avhjälpandet av sårbarheter i förhållande till de risker som föreligger, gäller fortsatt parallellt med detta.

9.3 **Samspel med annan lagstiftning**

9.3.1 *Förordning (EU) 2019/2144 och förordning (EU) nr 168/2013*

241. I artikel 2.2 c i cyberresiliensförordningen fastställs att förordningen inte är tillämplig på produkter med digitala element som omfattas av förordning (EU) 2019/2144. Förordning (EU) 2019/2144 ska tillämpas på ”fordon av kategorierna M, N och O enligt definitionen i artikel 4 i förordning (EU) 2018/858, och på system, komponenter och separata tekniska enheter som konstrueras och tillverkas för sådana fordon”.

242. På samma sätt har produkter med digitala element som omfattas av förordning (EU) nr 168/2013 undantagits från cyberresiliensförordningens tillämpningsområde genom kommissionens delegerade förordning (EU) 2025/1535. Förordning (EU) nr 168/2013 är tillämplig på fordon i kategori L och ”på system, komponenter och separata tekniska enheter, samt på delar och utrustning, som konstruerats och tillverkats för sådana fordon” (artikel 2.1).

243. Fordon som omfattas av dessa föreskrifter omfattas inte av cyberresiliensförordningen. Dessutom krävs ytterligare förtydliganden med avseende på räckvidden på undantaget för system, komponenter, separata tekniska enheter, delar och utrustning (i detta avsnitt benämnda *komponenter*) som utformats och konstruerats för sådana fordon och som betraktas som produkter med digitala element i den mening som avses i cyberresiliensförordningen.

244. Sådana komponenter anses inte omfattas av cyberresiliensförordningen, under förutsättning att de uteslutande har konstruerats och tillverkats för integrering i fordon som omfattas av förordningarna (EU) 2019/2144 och (EU) nr 168/2013. Detta är fallet oavsett om tillverkaren av komponenten säljer den direkt till fordonstillverkaren eller till en annan ekonomisk aktör i fordonsindustrins leveranskedja, så länge komponenten är tydligt avsedd och lämplig endast för slutgiltig integrering i dessa fordon.

245. En tillverkare som däremot säljer generiska komponenter som är produkter med digitala element och som kan integreras i olika typer av produkter, och inte enbart i fordon som omfattas av dessa förordningar, omfattas av cyberresiliensförordningen.

246. Bedömningen av huruvida en komponent har släppts ut på marknaden i den mening som avses i cyberresiliensförordningen måste bygga på de objektiva villkor under vilka den tillhandahålls. Om en tillverkare erbjuder en komponent som inte uteslutande lämpar sig för slutgiltig integrering i dessa fordon via distributionskanaler som är öppna för kunder utanför fordonsindustrins leveranskedja, till exempel allmänna försäljningsställen eller onlineförsäljningskanaler som tar emot beställningar från allmänheten, omfattas denna komponent av cyberresiliensförordningen, oavsett vad som anges om dess avsedda användning. Under sådana omständigheter kan komponenten inte anses vara konstruerad och tillverkad uteslutande för integrering i fordon som omfattas av förordningarna (EU) 2019/2144 och (EU) nr 168/2013, och tillverkaren måste uppfylla kraven i cyberresiliensförordningen. Däremot kan användningen av begränsade B2B-distributionskanaler som begränsas till fordonsindustrins leveranskedja tyda på att komponenten är konstruerad och tillverkad uteslutande för sådan integrering.

9.3.2 *EU-typkontrollintygens giltighet (artikel 69.1)*

247. Enligt artikel 69.1 i cyberresiliensförordningen ska ”EU-typkontrollintyg och beslut om godkännande som utfärdats avseende cybersäkerhetskrav för produkter med digitala element som omfattas av annan unionsharmoniseringslagstiftning än denna förordning [...] fortsätta att gälla till och med den 11 juni 2028, såvida de inte löper ut före den dagen, eller något annat anges i sådan annan unionsharmoniseringslagstiftning, i vilket fall de förblir giltiga enligt den lagstiftningen”.

248. Den fortsatta giltigheten av sådana intyg och beslut om godkännande bör tolkas som att de begränsas till de cybersäkerhetsrisker och motsvarande krav som omfattas av den unionsharmoniseringslagstiftning på grundval av vilken de utfärdades. För dessa risker är tillverkarna inte skyldiga att ompröva eller på nytt demonstrera efterlevnaden enbart för tillämpning av cyberresiliensförordningen under den giltighetsperiod som avses i artikel 69.1 för de produkter med digitala element som de avser att släppa ut på marknaden från och med den 11 december 2027 till och med den 11 juni 2028 ([31]). Detta gäller för intyg och beslut om godkännande som utfärdats i de fall då tillverkaren enligt den tillämpliga unionsharmoniseringslagstiftningen ska utföra bedömningen av överensstämmelse via ett anmält organ samt i de fall då tillverkaren frivilligt har valt att göra detta.

249. Om det finns ett giltigt intyg eller beslut om godkännande enligt annan harmoniserad unionslagstiftning är tillverkarna därmed inte undantagna från att genomföra en omfattande bedömning av cybersäkerhetsrisker enligt cyberresiliensförordningen (eller från andra skyldigheter enligt denna). Den gör det i stället möjligt för dem att förlita sig på befintliga certifieringar som bevis på efterlevnad av deras förfarande för bedömning av överensstämmelse, i den mån motsvarande cybersäkerhetsrisker redan omfattas. Om intyget eller beslutet om godkännande äger giltighet enligt annan harmoniserad unionslagstiftning som sträcker sig längre än till och med den 11 juni 2028, får tillverkaren enligt cyberresiliensförordningen dock endast förlita sig på ett sådant intyg eller beslut till och med den 11 juni 2028.

250. Om den bedömning av cybersäkerhetsrisker som utförts i enlighet med artikel 13.2 identifierar ytterligare risker som inte omfattas av de cybersäkerhetskrav som ligger till grund för det befintliga intyget eller beslutet om godkännande, är tillverkarna fortsatt ansvariga för att åtgärda dessa risker i enlighet med cyberresiliensförordningen. I sådana fall kräver efterlevnaden att de identifierade luckorna bedöms och minskas, oavsett det befintliga intygets eller beslutets fortsatta giltighet.

251. Detta kan illustreras genom att betänka ett fall där en produkt med digitala element omfattas av de cybersäkerhetskrav som fastställs i kommissionens delegerade förordning (EU) 2022/30 om komplettering av direktiv 2014/53/EU (den delegerade förordningen om direktivet om radioutrustning) och där ett EU-typintyg eller ett beslut om godkännande har utfärdats på grundval av dessa krav. I det fallet förblir intyget eller beslutet giltigt i enlighet med artikel 69.1 för de cybersäkerhetsrisker som omfattas av det intyget och som har att göra med de väsentliga kraven rörande cybersäkerhet i direktiv 2014/53/EU (direktivet om radioutrustning).

252. I sådana fall behöver inte tillverkarna, enligt cyberresiliensförordningen, ompröva eller på nytt påvisa överensstämmelse med avseende på de risker som redan omfattas av dessa intyg, så länge det relevanta intyget eller beslutet om godkännande är giltigt och under alla omständigheter inte efter den 11 juni 2028. Detta inbegriper till exempel cybersäkerhetsrisker rörande nätskydd, skydd av personuppgifter och integritet eller förhindrande av bedrägeri (i den mån dessa risker omfattas av det intyget) som är kopplade till kraven på cybersäkerhet i direktivet om radioutrustning och återspeglas i bedömningen av överensstämmelse.

253. Om den bedömning av cybersäkerhetsrisker som genomförts i enlighet med artikel 13.2 i cyberresiliensförordningen identifierar ytterligare cybersäkerhetsrisker som inte omfattas av dessa intyg är tillverkarna dock fortsatt ansvariga för att hantera dessa risker i enlighet med cyberresiliensförordningen. Detta kan till exempel inbegripa risker rörande processer för sårbarhetshantering, uppgiftsminimering och minskning av attackytan, eller andra produktspecifika cybersäkerhetsaspekter som inte tas upp i dessa intyg eller, i vilket fall som helst, som inte omfattas av de väsentliga kraven rörande cybersäkerhet i direktivet om radioutrustning.

254. Det faktum att det finns ett giltigt EU-typintyg eller godkännandebeslut enligt direktivet om radioutrustning för dess väsentliga krav rörande cybersäkerhet är därför inte i sig ett bevis för ett fullständigt uppfyllande av kraven i cyberresiliensförordningen. Detta gör det i stället möjligt för tillverkarna att förlita sig på det intyget eller beslutet som bevis på efterlevnad för motsvarande risker, samtidigt som det säkerställs att eventuella kvarstående eller nyligen identifierade risker bedöms och minskas i enlighet med cyberresiliensförordningen.

([31]) Produkter med digitala element som släppts ut på marknaden före den 11 december 2027 omfattas av den unionslagstiftning som var tillämplig vid tidpunkten för utsläppandet på marknaden, och om dessa produkter uppfyllde kraven i denna lagstiftning kan de säljas och tas i bruk, såvida de inte från och med den 11 december 2027 genomgår väsentliga ändringar. För begreppet ”utsläppande på marknaden” och ”tillhandahållande på marknaden”, se även avsnitt *2.1 Utsläppande på marknaden* i detta dokument samt kapitel 2 i blåboken.

255. Om en produkt med digitala element omfattas av de cybersäkerhetsrelaterade väsentliga kraven rörande hälsa och säkerhet i förordning (EU) 2023/1230 (maskinförordningen), som är fullt tillämpliga från och med den 20 januari 2027, och om ett EU-typintyg eller ett beslut om godkännande har utfärdats på grundval av dessa krav, förblir detta intyg eller beslut om godkännande likaledes giltigt i enlighet med artikel 69.1 i cyberresiliensförordningen för de cybersäkerhetsrisker som omfattas av maskinförordningen.

256. Detta gäller särskilt cybersäkerhetsaspekter som rör skydd mot korruption samt kontrollsystemens säkerhet och tillförlitlighet, i enlighet med avsnitten 1.1.9 och 1.2.1 i bilaga III till maskinförordningen. Tillverkarna behöver inte enligt cyberresiliensförordningen ompröva eller på nytt påvisa överensstämmelse för dessa risker så länge som det relevanta intyget eller beslutet om godkännande är giltigt och under alla omständigheter inte efter den 11 juni 2028. Detta gäller i den mån som dessa risker har åtgärdats som en del av bedömningen av överensstämmelse inom ramen för maskinförordningen.

257. Precis som med de ovannämnda väsentliga kraven rörande cybersäkerhet i direktivet om radioutrustning, i de fall ytterligare cybersäkerhetsrisker identifieras i den bedömning av cybersäkerhetsrisker som utförs i enlighet med artikel 13.2 i cyberresiliensförordningen vilka inte omfattas av det relevanta intyg som utfärdats i enlighet med maskinförordningen och som har att göra med cybersäkerhetskraven i den förordningen, är tillverkarna fortsatt ansvariga för att åtgärda dessa risker i enlighet med cyberresiliensförordningen.