C/2026/6013

2026.11.17.

A BIZOTTSÁG KÖZLEMÉNYE

A Bizottság iránymutatása az (EU) 2024/2847 rendelet (a kiberrezilienciáról szóló rendelet) alkalmazásáról

(C/2026/6013)

Tartalom

Oldal

1. BEVEZETÉS ... 3
   1.1. A kiberrezilienciáról szóló rendelet ... 3
   1.2. Az iránymutatás célja ... 3
2. HATÁLY ... 4
   2.1. Forgalomba hozatal ... 4
   2.2. A szoftver mint digitális elemeket tartalmazó termék ... 5
   2.3. Számítógépes kód ... 6
   2.4. Hardver és szoftver digitális elemeket tartalmazó terméket alkotó kombinációja ... 7
   2.5. Adatkapcsolat ... 8
   2.6. Komplex rendszerek ... 8
   2.7. A kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt tervezett, digitális elemeket tartalmazó termékek ... 9
3. SZABAD ÉS NYÍLT FORRÁSKÓDÚ SZOFTVER ... 11
   3.1. Annak meghatározása, hogy a szabad és nyílt forráskódú szoftverek a szereplő felelősségi körébe tartoznak-e ... 12
   3.2. Annak meghatározása, hogy a szabad és nyílt forráskódú szoftver az uniós piacon forgalomba hozott-e 13
      3.2.1. Ár felszámítása ... 13
      3.2.2. Egyéb szolgáltatások monetizálása vagy személyes adatok feldolgozásának előírása ... 13
      3.2.3. Támogatási szolgáltatások ... 14
      3.2.4. Adományok ... 15
      3.2.5. A szabad és nyílt forráskódú szoftver finanszírozása ... 15
      3.2.6. Nonprofit célok elérésére létrehozott nonprofit szervezetek ... 16
      3.2.7. Más gyártók általi integráció ... 16
   3.3. A nyílt forráskódú szoftverek támogatói ... 16
      3.3.1. A szabad és nyílt forráskódú szoftver tartós támogatása és életképességének biztosítása ... 17
   3.4. Közreműködők és továbbfelhasználás ... 18
   3.5. Szemléltető forgatókönyvek ... 19
4. JELENTŐS MÓDOSÍTÁSOK ÉS TARTALÉK ALKATRÉSZEK ... 21
   4.1. Fizikai javítások ... 22
   4.2. Tartalék alkatrészek ... 23
   4.3. Szoftverfrissítések mint jelentős módosítások ... 24

4.4. A jelentős módosítás következményei 27
4.4.1. Az eredeti gyártótól eltérő személy által végrehajtott jelentős módosítások 28
4.4.2. Az eredeti gyártó által végrehajtott jelentős módosítások 29
5. TÁMOGATÁSI IDŐSZAK 29
5.1. Jelentős módosítások és a támogatási időszak 31
6. DIGITÁLIS ELEMEKET TARTALMAZÓ FONTOS ÉS KRITIKUS FONTOSSÁGÚ TERMÉKEK 32
6.1. Alapvető funkciók 33
6.2. A digitális elemeket tartalmazó fontos és kritikus fontosságú termékek megfelelőségértékelése 36
6.3. A megfelelőség vélelmét érintő szempontok 38
7. A DIGITÁLIS ELEMEKET TARTALMAZÓ TERMÉKEK ÉS AZ ALKOTÓELEMEK KIBERBIZTONSÁGI KOCKÁZATÉRTÉKELÉSE ÉS INTEGRÁLÁSA 41
7.1. A kiberbiztonsági kockázatok értékeléséről és kezeléséről 41
7.2. A digitális elemeket tartalmazó termékeknek a kockázatok alapján megfelelő szintű kiberbiztonságot biztosító tervezéséről, fejlesztéséről és gyártásáról 42
7.3. A külső függőségekkel és az integrált alkotóelemekkel kapcsolatos kockázatértékelés és kellő gondosság 42
7.4. A kockázatértékelések és a megfelelőségi dokumentáció újrafelhasználása digitális elemeket tartalmazó termékcsaládok esetében 44
8. TÁVOLI ADATKEZELÉS 44
8.1. Mi minősül távoli adatkezelési megoldásnak a digitális elemeket tartalmazó termékek esetében? 45
8.1.1. A „távolról” fogalma 46
8.1.2. Az adatkezelés hiánya megakadályozná-e a digitális elemeket tartalmazó termék valamely funkciójának ellátását? 46
8.1.3. A szoftvert a gyártó tervezte és fejlesztette ki, vagy azt a gyártó felelőssége mellett tervezték és fejlesztették ki? 47
8.2. A távoli adatkezelési megoldások gyakorlati és technikai vonatkozásai, a harmadik fél által nyújtott megoldások igénybevétele 49
8.3. A távoli adatkezelési megoldások felhasználási esetei 50
8.3.1. Mobilbanki alkalmazás 51
8.3.2. Intelligens termosztát 52
8.3.3. E-olvasó 53
8.3.4. Ipari robot 53
8.3.5. Mobilhálózat 53
9. TOVÁBBI ELEMEK 54
9.1. Jelentéstételi kötelezettségek 54
9.2. Sérülékenységek kezelése 56
9.2.1. Upstream jelentéstétel és a biztonsági javítások megosztása 56
9.2.2. Ismert kihasználható sérülékenységek 57
9.2.3. Hatékony és rendszeres tesztelés és felülvizsgálat 58
9.3. Egyéb jogszabályokkal való kölcsönhatás 59
9.3.1. Az (EU) 2019/2144 rendelet és a 168/2013/EU rendelet 59
9.3.2. Az EU-típusvizsgálati tanúsítványok érvényessége (69. cikk (1) bekezdés) 59

1. **BEVEZETÉS**

1.1. **A kiberrezilienciáról szóló rendelet**

1. Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) ([1]) 2024. december 10-én lépett hatályba. A rendelet célja, hogy megerősítse az Unió kiberbiztonsággal kapcsolatos megközelítését, uniós szinten kezelje a kiberrezilienciát, valamint a digitális elemeket tartalmazó termékek uniós piacon történő forgalomba hozatalára és életciklusára vonatkozó alapvető kiberbiztonsági követelmények egységes szabályozási keretének meghatározása révén javítsa a belső piac működését.

2. A kiberrezilienciáról szóló rendelet az új uniós jogszabályi keretre épül, amely a termékek forgalmazása tekintetében az akkreditálás és piacfelügyelet előírásainak megállapításáról és a 339/93/EGK rendelet hatályon kívül helyezéséről szóló, 2008. július 9-i 765/2008/EK európai parlamenti és tanácsi rendeletből, valamint a termékek forgalomba hozatalának közös keretrendszeréről, valamint a 93/465/EGK tanácsi határozat hatályon kívül helyezéséről szóló, 2008. július 9-i 768/2008/EK európai parlamenti és tanácsi határozatból áll ([2]).

3. A piacfelügyeletet és a végrehajtást a nemzeti piacfelügyeleti hatóságok végzik. A kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek a piacfelügyeletről és a termékek megfelelőségéről, valamint a 2004/42/EK irányelv, továbbá a 765/2008/EK és a 305/2011/EU rendelet módosításáról szóló, 2019. június 20-i (EU) 2019/1020 európai parlamenti és tanácsi rendelet hatálya alá tartoznak. A Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) támogatja a gazdasági szereplőket és a tagállamokat a kiberrezilienciáról szóló rendelet alkalmazásában.

1.2. **Az iránymutatás célja**

4. A kiberrezilienciáról szóló rendelet 26. cikkének (1) bekezdése előírja a Bizottság számára, hogy iránymutatás közzétételével segítse a gazdasági szereplőket a rendelet alkalmazásában, különös tekintettel a mikrovállalkozások és a kis- és középvállalkozások (kkv-k) megfelelésének megkönnyítésére. A 26. cikk (2) bekezdése meghatározza azon szempontok minimális körét, amelyekkel az iránymutatásnak foglalkoznia kell. Ezek a következők: i. a kiberrezilienciáról szóló rendelet hatálya (különösen a távoli adatkezelési megoldások, valamint a szabad és nyílt forráskódú szoftverek), ii. a „támogatási időszakok" fogalma, iii. a kiberrezilienciáról szóló rendelet és más uniós jogszabályok közötti kölcsönhatás, és iv. a „jelentős módosítás" fogalma.

5. A Bizottság 2025. december 3-án gyakran ismételt kérdéseket tett közzé, amelyek célja, hogy segítsék a gazdasági szereplőket a kiberrezilienciáról szóló rendelet végrehajtására való felkészülésben ([3]).

6. Ezen iránymutatás célja, hogy segítse a gazdasági szereplőket a kiberrezilienciáról szóló rendeletnek való megfelelésben, továbbá támogassa a piacfelügyeleti hatóságok, a bejelentő hatóságok és a bejelentett szervezetek tevékenységeit, és ezáltal Unió-szerte biztosítsa a rendelet harmonizált végrehajtását. Ennek az iránymutatásnak nem az a célja, hogy a kiberrezilienciáról szóló rendeletet annak teljes terjedelmében lefedje, hanem az, hogy tisztázza egyes kulcsfontosságú rendelkezések indokolását és azok gyakorlati végrehajtásának lehetséges módját. Ez az iránymutatás a kiberrezilienciáról szóló rendeletre vonatkozik, más uniós jogszabályokra nem alkalmazandó.

([1]) HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) A Bizottság 2026. évi munkaprogramja egy „európai termékjogszabály" előterjesztését irányozza elő, amely aktualizálja az új jogszabályi keretet, valamint a piacfelügyeletre és a szabványosításra vonatkozó szabályokat: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52025DC0870.

([3]) A gyakran ismételt kérdések letölthetők a Bizottságnak a kiberrezilienciáról szóló rendelet végrehajtásával foglalkozó honlapjáról, a gyakran ismételt kérdések külön weboldaláról.

7. Ezen iránymutatás elkészítése során széles körű konzultációra került sor az érdekelt felekkel, többek között a digitális elemeket tartalmazó termékek kiberbiztonságával foglalkozó szakértői csoporttal ([4]), valamint egy 2026. március 3. és április 13. között tartott nyilvános konzultáció ([5]) keretében.

8. Ez az iránymutatás nem kötelező a kiberrezilienciáról szóló rendelet hatálya alá tartozó gazdasági vagy egyéb szereplőkre nézve. A kiberrezilienciáról szóló rendeletre vonatkozó hivatalos értelmezést csak az Európai Unió Bírósága adhat. Ennek ellenére a megfelelés támogatása és a rendelet hatékony végrehajtásához való hozzájárulás érdekében ez az iránymutatás meghatározza a kiberrezilienciáról szóló rendelet bizottsági értelmezését. Ezen túlmenően az iránymutatás számos példán szemlélteti az egyes rendelkezések alkalmazását. A példák célja azonban nem az eseti értékelés helyettesítése, amelyre mindig szükség lesz az egyes esetek sajátosságainak figyelembevételéhez.

9. A kiberrezilienciáról szóló rendelet 26. cikkével összhangban a Bizottság fontolóra veheti további iránymutatások kiadását, beleértve a rendelet és más uniós harmonizációs jogszabályok vagy más kapcsolódó uniós jogi aktusok hatálya alá tartozó gyártóknak szóló iránymutatást is. Ez az iránymutatás foglalkozhat például a kiberrezilienciáról szóló rendelet és a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról szóló (EU) 2024/1689 rendelet (MI-rendelet), valamint a pénzügyi ágazat digitális működési rezilienciájáról szóló (EU) 2022/2554 rendelet (DORA) közötti kölcsönhatással kapcsolatos kérdésekkel.

2. **HATÁLY**

2.1. **Forgalomba hozatal**

10. A kiberrezilienciáról szóló rendelet az uniós piacon forgalmazott, digitális elemeket tartalmazó termékekre vonatkozik. A „forgalmazás” a kiberrezilienciáról szóló rendelet 3. cikkének 22. pontjában foglalt meghatározása szerint az uniós piacon valamely, digitális elemeket tartalmazó termék gazdasági tevékenység keretében történő rendelkezésre bocsátása értékesítés vagy használat céljára, akár ellenérték fejében, akár ingyenesen. A 3. cikk 21. pontjával összhangban a digitális elemeket tartalmazó terméket akkor kell forgalomba hozottnak tekinteni, amikor első alkalommal forgalmazzák az uniós piacon.

11. A termékekre vonatkozó uniós szabályozásról szóló, 2022-ben közzétett útmutató (a továbbiakban: kék útmutató) ([6]) legutóbbi kiadásában foglalt iránymutatás megkönnyíti a termékekre vonatkozó uniós szabályok megértését és az új jogszabályi kerethez igazodó különböző ágazati jogi keretekre, köztük a kiberrezilienciáról szóló rendeletre kiterjedő egységes alkalmazását. A kék útmutató szerint a „forgalomba hozatal” és a „forgalmazás” fogalmát úgy kell értelmezni, mint amely „minden egyes termékre vonatkozik, nem pedig egy adott terméktípusra, függetlenül attól, hogy egyedi vagy sorozatgyártású-e” (2.3. szakasz).

12. Az új jogszabályi keret hatálya alá tartozó, digitális elemeket tartalmazó „hagyományosabb” termékek, például a gépek formájában megjelenő hardverek vagy a digitális elemeket tartalmazó rádióberendezések esetében a „forgalomba hozatal” fogalma kialakult, és a kék útmutató további iránymutatást nyújt annak tisztázásához, hogy az ilyen termékek mikor minősülnek forgalomba hozottnak. A kék útmutató 2.12. szakaszában szereplő „összefoglaló példák” további példákkal szolgálnak a „forgalomba hozatal” fogalmára.

13. Tekintettel azonban a digitális elemeket tartalmazó immateriális termékek, például az önálló szoftverek jellegére, további iránymutatásra van szükség arra vonatkozóan, hogy az ilyen, digitális elemeket tartalmazó termékek mikor tekinthetők forgalomba hozottnak. Amint a szoftver gyártási szakasza befejeződött, és a digitális elemeket tartalmazó terméket az uniós piacon a leendő felhasználóknak kínálják, úgy tekinthető, hogy gyártója ugyanazon, digitális elemeket tartalmazó szoftvertermékből több példányt is gyártott, és azokat értékesítés vagy használat céljára rendelkezésre bocsátotta. Valójában a digitális elemeket tartalmazó materiális termékekkel ellentétben az önálló szoftverekre nem vonatkoznak fizikai gyártási vagy készletkorlátozások: a szoftver letöltésre vagy

([4]) A bizottsági szakértői csoportok és más hasonló testületek nyilvántartásában szereplő, a digitális elemeket tartalmazó termékek kiberbiztonságával foglalkozó szakértői csoport.

([5]) Nyilvános konzultáció a kiberrezilienciáról szóló rendeletre vonatkozó bizottsági iránymutatás tervezetéről.

([6]) A Bizottság közleménye – A termékekre vonatkozó uniós szabályozásról szóló 2022. évi útmutató (A kék útmutató), 2022/C 247/01 (HL C 247., 2022.6.29., 1. o.).

értékesítésre való rendelkezésre bocsátásának minden egyes cselekménye új, azonos másolat létrehozását eredményezi a felhasználó számára. Mindaddig, amíg a szoftver e verzióját nem módosítják a kiberrezilienciáról szóló rendeletnek való megfelelést befolyásoló módon, úgy kell tekinteni, hogy az uniós piacon történő forgalomba hozatalra akkor került sor, amikor a terméket első alkalommal kínálták értékesítésre vagy használatra. A digitális elemeket tartalmazó szoftvertermék e verziója későbbi letöltésének vagy értékesítésének lehetőségét ezért olyan esetnek kell tekinteni, amikor ezt a digitális elemeket tartalmazó szoftverterméket forgalmazzák ([7]).

14. Ezért úgy kell tekinteni, hogy egy digitális elemeket tartalmazó önálló szoftverterméket akkor hoztak forgalomba, amikor gyártási szakasza befejeződött, és a szoftvert kereskedelmi tevékenység keretében először bocsátották rendelkezésre értékesítés vagy használat céljára az uniós piacon. Úgy kell tekinteni, hogy a gyártó ugyanazt a digitális elemeket tartalmazó szoftverterméket egyidejűleg több példányban is forgalomba hozta. Ezért, bár ugyanazon szoftver több példánya továbbra is digitális elemeket tartalmazó egyedi termék, azokat egyidejűleg forgalomba hozottnak kell tekinteni, függetlenül attól, hogy az egyes példányok birtokát vagy használati jogát mikor ruházzák át egy másik természetes vagy jogi személyre. Ugyanakkor, ha a gyártó különböző változatokban bocsát rendelkezésre szoftvert, amelyek a bennük foglalt alkotóelemek, konfigurációk vagy engedélyezett funkciók tekintetében eltérnek egymástól (például különböző operációs rendszerekhez készült összeállítások vagy különböző jellemzőkészletekkel rendelkező csomagok), ezek a változatok nem tekinthetők ugyanazon, digitális elemeket tartalmazó szoftvertermék több példányának. Ezért ezeket a forgalomba hozatal céljából különálló, digitális elemeket tartalmazó termékekként kell kezelni.

1. példa: Az „A” vállalkozás az „X” elnevezésű szoftverének 1.0.0 verzióját első alkalommal 2028. január 1-jén bocsátja rendelkezésre a honlapján értékesítés céljára. Ugyanezen a napon az 1. vevő megvásárolja az „X” szoftver 1.0.0 verziójának egy példányát. 2028. január 15-én a 2. vevő is megvásárolja az „X” szoftver 1.0.0 verziójának egy példányát. Az „X” szoftver 1.0.0 verziójának mindkét példánya 2028. január 1-jén forgalomba hozottnak minősül.

15. A szoftverfejlesztés iteratív jellegére tekintettel pontosítani szükséges, hogy a digitális elemeket tartalmazó szoftvertermék későbbi iterációit újonnan forgalomba hozottnak kell tekinteni, ha a kiberrezilienciáról szóló rendelet (41) preambulumbekezdésének megfelelően a már forgalomba hozott, digitális elemeket tartalmazó szoftvertermék „jelentős módosításának” minősülnek. A jelentős módosításnak nem minősülő iterációk tekintetében a gyártónak nem szükséges új megfelelőségértékelési eljárást végeznie, ezért a szoftver forgalomba hozatalának időpontját nem módosítják. A jelentős módosítások fogalmával kapcsolatos további iránymutatásért lásd a 4. szakaszt (*Substantial modifications*).

2. példa: Az „A” vállalkozás az „X” elnevezésű szoftverének 1.0.0 verzióját első alkalommal 2028. január 1-jén bocsátja rendelkezésre a honlapján értékesítés céljára. Ugyanezen a napon az 1. vevő megvásárolja az „X” szoftver 1.0.0 verziójának egy példányát. 2028. január 15-én az „A” vállalkozás kiadja az „X” szoftver frissített, 1.0.1 verzióját, amely nem minősül jelentős módosításnak. 2028. január 30-án a 2. vevő megvásárolja az „X” szoftver 1.0.1 verziójának egy példányát. Az „X” szoftver 1.0.0 és 1.0.1 verziójának mindkét példánya 2028. január 1-jén forgalomba hozottnak minősül.

16. A 13., 14. és 15. pontban meghatározott iránymutatás kizárólag annyiban alkalmazandó, amennyiben a digitális elemeket tartalmazó termék önálló szoftver. Más a helyzet például a szoftver és hardver kombinációja esetén, amelyről a 2.4. szakaszban (*Combination of hardware and software forming a product*) lesz szó.

2.2. **A szoftver mint digitális elemeket tartalmazó termék**

17. A kiberrezilienciáról szóló rendelet 3. cikkének 1. pontjában foglalt meghatározás szerint a digitális elemeket tartalmazó termék „szoftver- vagy hardvertermék és annak távoli adatkezelési megoldásai, beleértve a külön forgalomba hozott szoftver- vagy hardver-alkotóelemeket is”. Ezek a digitális elemeket tartalmazó termékek akkor tartoznak a kiberrezilienciáról szóló rendelet hatálya alá, ha rendeltetésük vagy észszerűen előrelátható használatuk magában foglal egy eszközhöz vagy hálózathoz való közvetlen vagy közvetett logikai vagy fizikai adatkapcsolatot.

([7]) A 13. cikk (11) bekezdésével összhangban a gyártók nyilvános szoftverarchívumokat tarthatnak fenn, amelyek megkönnyítik a felhasználók korábbi verziókhoz való hozzáférését. Ilyen esetekben a felhasználókat egyértelműen és könnyen hozzáférhető módon tájékoztatni kell a nem támogatott szoftver használatával kapcsolatos kockázatokról.

18. A kiberrezilienciáról szóló rendelet hatálya ezért a digitális elemeket tartalmazó termékek széles körére kiterjedhet, beleértve a következőket: i. digitálisan vagy fizikai formában értékesített önálló szoftverek, például alkalmazások és számítógépes programok, ii. hardver beágyazott szoftverrel (pl. dolgok internetéhez tartozó eszközök, laptopok, táblagépek), iii. önálló hardver (pl. integrált áramkörök, alaplapok), és iv. a hardver és a szoftver bármely olyan kombinációja, amelyet külön bocsátanak rendelkezésre, de együttes működésre szántak.

19. Az önálló szoftver ezért a kiberrezilienciáról szóló rendelet hatálya alá tartozik, ha azt digitális elemeket tartalmazó termékként hozzák forgalomba. Érdemes különbséget tenni a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó szoftvertermékek és a rendelet hatályán kívül eső, távoli szolgáltatásnyújtás között.

20. Ahhoz, hogy egy szoftver a kiberrezilienciáról szóló rendelet hatálya alá tartozzon, digitális elemeket tartalmazó szoftverterméket kell a felhasználó rendelkezésére bocsátani, amelyet az adott felhasználó szerez meg, és amelyet a felhasználó oldalán egy elektronikus információs rendszeren vagy annak részeként működtetnek. A felhasználó elektronikus információs rendszerére letöltött, telepített vagy más módon a felhasználó rendelkezésére bocsátott és a rendszerén futtatott szoftver megfelel ezeknek a kritériumoknak, ideértve például azt az esetet is, amikor a szoftver böngészőbővítmény vagy webes technológiák segítségével kifejlesztett, de helyi futtatás céljából rendelkezésre bocsátott alkalmazás formáját ölti.

21. Ezzel szemben a távolból futtatott szoftver, amelyhez a felhasználó csupán hozzáfér, önmagában ezen az alapon nem minősül digitális elemeket tartalmazó terméknek. A kiberrezilienciáról szóló rendelet (11) és (12) preambulumbekezdése megkülönbözteti a két esetet, kifejtve, hogy a távolról történő kezelés vagy tárolás nem magában is digitális elemeket tartalmazó termékként, hanem csak annyiban tartozik a kiberrezilienciáról szóló rendelet hatálya alá, amennyiben szükséges ahhoz, hogy a digitális elemeket tartalmazó termék ellássa funkcióit (vagyis a 3. cikk 2. pontjában meghatározott távoli adatkezelés fogalmán keresztül). Jellemzően ez a helyzet a webalkalmazások esetében, beleértve a progresszív webalkalmazásokat is, ahol a hozzáférés kizárólag webböngészőn keresztül történik. Ugyanez vonatkozik a honlapokra is: bár a honlapok – korlátozott mértékben – technikailag a felhasználó eszközén futnak, a kiberrezilienciáról szóló rendelet (12) preambulumbekezdéséből az következik, hogy maguk a honlapok nem tekinthetők digitális elemeket tartalmazó termékeknek, és csak annyiban tartoznak a kiberrezilienciáról szóló rendelet hatálya alá, amennyiben támogatják a digitális elemeket tartalmazó termék funkcióit, azaz amennyiben távoli adatkezelésnek minősülnek (a *8.* és különösen a *8.1.2.* szakaszban (*Would the absence of such data processing prevent the product with digital elements from performing one of its functions?*) részletesebben kifejtettek szerint).

3. példa: Egy mobilalkalmazást, amelyet a felhasználó letölt egy alkalmazás-áruházból és okostelefonjára telepít, a felhasználó rendelkezésére bocsátottak, és az a felhasználó eszközén fut, ennélfogva digitális elemeket tartalmazó terméknek minősül. Ha kereskedelmi tevékenység keretében hozzák forgalomba, a kiberrezilienciáról szóló rendelet hatálya alá tartozhat.

4. példa: Egy webes technológiák felhasználásával készült, de helyi telepítésre csomagolt asztali alkalmazást a felhasználó rendelkezésére bocsátottak, és az a felhasználó eszközén fut, ennélfogva digitális elemeket tartalmazó terméknek minősül. Ha kereskedelmi tevékenység keretében hozzák forgalomba, a kiberrezilienciáról szóló rendelet hatálya alá tartozhat.

5. példa: A felhasználó által kizárólag webböngészőn keresztül elért webalkalmazás nem digitális elemeket tartalmazó termék. Nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá, kivéve, ha támogatja egy digitális elemeket tartalmazó termék funkcióit. Ezzel szemben a helyben telepített kliensként a felhasználó rendelkezésére bocsátott és a felhasználó eszközén futó alkalmazás digitális elemeket tartalmazó terméknek minősül. Ha kereskedelmi tevékenység keretében hozzák forgalomba, a kiberrezilienciáról szóló rendelet hatálya alá tartozhat.

Ha ez a kliens egy vagy több funkciójának ellátása érdekében olyan távolról történő adatkezelésre támaszkodik, amely megfelel a távoli adatkezelés fogalmának, a távolról történő adatkezelés is a digitális elemeket tartalmazó termék részét képezi.

6. példa: Az olyan honlap, amely csupán információkat jelenít meg a látogatók számára, és nem támogatja valamely digitális elemeket tartalmazó termék funkcióit, önmagában nem digitális elemeket tartalmazó termék. Ennélfogva nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá.

2.3. **Számítógépes kód**

22. Azt is érdemes tisztázni, hogy a forráskód digitális elemeket tartalmazó szoftverterméknek minősülhet-e. A kiberrezilienciáról szóló rendelet meghatározása szerint a szoftver „egy elektronikus információs rendszer számítógépes kódból álló része” (3. cikk 4. pont). A számítógépes kód lehet i. bináris formátumú gépi kód, amely a számítógép processzora által közvetlenül végrehajtott utasítások sorozata, vagy ii. forráskód, azaz valamilyen programozási nyelven készült utasítások sorozata, amelyeket fordítani vagy értelmezni kell ahhoz, hogy a számítógép végrehajtsa azokat. A szoftvernek a kiberrezilienciáról szóló rendeletben szereplő fogalommeghatározása mindkettőre kiterjed.

23. Külön kérdés, hogy egy adott számítógépes kód rendelkezésre bocsátása digitális elemeket tartalmazó termék uniós piacon történő forgalomba hozatalának minősül-e, amely gazdasági tevékenység keretében történő rendelkezésre bocsátást feltételez. A forráskód esetében gyakran nem ez a helyzet. Például az a természetes vagy jogi személy, aki vagy amely nyilvánosan hozzáférhető adattárakban szabad és nyílt forráskódú számítógépes kódot oszt meg, a kiberrezilienciáról szóló rendelet alkalmazásában általában nem minősül az adott kódot az uniós piacon forgalomba hozó személynek – ezt részletesebben a 3. szakasz (*Free and open-source software*) tárgyalja. A digitális elemeket tartalmazó termék tervezési és fejlesztési szakaszában (pl. tesztelés vagy felülvizsgálat céljából) megosztott befejezetlen kód a kiberrezilienciáról szóló rendelet alkalmazásában szintén nem minősül forgalomba hozottnak, mivel gyártási szakasza még nem fejeződött be. Ugyanígy az oktatóanyagok vagy képzési anyagok részeként biztosított minta vagy demókód a kiberrezilienciáról szóló rendelet alkalmazásában nem minősül forgalomba hozottnak ([8]).

24. Ezzel szemben ha a gyártó digitális elemeket tartalmazó termékként számítógépes kódot bocsát ügyfelei rendelkezésére, e kódot forgalomba hozottnak kell tekinteni, függetlenül attól, hogy gépi kódról vagy forráskódról van-e szó ([9]).

7. példa: Az „A” vállalkozás forráskódra vonatkozó hasznosítási engedélyt ad a „B” vállalkozás számára egy testre szabható belső platform céljára úgy, hogy a forráskódot szövegfájlban adja át. A felhasználás előtt a „B” vállalkozásnál a forráskód adaptációjára és fordítására lehet szükség, ennek ellenére az „A” vállalkozás forgalomba hozza a forráskódot, amely ezért a kiberrezilienciáról szóló rendelet hatálya alá tartozik. Az „A” vállalkozás nem felelős azért, hogy a „B” vállalkozásnál elvégzett adaptáció és fordítás megfelel-e a kiberrezilienciáról szóló rendeletnek.

2.4. **Hardver és szoftver digitális elemeket tartalmazó terméket alkotó kombinációja**

25. Azt, hogy egy szoftver a digitális elemeket tartalmazó termék részét képezi-e, nem az alapján kell meghatározni, hogy a szoftvert hogyan és mikor juttatják el a felhasználóhoz, hanem az alapján, hogy a termék rendeltetésére és észszerűen előrelátható használatára tekintettel a szoftver szükséges-e a digitális elemeket tartalmazó termék tervezett funkcióinak ellátásához. Ha a digitális elemeket tartalmazó hardverterméket úgy tervezték, hogy funkcióinak ellátása érdekében az ugyanazon gyártó által biztosított konkrét szoftverrel működjön együtt, a hardver és a szoftver együttesen alkotja a digitális elemeket tartalmazó terméket. A digitális elemeket tartalmazó termék rendeltetésszerű működtetéséhez, konfigurálásához, ellenőrzéséhez vagy használatához szükséges szoftver ezért a digitális elemeket tartalmazó termék részét képezi még akkor is, ha azt a digitális elemeket tartalmazó hardvertermék forgalomba hozatalát követően külön csatornán (pl. alkalmazás-áruházon, letöltési linken vagy más digitális csatornán) keresztül szerzik be. Forgalomba hozatalára tehát ugyanabban az időpontban kerül sor, amikor a digitális elemeket tartalmazó hardvertermékek egységeit forgalomba hozzák.

8. példa: Egy hálózati nyomtatót digitális elemeket tartalmazó hardvertermékként hoznak forgalomba, míg a nyomtatási munkák küldéséhez, az eszköz konfigurálásához és működésének kezeléséhez szükséges illesztőprogramok a gyártó honlapjáról tölthetők le. Bár a nyomtatót és az illesztőprogramokat különböző csatornákon keresztül bocsátják rendelkezésre, ezek együttesen egyetlen, digitális elemeket tartalmazó terméket alkotnak, mivel a nyomtató az illesztőprogramok nélkül nem tudja betölteni rendeltetését.

9. példa: Viselhető fitneszeszközt hoznak forgalomba, amely a felhasználó szívritmusát és aktivitását méri, míg a mérések megjelenítéséhez, a korábbi adatok megtekintéséhez és az eszköz konfigurációjához a gyártó által biztosított okostelefon-alkalmazás szükséges. Bár az alkalmazást külön töltik le egy alkalmazás-áruházon keresztül, a viselhető eszköz és az alkalmazás együttesen egyetlen, digitális elemeket tartalmazó terméket alkot, mivel azok rendeltetésük szerint a digitális elemeket tartalmazó termék funkcióit együttes működésükkel biztosítják.

([8]) Emlékeztetni kell arra is, hogy a 4. cikk (3) bekezdése lehetővé teszi a gyártók számára a rendeletnek meg nem felelő befejezetlen szoftverek, mint például az alfa verziójú, béta verziójú vagy a kiadásra jelölt szoftverek rendelkezésre bocsátását, feltéve, hogy a befejezetlen szoftvereket csak a teszteléshez és a visszajelzések gyűjtéséhez szükséges ideig bocsátják rendelkezésre.

([9]) Másrészt meg kell jegyezni, hogy a termékfelelősségi jog alkalmazásában maga a számítógépes kód nem minősül terméknek, ezért az ilyen kódot forgalomba hozó gyártók a termékfelelősségről szóló (EU) 2024/2853 irányelv értelmében nem vonhatók felelősségre. Az említett irányelv (13) preambulumbekezdése kimondja, hogy „[a]z információ azonban nem tekinthető terméknek, ezért a termékfelelősségre vonatkozó szabályok nem alkalmazhatók a digitális fájlok, például médiafájlok vagy e-könyvek tartalmára vagy a szoftverek egyedüli forráskódjára”. Ez nem zárja ki, hogy a gyártók a nemzeti deliktuális felelősségi jog alapján felelősségre vonhatók legyenek.

2.5. **Adatkapcsolat**

26. A 2. cikk (1) bekezdése rögzíti, hogy a kiberrezilienciáról szóló rendelet „azokra a forgalmazott, digitális elemeket tartalmazó termékekre alkalmazandó, amelyek rendeltetése vagy észszerűen előrelátható használata magában foglal egy eszközhöz vagy hálózathoz való közvetlen vagy közvetett logikai vagy fizikai adatkapcsolatot”. A kiberrezilienciáról szóló rendelet hatálya szempontjából ezért nem az elektronika puszta jelenléte, hanem a digitális elemeket tartalmazó termék digitális információk cseréjére való képesség a meghatározó.

27. A „logikai kapcsolat” és a „fizikai kapcsolat” fogalommeghatározása a 3. cikkben megtalálható, a kiberrezilienciáról szóló rendelet azonban az „adatkapcsolat” és a „digitális adatok” fogalmát nem határozza meg. Ezért a kiberrezilienciáról szóló rendelet hatályának pontos lehatárolásához célszerű értelmezni, hogy mi minősül adatkapcsolatnak. Ez a határ különösen fontos a kizárólag elektromos jeleket használó, digitális elemeket tartalmazó termékek és a digitális kommunikációban részt vevő, ezért kiberbiztonsági kockázatoknak kitett termékek megkülönböztetéséhez.

28. A legalapvetőbb szinten az adatkapcsolat az információk bináris formában, azaz „0” és „1” értékek sorozataként történő továbbítását foglalja magában. A kimenet egyszerű be- és kikapcsolása (vagyis ahhoz „0” vagy „1” érték hozzárendelése) önmagában nem minősül adatkapcsolatnak, ha ezek az állapotok nem adatok megjelenítésére szolgálnak, vagy azokat nem digitális bemenettel olvassák be. Ahhoz, hogy adatkapcsolat álljon fenn, a bináris állapotokat egy forrásnak szándékosan információként kell kódolnia, és azoknak a rendeltetési helyen információként dekódolhatónak kell lenniük. Másként fogalmazva: léteznie kell egy olyan adónak, amely egy meghatározott rendszer szerint szándékosan hoz létre digitális szimbólumokat, valamint egy olyan vevőnek, amely képes e szimbólumokat adatként értelmezni. Ha az elektromos vagy elektronikus jeleket kizárólag valamely funkció aktiválására vagy működtetésére használják, digitálisan kódolt információk továbbítása nélkül, a kiberrezilienciáról szóló rendelet alkalmazásában nincs adatkapcsolat, ezért a digitális elemeket tartalmazó termék nem tartozik a 2. cikk (1) bekezdésének hatálya alá.

2.6. **Komplex rendszerek**

29. A kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek nemcsak egyetlen eszközből vagy szoftveres alkotóelemből állhatnak, hanem komplex rendszerek is lehetnek, beleértve a több hardver- és szoftverelemből álló rendszereket, amelyek egy bizonyos funkció ellátása érdekében együtt működnek. Ha az ilyen rendszert egyetlen, digitális elemeket tartalmazó termékként hozzák forgalomba, az a kiberrezilienciáról szóló rendelet értelmében digitális elemeket tartalmazó terméknek minősül.

30. Az ilyen komplex rendszereket gyakran hosszú tervezési és fejlesztési ciklusok jellemzik, amelyekhez esetlegesen a kiberrezilienciáról szóló rendelet alkalmazása előtt aláírt szerződés, valamint hosszabb működési élettartam és nagy fokú műszaki-szervezeti összetettség társul. Az ilyen, a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése után forgalomba hozott rendszer támaszkodhat a rendelet alkalmazásának megkezdése előtt forgalomba hozott alkotóelemekre, a meglévő architektúrákra vagy a széles körben használt interoperabilitási szabványokra, beleértve az egyéb uniós jogszabályokban vagy ágazatspecifikus keretekben említett szabványokat is. Mindez megnehezítheti vagy aránytalanná teheti e rendszerek egyes műszaki jellemzőinek olyan módosítását, hogy az ne befolyásolja rendeltetésüket, biztonságukat, megbízhatóságukat vagy a meglévő infrastruktúrával való interoperabilitásukat.

31. Ezek a jellemzők önmagukban nem zárják ki a komplex rendszereket a kiberrezilienciáról szóló rendelet hatálya alól. Inkább a rendelet kockázatalapú megközelítésének alkalmazását szemléltetik, amely lehetővé teszi a megfelelés különböző módokon történő igazolását a digitális elemeket tartalmazó termék jellemzőitől és korlátaitól függően, a kiberrezilienciáról szóló rendelet 13. cikkének (3) bekezdésével összhangban. Ezek a jellemzők hozzátartoznak e rendszerek rendeltetéséhez és működési környezetéhez, ennélfogva relevánsak az alapvető kiberbiztonsági követelményeknek (a továbbiakban: alapvető követelmények) való megfelelés értékelése szempontjából. Az (55) preambulumbekezdés kifejezetten elismeri, hogy egyes alapvető követelmények nem feltétlenül egyeztethetők össze teljes mértékben a digitális elemeket tartalmazó termék jellegével. Ilyen helyzet adódhat például akkor, ha a megfelelés aláásná a kötelező interoperabilitási követelményeket vagy a rendszer megfelelő működését.

32. Ennek megfelelően a gyártóknak a 13. cikk (2) bekezdésében említett kiberbiztonsági kockázatértékelés alapján kell kezelniük a kiberbiztonsági kockázatokat. Amint azt az (55) preambulumbekezdés is kifejti, egyes esetekben bizonyos alapvető követelmények nem alkalmazandók, vagy nem teljesíthetők a legkorszerűbb biztonsági

intézkedések végrehajtásával, például a rendszer rendeltetése miatt, amely megköveteli, hogy a digitális elemeket tartalmazó termék kölcsönhatásba lépjen a meglévő függőségekkel, vagy teljesítsen bizonyos interoperabilitási követelményeket. Ilyenkor a gyártóknak azonosítaniuk és dokumentálniuk kell ezeket a konkrét korlátokat, értékelniük kell a kapcsolódó kockázatokat, és megfelelő alternatív vagy kompenzációs kockázatcsökkentő intézkedéseket kell végrehajtaniuk annak érdekében, hogy ne ássák alá a digitális elemeket tartalmazó termék biztonságát. E célból mind a 31. cikkben említett műszaki dokumentáció, mind a II. mellékletben említett, a felhasználónak szóló információk és utasítások kulcsszerepet játszanak az azonosított korlátok, a kapcsolódó kiberbiztonsági kockázatok és a végrehajtott kockázatcsökkentő intézkedések átlátható leírásában. Azon kötelezettséggel összhangban, hogy a támogatási időszak alatt naprakészen kell tartani a kockázatértékelést, a gyártóknak rendszeresen újra kell értékelniük, hogy továbbra is fennállnak-e ilyen korlátok. Ha az ilyen korlátok idővel megszüntethetők vagy csökkenthetők, a gyártóknak ennek megfelelően frissíteniük kell a digitális elemeket tartalmazó terméket annak érdekében, hogy az elmozdulhasson a megfelelő szintű kiberbiztonság felé ([10]).

10. példa: Egy gyártó olyan digitális elemeket tartalmazó terméket hoz forgalomba, amely hálózati protokoll útján kommunikál külső rendszerekkel. Az alapvető követelmények alkalmazásának részeként a gyártó a kiberbiztonsági kockázatértékelés alapján megállapítja, hogy a digitális elemeket tartalmazó termék által kicserélt adatok bizalmas jellegének és integritásának biztosításához biztonságos kommunikációs protokoll használatára van szükség.

Rendeltetése azonban magában foglalja az olyan meglévő rendszerekkel való interoperabilitást, amelyek csak egy régebbi vagy kevésbé biztonságos protokollt támogatnak. Ilyenkor a gyártó alkalmazhatja az említett protokollt, ha ez az interoperabilitás eléréséhez szükséges, feltéve, hogy a kapcsolódó kiberbiztonsági kockázatokat más eszközökkel azonosítja és csökkenti.

Ha a digitális elemeket tartalmazó termék esetében a biztonságos protokoll és a kevésbé biztonságos protokoll támogatása műszakilag egyaránt megvalósítható, a gyártónak meg kell valósítania a biztonságos protokollt, és lehetővé kell tennie annak alapértelmezett használatát. A kevésbé biztonságos protokoll csak akkor lenne megengedett, ha az interoperabilitáshoz szükséges.

11. példa: Egy ipari automatizálási rendszer gyártója a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt vásárol néhány mikrovezérlőt. A gyártó elvégzi a kiberrezilienciáról szóló rendelet alkalmazásának megkezdését követően forgalomba hozandó ipari automatizálási rendszerére vonatkozó kiberbiztonsági kockázatértékelést. E kiberbiztonsági kockázatértékelés alapján a gyártó nem azonosítja az említett mikrovezérlők valamelyikének használatával kapcsolatos konkrét kiberbiztonsági kockázatokat. A gyártó integrálja ipari automatizálási rendszerébe, és biztosítja, hogy a digitális elemeket tartalmazó termék egésze (az ipari automatizálási rendszer) megfeleljen az alapvető követelményeknek.

2.7. **A kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt tervezett, digitális elemeket tartalmazó termékek**

33. Egyes esetekben a gyártó a kiberrezilienciáról szóló rendelet alkalmazásának 2027. december 11-i megkezdését követően hozza forgalomba a digitális elemeket tartalmazó termék azon egységeit, amelyeket a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt tervezett és kifejlesztett típusnak vagy modellnek megfelelően gyártottak. Ilyenkor az e rendeletnek való megfelelés nem feltétlenül követeli meg a digitális elemeket tartalmazó termék említett egységeinek újratervezését. A gyártónak a kiberrezilienciáról szóló rendelet 13. cikkének (2) bekezdésével összhangban kiberbiztonsági kockázatértékelést kell végeznie annak érdekében, hogy a digitális elemeket tartalmazó termék rendeltetése és észszerűen előrelátható használata alapján meghatározza, hogy az I. melléklet I. részében meghatározott alapvető követelmények közül melyek alkalmazandók az adott, digitális elemeket tartalmazó termékre, és hogyan hajtják végre ezeket a követelményeket.

34. Ha a kockázatértékelés eredménye azt mutatja, hogy a digitális elemeket tartalmazó termék már tartalmaz megfelelő és hatékony biztonsági intézkedéseket a releváns kockázatok kezelésére, a gyártó támaszkodhat ezekre a meglévő intézkedésekre a kiberrezilienciáról szóló rendeletnek való megfelelés igazolása érdekében. Maga a kiberrezilienciáról szóló rendelet nem ír elő kötelezettséget új biztonsági jellemzők bevezetésére vagy a digitális elemeket tartalmazó termék újratervezésére, ha ez nem szükséges az azonosított kockázatok kezeléséhez.

([10]) Meg kell jegyezni, hogy az e bekezdésben meghatározott megfontolások adott esetben a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó valamennyi termékre alkalmazandók, nem csak a „komplex rendszerekre”.

35. Mindazonáltal a gyártóra továbbra is vonatkoznak a kiberrezilienciáról szóló rendeletben meghatározott kötelezettségek. Ezek közé tartozik annak biztosítása, hogy a digitális elemeket tartalmazó termék forgalomba hozatala előtt sor kerüljön az alkalmazandó megfelelőségértékelési eljárás elvégzésére, az EU-megfelelőségi nyilatkozat elkészítésére és a CE-jelölés elhelyezésére. Az e követelményeknek való megfelelés független attól, hogy a digitális elemeket tartalmazó termék kialakítása a kockázatértékelés eredményeként módosítást igényelt-e. Ha a gyártó a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt tervezett, de az említett időpontot követően forgalomba hozott, digitális elemeket tartalmazó termékek esetében nem tudja igazolni, hogy a kockázatértékelést milyen módon vették figyelembe a digitális elemeket tartalmazó termék tervezési és fejlesztési szakaszában, a 13. cikk (2) bekezdésében foglalt kötelezettséget úgy kell értelmezni, hogy a gyártóknak kiberbiztonsági kockázatértékelést kell végezniük, és ennek alapján igazolniuk kell, hogy a digitális elemeket tartalmazó termék megfelelő biztonsági intézkedéseket tartalmaz a kiberbiztonsági kockázatok minimalizálására, az incidensek megelőzésére és hatásuk minimalizálására, többek között a felhasználók egészségével és biztonságával kapcsolatban.

36. Ennek megfelelően a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt tervezett, digitális elemeket tartalmazó termékek újratervezés nélkül is forgalomba hozhatók a kiberrezilienciáról szóló rendelet alapján, feltéve, hogy a gyártó a kiberbiztonsági kockázatértékelés és a műszaki dokumentáció révén igazolni tudja, hogy a digitális elemeket tartalmazó termék a rendeltetése és észszerűen előrelátható használata fényében megfelelő kiberbiztonsági szintet ér el, és megfelel az alapvető kiberbiztonsági követelményeknek.

37. Érdemes továbbá egyértelművé tenni a megfelelőségértékelési kötelezettségek alkalmazását azon digitális elemeket tartalmazó termékek gyártói számára, amelyeket a kiberrezilienciáról szóló rendelet alkalmazásának megkezdését követően hoztak forgalomba, de amelyeket az említett időpont előtt tervezett és kifejlesztett típusnak vagy modellnek megfelelően gyártottak. A 13. cikk (12) bekezdésével összhangban a gyártónak a vonatkozó megfelelőségértékelési eljáráson keresztül igazolnia kell, hogy a digitális elemeket tartalmazó terméke megfelel az alkalmazandó alapvető követelményeknek, és erre vonatkozó bizonyítékot kell belefoglalnia a termék műszaki dokumentációjába (VII. melléklet 6. pont).

38. E követelmények alkalmazását azonban a kiberbiztonsági kockázatértékelés és a digitális elemeket tartalmazó termék kiberbiztonsági kockázati profiljára tekintettel kell értelmezni. Különösen a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt tervezett (de az említett időpontot követően forgalomba hozott) és a 32. cikk (1) bekezdése szerinti megfelelőségértékelési eljárás tárgyát képező, digitális elemeket tartalmazó termékek esetében ha a kockázatértékelés által igazolt módon a digitális elemeket tartalmazó termék már magában foglal megfelelő és hatékony biztonsági intézkedéseket az adott termék kockázatainak kezelésére, a megfelelőségértékelési eljárás részeként történő bizonyításra vonatkozó kötelezettség nem értelmezhető úgy, hogy a gyártónak a digitális elemeket tartalmazó ilyen termékek eredeti tervezési és fejlesztési szakaszára vonatkozó vizsgálati eredményeket kell benyújtania. Erre nincs szükség, mivel nem járulna hozzá a digitális elemeket tartalmazó termék biztonságának növeléséhez. Ha ennek ellenére vizsgálatokra lehet szükség, a gyártóktól nem várható el, hogy az összes termékváltozaton elvégzett vizsgálatokról bizonyítékot szolgáltassanak, ugyanakkor a 7.4. szakaszban (*Reuse of risk assessments and conformity documentation for families of products with digital elements*) részletesebben tárgyalt módon a digitális elemeket tartalmazó termékcsaládok között csoportosíthatják a vizsgálatokat.

39. Mindazonáltal a gyártónak bizonyítékot kell szolgáltatnia az I. melléklet II. részében meghatározott sérülékenységkezelési eljárásoknak való megfelelésére vonatkozóan, a 13. cikk (3) bekezdésével összhangban naprakészen kell tartania kockázatértékelését, és teljesítenie kell a kiberrezilienciáról szóló rendeletben meghatározott valamennyi egyéb kötelezettséget, többek között a felhasználóknak a 13. cikk (18) bekezdése szerint adott tájékoztatás és utasítások formájában.

12. példa: Egy gyártó olyan mikrovezérlőt hoz forgalomba, amelyet a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt terveztek és fejlesztettek ki. A mikrovezérlőt digitális elemeket tartalmazó elektronikus termékek széles körébe kívánják integrálni, beleértve a konnektivitási funkciókkal rendelkező, digitális elemeket tartalmazó termékeket is.

A mikrovezérlő új egységeinek a kiberrezilienciáról szóló rendelet alkalmazását követő forgalomba hozatala előtt a gyártó a 13. cikk (2) bekezdésével összhangban kiberbiztonsági kockázatértékelést végez. A mikrovezérlő rendeltetése és észszerűen előrelátható használata alapján a gyártó azonosítja a releváns kiberbiztonsági kockázatokat, például a jogosulatlan hozzáférést, a szoftverek vagy adatok manipulálását, valamint a rendelkezésre álló interfészekkel való visszaélést.

A kockázatértékelés eredménye azt mutatja, hogy a mikrovezérlő az eredeti formájában már tartalmaz megfelelő és hatékony biztonsági intézkedéseket az azonosított kockázatok kezelésére. A gyártó ezért arra a következtetésre jut, hogy a digitális elemeket tartalmazó termék megfelel az I. melléklet I. részében meghatározott vonatkozó alapvető követelményeknek, és nincs szükség további biztonsági funkciók újratervezésére vagy bevezetésére.

Ha nem igazolható, hogy az eredeti tervezési és fejlesztési szakaszban milyen módon vették figyelembe a kiberbiztonsági kockázatértékelést, a gyártó dokumentálja az aktuális kiberbiztonsági kockázatértékelést, és kifejti, hogy a meglévő tervezés és intézkedések hogyan csökkentik az azonosított kockázatokat. A gyártónak nem kell újra elkészítenie a korábbi tervezési vagy tesztelési dokumentációt, mivel ez nem járulna hozzá a digitális elemeket tartalmazó termék kiberbiztonságának fokozásához. Ha a mikrovezérlő több változata ugyanazon a kialakításon alapul, és azonos kiberbiztonsági kockázati profillal rendelkezik, a gyártó az érintett termékcsaládra vonatkozó reprezentatív bizonyítékokra is támaszkodhat.

A gyártó biztosítja továbbá az I. melléklet II. részében meghatározott sérülékenységkezelési követelményeknek való megfelelést, többek között azáltal, hogy fenntartja a sérülékenységek kezelésére és orvoslására szolgáló eljárásokat, és a 13. cikk (3) bekezdésével összhangban folyamatosan felülvizsgálja a kiberbiztonsági kockázatértékelést.

Ilyen körülmények között a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt tervezett mikrovezérlő újratervezés nélkül is forgalomba hozható, feltéve, hogy a gyártó a kiberbiztonsági kockázatértékelés és a műszaki dokumentáció révén igazolni tudja, hogy a rendeltetése és az észszerűen előrelátható használata fényében megfelelő szintű kiberbiztonságot ér el, és megfelel az alkalmazandó alapvető követelményeknek.

3. **SZABAD ÉS NYÍLT FORRÁSKÓDÚ SZOFTVER**

40. Amint arra a *2.1.* szakasz (*Placing on the market*) emlékeztet, a kiberrezilienciáról szóló rendelet azokra a digitális elemeket tartalmazó termékekre alkalmazandó, amelyeket kereskedelmi tevékenység keretében első alkalommal forgalmaznak („forgalomba hoznak”) az uniós piacon, valamint minden olyan későbbi esetre, amely ugyanazon, digitális elemeket tartalmazó termék forgalmazásának minősül. A kék útmutató (2.2. szakasz) egyértelművé teszi, hogy „kereskedelmi tevékenység” alatt áruk fizetés ellenében vagy ingyenesen, üzleti összefüggésben történő rendelkezésre bocsátását kell érteni, és azt csak eseti alapon lehet értékelni, figyelembe véve a rendelkezésre bocsátás rendszerességét, a termék tulajdonságait, a szállító szándékait stb.

41. A kereskedelmi tevékenység keretében történő rendelkezésre bocsátást számos körülmény jellemzi, amelyeket a kék útmutató részletesen dokumentál, és amelyekre a kiberrezilienciáról szóló rendelet (15) preambulumbekezdése is emlékeztet. Ezek közé tartozhat az ár közvetlen felszámítása, valamint az, hogy „díjat számítanak fel a műszaki támogatási szolgáltatásokért, amennyiben ez nem kizárólag a tényleges költségek megtérülését szolgálja a pénzszerzési szándék révén, például olyan szoftverplatform biztosításával, amelyen keresztül a gyártó pénzzé tesz más szolgáltatásokat, a használat feltételeként szabva a személyes adatoknak nem kizárólag a szoftver biztonságának, kompatibilitásának vagy interoperabilitásának javítása céljából történő kezelését, vagy a digitális elemeket tartalmazó termék tervezésével, fejlesztésével és rendelkezésre bocsátásával kapcsolatos költségeket meghaladó adományok elfogadása révén” ((15) preambulumbekezdés) ([11]).

42. A kiberrezilienciáról szóló rendelet azonban elismeri a „szabad és nyílt forráskódú szoftverek” fejlesztésének és közzétételének különböző módjaiban rejlő sajátosságokat, és iránymutatást nyújt annak megállapításához, hogy a szabad és nyílt forráskódú szoftver a rendelet értelmében (azaz kereskedelmi tevékenység keretében) forgalomba hozott, digitális elemeket tartalmazó termék-e. A (18) preambulumbekezdésben kifejtett módon „annak meghatározásakor, hogy a tevékenység kereskedelmi vagy nem kereskedelmi jellegű-e, nem kell figyelembe venni a digitális elemeket tartalmazó termék kifejlesztésének puszta körülményeit, illetve a fejlesztés finanszírozásának módját”. Konkrétabban annak „érdekében, hogy egyértelmű legyen a különbségtétel a fejlesztési és a rendelkezésre bocsátási szakasz között, a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó, a gyártók által pénzzé nem tett termékek rendelkezésre bocsátása nem tekinthető gazdasági tevékenységnek”.

([11]) Emlékeztetni kell arra is, hogy bár a digitális elemeket tartalmazó termékeket gyakran a személyes adatok kezelése révén (is) monetizálják, a személyes adatok védelme alapvető jog, ezért a személyes adatok nem tekinthetők árunak, amint azt a digitális tartalom szolgáltatására és digitális szolgáltatások nyújtására irányuló szerződések egyes vonatkozásairól szóló, 2019. május 20-i (EU) 2019/770 európai parlamenti és tanácsi irányelv (24) preambulumbekezdése jelzi (*HL L 136., 2019.5.22., 1. o.*, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Ezért érdemes i. tisztázni, hogy mi a szabad és nyílt forráskódú szoftver, ii. pontosítani, hogy mikor tekintendő egy természetes vagy jogi személy felelősségi körébe tartozónak, valamint iii. példák bemutatásával segíteni az érdekelt feleket annak megértésében, hogy a szabad és nyílt forráskódú szoftver terjesztése mikor minősül forgalomba hozatalnak. Amennyiben a szabad és nyílt forráskódú szoftvert nem hozzák forgalomba, az nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá, kivéve, ha a közzétevő jogalany olyan jogi személy, amely megfelel a „nyílt forráskódú szoftverek támogatója" (a továbbiakban: támogató) 3. cikk 14. pontja szerinti fogalommeghatározásának. Ebben az esetben csak a 24. cikkben meghatározott kötelezettségek vonatkoznak rá.

44. A 3. cikk 48. pontjában foglalt fogalommeghatározás szerint a szabad és nyílt forráskódú szoftver „olyan szoftver, amelynek forráskódja nyíltan megosztott, és amelyet olyan szabad és nyílt forráskódú licenc alapján bocsátanak rendelkezésre, amely minden jogot biztosít arra, hogy azt szabadon hozzáférhetővé, használhatóvá, módosíthatóvá és továbbterjeszthetővé tegyék". Bár ez az iránymutatás nem azonosít olyan konkrét szabad és nyílt forráskódú licenceket, amelyek összeegyeztethetők a 3. cikk 48. pontjában foglalt fogalommeghatározással, e rendelkezés szövegéből az következik, hogy a kiberrezilienciáról szóló rendelet alkalmazásában csak azok a szoftverek minősülnek szabad és nyílt forráskódú szoftvernek, amelyek együttesen megfelelnek két feltételnek: i. a szoftvert szabad és nyílt forráskódú licenc alapján kell rendelkezésre bocsátani, amely a 3. cikk 48. pontjában említett jogok teljes körét biztosítja, és ii. a forráskódját nyíltan meg kell osztani.

45. Az a követelmény, hogy a licencnek biztosítania kell, hogy a szoftver „ingyenesen hozzáférhető, használható, módosítható és továbbterjeszthető" legyen, a szabad és nyílt forráskódú szoftver hagyományos értelmezését tükrözi, nevezetesen azt, hogy a felhasználók számára lehetővé kell tenni a forráskódhoz való hozzáférést, annak indokolatlan korlátozás nélküli használatát, módosítását és az eredeti vagy módosított verziók továbbterjesztését. A forráskódhoz való hozzáférés ezért a többi jog gyakorlásának szükséges előfeltétele: a forráskódhoz való hozzáférés nélkül gyakorlatilag nem lehetséges a szoftver módosítása vagy érdemi újrafelhasználása.

46. A 3. cikk 48. pontja azonban a licencfeltételek kizárólagos említésén túlmenően kifejezetten előírja a forráskód „nyíltan megosztott" voltát. „Nyíltan megosztott" a forráskód, ha azt – korlátozott vagy feltételes átadása helyett – nyilvánosan hozzáférhetővé teszik („upstream" vagy „downstream" szereplők számára). Ennek megfelelően a szabad és nyílt forráskódú licenc alapján terjesztett szoftverek, amelyek forráskódját csak fizető ügyfelekkel vagy korlátozott felhasználói csoporttal osztják meg (vagy csak ezek számára való megosztása engedélyezett), a 3. cikk 48. pontja értelmében nem minősülnek szabad és nyílt forráskódú szoftvernek. A kiberrezilienciáról szóló rendelet alkalmazásában ezért csak azok a szoftverek minősülnek szabad és nyílt forráskódú szoftvernek, amelyek forráskódja nyilvánosan hozzáférhető, és amelyeket a 3. cikk 48. pontjában említett jogok teljes körét biztosító szabad és nyílt forráskódú licenc alapján engedélyeztek.

3.1. **Annak meghatározása, hogy a szabad és nyílt forráskódú szoftverek a szereplő felelősségi körébe tartoznak-e**

47. A kiberrezilienciáról szóló rendelet kulcsfontosságú feladatokat ró azokra a gazdasági szereplőkre, amelyek digitális elemeket tartalmazó termékeket bocsátanak rendelkezésre az uniós piacon. Meghatározása szerint gyártó az a természetes vagy jogi személy, aki vagy amely a saját neve vagy védjegye alatt digitális elemeket tartalmazó terméket bocsát rendelkezésre, és ezt kereskedelmi tevékenység keretében teszi (ezáltal forgalomba hozza azt). Hasonlóképpen: importőr az az EU-ban letelepedett természetes vagy jogi személy, aki vagy amely az EU-n kívül letelepedett személy digitális elemeket tartalmazó termékét rendelkezésre bocsátja, és ezt kereskedelmi tevékenység keretében teszi (ezáltal forgalomba hozza azt). A támogatói kötelezettségek arra a jogi személyre vonatkoznak, amely kereskedelmi tevékenységekre szánt, szabad és nyílt forráskódú szoftvert bocsát rendelkezésre ([12]), de azt a kiberrezilienciáról szóló rendelet értelmében nem hozza forgalomba.

48. Ezért annak megállapításához, hogy egy természetes vagy jogi személy forgalomba hoz-e szabad és nyílt forráskódú szoftvert az uniós piacon, először is tisztázni kell, hogy a szabad és nyílt forráskódú szoftvert ténylegesen az adott természetes vagy jogi személy bocsátja-e rendelkezésre. A kiberrezilienciáról szóló rendelet szerinti alkalmazandó kötelezettségek helyes megállapítása érdekében alapvető fontosságú annak meghatározása, hogy a természetes vagy jogi személy ténylegesen rendelkezésre bocsátja-e a szabad és nyílt forráskódú szoftvert. Amint arra a (18) preambulumbekezdés emlékeztet, a kiberrezilienciáról szóló rendelet nem alkalmazandó azokra a természetes vagy jogi személyekre, akik vagy amelyek forráskóddal járulnak hozzá az olyan szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékekhez, amelyek nem tartoznak a felelősségi körükbe.

([12]) Ez szükséges, de nem elégséges feltétele annak, hogy egy jogi személy nyílt forráskódú szoftver támogatójának minősüljön, mivel e minőségre vonatkozóan a 3. cikk 14. pontjában foglalt fogalommeghatározás további feltételeket rögzít.

49. Tekintettel a szabad és nyílt forráskódú szoftver – gyakran több közreműködőt, decentralizált együttműködési modelleket, valamint a közreműködés és a döntéshozatal szétválasztását magában foglaló – fejlesztésének sajátosságaira, célszerű egyértelművé tenni, hogy a szabad és nyílt forráskódú szoftver az azt közzétevő és a fejlesztési, kiadási és terjesztési döntések felett elsődleges ellenőrzést gyakorló természetes vagy jogi személyek (gyakori elnevezéssel: „karbantartók") „felelősségi körébe" tartozik. Azok a személyek, akik forráskóddal hozzájárulnak a szoftverhez, de a kiadások, ütemtervek vagy irányítási döntések felett nem rendelkeznek ellenőrzéssel, „közreműködőknek" minősülnek; ilyenkor a szabad és nyílt forráskódú szoftver nem tartozik a felelősségi körükbe, annak ellenére, hogy ahhoz forráskóddal járultak hozzá. A technikai engedélyek – például a hozzáférési engedély – puszta megléte nem elegendő annak megállapításához, hogy a szabad és nyílt forráskódú szoftver az adott személy felelősségi körébe tartozik; a felelősség a szabad és nyílt forráskódú szoftvert közzétevő és ellenőrző személyeket terheli.

13. példa: Egy vállalkozás egyéni fejlesztője vagy alkalmazottja „pull" vagy „merge" kérést küld, amely egy szabad és nyílt forráskódú szoftverprojekt biztonsági javítását vagy új jellemzőjét tartalmazza. A projekt karbantartói felülvizsgálják és elfogadják a kódot, azt a fő adattárban összefésülik, majd új kiadásba foglalják. Ebben az esetben a „pull" kérést küldő személy „közreműködő", és nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá. Bár forráskóddal hozzájárult a szoftverhez, e személy nem gyakorol elsődleges ellenőrzést a fejlesztési, kiadási vagy terjesztési döntések felett.

3.2. **Annak meghatározása, hogy a szabad és nyílt forráskódú szoftver az uniós piacon forgalomba hozott-e**

50. Miután megállapítást nyert, hogy a szabad és nyílt forráskódú szoftver egy természetes vagy jogi személy felelősségi körébe tartozik, azt kell megállapítani, hogy az adott személy azt kereskedelmi tevékenység keretében bocsátja-e rendelkezésre, és ezáltal forgalomba hozatalt valósít-e meg.

3.2.1. *Ár felszámítása*

51. Ha a szabad és nyílt forráskódú szoftvert rendelkezésre bocsátó természetes vagy jogi személy magáért a szoftverért árat számít fel (pl. az előfordított bináris kódot díjfizetés fejében biztosítja), az adott személy digitális elemeket tartalmazó terméket hoz forgalomba. A szabad és nyílt forráskódú szoftvert forgalomba hozó személy ezért a kiberrezilienciáról szóló rendelet szerint gyártónak minősül.

52. A szabad és nyílt forráskódú szoftverek gyártói sok esetben bocsátják rendelkezésre a szoftverük ingyenes (gyakori elnevezéssel: „közösségi") verzióját, amelynek kódbázisa (közel) azonos a fizetős verzióéval. Ezek a digitális elemeket tartalmazó termékek azonban különböző termékek: a fizetős verziót valamilyen módon (pl. ár felszámításával vagy az e szakaszban tárgyalt egyéb módon) monetizálják, ennélfogva azt forgalomba hozottnak kell tekinteni, ami a gyártónál kötelezettségeket keletkeztet. Az ingyenesen rendelkezésre bocsátott (vagy közösségi) változat nem monetizált, ezért a kiberrezilienciáról szóló rendelet alkalmazásában nem minősül forgalomba hozottnak. Ugyanez a helyzet akkor is, ha a fizetős verzió egy „továbbfejlesztett" kereskedelmi verzió, amely kiterjeszti az ingyenesen rendelkezésre bocsátott verzió kódbázisát, vagy (pl. az „open-core" modell esetében) az ingyenes verziót egy digitális elemeket tartalmazó átfogóbb termékbe építi be.

53. Ha a közösségi verziót rendelkezésre bocsátó személy jogi személy, a támogatói kötelezettségek az általa ingyenesen rendelkezésre bocsátott (közösségi) verzió tekintetében e jogi személyre is vonatkoznak. Ha a jogalany természetes személy, az ingyenesen rendelkezésre bocsátott (közösségi) verzió nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá.

3.2.2. *Egyéb szolgáltatások monetizálása vagy személyes adatok feldolgozásának előírása*

54. A szabad és nyílt forráskódú szoftvert közzétevő természetes vagy jogi személy azt akkor is forgalomba hozhatja (kereskedelmi tevékenység keretében rendelkezésre bocsáthatja), ha biztosítja azt a szoftvert, amelyen keresztül más, digitális elemeket tartalmazó termékeket vagy szolgáltatásokat monetizál, vagy ha a felhasználás feltételeként a személyes adatok nem kizárólag a szoftver biztonságának, kompatibilitásának vagy interoperabilitásának javítása céljából történő kezelését írja elő.

14. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú piactér-alkalmazást tesz közzé. Az ingyenesen elérhető alkalmazás lehetővé teszi a felhasználók számára, hogy azon keresztül árukat vagy szolgáltatásokat vásároljanak. Az alkalmazás lehetővé teszi az azt közzétevő személy számára, hogy az alkalmazáson keresztül kínált, digitális elemeket tartalmazó egyéb termékeket és szolgáltatásokat monetizáljon (pl. hirdetések, jutalékok vagy előfizetési díjak révén). Az alkalmazást ezért kereskedelmi tevékenység keretében forgalomba hozottnak kell tekinteni.

15. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú VPN-t tesz közzé. Az alkalmazás ingyenesen elérhető, de a felhasználók fizetés ellenében további szerverekhez vagy célzott IP-címekhez férhetnek hozzá. Az alkalmazás lehetővé teszi a közzétevő személy számára, hogy az alkalmazáson keresztül kínált egyéb szolgáltatásokat monetizáljon, ezért kereskedelmi tevékenység keretében forgalomba hozottnak kell tekinteni.

16. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú aktivitásmérő alkalmazást tesz közzé. Az alkalmazás ingyenesen elérhető, de használatának feltétele a felhasználók személyes adatainak olyan célokból történő kezelése, mint a célzott hirdetések vagy a szoftver biztonságához, kompatibilitásához vagy interoperabilitásához nem kapcsolódó elemzések. Mivel az ilyen adatkezelést a felhasználás feltételeként írja elő, az alkalmazást kereskedelmi tevékenység keretében forgalomba hozottnak kell tekinteni.

3.2.3. *Támogatási szolgáltatások*

55. Önmagában az, hogy a szabad és nyílt forráskódú szoftvert közzétevő természetes vagy jogi személy ahhoz kapcsolódóan fizetős támogatási szolgáltatásokat is kínál, nem jelenti azt, hogy a digitális elemeket tartalmazó terméket kereskedelmi tevékenység keretében bocsátják rendelkezésre. A támogatási szolgáltatások magukban foglalhatnak olyan tevékenységeket, mint például a szoftver vevő általi használatával, dokumentálásával, konfigurálásával és telepítésével kapcsolatos tanácsadás, képzés vagy szakmai szolgáltatások.

56. A döntő szempont az, hogy magához a szabad és nyílt forráskódú szoftverhez való hozzáférés (azaz a digitális elemeket tartalmazó termék rendelkezésre bocsátása) – beleértve annak karbantartását is – ellenszolgáltatáshoz kötött-e, nem pedig az, hogy egy szabadon hozzáférhető, digitális elemeket tartalmazó termékhez kapcsolódóan nyújtanak-e szakmai szolgáltatásokat – a kiberrezilienciáról szóló rendelet (18) preambulumbekezdése is ezt jelzi („a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó, a gyártók által pénzzé nem tett termékek rendelkezésre bocsátása nem tekinthető gazdasági tevékenységnek”). Nem minősül forgalomba hozottnak az a szabad és nyílt forráskódú szoftver, amely szabadon letölthető és telepíthető, és amelyhez a felhasználók a saját döntésük alapján külön vásárolhatnak szakmai szolgáltatásokat.

57. Ezzel szemben egyes esetekben a digitális elemeket tartalmazó termék egy adott verziójához való hozzáférés, beleértve bizonyos előnyöket, például a technikai segítségnyújtást vagy a teljesítményoptimalizálást, ellenszolgáltatáshoz kötött. Ilyenkor a rendelkezésre bocsátás a digitális elemeket tartalmazó termék kereskedelmi tevékenység keretében történő, monetizált rendelkezésre bocsátásának minősül, ennélfogva a terméket forgalomba hozottnak kell tekinteni. Ide tartoznak azok az esetek is, amikor kereskedelmi megállapodás alapján fizetős kiadást vagy vállalati verziót bocsátanak rendelkezésre, függetlenül attól, hogy szabad és nyílt forráskódú licenc alapján funkcionálisan egyenértékű szoftver is elérhető-e ingyenesen.

17. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú operációs rendszert tesz közzé, amelynek fizetős verziója támogatási szolgáltatásokat, például technikai segítségnyújtást vagy teljesítményoptimalizálást foglal magában. Az operációs rendszer fizetős verzióját kereskedelmi tevékenység keretében forgalomba hozottnak kell tekinteni.

18. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú parancssori eszközt tesz közzé. Az eszköz szabadon hozzáférhető, bárki letöltheti és telepítheti. A természetes vagy jogi személy külön szakmai szolgáltatásokat kínál, például opcionális tanácsadási szolgáltatásokat, amelye célja a felhasználók képzése és az eszköz telepítésében és használatában való támogatása. A szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak.

58. Különösen a szabad és nyílt forráskódú szoftvert közzétevő természetes személyek esetében a digitális elemeket tartalmazó termékhez való hozzáféréssel közvetlenül összekapcsolt technikai segítségnyújtás továbbra sem minősül kereskedelmi tevékenységnek, ha – amint azt a kiberrezilienciáról szóló rendelet (15) preambulumbekezdése jelzi – a felszámított ár csak a tényleges költségek megtérülését szolgálja. Az ilyen tényleges költségek magukban foglalják az adott szoftver tervezésével, fejlesztésével és karbantartásával kapcsolatos különböző költségeket, beleértve az adott személy észszerű megélhetési költségeit is. Ezért az, ha a szabad és nyílt forráskódú szoftvert közzétevő természetes személy a költségei fedezése és méltányos ellenszolgáltatás megszerzése céljából technikai segítséget nyújt, pusztán ezen az alapon nem tekinthető e szoftver uniós piacon történő forgalomba hozatalának.

59. Az a természetes vagy jogi személy, aki vagy amely a felelősségi körébe nem tartozó szabad és nyílt forráskódú szoftverhez kapcsolódó technikai segítségnyújtást kínál, nem tekinthető úgy, hogy az említett szoftvert forgalomba hozza, kivéve, ha az adott személy a 22. cikkel összhangban az ilyen segítségnyújtás részeként jelentősen módosítja a szabad és nyílt forráskódú szoftvert.

19. példa: Egy szolgáltató nem teszi közzé a szabad és nyílt forráskódú szoftvert, de segíti a vevőt annak helyszíni szerverére történő telepítésében. Ezt a szabad és nyílt forráskódú szoftver jelentős módosítása nélkül teszi. Ezért nem tekintendő úgy, hogy a szolgáltató szabad és nyílt forráskódú szoftvert hoz forgalomba.

3.2.4. *Adományok*

60. A szabad és nyílt forráskódú szoftverprojekteket közzétevő természetes vagy jogi személyek rendszeresen lehetőséget biztosítanak a szoftver felhasználói számára arra, hogy önkéntesen pénzt adományozzanak azért, hogy köszönetet mondjanak a projekt közzétevőjének vagy közzétevőinek, és biztosítsák a projekt aktív fenntartását.

61. A kiberrezilienciáról szóló rendelet (15) preambulumbekezdésében foglaltak szerint „[a]z adományok nyereségszerzési szándék nélküli elfogadása nem minősül kereskedelmi tevékenységnek”. Önmagában az adományozási platformra vagy az adományok gyűjtésére szolgáló hasonló eszközökre mutató link beillesztése nem tekinthető nyereségszerzési szándéknak, még akkor sem, ha az adományok révén beszedett összeg meghaladja a digitális elemeket tartalmazó termék tervezésével, fejlesztésével és rendelkezésre bocsátásával kapcsolatos költségeket. Ez magában foglalja a jogi személy által alkalmazott közreműködők észszerű kompenzációját és/vagy a természetes személy észszerű megélhetési költségeit. Az adományok természeténél fogva az azokból származó bevétel időben változó, ezért bizonyos fokú rugalmasság indokolt annak értékelésekor, hogy a kizárólag adományok révén monetizált szabad és nyílt forráskódú szoftver forgalomba hozottnak minősül-e. Ezért nem valószínű, hogy a kizárólag adományokból támogatott szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak minősül.

20. példa: Egy természetes vagy jogi személy egy nyilvános online adattárban szabad és nyílt forráskódú szoftvereszközt tesz közzé, amelyet szabad és nyílt forráskódú licenc alapján bárki letölthet, használhat, módosíthat és továbbterjeszthet. A közzétevő felkéri a felhasználókat, hogy egy adományozási platformon keresztül nyújtsanak önkéntes adományokat a projekt folyamatos fejlesztéséhez és karbantartásának támogatásához. A szoftverhez, annak forráskódjához és frissítéseihez való hozzáférés adományozástól független. A szabad és nyílt forráskódú szoftver nem minősül kereskedelmi tevékenység keretében rendelkezésre bocsátottnak, és a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak.

62. Mindazonáltal vannak olyan esetek, amikor az adományokból támogatott szabad és nyílt forráskódú szoftver forgalomba hozottnak tekinthető. Ez a helyzet akkor, ha a körülmények átfogó értékelése alapján az adományok valójában egyenértékűek a digitális elemeket tartalmazó termékhez vagy annak bizonyos funkcióihoz való hozzáférésért felszámított árral. Ez különösen akkor fordulhat elő, ha a szabad és nyílt forráskódú szoftverhez, az alapvető funkciókhoz vagy a frissítésekhez való hozzáférés a gyakorlatban adományozáshoz kötött, vagy ha az adományokhoz olyan szerződéses vagy kizárólagos előnyök kapcsolódnak, amelyek túlmutatnak a közösségi előnyökön.

21. példa: Egy természetes vagy jogi személy szabad és nyílt forráskódú licenc alapján tesz közzé digitális elemeket tartalmazó szoftverterméket, de csak az adományozó felhasználók számára biztosít letölthető kiadásokat és biztonsági frissítéseket. Azok a felhasználók, akik nem adományoznak, nem férnek hozzá a szoftver aktuális verziójához.

Ebben az esetben az adomány valójában a digitális elemeket tartalmazó termékhez való hozzáférés feltétele, ennélfogva előírása ár felszámítását valósítja meg. A szabad és nyílt forráskódú szoftvert ezért a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak kell tekinteni.

22. példa: Egy természetes vagy jogi személy nyilvánosan hozzáférhetővé teszi a szabad és nyílt forráskódú szoftver forráskódját, de az előfordított bináris kódot, a rendszeres frissítéseket és a garantált biztonsági javításokat csak adományozók számára biztosít. Ebben az esetben az adományok a digitális elemeket tartalmazó termék alapvető jellemzőihez való hozzáféréshez kapcsolódnak, és az adott termék rendelkezésre bocsátásáért adott ellenszolgáltatásnak minősülnek. A szabad és nyílt forráskódú szoftvert ezért kereskedelmi tevékenység keretében forgalomba hozottnak kell tekinteni.

3.2.5. *A szabad és nyílt forráskódú szoftver finanszírozása*

63. Az, hogy egy harmadik fél fizetett egy szabad és nyílt forráskódú szoftver fejlesztéséért, illetve azt szponzorálta vagy más módon finanszírozta, önmagában nem határozza meg, hogy az adott szabad és nyílt forráskódú szoftver forgalomba hozottnak minősül-e. A szabad és nyílt forráskódú szoftver-ökoszisztémában bevett gyakorlat, hogy az egyéni fejlesztők, az alapítványok vagy a közösségek vállalkozásoktól, közjogi szervektől vagy más szponzoroktól finanszírozásban részesülnek annak érdekében, hogy konkrét jellemzőkön dolgozzanak, hibákat javítsanak ki, vagy kritikus fontosságú alkotóelemeket tartsanak fenn. Ez a finanszírozás számos formát ölthet, beleértve a vissza nem térítendő támogatásokat, a hibák azonosításáért felajánlott („bug bounty”) díjakat, a szponzorálást, a szolgáltatási szerződéseket vagy a fizetés ellenében végzett fejlesztési munkákat.

64. A már jelzett módon a kiberrezilienciáról szóló rendelet (18) preambulumbekezdése pontosítja, hogy „annak meghatározásakor, hogy a tevékenység kereskedelmi […] jellegű-e, nem kell figyelembe venni a digitális elemeket tartalmazó termék kifejlesztésének puszta körülményeit, illetve a fejlesztés finanszírozásának módját”.

65. Ezért ha hozzáférés, felhasználás, módosítás és továbbterjesztés céljából a szabad és nyílt forráskódú szoftvert nyíltan megosztják és mindenki számára szabadon hozzáférhetővé teszik, annak megállapításában, hogy a szoftver forgalomba hozott-e, nem játszhat szerepet az, hogy egy kereskedelmi szervezet esetleg fizetett az adott projektért. Valójában ha az említett szabad és nyílt forráskódú szoftvert egyébként nem monetizálják, nem tekinthető forgalomba hozottnak. Amennyiben a szabad és nyílt forráskódú szoftver fejlesztését finanszírozó vállalkozás (és bármely más vállalkozás) integrálja azt a digitális elemeket tartalmazó termékébe, a vállalkozásnak a kiberrezilienciáról szóló rendelet 13. cikkének (5) bekezdésével összhangban kellő gondossággal kell eljárnia.

23. példa: Egy egyéni fejlesztő szabad és nyílt forráskódú szoftverprojektet tesz közzé, és aktívan karbantartja azt. Az „A" gyártó felkéri az egyéni fejlesztőt az adott szabad és nyílt forráskódú szoftvert külön jellemzővel való kiegészítésére, és finanszírozza a fejlesztést. A fejlesztő a jellemzőt hozzáadja a szabad és nyílt forráskódú szoftver kódbázisához, nyíltan megosztja azt, és mindenki számára szabadon hozzáférhetővé teszi hozzáférés, felhasználás, módosítás és továbbterjesztés céljából. Nem tekintendő úgy, hogy az egyéni fejlesztő forgalomba hozta a szóban forgó szabad és nyílt forráskódú szoftvert. Ha a gyártó a szabad és nyílt forráskódú szoftvert integrálja a digitális elemeket tartalmazó termékébe, a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia.

3.2.6. *Nonprofit célok elérésére létrehozott nonprofit szervezetek*

66. Amennyiben a szabad és nyílt forráskódú szoftvert közzétevő jogi személy nonprofit szervezet, és azt „úgy hozzák létre, hogy a költségek utáni összes bevételt nonprofit célok elérésére használják fel" (a kiberrezilienciáról szóló rendelet (18) preambulumbekezdése), az általa közzétett szabad és nyílt forráskódú szoftver nem minősül forgalomba hozottnak. Ha ez a jogi személy rendelkezik a „támogató" ismérveivel, a megfelelő kötelezettségek vonatkoznak rá (a kiberrezilienciáról szóló rendelet 24. cikke).

24. példa: Egy jogi személy szabad és nyílt forráskódú böngészőt tesz közzé, amelyet közvetlenül a keresőmotor-partnerségeken keresztül monetizálnak, de a teljes nettó eredményét nonprofit célokra használják fel. A böngésző a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak. A közzétevő jogi személyre a támogatói kötelezettségek vonatkoznak.

3.2.7. *Más gyártók általi integráció*

67. Egyes esetekben a szabad és nyílt forráskódú szoftvert egy egyértelműen azonosítható természetes vagy jogi személy teszi közzé, de a szabad és nyílt forráskódú szoftvert „más gyártók digitális elemeket tartalmazó saját termékeikbe történő integrálásra szánják". Ilyenkor ezen iránymutatás korábbi szakaszaival összhangban a szabad és nyílt forráskódú szoftver nem minősül az uniós piacon forgalomba hozottnak, kivéve, ha azt a közzétevő személy (az eredeti gyártó) is monetizálja.

68. Ha a szabad és nyílt forráskódú szoftvert nem hozzák forgalomba, az azt közzétevő jogi személyt – ha tartós támogatást nyújt – a „támogató" fogalommeghatározásával összhangban támogatói kötelezettségek terhelik.

25. példa: Egy jogi személy szabad és nyílt forráskódú szoftverkönyvtárat tesz közzé felhasználói felületek kialakításához. A könyvtár rendelkezésre bocsátását nem monetizálja, hanem azt integrálja az egyik digitális elemeket tartalmazó termékébe (amelyet viszont forgalomba hoznak). A könyvtár a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak, de digitális elemeket tartalmazó termékekbe való integrálásra szánják. A közzétevő jogi személy a könyvtár támogatója.

26. példa: Egy jogi személy operációs rendszert hoz forgalomba, emellett szabad és nyílt forráskódú szoftverkönyvtárakat is közzétesz, amelyek az operációs rendszer felhasználói számára referenciaimplementációként szolgálnak. A jogi személy nem monetizálja a szabad és nyílt forráskódú szoftverkönyvtárakat, amelyeket más, digitális elemeket tartalmazó termékekbe való integrálásra szánnak. A közzétevő jogi személy a szabad és nyílt forráskódú szoftverkönyvtárak támogatója.

3.3. **A nyílt forráskódú szoftverek támogatói**

69. A kiberrezilienciáról szóló rendelet bevezeti a „nyílt forráskódú szoftverek támogatójának" új jogi kategóriáját, „[f]igyelembe véve a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó, [a kiberrezilienciáról szóló] rendelet értelmében nyilvánosságra hozott, de a piacon nem forgalmazott számos termék kiberbiztonságának fontosságát" (a kiberrezilienciáról szóló rendelet (19) preambulumbekezdése).

70. Egyes esetekben a szabad és nyílt forráskódú szoftvert olyan jogi személy teszi közzé a kiberrezilienciáról szóló rendelet értelmében vett forgalmazás nélkül, amelynek „célja vagy célkitűzése, hogy rendszeres és tartós támogatást nyújtson [gazdasági tevékenységekhez szánt, szabad és nyílt forráskódú szoftverek] fejlesztéséhez, és amely biztosítja az említett termékek életképességét" (a kiberrezilienciáról szóló rendelet 3. cikkének 14. pontja). Ilyenkor az említett jogi személyre a támogatói kötelezettségek vonatkoznak.

71. A támogató „a gyártótól eltérő jogi személy”, mivel a gyártó definíció szerint az a természetes vagy jogi személy, aki vagy amely a digitális elemeket tartalmazó termékeket saját neve vagy védjegye alatt forgalomba hozza. Jogi személy csak olyan, szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek támogatója lehet, amelyeket közzétesznek, de a kiberrezilienciáról szóló rendelet értelmében nem forgalmaznak. A támogató fogalma ezért a szabad és nyílt forráskódú szoftver olyan konkrét eseteire vonatkozik, amelyeket „végső soron kereskedelmi tevékenységekre szánnak, mint például kereskedelmi szolgáltatásokba vagy digitális elemeket tartalmazó, pénzzé tett termékekbe való integrálásra” (a kiberrezilienciáról szóló rendelet (19) preambulumbekezdése ([13])), de amelyeket a kiberrezilienciáról szóló rendelet értelmében nem forgalmaznak, és amelyek tekintetében a szabad és nyílt forráskódú szoftvert közzétevő jogi személy szisztematikus támogatást biztosít.

72. Az, hogy a jogi személy egy adott szabad és nyílt forráskódú szoftver támogatója, nem jelenti azt, hogy az általa közzétett többi szabad és nyílt forráskódú szoftver tekintetében is szükségszerűen támogató. Ugyanígy az, hogy a jogi személy egy adott szabad és nyílt forráskódú szoftver gyártója, nem jelenti azt, hogy nem lehet más szabad és nyílt forráskódú szoftver támogatója. Ez utóbbi eset magában foglalja azt is, ha a jogi személy a *3.2.1.* szakaszban (*Charging a price*) leírtak szerint ugyanazon szabad és nyílt forráskódú szoftver „közösségi” verzióit bocsátja rendelkezésre.

73. Egy jogi személy ezért egyszerre lehet egy adott szabad és nyílt forráskódú szoftver támogatója (e minőségében rendszeres és tartós támogatást nyújt, és biztosítja a szoftver életképességét) és egy másik szabad és nyílt forráskódú szoftver gyártója (amelyet e minőségében forgalomba hoz). Más szóval elvárás lehet, hogy ugyanaz a jogi személy különböző szerepeket töltsön be a különböző szabad és nyílt forráskódú szoftverprojektekben.

74. A jogi személynek az általa közzétett minden egyes szabad és nyílt forráskódú szoftver esetében meg kell győződnie arról, hogy az a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak minősül-e. Ha igen, a jogi személy a szoftver gyártójának minősül. Ha a szabad és nyílt forráskódú szoftver nem minősül forgalomba hozottnak, a jogi személy akkor lehet annak támogatója, ha a szoftvert kereskedelmi tevékenységekre szánják, és ha azt a jogi személy a „támogató” fogalommeghatározásával összhangban tartja fenn ([14]).

3.3.1. *A szabad és nyílt forráskódú szoftver tartós támogatása és életképességének biztosítása*

75. A (19) preambulumbekezdés kifejti, hogy a digitális elemeket tartalmazó termék fejlesztéséhez nyújtott tartós támogatás többek között a következőket foglalhatja magában: i. a szoftverfejlesztési együttműködési platformok tárhelyszolgáltatását és kezelését, ii. a forráskód vagy szoftver tárhelyszolgáltatását, iii. a szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékek irányítását vagy kezelését, valamint iv. a digitális elemeket tartalmazó termékek fejlesztésének irányítását.

76. Ilyen helyzet adódhat például egy olyan jogi személy esetében, amely a szabad és nyílt forráskódú szoftvert a digitális elemeket tartalmazó saját termékeibe való integrálás céljából fejleszti, majd forgalomba hozatal nélkül közzéteszi. Ezt a *3.2.7.* szakasz (*Integration by other manufacturers*) is tárgyalja. Ebben az esetben a jogi személy nem a szoftver gyártója, de annak támogatója lehet. Emellett az előző szakaszokban kifejtett módon az a jogi személy, amely ugyanazon szabad és nyílt forráskódú szoftver ingyenes (vagy közösségi) verzióját és monetizált verzióját is közzéteszi, az ingyenes (vagy közösségi) verzió támogatójának, a monetizált verzió gyártójának minősül.

77. Ugyanígy az a jogi személy, amely szabad és nyílt forráskódú szoftvert monetizál, de nonprofit szervezet, amelynek a teljes nettó eredményét nonprofit célok elérésére használják fel (és ennélfogva, amint azt a *3.2.6.* szakasz (*Not-for-profit entities*) tárgyalja, a szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak), az általa közzétett szabad és nyílt forráskódú szoftver támogatója.

78. Emellett egyes alapítványok különböző irányítási formákkal rendelkező együttműködési platformokat kínálnak, amelyek lehetővé teszik a gyártók számára, hogy rendszeresen hozzájáruljanak a szabad és nyílt forráskódú szoftver fejlesztéséhez, és/vagy amelyeket a gyártók rendszeresen finanszíroznak. Az ilyen alapítvány a gazdasági tevékenységekre szánt konkrét szabad és nyílt forráskódú szoftver támogatója, amely a szoftverhez tartós támogatást nyújt. A *3.3.* szakaszban (*Open-source software stewards*) kifejtettek szerint azonban az ilyen alapítványra nem feltétlenül vonatkoznak a kiberrezilienciáról szóló rendelet szerinti kötelezettségek az általa saját tárhelyen működtetett egyéb konkrét szabad és nyílt forráskódú szoftver tekintetében, ha nem nyújt szisztematikus támogatást egy adott szabad és nyílt forráskódú szoftverhez, nem biztosítja annak életképességét, és/vagy ha az adott szoftvert nem kereskedelmi tevékenységekre szánják.

([13]) Ez a fogalom jelenik meg a „nyílt forráskódú szoftverek támogatójának” a kiberrezilienciáról szóló rendelet 3. cikkének 14. pontjában foglalt fogalommeghatározásában szereplő „gazdasági tevékenységekhez szánt” fordulatban is.

([14]) A jogi személyre emellett nem feltétlenül vonatkoznak a kiberrezilienciáról szóló rendelet szerinti kötelezettségek, nevezetesen ha i. az adott szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak, és ii. a jogi személy az adott szabad és nyílt forráskódú szoftver tekintetében nem felel meg a „támogató” fogalommeghatározásának.

79. Az alapítványok és hasonló szervezetek típusában jelentősen eltérő „tartós támogatást” nyújthatnak a szabad és nyílt forráskódú szoftverek egyes projektjeihez. Egyes jogi személyek például csak nem technikai jellegű támogatást nyújtanak, például a projektek márkaépítését irányítják, irányítási szabályokat állapítanak meg, közösségi rendezvényeket szerveznek vagy adományokat gyűjtenek. Más szervezetek is biztosítják a projekt működtetéséhez szükséges mögöttes informatikai infrastruktúrát, például forráskód-adattárak elhelyezését, verziókövető rendszerek biztosítását vagy aláírási kulcsok generálását. Mások kiterjedtebb típuskörben nyújtanak támogatást: aktívan hozzájárulnak a projekt mérnöki erőforrásaihoz például fejlesztők alkalmazásával, emellett koordinálják a fejlesztési munkát, elvégzik a kódok felülvizsgálatát vagy összefésülését, menedzselik a szoftverkiadásokat, illetve kezelik a sérülékenységi jelentéseket és a biztonsági javításokat. Míg a kiberrezilienciáról szóló rendelet szerint támogatónak minősülő valamennyi jogalanynak meg kell felelnie a 24. cikk (1) és (2) bekezdésében foglalt kötelezettségeknek, a 14. cikk (1), (3) és (8) bekezdésében meghatározott kötelezettségek e jogalanyokra való alkalmazásának mértéke az általuk nyújtott támogatás típusától függően változik, a 24. cikk (3) bekezdésével összhangban.

80. Például a kizárólag nem technikai támogatást nyújtó támogató definíció szerint nem vesz részt a digitális elemeket tartalmazó termék fejlesztésében, ezért nem köteles bejelenteni az aktívan kihasznált sérülékenységeket. Az említett támogató továbbá nem biztosít hálózati és információs rendszereket e digitális elemeket tartalmazó termékek fejlesztéséhez, ennélfogva nem köteles jelenteni a súlyos incidenseket az ENISA-nak és a CSIRT-eknek vagy az érintett felhasználóknak. Mindazonáltal, ha a támogató – pl. külső forrásokból, többek között biztonsági kutatóktól származó jelentés révén – tudomást szerez egy aktívan kihasznált sérülékenységről, kiberbiztonsági politikájával összhangban meg kell osztania az információkat a digitális elemeket tartalmazó termék karbantartóival. A digitális elemeket tartalmazó termékek karbantartóinak és/vagy a támogatóknak fontolóra kell venniük a sérülékenység 15. cikk szerinti önkéntes bejelentését is.

81. Másrészt, ha a támogató biztosítja a mögöttes informatikai infrastruktúrát bizonyos digitális elemeket tartalmazó termékekhez, a 14. cikk (3) bekezdésével összhangban be kell jelentenie az ENISA-nak és a CSIRT-eknek az ezen infrastruktúrával kapcsolatos minden olyan súlyos incidenst, amely hatással van a digitális elemeket tartalmazó termékek biztonságára. Adott esetben valamennyi felhasználót tájékoztatni kell (pl. általános bejelentés útján). Amint azt az előző pontban jeleztük, bár a támogatónak nem kell bejelentenie a tudomására jutott, aktívan kihasznált sérülékenységeket, elő kell mozdítania a sérülékenységek helyes kezelését, és fontolóra kell vennie a 15. cikk szerinti önkéntes jelentéstételt.

82. Végül ha egy támogató műszaki erőforrásokat is biztosít digitális elemeket tartalmazó konkrét termékekhez, a következő kötelezettségek is terhelik: i. a 14. cikk (1) bekezdésével összhangban be kell jelentenie azokat az aktívan kihasznált sérülékenységeket, amelyekről tudomást szerez, ii. adott esetben valamennyi felhasználót tájékoztatnia kell. Amennyiben a támogató közvetlen kapcsolatban is áll az érintett felhasználókkal, a 14. cikk (8) bekezdésével összhangban közvetlenül tájékoztatnia kell őket is.

83. Amennyiben egy szervezet már nem nyújt tartós és szisztematikus támogatást egy adott szabad és nyílt forráskódú szoftverhez, előfordulhat, hogy már nem felel meg a támogató fogalommeghatározásának, ezért a vonatkozó kötelezettségek sem terhelik. Ilyenkor ajánlott, hogy a jogalany egyértelműen közölje az adott szabad és nyílt forráskódú szoftverre vonatkozóan a jogállásában bekövetkezett változást.

84. Bizonyos helyzetekben az adott projekt támogatójaként eljárt jogalany dönthet úgy, hogy közvetlenül monetizálja a projektet, és ezáltal forgalomba hozza a digitális elemeket tartalmazó terméket. Ezzel a jogalanyra nézve beállnak a kiberrezilienciáról szóló rendelet szerinti gyártói kötelezettségek. Ilyen körülmények között e jogalany a digitális elemeket tartalmazó termék gyártójának minősül attól a naptól kezdve, amikor azt forgalomba hozza (de nem azon korábbi verziók tekintetében, amelyek tekintetében támogatóként járt el).

3.4. **Közreműködők és továbbfelhasználás**

85. A 3.1. szakaszban (*Determining if free and open-source software is* under one's responsibility) már említett módon a kiberrezilienciáról szóló rendelet egyértelművé teszi, hogy nem alkalmazandó „azokra a természetes vagy jogi személyekre, akik forráskóddal járulnak hozzá az olyan szabad és nyílt forráskódú szoftvernek minősülő, digitális elemeket tartalmazó termékekhez, amelyek nem tartoznak a felelősségi körükbe” ((18) preambulumbekezdés).

86. A szabad és nyílt forráskódú szoftver-alkotóelemeket a saját, digitális elemeket tartalmazó termékeikbe integráló gyártók sem lesznek felelősek azért, hogy az ilyen alkotóelemek egyedileg megfeleljenek a kiberrezilienciáról szóló rendeletnek, még akkor sem, ha a gyártók forráskóddal járulnak hozzá azok karbantartásához.

87. Ugyanígy önmagában az, hogy a gyártók szabad és nyílt forráskódú szoftver-alkotóelemeket integrálnak a digitális elemeket tartalmazó saját (monetizált) termékeikbe, nincs hatással az adott szabad és nyílt forráskódú szoftver-alkotóelemnek a kiberrezilienciáról szóló rendelet szerinti státuszára. A forgalomba nem hozott szabad és nyílt forráskódú szoftver-alkotóelemek karbantartóit nem terhelik kötelezettségek más olyan szervezetekkel összefüggésben, amelyek ezeket az alkotóelemeket integrálhatják a digitális elemeket tartalmazó termékeikbe. Az, hogy a kiberrezilienciáról szóló rendelet az adott szabad és nyílt forráskódú szoftver-alkotóelemre alkalmazandó-e, kizárólag attól függ, hogy az azt közzétevő természetes vagy jogi személy forgalomba hozza-e azt.

88. Mindazonáltal a digitális elemeket tartalmazó, szabad és nyílt forráskódú szoftver-alkotóelemeket integráló termékek gyártóinak a digitális elemeket tartalmazó saját termékeik tekintetében meg kell felelniük a kiberrezilienciáról szóló rendeletnek. A 13. cikk (5) bekezdésével összhangban a kellő gondosságra vonatkozó kötelezettség is terheli őket az általuk integrált szabad és nyílt forráskódú szoftver-alkotóelemek tekintetében. Emellett a 13. cikk (6) bekezdésével összhangban jelenteniük kell az integrált alkotóelemek sérülékenységeit, és meg kell osztaniuk a biztonsági javításokat. A témával kapcsolatos további iránymutatásért lásd a *9.2.1.* szakaszt (*Reporting upstream and sharing security fixes*).

3.5. **Szemléltető forgatókönyvek**

89. Az alábbiakban felsorolt példák teljesen elméleti jellegűek, és csak a fenti szakaszokban ismertetett különböző esetek szemléltetésére szolgálnak.

27. példa: „A” egyéni fejlesztő szabad és nyílt forráskódú szoftvert fejlesztett ki. „A” fejlesztő ezt a szabad és nyílt forráskódú szoftvert saját neve vagy védjegye alatt teszi közzé, de a használatáért nem számít fel árat. A szoftvert nyíltan megosztja és az hozzáférés, felhasználás, módosítás és továbbterjesztés céljából mindenki számára szabadon hozzáférhető. „A” fejlesztő az önkéntes adományok gyűjtésére szolgáló platformra mutató linket is mellékel.

A „B”, a „C” és a „D” vállalkozás ezt a szabad és nyílt forráskódú szoftvert integrálja saját, digitális elemeket tartalmazó termékeibe. A folyamatos karbantartás támogatása érdekében a „B”, a „C” és a „D” vállalkozás önkéntes adományokat nyújt „A” fejlesztőnek. Ezek az adományok lehetővé teszik „A” fejlesztő számára, hogy aktívan fenntartsa a projektet.

A szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak. „A” fejlesztőt nem terhelik a kiberrezilienciáról szóló rendelet szerinti kötelezettségek. A „B”, a „C” és a „D” vállalkozásnak a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia, amikor integrálja a szabad és nyílt forráskódú szoftvert a digitális elemeket tartalmazó saját termékeibe.

28. példa: Az „F” nonprofit alapítvány szabad és nyílt forráskódú szoftver-alkotóelemet tesz közzé más, digitális elemeket tartalmazó kereskedelmi termékekbe való integrálás céljából. Az „F” alapítvány vállalja, hogy a szabad és nyílt forráskódú szoftver tartós támogatásával biztosítja annak életképességét és elterjedését. Az „A”, a „B” és a „C” vállalkozás ezt a szabad és nyílt forráskódú szoftvert integrálja saját, digitális elemeket tartalmazó termékeibe. Az „A” és a „B” vállalkozás fejlesztői idejének egy részével önkéntesen hozzájárul az „F” alapítványon belüli szabad és nyílt forráskódú szoftverprojektek fejlesztéséhez és karbantartásához, beleértve az adott szabad és nyílt forráskódú szoftvert is.

Mivel az „F” alapítvány nonprofit szervezet, amelynek kialakítása biztosítja, hogy a teljes nettó eredményét nonprofit célok elérésére használják fel, a szabad és nyílt forráskódú szoftver a kiberrezilienciáról szóló rendelet értelmében nem minősül forgalomba hozottnak. Az „F” alapítvány a szabad és nyílt forráskódú szoftver támogatója, és a 24. cikkben meghatározott megfelelő kötelezettségek vonatkoznak rá. Az „A”, a „B” és a „C” vállalkozásnak a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia, amikor integrálja a szabad és nyílt forráskódú szoftvert a digitális elemeket tartalmazó saját termékeibe.

29. példa: Az „A” vállalkozás szabad és nyílt forráskódú szoftver-alkotóelemet fejlesztett ki a digitális elemeket tartalmazó saját termékeibe való integrálás céljára. Ezt a szabad és nyílt forráskódú szoftvert saját neve vagy védjegye alatt külön is közzéteszi, és aktívan karbantartja. Használatáért azonban nem számít fel díjat, és más módon sem monetizálja. A „B”, a „C” és a „D” vállalkozás ezt a szabad és nyílt forráskódú szoftvert integrálja a digitális elemeket tartalmazó saját termékeibe, és fejlesztői idejének egy részével önkéntesen hozzájárul annak karbantartásához.

A szabad és nyílt forráskódú szoftvert a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak kell tekinteni. Az „A” vállalkozás a szoftvernek nem gyártója, hanem támogatója. A „B”, a „C” és a „D” vállalkozásnak a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia, amikor integrálja a szabad és nyílt forráskódú szoftvert a digitális elemeket tartalmazó saját termékeibe.

30. példa: Az „A” vállalkozás saját neve vagy védjegye alatt szabad és nyílt forráskódú szoftvert tesz közzé, és azt fizetős verzióban kínálja, amely bizonyos előnyöket, például technikai segítségnyújtást vagy teljesítményoptimalizálást is magában foglal. A „B”, a „C” és a „D” vállalkozás fejlesztői hozzájárulnak a szabad és nyílt forráskódú szoftver karbantartásához, amely azonban továbbra is az „A” vállalkozás ellenőrzése alatt marad.

Az „A” vállalkozás az adott szabad és nyílt forráskódú szoftver gyártójának minősül ([15]). A „B”, a „C” és a „D” vállalkozásra az adott szabad és nyílt forráskódú szoftver tekintetében nem vonatkoznak a kiberrezilienciáról szóló rendelet szerinti kötelezettségek. Ha az említett szabad és nyílt forráskódú szoftvert integrálják saját, digitális elemeket tartalmazó termékeikbe, a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárniuk.

31. példa: Az „A” vállalkozás saját neve vagy védjegye alatt szabad és nyílt forráskódú szoftvert tesz közzé, és folyamatos karbantartással biztosítja annak hosszú távú életképességét, hogy lehetővé tegye a szoftver integrálását más vállalkozások digitális elemeket tartalmazó termékeibe. Az „A” vállalkozás nem számít fel díjat a felhasználásáért, nem kezel a digitális elemeket tartalmazó terméken keresztül gyűjtött személyes adatokat, és nem értékesít támogatási szolgáltatásokat a szabad és nyílt forráskódú szoftver közzétételével kapcsolatban.

A „B” vállalkozás kóddal és fejlesztői idővel járul hozzá a szabad és nyílt forráskódú szoftver karbantartásához, de azt kereskedelmi jelleggel nem terjeszti. A „B” vállalkozás a szabad és nyílt forráskódú szoftver terjesztésétől függetlenül technikai támogatási szolgáltatásokat nyújt. A szóban forgó szabad és nyílt forráskódú szoftver vonatkozásában az „A” vállalkozás tekintendő támogatónak, míg a „B” vállalkozásnak a kiberrezilienciáról szóló rendelet alapján nincsenek kötelezettségei az adott szoftver tekintetében.

32. példa: Szabad és nyílt forráskódú szoftver-alkotóelemet tesz közzé egy olyan nonprofit szervezet, amelynek kialakítása biztosítja, hogy a teljes nettó eredményét nonprofit célok elérésére használják fel. A szervezet tartós támogatást nyújt, hogy biztosítsa a projekt hosszú távú életképességét. A karbantartás finanszírozása közfinanszírozásból, például kutatási támogatásokból történik. A további fejlesztéseket, beleértve az új jellemzőket is, adományokból és konkrét projektekből finanszírozzák, amelyeket azokkal a gyártókkal partnerségben hajtanak végre, amelyek a szabad és nyílt forráskódú szoftvert integrálják a digitális elemeket tartalmazó termékeikbe. Ezek a jellemzők beépülnek a szabad és nyílt forráskódú szoftver kódbázisába.

A szabad és nyílt forráskódú szoftvert közzétevő nonprofit szervezet tekintendő az adott szabad és nyílt forráskódú szoftver-alkotóelem támogatójának. Az egyes jellemzők fejlesztésében közreműködő gyártó nem válik az adott szabad és nyílt forráskódú szoftver-alkotóelem gyártójává. Ha a gyártó az adott szabad és nyílt forráskódú szoftver-alkotóelemet integrálja saját, digitális elemeket tartalmazó termékébe, a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia.

33. példa: Egy nonprofit szervezet, amelynek kialakítása biztosítja, hogy a teljes nettó eredményét nonprofit célok elérésére használják fel, szoftverfejlesztő csomagot (SDK) tesz közzé, és biztosítja annak folyamatos karbantartását. Az SDK-t nyíltan megosztják és az hozzáférés, felhasználás, módosítás és továbbterjesztés céljából mindenki számára szabadon hozzáférhető. A finanszírozás a nonprofit szervezetnek fizetett tagsági díjakból történik, a tagszervezetek által alkalmazott fejlesztők pedig kóddal és egyéb erőforrásokkal járulnak hozzá az SDK fejlesztéséhez. Gyártók az SDK-t más, digitális elemeket tartalmazó termékek gyártásához használják fel alkotóelemként.

Az SDK támogatója az a nonprofit szervezet, amely közzéteszi. Az alapítvány tagjai nem felelnek azért, hogy az SDK megfelel-e a kiberrezilienciáról szóló rendeletnek. Amennyiben a gyártók az SDK-t saját, digitális elemeket tartalmazó termékük gyártásához használják, a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárniuk.

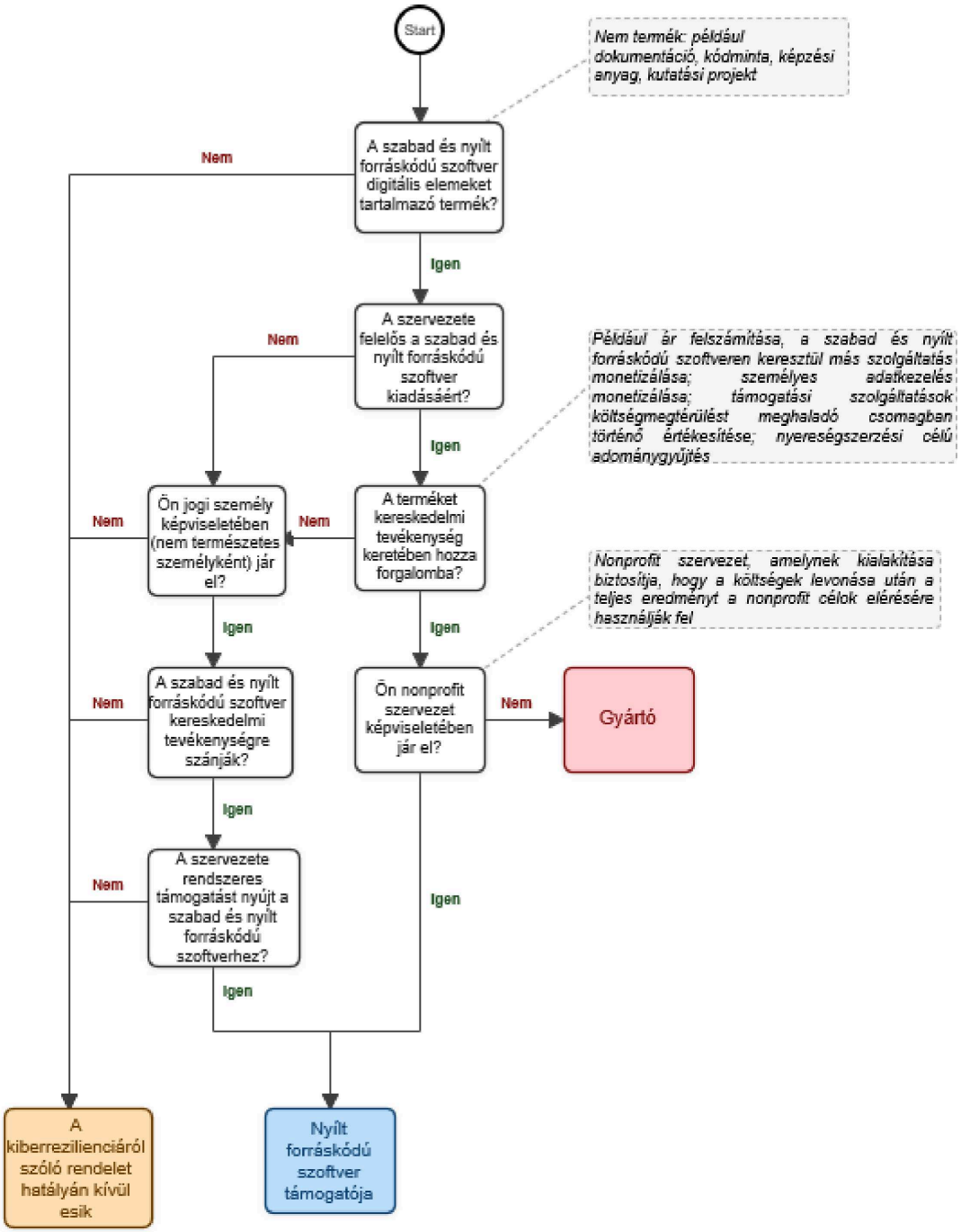
34. példa: Egy egyéni fejlesztő egy adott programozási nyelv nyilvános csomagtárában szabad és nyílt forráskódú szoftverkönyvtárat tesz közzé, és azt aktívan karbantartja. A csomagdokumentációban a fejlesztő adománygyűjtési célú linket tüntet fel. Egy gyártó ingyenesen letölti ezt a könyvtárat az adattárból, és integrálja azt saját, digitális elemeket tartalmazó termékébe.

Az egyéni fejlesztőt és a csomagtárat nem terhelik a kiberrezilienciáról szóló rendelet szerinti kötelezettségek. A könyvtárat integráló gyártónak a 13. cikk (5) bekezdésével összhangban kellő gondossággal kell eljárnia.

([15]) Kivéve, ha az „A” vállalkozás nonprofit szervezet, amelynek kialakítása biztosítja, hogy a teljes nettó eredményét nonprofit célok elérésére használják fel, amely esetben a vállalkozás az adott szabad és nyílt forráskódú szoftver támogatója.

1. ábra:

Stilizált folyamatábra a kiberrezilienciáról szóló rendelet hatálya alá tartozó szabad és nyílt forráskódú szoftverek azonosításához



4. JELENTŐS MÓDOSÍTÁSOK ÉS TARTALÉK ALKATRÉSZEK

90. A kiberrezilienciáról szóló rendelet 3. cikkének 30. pontjában foglalt meghatározás szerint a jelentős módosítás „a digitális elemeket tartalmazó termék olyan módosítása a forgalomba hozatalát követően, amely [i.] hatással van a digitális elemeket tartalmazó termék I. melléklet I. részében meghatározott alapvető kiberbiztonsági követelményeknek való megfelelésre, vagy [ii.] annak a rendeltetésnek a módosulását eredményezi, amely tekintetében a digitális elemeket tartalmazó terméket értékelték”.

91. A jelentős módosítás fogalma a kiberrezilienciáról szóló rendelet szerinti kötelezettségek megállapítása szempontjából számos esetben releváns, többek között a következőkben:

a) a 21. cikkel összhangban a már forgalomba hozott, digitális elemeket tartalmazó terméken jelentős módosítást végrehajtó importőrt vagy forgalmazót kell a termék gyártójának tekinteni;

b) a 22. cikkel összhangban minden olyan természetes vagy jogi személy, aki vagy amely digitális elemeket tartalmazó terméken jelentős módosítást hajt végre, és azt forgalmazza, a termék gyártójának tekintendő;

c) a 69. cikk (2) bekezdésével összhangban minden olyan természetes vagy jogi személy, aki vagy amely 2027. december 11. előtt forgalomba hozott, digitális elemeket tartalmazó terméken 2027. december 11. után jelentős módosítást hajt végre, és azt forgalomba hozza, a termék gyártójának tekintendő;

d) a 2027. december 11. után forgalomba hozott, digitális elemeket tartalmazó termékek gyártói esetében annak meghatározása érdekében, hogy a digitális elemeket tartalmazó terméket alá kell-e vetni új megfelelőségértékelési eljárásnak az említett időpontot követően bekövetkezett változások miatt, különös tekintettel a szoftverfejlesztés iteratív jellegére.

92. Ezért fontos iránymutatást nyújtani annak érdekében, hogy a gazdasági szereplők megértsék, hogy a hardver- vagy szoftvermódosítások mikor minősülnek jelentős módosításnak.

4.1. **Fizikai javítások**

93. A kiberrezilienciáról szóló rendelet (42) preambulumbekezdése kimondja, hogy „[a]mennyiben valamely digitális elemeket tartalmazó termék az (EU) 2024/1781 európai parlamenti és tanácsi rendelet 2. cikkének 18., 19. és 20. pontjában meghatározott »felújítás«, »karbantartás« és »javítás« hatálya alá tartozik, az nem feltétlenül vezet a termék lényegi módosításához, ha például a rendeltetés és a funkciók nem változnak, és a kockázat szintje változatlan marad. A digitális elemeket tartalmazó termék gyártó általi korszerűsítése azonban e termék tervezésének és fejlesztésének megváltozásához vezethet, ezért hatással lehet annak rendeltetésére és az e rendeletben meghatározott követelményeknek való megfelelésére”. Ez összhangban van a kék útmutató 2.1. szakaszával, amely a következőkre hívja fel a figyelmet: „Új terméknek kell tekinteni azt a terméket, amely használatbavételét követően jelentős változásokon vagy átalakításon esett át, ha: i. eredeti teljesítménye, rendeltetése vagy típusa módosul, anélkül, hogy ezt a kezdeti kockázatértékelés előirányozta volna, ii. a veszély jellege megváltozott vagy a kockázat szintje növekedett a vonatkozó uniós harmonizációs jogszabályhoz képest, és iii. a terméket forgalmazzák (vagy üzembe helyezik, ha az alkalmazandó jogszabályok hatálya az üzembe helyezésre is kiterjed). Ezt eseti alapon, és főként a jogszabály céljára tekintettel és az adott jogszabály hatálya alá tartozó terméktípusok figyelembevételével kell elbírálni.”

94. A már forgalomba hozott, digitális elemeket tartalmazó termékek fizikai módosítását eredményező felújítási, karbantartási vagy javítási műveletek nem feltétlenül minősülnek jelentős módosításnak. Ezért eseti értékelést kell végezni annak megállapítása érdekében, hogy a fizikai módosítás befolyásolja-e a digitális elemeket tartalmazó termék I. melléklet I. részében foglalt alapvető követelményeknek való megfelelését, vagy a kiberbiztonsági kockázatértékelés tárgyát képező termék rendeltetésének megváltozását eredményezi-e.

95. A hibás alkatrészek vagy használt cikkek jobb teljesítményt nyújtó alkatrészekre való cseréje (pl. a műszaki fejlődés miatt vagy azért, mert a régi alkatrészt már nem gyártják) önmagában nem vonja maga után a digitális elemeket tartalmazó javított termék jelentős módosítását. Jelentős módosításnak csak abban az esetben minősül, ha a teljesítményváltozás vagy a digitális elemeket tartalmazó javított termék működési módja i. befolyásolja az alapvető követelményeknek való megfelelését, vagy ii. a rendeltetés olyan megváltozását eredményezi, amelyre a kockázatértékelés nem terjedt ki.

35. példa: Egy szerver gyártója javítási művelet keretében egy hibás RAM-ot új, jobb teljesítményű RAM-ra cserél. Ez nem érinti a szerver alapvető követelményeknek való megfelelését. A szerver teljesítménye jobb, de az új teljesítmény a szervernek a kiberbiztonsági kockázatértékelésben figyelembe vett rendeltetésszerű használatán belül marad. A szerver nem tekintendő jelentősen módosítottnak.

4.2. **Tartalék alkatrészek**

96. A kiberrezilienciáról szóló rendelet 2. cikkének (6) bekezdése megállapítja, hogy a rendelet nem alkalmazandó azokra a tartalék alkatrészekre, amelyek azonos alkotóelemek pótlására szolgálnak, és amelyeket ugyanazoknak az előírásoknak megfelelően gyártottak, mint az említett alkotóelemeket. A (29) preambulumbekezdés továbbá kimondja, hogy a mentesség kiterjed mind a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt forgalmazott, digitális elemeket tartalmazó termékek tartalék alkatrészeire, mind pedig azokra a tartalék alkatrészekre, amelyek már átestek a rendeletben meghatározott megfelelőségértékelési eljáráson.

97. A kiberrezilienciáról szóló rendelet 2. cikkének (6) bekezdésében foglalt mentességet úgy kell értelmezni, hogy az csak akkor alkalmazandó, ha a tartalék alkatrészt kifejezetten (2027. december 11. előtt vagy után) már forgalomba hozott, digitális elemeket tartalmazó termék javítása vagy tartósságának meghosszabbítása céljából bocsátják rendelkezésre. Ha egy digitális elemeket tartalmazó terméket önálló termékként bocsátanak rendelkezésre úgy, hogy az semmilyen módon nem kapcsolódik egy digitális elemeket tartalmazó, már meglévő termék karbantartásához vagy javításához, az a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak minősül, és nem tekintendő a 2. cikk (6) bekezdésének hatálya alá tartozó tartalék alkatrésznek. A karbantartási vagy javítási célnak egyértelműen ki kell tűnnie a rendelkezésre bocsátás kontextusából, például a digitális elemeket tartalmazó termék vagy termékcsalád megrendelésben vagy kereskedelmi ajánlatban való azonosítása, illetve értékesítés utáni vagy szolgáltatási csatornákon keresztül történő rendelkezésre bocsátása révén. Az ezt alátámasztó bizonyítékokat a piacfelügyeleti hatóságok számára is elérhetővé kell tenni. Az a tény, hogy a digitális elemeket tartalmazó termék műszakilag felhasználható valamely alkotóelem helyettesítésére, önmagában nem elegendő ahhoz, hogy ilyen elemek hiányában a termék a mentesség hatálya alá tartozzon.

98. Következésképpen, ha egy tartalék alkatrész azonos egy olyan, digitális elemeket tartalmazó termékben már szereplő alkotóelemmel, amelyet a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt vagy a rendeletnek megfelelően hoztak forgalomba, maga a tartalék alkatrész nem tartozik a rendelet hatálya alá.

99. Annak értékelése során, hogy egy tartalék alkatrészt egy alkotóelemmel azonosnak kell-e tekinteni, a digitális elemeket tartalmazó termékben betöltött funkcionális szerepére és a kiberbiztonság szempontjából esetlegesen releváns jellemzőkre kell összpontosítani. Bár mindig eseti értékelésre van szükség, azok a különbségek, amelyek nem befolyásolják az alkotóelem biztonsági jellemzőit vagy kiberbiztonsági kockázati profilját, önmagukban nem zárják ki azt, hogy az adott tartalék alkatrész a kiberrezilienciáról szóló rendelet 2. cikke (6) bekezdésének hatálya alá tartozzon.

100. Ezzel szemben az alkotóelemek kiberbiztonsága szempontjából releváns jellemzők – például algoritmusok, protokollok, kriptográfiai mechanizmusok, hozzáférés-ellenőrzési jellemzők vagy egyéb biztonsági vonatkozású jellemzők – közötti különbségek azt jelenthetik, hogy az új alkotóelem nem tekinthető azonosnak azzal, amelynek a helyettesítésére szánják.

101. Ha a tartalék alkatrész nem azonos az eredeti alkotóelemmel, a tartalék alkatrész önmagában is digitális elemeket tartalmazó terméknek minősül, ennélfogva a kiberrezilienciáról szóló rendelet hatálya alá tartozik. Ilyenkor az alapvető követelményeknek való megfelelést a csere-alkotóelem rendeltetésére tekintettel kell értékelni. Különösen fontos a csere-alkotóelem azon funkciója, hogy biztosítsa a digitális elemeket tartalmazó meglévő termékkel való kompatibilitást vagy interoperabilitást, beleértve azt az esetet is, amikor az említett termék a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt forgalomba hozott, digitális elemeket tartalmazó termék. Ha bizonyos alapvető követelmények az említett rendeltetés vagy műszaki korlátok miatt észszerűen nem teljesíthetők, a gyártónak ezt jeleznie kell a kiberbiztonsági kockázatértékelésben, és megfelelő alternatív vagy kompenzációs kockázatcsökkentő intézkedéseket kell végrehajtania annak érdekében, hogy ne ássa alá a digitális elemeket tartalmazó termék biztonságát. Amint azt a *2.6.* szakasz (*Complex systems*) is tárgyalja, mind a műszaki dokumentáció, mind a felhasználónak szóló információk és utasítások kulcsszerepet játszanak az azonosított korlátok, a kapcsolódó kiberbiztonsági kockázatok és a végrehajtott kockázatcsökkentő intézkedések átlátható leírásában. Amint azt a *4.1.* szakasz (*Physical repairs*) kifejti, a hibás alkatrészek vagy elhasználódott cikkek jobb teljesítményt nyújtó alkatrészekre való cseréje önmagában nem vonja maga után a digitális elemeket tartalmazó javított termék jelentős módosítását.

36. példa: Egy gyártó összekapcsolt vezérlőket hozott forgalomba az uniós piacon. Az egyik esetben a vezérlőt 2026-ban, a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt hozták forgalomba. A másik esetben a vezérlőt 2028-ban hozták forgalomba a kiberrezilienciáról szóló rendeletnek megfelelően. 2028-ban mindkét típusú vezérlő digitális kommunikációs modulja meghibásodik. A gyártó tartalék alkatrészként olyan cseremodult szállít, amely azonos az eredetivel, és amelyet ugyanazon előírásoknak megfelelően gyártottak.

A cseremodul mindkét esetben a 2. cikk (6) bekezdése szerinti mentesség hatálya alá tartozik. Maga a tartalék alkatrész nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá, még akkor sem, ha digitális elemeket tartalmazó termékről van szó, mivel egy digitális elemeket tartalmazó termék azonos alkotóelemét pótolja. A javítás nem minősül a digitális elemeket tartalmazó termék jelentős módosításának.

37. példa: Egy gyártó 2026-ban, a kiberrezilienciáról szóló rendelet alkalmazásának kezdőnapja előtt kapcsolt ipari vezérlőt hozott forgalomba az uniós piacon. 2028-ban a vezérlő kommunikációs mikrocsipje meghibásodik. Mivel a gyártó már nem gyártja ezt a csipet, a kompatibilitás fenntartása és a folyamatos működés érdekében tartalék alkatrészként azonos funkciójú, de eltérő kriptográfiai megvalósítással és frissített biztonságos rendszerindítási mechanizmussal rendelkező újabb csipet szállít.

Ebben az esetben a cserecsip nem tekinthető azonosnak, mivel a kriptográfiai megvalósítás és a biztonságos rendszerindítási mechanizmus eltérései befolyásolják a csip kiberbiztonsági tulajdonságait. Ezért a 2. cikk (6) bekezdése szerinti mentesség nem alkalmazható, és a csip a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó terméknek minősül. A cserealkatrész megfelelőségét a rendeltetése fényében kell értékelni, beleértve a kiberrezilienciáról szóló rendelet alkalmazásának megkezdése előtt forgalomba hozott, digitális elemeket tartalmazó termékkel való interoperabilitás biztosításában betöltött szerepét is.

38. példa: Egy gyártó 2028-ban a kiberrezilienciáról szóló rendeletnek megfelelően intelligens épületvezérlőt hoz forgalomba. 2029-ben az említett vezérlő vezeték nélküli modulja meghibásodik. Mivel a gyártó már nem gyártja ezt a modult, tartalék alkatrészként új modult szállít, amely ugyanazt a funkciót látja el ugyanazon kommunikációs protokollok és biztonsági mechanizmusok alkalmazásával, de más lapkakészleten alapul, és olyan frissített firmware-rel rendelkezik, amely nem változtatja meg a kiberbiztonság szempontjából esetlegesen releváns jellemzőket.

Ebben az esetben a cseremodul azonosnak tekinthető. A modul ezért a 2. cikk (6) bekezdése szerinti mentességben részesül, és nem tartozik a kiberrezilienciáról szóló rendelet hatálya alá.

102. A tartalék alkatrészekre vonatkozó mentesség attól függetlenül alkalmazandó, hogy a tartalék alkatrész a digitális elemeket tartalmazó termék valamely alkotóelemét pótolja-e, vagy egy nagyobb termék részét képező, digitális elemeket tartalmazó teljes terméket pótol-e, beleértve azt az esetet is, amikor a digitális elemeket tartalmazó nagyobb termék több integrált alkotóelemből áll, feltéve, hogy a cserealkatrészt az előző bekezdésekben kifejtett módon kifejezetten tartalék alkatrészként szállítják.

39. példa: 2027-ben egy gyártó olyan ipari automatizálási rendszert hoz forgalomba, amelynek egyik alkotóeleme a programozható logikai vezérlő (PLC). 2031-ben a PLC központi feldolgozó egysége (CPU) meghibásodik. A gyártó két javítási lehetőséget kínál: i. az eredetileg telepített CPU-val azonosnak tekinthető csere-CPU szállítása, vagy ii. teljes csere-PLC szállítása, amely azonosnak tekinthető az eredetileg telepített PLC-vel. A cseredarabot minden esetben a gyártó értékesítés utáni szolgáltatási csatornáján keresztül, tartalék alkatrészként bocsátják rendelkezésre, és egyértelműen meghatározzák azt az ipari automatizálási rendszert, amelyhez a cseredarabot szánják. A csere mindkét esetben a 2. cikk (6) bekezdése szerinti mentesség hatálya alá tartozik, függetlenül attól, hogy a csere a PLC-n belüli alkotóelemre vagy a PLC egészére vonatkozik-e.

4.3. **Szoftverfrissítések mint jelentős módosítások**

103. A szoftverfejlesztés iteratív folyamat; a már forgalomba hozott, digitális elemeket tartalmazó szoftvertermékeket gyakran és folyamatosan frissítik. Ebben az összefüggésben érdemes további iránymutatást nyújtani annak megállapításához, hogy mikor kell a szoftvert jelentősen módosítottnak tekinteni. Az iránymutatás célja különösen az, hogy a digitális elemeket tartalmazó szoftvertermékek azon gyártóit, akik saját termékeiken változtatásokat hajtanak végre, segítse annak megállapításában, hogy a változtatások jelentős módosításnak minősülnek-e.

104. A (39) preambulumbekezdés szerint a digitális elemeket tartalmazó termék lényegi módosítása valósul meg, ha a megváltoztatják a kiberbiztonsági kockázat szintjét, a gyártó pedig a kockázatértékelésben és következésképpen az alapvető követelmények végrehajtása során nem vette figyelembe a megváltozott vagy további kockázatot. A gyártónak ezért eseti alapon értékelnie kell, hogy a szoftverfrissítés új vagy megnövekedett kiberbiztonsági kockázatokat eredményez-e, és hogy ezeket a kockázatokat a kockázatértékelés már kezelte-e.

105. Ha a gyártó olyan új funkciókat vezet be a digitális elemeket tartalmazó termékbe, amelyek a termék rendeltetésének egészét érintő változást eredményeznek, valószínű, hogy a gyártó nem vette figyelembe ezeket a változásokat a kockázatértékelésében. Ilyen körülmények között a változás általában jelentős módosításnak minősül.

40. példa: Egy gyártó olyan műszerfalat hoz forgalomba, amely adatokat gyűjt gépekről, valamint tendenciákat és riasztásokat jelenít meg, de a gépek irányítására nem képes. A gyártó ezt követően kifejleszti a műszerfal új verzióját, és abban olyan funkciókat vezet be, amelyek lehetővé teszik számára a gépek irányítását, többek között a működési paraméterek beállításával és a gépek meghibásodást követő újraindításával. E változások eredményeként a műszerfal rendeltetése meghaladja a kockázatértékelésben előirányzottakat: a helyzetismereti eszköz egy olyan, digitális elemeket tartalmazó termékké alakult, amelynek rendeltetése más eszközök operatív kontrollja. A műszerfal ezért jelentősen módosult.

41. példa: Egy gyártó olyan fogyasztói szoftveralkalmazást hoz forgalomba, amelynek célja személyes adatok, például e-mailek, üzenetek vagy dokumentumok rendszerezése és megjelenítése, valamint az alapvető keresési és szűrési funkciók támogatása. A gyártó ezt követően olyan frissítést vezet be, amely lehetővé teszi az alkalmazás számára, hogy automatikusan elemezze a felhasználói tartalmat annak érdekében, hogy viselkedési profilokat hozzon létre, és automatizált döntéseket hozzon, amelyek felhasználói beavatkozás nélkül befolyásolják a tartalom rangsorolását, törlését vagy ajánlását. E változás eredményeként a szoftver rendeltetése megváltozik: a felhasználó által ellenőrzött információkezelési eszköz automatizált döntéshozatali rendszerré alakul, ami a kockázatértékelésben nem szerepelt. Az alkalmazás ezért jelentősen módosult.

106. Ugyanakkor azonban lehetséges, hogy a gyártó fokozatosan vezet be olyan új funkciókat, amelyek már szerepelnek a kockázatértékelésében, vagy amelyek önmagukban nem változtatják meg a digitális elemeket tartalmazó termék kiberbiztonsági kockázati profilját. Ilyen helyzet adódhat például akkor, ha a gyártó előre jelezte e funkciók fejlesztését, már leírta és értékelte a kapcsolódó kockázatokat, és megfelelő kockázatcsökkentő intézkedéseket hajtott végre az alapvető követelményeknek való folyamatos megfelelés biztosítása érdekében. Ez akkor is előfordulhat, ha az új funkciók nem vezetnek be olyan változtatásokat, amelyek új vagy megnövekedett kockázatokat eredményeznek. Az ilyen jellegű frissítések ezért nem tekintendők jelentős módosításoknak, mivel nem növelik a kiberbiztonsági kockázatot, és következésképpen nem változtatják meg az alapvető követelmények végrehajtását.

42. példa: Egy üzenetküldő alkalmazást eredetileg közvetlen üzenetküldésre korlátozódó funkciókkal adnak ki. A gyártó kockázatértékelése kiterjed a csoportos üzenetküldés későbbi bevezetésére, beleértve például az üzenettovábbítás megnövekedett összetettségét. Egy későbbi frissítés során a gyártó csoportos csevegési funkciót, valamint adminisztrátori kontrollokat és moderálási eszközöket vezet be, amelyeket az eredeti tervben már előirányoztak és értékeltek. A frissítés olyan funkciókat vezet be, amelyek az eredeti rendeltetés és a kockázatértékelés körébe tartoznak. Az üzenetküldő alkalmazás ezért nem módosult jelentősen.

43. példa: Egy gyártásfelügyeleti rendszert olyan formában hoznak forgalomba, amelyben a csak olvasható műszerfalak engedélyezettek, míg az automatizált vezérlési jellemzők jelen vannak a rendszer architektúrájában, de le vannak tiltva. A gyártó kockázatértékelése kifejezetten kiterjed az automatizált vezérlési ciklusok jövőbeli aktiválására, beleértve a zárthurkú vezérléssel kapcsolatos kiberbiztonsági kockázatokat, valamint az olyan biztonsági elemeket, mint az üzemeltető általi felülbírálás mechanizmusai és a hibabiztos állapotok. Egy későbbi frissítés során a gyártó engedélyezi az automatizált vezérlési jellemzőket, és aktiválja az eredetileg értékelt biztonsági elemeket. A termelés-ellenőrzési rendszer ezért nem módosult jelentősen.

107. Ezzel szemben még a korlátozott vagy látszólag kisebb jelentőségű új funkciók is jelentős kiberbiztonsági kockázatokat eredményezhetnek, amelyek hatással vannak az alapvető követelményeknek való megfelelésre. A jelentős módosítás értékelésének ezért nem a változás mértékén vagy összetettségén kell alapulnia, hanem a digitális elemeket tartalmazó termék kiberbiztonsági kockázati profiljára és következésképpen az alapvető követelmények végrehajtására gyakorolt lehetséges káros hatásán.

44. példa: Egy gyártó a szoftveralkalmazását a felhasználót „megjegyző” vagy tartós bejelentkezési jellemző hozzáadásával frissíti, amely a felhasználói kényelem javítása érdekében helyben tárolja a hitelesítési tokeneket. Bár a funkció alkalmazási köre korlátozott, olyan új – tokenlopáshoz, jogosulatlan hozzáféréshez és munkamenet-eltérítéshez kapcsolódó – kockázatokat eredményez, amelyeket a kockázatértékelés nem vett figyelembe. Az aktualizálás ezért hatással van az alapvető követelményeknek való megfelelésre. A szoftveralkalmazás jelentősen módosult.

45. példa: Egy gyártó új naplózási és diagnosztikai jellemzővel egészíti ki a digitális elemeket tartalmazó meglévő szoftvertermékét, lehetővé téve a részletes rendszernaplók hibaelhárítási célú exportálását. Bár a funkció látszólag nem jelentős, érzékeny műveleti adatok titkosítatlan formátumban történő gyűjtését és tárolását eredményezi, ami olyan adatkitettségi kockázatokat eredményez, amelyeket korábban nem értékeltek vagy csökkentettek. A változás ezért jelentős hatással lehet a digitális elemeket tartalmazó termék kiberbiztonsági kockázati profiljára. A digitális elemeket tartalmazó szoftvertermék jelentősen módosult.

108. A kiberrezilienciáról szóló rendelet (39) preambulumbekezdésével összhangban a biztonsági frissítések általában nem tekintendők jelentős módosításnak, mivel elsődleges céljuk a digitális elemeket tartalmazó termékkel kapcsolatos kiberbiztonsági kockázat szintjének csökkentése. Ezért az olyan biztonsági frissítés, amely nem módosítja a termék rendeltetését, és nem eredményez új kiberbiztonsági kockázatokat, nem tekinthető jelentős módosításnak még akkor sem, ha a frissítéssel bevezetett változtatások technikailag jelentősek. Ez magában foglalja azt az esetet is, amikor bizonyos funkciókat kizárólag az azonosított sérülékenységek csökkentése és az alapvető követelményeknek való folyamatos megfelelés biztosítása céljából módosítanak vagy korlátoznak.

46. példa: Egy gyártó biztonsági frissítést alkalmaz egy digitális elemeket tartalmazó termék kódbázisában lévő sérülékenység kezelésére, amelynek során kijavít egy potenciálisan puffertúlcsordulást eredményező bemeneti validálási hibát, vagy olyan logikai hibát javít, amely a nem megfelelő munkamenettoken-hitelesítés révén lehetővé teszi a hitelesítés megkerülését. A frissítés anélkül módosítja a szoftver belső implementációját, hogy befolyásolná a termék rendeltetését, vagy új kitettséget eredményezne. A frissítés kizárólagos célja a kiberbiztonsági kockázat csökkentése. A biztonsági frissítés nem tekintendő jelentős módosításnak.

47. példa: Egy gyártó olyan biztonsági frissítést vezet be, amely megerősíti a meglévő biztonsági konfigurációkat, például szigorítja a tűzfalra vonatkozó szabályokat, letiltja a használaton kívüli hálózati portokat, megváltoztatja az alapértelmezett adminisztrátor jelszavára vonatkozó szabályokat, vagy – ha a funkció már rendelkezésre állt vagy azt előirányozták – kötelezővé teszi a többtényezős hitelesítést. Bár a frissítés hatással lehet arra, hogy a felhasználók hogyan konfigurálják a digitális elemeket tartalmazó terméket vagy hogyan férnek hozzá ahhoz, nem változtatja meg annak rendeltetését, és kizárólag kiberbiztonsági helyzetének javítását szolgálja. A biztonsági frissítés nem tekintendő jelentős módosításnak.

48. példa: Egy gyártó olyan digitális elemeket tartalmazó szoftverterméket hoz forgalomba, amely a termék műszaki dokumentációjában és kockázatértékelésében leírtak szerint több kriptográfiai algoritmust és kulcsméretet támogató, konfigurálható titkosítási keret használatával biztosítja a kommunikációt. A kockázatértékelés kiterjed a digitális elemeket tartalmazó termékben biztosított valamennyi kriptográfiai lehetőségre, és előrevetíti bizonyos algoritmusok jövőbeli elavulását. A kockázatértékelés kockázatcsökkentő intézkedéseket is tartalmaz, például kriptográfiai agilitást, belső kulcskezelést és kompatibilitási tesztelést. A kriptográfiai iránymutatások alakulására reagálva a gyártó olyan biztonsági frissítést alkalmaz, amely egy elavult algoritmus letiltását követően erősebb, már támogatott alternatívát aktivál anélkül, hogy új külső függőségeket vezetne be vagy megváltoztatná az adatáramlást. Mivel a frissítés olyan biztonsági intézkedést hajt végre, amelyet az eredeti kialakítás részeként terveztek és értékeltek, továbbá nem eredményez új kiberbiztonsági kockázatokat, a biztonsági frissítés nem tekintendő jelentős módosításnak.

109. Ezzel szemben egy biztonsági frissítés jelentős módosításnak minősülhet, ha biztonsági célkitűzése ellenére azt eredményezi, hogy a digitális elemeket tartalmazó termék rendeltetése az eredetileg tervezettnél nagyobb mértékben módosul, vagy új vagy megnövekedett kiberbiztonsági kockázatokat eredményez. Ilyen helyzet adódhat például akkor, ha a frissítés a kockázatértékelésben nem előirányzott módon lényegesen megváltoztatja az adott termék határait vagy függőségi struktúráját, például az adatáramlások lényeges megváltoztatásával vagy új, kívülről elérhető interfészek hozzáadásával.

49. példa: Egy gyártó digitális elemeket tartalmazó szoftverterméket hoz forgalomba, amelynek rendeltetése, hogy a felhasználó eszközén tárolt adatfájlok helyi titkosításával lehetővé tegye a felhasználók számára a fájlok igény szerinti titkosítását és dekódolását. Miután sérülékenységet fedez fel a titkosítási munkafolyamatban, a gyártó biztonsági frissítést alkalmaz, amely eltávolítja a helyi titkosítási funkciót, és helyette előírja, hogy minden fájlt fel kell tölteni a gyártó által működtetett távoli titkosítási szolgáltatásba, ott kell tárolni és ott kell kezelni. E változás eredményeként a digitális elemeket tartalmazó termék már nem végez az eredeti rendeltetés szerinti helyi titkosítást, hanem távoli titkosítási és adatkezelési szolgáltatásként működik. Bár a frissítést biztonsági okokból vezetik be, a kockázatértékelésben nem előirányzott módon alapvetően megváltoztatja a termék rendeltetését, ennélfogva jelentős módosításnak minősül.

50. példa: Egy gyártó digitális elemeket tartalmazó szoftverterméket hoz forgalomba, amely bevált titkosítási protokoll és a kulcséletciklus belső kezelése útján gondoskodik a digitális elemeket tartalmazó termék alkotóelemei közötti biztonságos kommunikációról. Újonnan azonosított kriptográfiai hiányosságokra reagálva a gyártó biztonsági frissítést vezet be, és annak keretében a meglévő titkosítási mechanizmust másik protokollal váltja fel, amely harmadik fél által működtetett külső kulcskezelési szolgáltatás használatát követeli meg. E változás eredményeként a digitális elemeket tartalmazó termék függőségei és adatáramlásai lényegesen megváltoznak: új külső interfészek bevezetése mellett a termék a kockázatértékelésben figyelembe nem vett, harmadik fél által nyújtott szolgáltatásokra támaszkodik. Bár a frissítést biztonsági okokból vezetik be, új kiberbiztonsági kockázatokat eredményez, ezért jelentős módosításnak minősül.

110. A fenti 104. pontban említett módon azt, hogy egy szoftverfrissítés jelentős módosításnak minősül-e, eseti alapon kell értékelni. Az értékelés során a gyártók – nem kimerítő jelleggel – mérlegelhetik, hogy a szoftverfrissítés

a) bevezet-e új fenyegetésvektorokat, például további interfészeket, kommunikációs csatornákat, futtatási környezeteket vagy külső függőségeket, amelyeken keresztül a fenyegetések megvalósulhatnak;

b) lehetővé tesz-e új támadási forgatókönyveket, például a digitális elemeket tartalmazó termékhez vagy az általa kezelt adatokhoz való jogosulatlan hozzáférés, azok manipulációja, az azokba való beavatkozás vagy az azokkal való visszaélés valószínű új módjait;

c) megváltoztatja-e a korábban azonosított támadási forgatókönyvek valószínűségét, például azáltal, hogy csökkenti az azok kiaknázásához szükséges erőfeszítéseket vagy szakértelmet, növeli a nem megbízható szereplőknek való kitettséget, vagy gyengíti a meglévő biztonsági elemeket;

d) megváltoztatja-e a korábban azonosított támadási forgatókönyvek potenciális hatását, beleértve például az érintett adatok vagy funkciók körét, az üzemeltetési, biztonsági vagy gazdasági következmények súlyosságát, vagy az incidens észlelésére, elszigetelésére vagy az azt követő helyreállításra való képességet.

111. Egyes esetekben a szoftverfrissítés nem vezet be új fenyegetésvektorokat, nem tesz lehetővé új támadási forgatókönyveket, és nem változtatja meg lényegesen a korábban azonosított támadási forgatókönyvek valószínűségét vagy hatását. Ez azt jelezheti, hogy a frissítés nem eredményez új vagy megnövekedett kiberbiztonsági kockázatokat, feltéve, hogy a kockázatértékelésben alapul vett feltételezések és kockázatcsökkentő intézkedések továbbra is érvényesek és hatékonyak. Ezért valószínű, hogy a frissítés nem minősül jelentős módosításnak.

112. Ezzel szemben a szoftverfrissítés új fenyegetésvektorokat vezethet be, új támadási forgatókönyveket tehet lehetővé, vagy lényegesen megváltoztathatja a meglévő támadási forgatókönyvek valószínűségét vagy hatását. Ilyenkor a gyártónak újra kell értékelnie a digitális elemeket tartalmazó termék kiberbiztonsági kockázatait, és meg kell állapítania, hogy az alapvető követelmények továbbra is teljesülnek-e, beleértve azt is, hogy a frissítés olyan új vagy megnövekedett kockázatokat eredményez-e, amelyekkel a kockázatértékelés nem számol.

113. Az, hogy a szoftverfrissítés jelentős módosításnak minősül-e, releváns annak meghatározásakor, hogy a kiberrezilienciáról szóló rendelet szerinti, a 91. pontban meghatározott egyes kötelezettségek alkalmazandók-e. E minősítéstől függetlenül azonban a gyártók továbbra is felelősek a szoftverfrissítések és a digitális elemeket tartalmazó termékeik biztonságának garantálásáért a támogatási időszak alatt, a kiberrezilienciáról szóló rendelet I. mellékletének II. részében meghatározott sérülékenységkezelési követelményekkel összhangban. Továbbá, függetlenül attól, hogy a szoftverfrissítések jelentős módosításnak minősülnek-e vagy sem, a gyártóknak a 13. cikk (7) bekezdésével és a 31. cikk (2) bekezdésével összhangban folyamatosan biztosítaniuk kell a kockázatértékelés és a műszaki dokumentáció pontosságát, teljességét és naprakész voltát.

4.4. **A jelentős módosítás következményei**

114. A már forgalomba hozott, digitális elemeket tartalmazó termék eredeti gyártójától eltérő szereplő által végzett jelentős módosítás következményeivel a kiberrezilienciáról szóló rendelet 21. és 22. cikke foglalkozik. A 21. cikk az importőrökre és a forgalmazókra vonatkozik, míg a 22. cikk a gyártótól, importőrtől vagy forgalmazótól eltérő bármely természetes vagy jogi személyre vonatkozik.

115. Amennyiben a jelentős módosítást a digitális elemeket tartalmazó termék eredeti gyártója végzi, a következmények a jelentős („lényeges”) módosításnak a kiberrezilienciáról szóló rendelet (41) preambulumbekezdésében említett, általánosan elfogadott fogalmából erednek, részletesebb kifejtésüket a kék útmutató 2.1. szakasza tartalmazza. Az említett szakasz kimondja, hogy a forgalomba hozatalt követően jelentős változásokon vagy nagyjavításon átesett terméket új terméknek kell tekinteni, ha eredeti teljesítménye, célja vagy típusa megváltozott, a veszély jellege megváltozott vagy a kockázat szintje nőtt, és a digitális elemeket tartalmazó terméket forgalmazzák.

116. Az általánosan megállapított következmény ezért az, hogy ha a digitális elemeket tartalmazó termék módosítása jelentős módosításnak minősül, és a digitális elemeket tartalmazó módosított terméket forgalmazzák, azt a kiberrezilienciáról szóló rendelet alkalmazásában digitális elemeket tartalmazó új terméknek kell tekinteni. Következésképpen a jelentősen módosított termék forgalmazása új forgalomba hozatalnak minősül. Ez attól függetlenül érvényes, hogy a jelentős módosítást az eredeti gyártó vagy más személy végzi-e. Annak biztosítása érdekében, hogy a kiberrezilienciáról szóló rendeletet egységesen és arányosan alkalmazzák a jelentős módosítást végrehajtó szereplők különböző kategóriáira, a következő alszakaszok a jelentős módosítást végrehajtó személynek a digitális elemeket tartalmazó, jelentősen módosított termék forgalomba hozatalakor felmerülő kötelezettségeivel foglalkoznak. A digitális elemeket tartalmazó termék támogatási időszakát érintő következményekkel az 5. szakasz (*Support period*) foglalkozik.

4.4.1. *Az eredeti gyártótól eltérő személy által végrehajtott jelentős módosítások*

117. A 21. és 22. cikkel összhangban, ha a már forgalomba hozott, digitális elemeket tartalmazó termék jelentős módosítását a digitális elemeket tartalmazó termék gyártójától eltérő természetes vagy jogi személy végzi, a jelentős módosítást végző és a digitális elemeket tartalmazó módosított terméket forgalmazó személyt kell a digitális elemeket tartalmazó módosított termék gyártójának tekinteni, függetlenül attól, hogy az említett személy részt vett-e az említett termék eredeti tervezésében vagy forgalomba hozatalában.

118. A 22. cikk pontosítja, hogy ha a módosítás nem befolyásolja a digitális elemeket tartalmazó termék egészének kiberbiztonságát, a módosítást végző személyre csak a digitális elemeket tartalmazó terméknek a jelentős módosítás által érintett része tekintetében vonatkoznak a 13. és 14. cikkben meghatározott kötelezettségek.

119. Amennyiben egy jelentős módosítás befolyásolja az alapvető követelményeknek való megfelelést, de nem befolyásolja negatívan a digitális elemeket tartalmazó termék egészének kiberbiztonságát, a módosítást végző személyre csak a digitális elemeket tartalmazó termék jelentősen módosított része tekintetében vonatkozik a 13. cikk (beleértve az alapvető követelményeknek való megfelelés biztosítására és a megfelelőségértékelési eljárás elvégzésére vonatkozó kötelezettséget) és a 14. cikk (jelentéstételi kötelezettségek) ([16]). Ezenkívül az eredeti gyártónak a kiberrezilienciáról szóló rendelet szerinti kötelezettségei továbbra is alkalmazandók a forgalomba hozott, digitális elemeket tartalmazó eredeti termékre; ez biztosítja a sérülékenységkezelés és a módosítással nem érintett részek megfelelőségének folytonosságát.

120. A jelentős módosítás esete nem keverendő össze az integráció eseteivel, amikor egy személy alkotóelemek összeállításával (beleértve adott esetben azok módosítását is) digitális elemeket tartalmazó új terméket hoz létre, amelyet maga hoz forgalomba. Ilyenkor az integrátor nem egy másik gyártó által már forgalomba hozott, digitális elemeket tartalmazó terméket módosít, hanem új, digitális elemeket tartalmazó saját terméket hoz forgalomba. A kiberrezilienciáról szóló rendelet alkalmazásában az integrátor a digitális elemeket tartalmazó új termék gyártója, és e minőségében a digitális elemeket tartalmazó termék egésze tekintetében teljes mértékben meg kell felelnie a rendeletnek. Amennyiben a gyártó a kiberrezilienciáról szóló rendelet hatálya alá tartozó alkotóelemeket integrál, támaszkodhat az alkotóelemek gyártóinak megfelelési tevékenységeire annak érdekében, hogy megkönnyítse a kiberrezilienciáról szóló rendeletnek való saját megfelelését.

51. példa: Egy vállalkozás használatra kész mikrovezérlő modulokat és konnektivitási alkotóelemeket vásárol harmadik félnek minősülő beszállítóktól, védett firmware-t és érzékelőcsomagot fejleszt, majd azokat digitális elemeket tartalmazó termékké állítja össze, amelyet összekapcsolt mezőgazdasági monitoringeszközként a saját neve alatt hoz forgalomba. Bár a vállalkozás módosította az alapul szolgáló mikrovezérlő modulokat, és azokat más alkotóelemekkel kombinálta, nem egy már forgalomba hozott, digitális elemeket tartalmazó terméket módosít jelentősen, hanem új, digitális elemeket tartalmazó terméket hoz forgalomba. A vállalkozás a kiberrezilienciáról szóló rendelet alkalmazásában a mezőgazdasági monitor gyártója, és a mezőgazdasági monitor egésze tekintetében köteles megfelelni a rendeletnek.

([16]) A kék útmutató 2.1. szakasza szerint „[n]em szükséges megismételni a vizsgálatokat, vagy új dokumentációt készíteni a módosítás által nem érintett tényezőket illetően. A terméken a változtatásokat megvalósító vagy azokat megrendelő természetes vagy jogi személy feladata annak bizonyítása, hogy nem szükséges frissíteni a műszaki dokumentáció minden elemét. A terméken a változtatásokat megvalósító vagy azokat megrendelő természetes vagy jogi személy felelős a módosított termék megfelelőségéért, és még akkor is el kell készítenie a megfelelőségi nyilatkozatot, ha meglévő vizsgálatokat és műszaki dokumentációt használ”.

121. Amennyiben az eredeti gyártótól eltérő személy által végzett jelentős módosítás negatívan befolyásolja a digitális elemeket tartalmazó termék egészének kiberbiztonságát, például azért, mert a módosítás már nem egy konkrét alkotóelemre vagy alrendszerre irányul vagy korlátozódik, a forgalmazott, digitális elemeket tartalmazó módosított terméket teljes egészében a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó új termékként kell kezelni. Ilyenkor a termék általános kiberbiztonsági kockázati profilja megváltozott, és a módosítás nem értékelhető a digitális elemeket tartalmazó termék egészének figyelembevétele nélkül. A módosítást végző személyre a 13. és 14. cikkben meghatározott gyártói kötelezettségek a digitális elemeket tartalmazó módosított termék egésze tekintetében vonatkoznak.

4.4.2. *Az eredeti gyártó által végrehajtott jelentős módosítások*

122. Amennyiben a jelentős módosítást az eredeti gyártó végzi, többek között a digitális elemeket tartalmazó szoftvertermékek iteratív fejlesztésével összefüggésben, a kiberrezilienciáról szóló rendelet alkalmazásában továbbra is ez a gyártó minősül gyártónak. A digitális elemeket tartalmazó, jelentősen módosított terméket azonban újonnan forgalomba hozottnak kell tekinteni.

123. A kék útmutató 2.1. szakaszával összhangban a jelentősen módosított, digitális elemeket tartalmazó terméket forgalomba hozó eredeti gyártó újra felhasználhatja a meglévő dokumentációt és vizsgálatokat a digitális elemeket tartalmazó termék azon vonatkozásai tekintetében, amelyeket a jelentős módosítás nem érint. Különösen abban az esetben, ha a gyártó ugyanazon, digitális elemeket tartalmazó termék jelentősen módosított verzióit hozza forgalomba, a megfelelőségértékelési eljárásnak a digitális elemeket tartalmazó termék jelentősen módosított részeire kell összpontosítania. Ugyanígy akkor, ha harmadik fél által végzett megfelelőségértékelésre kerül sor, a megfelelőségértékelő szervezetnek az értékelését a jelentősen módosított részekre kell összpontosítania. A digitális elemeket tartalmazó termék módosítással nem érintett részei esetében újra felhasználhatja a meglévő dokumentációt és vizsgálati eredményeket.

124. Az előző alszakaszban meghatározott arányossági megfontolások a 2027. december 11. előtt forgalomba hozott, digitális elemeket tartalmazó termék eredeti gyártója által végzett jelentős módosításokra is alkalmazandók. Az eredeti gyártó által végzett ilyen jelentős módosítás önmagában nem kötelezi a gyártót arra, hogy az említett időpont előtt forgalomba hozott, digitális elemeket tartalmazó termék egésze tekintetében biztosítsa a kiberrezilienciáról szóló rendeletnek való teljes megfelelést, kivéve, ha a módosítás a digitális elemeket tartalmazó termék egészének kiberbiztonságát negatívan befolyásolja. Amennyiben a módosítás nem érinti a digitális elemeket tartalmazó termék egészének kiberbiztonságát, az eredeti gyártónak a módosítással kapcsolatos kötelezettségeit a jelentősen módosított alkatrészekre kell korlátozni.

5. **TÁMOGATÁSI IDŐSZAK**

125. A kiberrezilienciáról szóló rendelet 13. cikkének (8) bekezdése előírja a gyártók számára a támogatási időszak meghatározását, amely alatt biztosítaniuk kell, hogy a digitális elemeket tartalmazó termék és alkotóelemei sérülékenységeit hatékonyan és az I. melléklet II. részében meghatározott alapvető követelményekkel összhangban kezeljék. A támogatási időszak tükrözi annak az időtartamnak a hosszúságát, amely alatt a digitális elemeket tartalmazó terméket várhatóan használni fogják (várható használati idő), és azt a 13. cikk (8) bekezdésében előírt kritériumokra tekintettel kell megállapítani, ideértve különösen az észszerű felhasználói elvárásokat, a digitális elemeket tartalmazó termék jellegét, beleértve annak rendeltetését is, valamint a digitális elemeket tartalmazó termékek élettartamát meghatározó vonatkozó uniós jogot ([17]). Összességében ezeket a kritériumokat oly módon kell figyelembe venni, hogy a támogatási időszak meghatározásakor biztosított legyen az arányosság.

([17]) A 13. cikk (8) bekezdésének megfelelően figyelembe vehető további kritériumok közé tartoznak a más gyártók által forgalomba hozott, hasonló funkciókat kínáló, digitális elemeket tartalmazó termékek támogatási időszakai, a működési környezet elérhetősége, az alapvető funkciókat nyújtó és harmadik felektől beszerzett integrált alkotóelemek támogatási időszakai, valamint a közigazgatási együttműködési csoport (ADCO) és a Bizottság által nyújtott releváns útmutatás.

126. A 13. cikk (8) bekezdése előírja továbbá, hogy a támogatási időszaknak legalább öt évnek kell lennie, kivéve, ha a terméket várhatóan öt évnél rövidebb ideig használják, amely esetben a támogatási időszaknak meg kell felelnie a várható használati időnek. A minimális támogatási időszak ezért csak biztonsági elemként szolgál, amely garantálja, hogy a sérülékenységeket kellően hosszú ideig kezeljék, ugyanakkor lehetővé teszi a gyártók számára, hogy figyelembe vegyék a valóban rövidebb várható felhasználási idővel rendelkező, digitális elemeket tartalmazó termékeket. A (60) preambulumbekezdés további iránymutatást nyújt e tekintetben, egyértelművé téve, hogy azoknak a digitális elemeket tartalmazó termékeknek, amelyekről észszerűen feltételezhető, hogy öt évnél hosszabb ideig használják őket, ennek megfelelően hosszabb támogatási időszakokkal kell rendelkezniük. Az ötéves támogatási időszak ezért nem tekinthető alapértelmezettnek a digitális elemeket tartalmazó valamennyi termék esetében. Ehelyett a gyártónak a 13. cikk (8) bekezdésében említett kritériumokra tekintettel kell meghatároznia a megfelelő támogatási időszakot.

127. A 13. cikk (19) bekezdése előírja a gyártók számára, hogy a vásárláskor egyértelműen és érthetően tüntessék fel a támogatási időszak végét (legalább a hónapot és az évet). Előírja továbbá a gyártók számára, hogy a támogatási időszak lejártát követően értesítést jelenítsenek meg a felhasználók számára, ha ez a digitális elemeket tartalmazó termék jellegére tekintettel műszakilag megvalósítható. E kötelezettség célja, hogy átláthatóságot biztosítson a felhasználók számára a biztonsági támogatás várható időtartamát illetően.

128. A digitális elemeket tartalmazó szoftvertermékek esetében, amelyeket gyakran iteratív módon fejlesztenek ki és adnak ki, és amelyeknek idővel gyakran hozhatják forgalomba jelentősen módosított verzióit, a támogatási időszakot e fejlesztési modell fényében kell értelmezni. A forgalomba hozott, digitális elemeket tartalmazó szoftvertermékek minden jelentősen módosított verziójának rendelkeznie kell a 13. cikk (8) bekezdésének megfelelő, bejelentett támogatási időszakkal. Ez magában foglalja a legalább ötéves minimális támogatási időszakot, kivéve, ha az adott verzió várható használati ideje bizonyíthatóan rövidebb, amint azt a (60) preambulumbekezdés is egyértelművé teszi. Az *5.1.* szakasz (*Substantial modifications and the support period*) pontosítja, hogy ha a jelentős módosítás nem vezet a digitális elemeket tartalmazó termék várható használati idejét eredetileg meghatározó tényezők megváltozásához, akkor a módosítás nem érinti az eredeti támogatási időszakot (akkor sem, amikor a fennmaradó támogatási időszak öt évnél rövidebb).

129. A 13. cikk (10) bekezdése rugalmasságot biztosít a digitális elemeket tartalmazó szoftvertermékek tekintetében azáltal, hogy lehetővé teszi a gyártók számára, hogy bizonyos feltételek mellett csak a digitális elemeket tartalmazó szoftvertermék legutóbb forgalomba hozott verziója esetében biztosítsák az I. melléklet II. részének 2. pontjában meghatározott sérülékenységkezelési követelménynek (a sérülékenységek kezelése és orvoslása) való megfelelést. Ez akkor megengedett, ha a korábban forgalomba hozott verziók felhasználói díjmentesen hozzáférnek a legutóbb forgalomba hozott verzióhoz, és nem merülnek fel többletköltségek azon hardver- és szoftverkörnyezet hozzáigazításával kapcsolatban, amelyben az említett termék eredeti verzióját használják.

130. A 13. cikk (10) bekezdésének alkalmazásában a „többletköltségek” fogalmát gyakorlati és arányos módon kell értelmezni, figyelembe véve a szoftverkarbantartás és -üzemeltetés szokásos és várható gyakorlatait. Nem foglalja magában a szoftverfrissítések alkalmazásával vagy a biztonságos működési környezet fenntartásával járó észszerű operatív erőfeszítéseket, például a személyzeti időt, a rutintesztelést, a konfigurációs kiigazításokat vagy a mögöttes szoftverfüggőségek korszerűsítését, amelyek az életciklusuk végét elért alkotóelemek vagy az ismert biztonsági sérülékenységek kezeléséhez szükségesek. A „többletköltségek” ugyanis olyan terhek, amelyek túlmutatnak a szoftverfrissítésekkel összefüggésben általában várható terhek körén; ilyen költség például az új hardverek kötelező beszerzése, az infrastruktúra cseréje vagy a működési környezet alapvető változása.

131. A folyamatosan fejlődő, digitális elemeket tartalmazó szoftvertermékek esetében a gyártók viszonylag rövid időközönként hozhatnak forgalomba egymást követő, jelentősen módosított verziókat, és elvárhatják a felhasználóktól a rendszeres frissítést. Ilyenkor az egyes jelentősen módosított verziók bejelentett támogatási időszakának a forgalomba hozatal időpontjában meg kell felelnie a 13. cikk (8) bekezdésének. A gyártónak tehát új támogatási időszakot kell bejelentenie a jelentősen módosított verzióra vonatkozóan. A gyártók azonban a 13. cikk (10) bekezdése alapján megszüntethetik a korábbi verziók sérülékenységeinek kezelését és orvoslását, ha a felhasználók ingyenesen és a fent említett többletköltségek nélkül frissíthetnek újabb verzióra, még akkor is, ha ez

az érintett korábbi verziók esetében ténylegesen rövidebb támogatási időszakot eredményez ([18]). A gyártóra továbbra is vonatkoznak az I. melléklet II. részében foglalt egyéb sérülékenységkezelési követelmények, valamint a 14. cikkben foglalt jelentéstételi kötelezettségek. Amint azt a (40) preambulumbekezdés is kifejti, ezek a követelmények többek között a forgalomba hozott, digitális elemeket tartalmazó szoftvertermék valamennyi későbbi, jelentősen módosított verziója tekintetében magukban foglalják i. a sérülékenységek összehangolt nyilvánosságra hozatalára vonatkozó politika fenntartását, valamint ii. a potenciális sérülékenységekre vonatkozó információk megosztását megkönnyítő intézkedéseket ([19]).

52. példa: Egy gyártó okostelefon-modellt hoz forgalomba az uniós piacon, és a forgalomba hozatal időpontjától számított X éves támogatási időszakot jelent be, amelynek során biztonsági frissítéseket biztosít a sérülékenységek kezelésére. Ezen időszak alatt a gyártó rendszeres szoftverfrissítéseket ad ki az operációs rendszer jelentősen módosított verziói mellett, amelyeket a felhasználók ingyenesen telepíthetnek anélkül, hogy új hardverre lenne szükségük.

A gyártó a 13. cikk (10) bekezdésével összhangban kezelheti és orvosolhatja az adott okostelefon-modellhez rendelkezésre bocsátott operációs rendszer legújabb verziójának sérülékenységeit, feltéve, hogy a korábbi verziók díjmentesen és többletköltségek nélkül frissíthetők. A támogatási időszak alatt a gyártó továbbra is köteles megfelelni a sérülékenységek kezelésére – például a sérülékenységek összehangolt nyilvánosságra hozatalára és az információmegosztásra irányuló intézkedésekre – vonatkozó egyéb követelményeknek.

53. példa: Egy gyártó digitális elemeket tartalmazó vállalati szoftverterméket hoz forgalomba, és néhány havonta jelentősen módosított verziókat ad ki, amelyekben biztonsági fejlesztések és új jellemzők jelennek meg, és biztosított a frissített operációs rendszerekkel és platformokkal való kompatibilitás. Minden egyes verziót a 13. cikk (8) bekezdésével összhangban bejelentett támogatási időszakkal hoznak forgalomba. A gyártó elvárja, hogy a felhasználók az üzemszerű működés részeként rendszeresen frissítsék a rendszert, és ingyenes hozzáférést biztosít a legújabb verzióhoz. A frissítések alkalmazása észszerű operatív erőfeszítést igényelhet, például tesztelést vagy a konfigurációs beállítások módosítását, de nem jár többletköltségekkel, például új hardver beszerzésével vagy alapvető infrastrukturális változtatásokkal. Ebben az összefüggésben a gyártó a 13. cikk (10) bekezdésére hivatkozva megszüntetheti a korábbi verziók sérülékenységeinek kezelését és orvoslását, ha a felhasználók a legújabb verzióra frissíthetnek, ugyanakkor minden későbbi, jelentősen módosított verzió esetében továbbra is meg kell felelnie az egyéb sérülékenységkezelési követelményeknek.

5.1. **Jelentős módosítások és a támogatási időszak**

132. A 4.4. szakaszban (*Consequences of a substantial modification*) foglaltak szerint, ha a digitális elemeket tartalmazó termék módosítása jelentős módosításnak minősül, és a digitális elemeket tartalmazó módosított terméket forgalmazzák, azt a kiberrezilienciáról szóló rendelet alkalmazásában új terméknek kell tekinteni, és a digitális elemeket tartalmazó, jelentősen módosított termék forgalmazása új forgalomba hozatalnak minősül. Ezért érdemes tisztázni, hogy ez az új forgalomba hozatal milyen hatást gyakorol a digitális elemeket tartalmazó, jelentősen módosított termék támogatási időszakára.

133. A digitális elemeket tartalmazó, jelentősen módosított termék támogatási időszakát a termék várható használati ideje alapján, a kiberrezilienciáról szóló rendelet 13. cikkének (8) bekezdésében meghatározott kritériumokra tekintettel kell meghatározni. A jelentős módosítást ezért e kritériumok alapján újra kell értékelni, de ez nem eredményezi automatikusan a támogatási időszak újbóli megállapítását vagy akár meghosszabbítását. A döntő kérdés az, hogy a jelentős módosítás hatással van-e azokra a tényezőkre, amelyek eredetileg meghatározták a termék várható használati idejét, és ennélfogva az eredeti támogatási időszakot.

([18]) Emlékeztetni kell a 13. cikk (19) bekezdésében foglalt előírásra, amely szerint ha a digitális elemeket tartalmazó termék jellegére tekintettel műszakilag megvalósítható, a gyártóknak értesítést kell megjeleníteniük a felhasználók számára, amelyben tájékoztatják őket arról, hogy a digitális elemeket tartalmazó termékük elérte a támogatási időszak végét. Ezért ha a korábbi verziók sérülékenységeinek kezelése és orvoslása megszűnik, akkor – ha ez műszakilag megvalósítható – tájékoztatni kell azokat a felhasználókat, akik nem frissítettek a legújabb verzióra.

([19]) Meg kell jegyezni, hogy ha a felhasználók többletköltségek nélkül frissíthetnek a szoftver legújabb verziójára, a gyártók dönthetnek úgy, hogy továbbra is kezelik és orvosolják a szoftver korábbi verzióinak sérülékenységeit, többek között fizetés ellenében vagy más kereskedelmi megállapodások alapján. A kiberrezilienciáról szóló rendelet nem írja elő a gyártók számára, hogy díjmentesen biztonsági frissítéseket biztosítsanak a korábbi verziókhoz.

134. Amennyiben a jelentős módosítás nem érinti ezeket a tényezőket, a 13. cikk (8) bekezdésében meghatározott kritériumok továbbra is ugyanazt a várható használati időt jelzik, mint amelyet eredetileg meghatároztak, és a digitális elemeket tartalmazó módosított termék támogatási időszakának igazodnia kell az eredetileg forgalomba hozott termék fennmaradó várható használati idejéhez. Jellemzően ez a helyzet akkor, ha a várható használati időt elsősorban olyan tényezők (például a hardver-alkotóelemek fizikai tartóssága) határozzák meg, amelyeken a módosítás nem változtat, amikor is a jelentős módosítás csak a szoftver funkcióit vagy a háttérszolgáltatásokat érinti.

54. példa: Egy gyártó robotporszívót hoz forgalomba, amelynek várható használati ideje X év, amelyet a digitális elemeket tartalmazó termék jellege – többek között a hardver-alkotóelemek fizikai tartóssága és kopási jellemzői – alapján, valamint a termék élettartamára vonatkozó észszerű felhasználói elvárások figyelembevételével határoznak meg. A gyártó X éves támogatási időszakot határoz meg. Y év elteltével a gyártó olyan szoftverfrissítést ad ki, amely jelentős módosításnak minősül: új tisztítási módokat és navigációs jellemzőket vezet be. A szoftverfrissítés nem befolyásolja a hardver fizikai tartósságát, és nem változtatja meg az adott termék élettartamával kapcsolatos észszerű felhasználói elvárásokat. A 13. cikk (8) bekezdése szerinti kritériumok ezért továbbra is ugyanazt a várható felhasználási időt jelzik. A digitális elemeket tartalmazó módosított termék támogatási időszaka összhangban van az eredetileg meghatározott fennmaradó várható használati idővel.

55. példa: Egy gyártó digitális elemeket tartalmazó terméket hoz forgalomba összetett ipari gépként, amelynek felhőalapú háttérrendszere távoli adatkezelési megoldásnak minősül. A várható használati idő X év, amelyet az észszerű felhasználói elvárásokra és a digitális elemeket tartalmazó termék jellegére – például a gép hardverének fizikai tartósságára, valamint a várható kopásra és elhasználódásra – tekintettel határoznak meg. A támogatási időszakot a várható használati időhöz igazodóan X évben állapítják meg. Y év elteltével a gyártó újratervezi a felhőalapú háttérrendszert (a távoli adatkezelési megoldást), valamint új API-kat és adatáramlásokat vezet be. Mindezek együttesen a digitális elemeket tartalmazó termék jelentős módosításának minősülnek, de nem változtatják meg a termék jellegét, és nem befolyásolják a felhasználói elvárásokat. A 13. cikk (8) bekezdése szerinti kritériumok ezért továbbra is ugyanazt a várható felhasználási időt jelzik. A digitális elemeket tartalmazó módosított termék támogatási időszaka összhangban van az eredetileg meghatározott fennmaradó várható használati idővel.

135. Amennyiben a jelentős módosítás érinti azokat a tényezőket, amelyek eredetileg meghatározták a digitális elemeket tartalmazó termék várható használati idejét, a gyártónak a 13. cikk (8) bekezdésében foglalt kritériumokat megfelelően alkalmazva, az új várható használati időhöz igazodóan újra kell számítania a támogatási időszakot. Ilyen helyzet adódhat például a termék üzemi élettartamát meghosszabbító, revitalizáló hardvermódosítások, vagy a termék alapvető szoftverének olyan jelentős átprogramozása vagy átírása esetén, amely lényegesen megváltoztatja a várható használati időt ([20]).

56. példa: Egy gyártó programozható logikai vezérlőt (PLC) hoz forgalomba, amelynek várható használati ideje X év; ezt elsősorban a digitális elemeket tartalmazó termék jellege és a mögöttes hardver tartóssága alapján határozzák meg. A támogatási időszakot ehhez igazodóan állapítják meg. Évekkel az első forgalomba hozatalt követően a gyártó jelentős módosítást hajt végre, amelynek keretében a PLC beágyazott számítási platformját – beleértve a processzort, a memóriát és a futtatási környezetet – jelentősen hosszabb üzemi élettartamra tervezett, újgenerációs alkotóelemekkel váltja fel. A módosítás eredményeként megváltoznak az észszerű felhasználói elvárások és a digitális elemeket tartalmazó termék jellege: a PLC felhasználója most észszerűen elvárhatja, hogy a PLC az eredetileg bejelentett várható használati időn túl is produktív használatban maradjon, amit az új számítási platform támogat. A 13. cikk (8) bekezdése szerinti kritériumok ezért hosszabb várható használati időt jeleznek, így a gyártó ennek megfelelően újraszámítja az adott PLC támogatási időszakát.

6. **DIGITÁLIS ELEMEKET TARTALMAZÓ FONTOS ÉS KRITIKUS FONTOSSÁGÚ TERMÉKEK**

136. A kiberrezilienciáról szóló rendelet 7. cikkének (1) bekezdése megállapítja, hogy azok a digitális elemeket tartalmazó termékek, amelyek a rendelet III. mellékletében meghatározott termékkategóriák alapvető funkcióival rendelkeznek, „digitális elemeket tartalmazó fontos termékeknek” minősülnek. A III. melléklet a digitális elemeket tartalmazó fontos termékeket az I. és a II. osztályba sorolja. Hasonlóképpen a 8. cikk (1) bekezdése megállapítja, hogy a kiberrezilienciáról szóló rendelet IV. mellékletében meghatározott termékkategória alapvető funkciójával rendelkező, digitális elemeket tartalmazó termékek „digitális elemeket tartalmazó kritikus fontosságú termékeknek” minősülnek ([21]).

([20]) Emlékeztetni kell arra, hogy a *4.1.* szakaszban (*Physical repairs*) jelzett módon a felújítási, karbantartási vagy javítási műveletek általában nem minősülnek jelentős módosításnak.

([21]) Az (EU) 2025/2392 bizottsági végrehajtási rendelet meghatározza a fontos és kritikus fontosságú termékek kategóriáinak műszaki leírását.

137. A digitális elemeket tartalmazó termék fontos vagy kritikus fontosságú, vagy ellenkezőleg az „alapértelmezett” kategóriába ([22]) való besorolása azon megfelelőségértékelési eljárás meghatározásakor releváns, amelyet a gyártónak a 32. cikkel összhangban el kell végeznie, mielőtt a digitális elemeket tartalmazó terméket forgalomba hozhatja. Nevezetesen a digitális elemeket tartalmazó, az alapértelmezett kategóriába tartozó termék esetében az A. modulon alapuló belső ellenőrzési eljárás („önértékelés”) mindenkor alkalmazható ([23]). Az I. vagy II. osztályba tartozó, digitális elemeket tartalmazó fontos termékekre és a digitális elemeket tartalmazó kritikus fontosságú termékekre szigorúbb megfelelőségértékelési eljárások vonatkoznak. Ez nem foglalja magában azokat a forgalomba hozott, szabad és nyílt forráskódú szoftvernek minősülő, I. vagy II. osztályba tartozó, digitális elemeket tartalmazó fontos termékeket, amelyek esetében a gyártók a 32. cikk (5) bekezdésével összhangban alkalmazhatják az alapértelmezett kategória eljárásait.

138. Az alapvető funkció fogalma ezért elengedhetetlen ahhoz, hogy a gyártó meghatározza az alkalmazandó megfelelőségértékelési rendszert. Ezt a fogalmat azonban a kiberrezilienciáról szóló rendelet nem határozza meg kifejezetten. A digitális elemeket tartalmazó termékek számos funkciót elláthatnak, amelyek közül néhány kiegészítő jellegű lehet a termék alapvető funkcióihoz képest, és nem befolyásolhatják a terméknek az alapértelmezett, fontos (I. osztály), fontos (II. osztály), illetve kritikus fontosságú kategóriába való besorolását. Ezért érdemes további iránymutatást nyújtani, amely segíti a gyártókat a vonatkozó megfelelőségértékelési eljárások helyes végrehajtásában, és segíti a piacfelügyeleti hatóságokat a kiberrezilienciáról szóló rendelet Unió-szerte harmonizált végrehajtásának biztosításában.

6.1. **Alapvető funkciók**

139. A digitális elemeket tartalmazó termék alapvető funkciói a termék fő jellemzőit és műszaki képességeit jelentik, amelyek nélkül nem lenne képes elérni rendeltetését. A termék egyedi kontextusának és felhasználási feltételeinek fényében értékelhető, figyelembe véve többek között a gyártó által a használati utasításban, a promóciós vagy értékesítési anyagokban és nyilatkozatokban, valamint a műszaki dokumentációban megadott információkat.

57. példa: A digitális elemeket tartalmazó szoftvertermék absztrakciós réteget biztosít a mögöttes hardver felett, és kezeli a szoftver-alkotóelemek futtatását. Fő jellemzői közé tartozik a hardver és a perifériás inicializálás, a folyamat- és memóriamenedzsment, a bemeneti/kimeneti ellenőrzés, az ütemezés, az erőforrás-elosztás, valamint a rendszerszolgáltatások és az alkalmazásprogramozási felületek (API-k) expozíciója, amelyeken keresztül az alkalmazások kölcsönhatásba lépnek az eszköz hardver- és szoftvererőforrásaival. A műszaki dokumentáció jelzi, hogy a digitális elemeket tartalmazó termék számítástechnikai erőforrásokat hangol össze, rendszerkonfigurációkat érvényesít, és szabványosított interfészeket biztosít a szoftvermodulokhoz és a csatlakoztatott perifériákhoz. A gyártó kiemeli, hogy ezek a képességek lehetővé teszik, hogy a platform olyan központi szoftverkörnyezetként szolgáljon, amelyen az alkalmazások megbízhatóan futtathatók. A digitális elemeket tartalmazó termék alapvető funkciója az (EU) 2025/2392 végrehajtási rendelet I. mellékletének 11. pontjában leírt operációs rendszer.

140. A digitális elemeket tartalmazó termék funkciói ritkán korlátozódnak kizárólag az alapvető funkciókra, mivel a digitális elemeket tartalmazó termékek gyakran – vagy talán minden esetben – olyan további funkciókat is ellátnak, amelyek nem járulnak hozzá a termék alapvető funkcióihoz. Ez magában foglalhatja olyan alkotóelemek beépítését is, amelyek maguk is rendelkeznek egy másik, digitális elemeket tartalmazó fontos vagy kritikus fontosságú termék funkcióival. Az a tény azonban, hogy a digitális elemeket tartalmazó termék a digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékek műszaki leírásában részletezett funkcióktól eltérő vagy azokat kiegészítő funkciókat lát el, önmagában nem akadályozza meg a terméket abban, hogy rendelkezzen egy ilyen alapvető funkcióval.

([22]) Az „alapértelmezett” kategória fogalmát a kiberrezilienciáról szóló rendelet nem határozza meg. A kifejezés e dokumentumban olyan, digitális elemeket tartalmazó termékeket jelöl, amelyek nem rendelkeznek a kiberrezilienciáról szóló rendelet III. vagy IV. mellékletében meghatározott termékkategória alapvető funkciójával, és amelyek következésképpen a 32. cikk (1) bekezdésében meghatározott megfelelőségértékelési rendszer hatálya alá tartoznak.

([23]) A gyártó mindazonáltal mindig dönthet úgy, hogy a 32. cikk (1) bekezdésében meghatározottak szerinti szigorúbb megfelelőségértékelési eljárást alkalmaz.

2. ábra:

Annak szemléltetése, hogy az alkalmazandó megfelelőségértékelési eljárást az alapvető funkciók, nem pedig a kiegészítő funkciók határozzák meg



141. Előfordulhat, hogy a digitális elemeket tartalmazó termék képes ellátni egy fontos vagy kritikus fontosságú termékkategória funkcióit, de ennek ellenére az adott termékkategóriától eltérő alapvető funkcióval rendelkezik. Ezekben az esetekben az említett, digitális elemeket tartalmazó termék nem minősül digitális elemeket tartalmazó fontos vagy kritikus fontosságú terméknek. Amint azt a kiberrezilienciáról szóló rendelet 7. cikkének (1) bekezdése a digitális elemeket tartalmazó fontos termékek tekintetében kifejezetten kimondja (ugyanezt a logikát alkalmazva a digitális elemeket tartalmazó kritikus fontosságú termékekre), egy digitális elemeket tartalmazó fontos vagy kritikus fontosságú termék puszta integrálása önmagában nem teszi a digitális elemeket tartalmazó terméket digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékké.

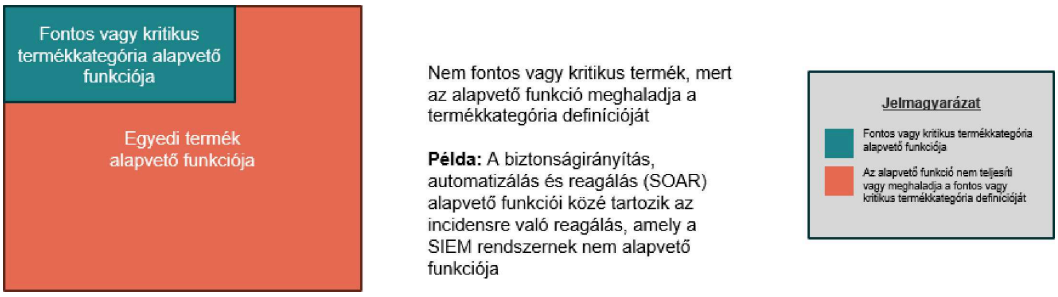
58. példa: Egy okostelefon olyan operációs rendszert integrál, amely az (EU) 2025/2392 végrehajtási rendelet I. mellékletének 11. pontjában leírt funkciókat biztosítja. Az operációs rendszer lehetővé teszi a hardvererőforrások kezelését és a szoftveralkalmazások végrehajtását, az okostelefon egésze ugyanakkor más alapvető funkcióval rendelkezik (pl. lehetővé teszi a felhasználók számára a kommunikációt, valamint az információkhoz és szolgáltatásokhoz való hozzáférést). Az operációs rendszer puszta integrálása nem jelenti azt, hogy az okostelefon alapvető funkciója operációs rendszer.

142. Egyes digitális elemeket tartalmazó termékek hasonlóak lehetnek egy fontos vagy kritikus fontosságú termékkategóriához, vagy ugyanahhoz az általános termékcsaládhoz tartozhatnak, alapvető funkcióik azonban jelentősen meghaladhatják az adott kategória alapvető funkcióit, vagy jelentősen elmaradhatnak azoktól. Más a helyzet akkor, ha a digitális elemeket tartalmazó termék olyan további funkciókat tartalmaz, amelyek csupán kiegészítik vagy javítják az alapvető funkciót, amely viszont egy fontos vagy kritikus fontosságú termékkategóriának felel meg; ilyenkor a digitális elemeket tartalmazó termék megtartja az adott kategória alapvető funkcióit, és ennek megfelelően sorolják be. Az értékelésnek a termék fő jellemzőin és műszaki képességein kell alapulnia, amelyeket objektíven, a termék rendeltetésének fényében kell vizsgálni, nem pedig a digitális elemeket tartalmazó termék leírásának vagy forgalmazásának módján, ha a leírás nem tükrözi a termék tényleges műszaki jellemzőit.

59. példa: A biztonságirányítási, automatizálási és reagálási (SOAR) szoftverek gyakran képesek a „biztonsági információkat és eseményeket kezelő (SIEM) rendszerek” kategóriájába tartozó, digitális elemeket tartalmazó termékek funkcióinak ellátására, azaz több forrásból adatokat gyűjtenek, korrelálják és elemzik, valamint biztonsági célokból hasznosítható információként mutatják be azokat. A szoftver alapvető funkciója azonban jelentősen meghaladja a SIEM definícióját, mivel olyan, a szoftver műszaki képességeinek alapvető elemét képező szolgáltatásokat is magában foglal, mint az incidensekre való reagálás. Ezért általában nem tekinthető úgy, hogy a SOAR-szoftver alapvető funkciója a SIEM-rendszer.

3. ábra:

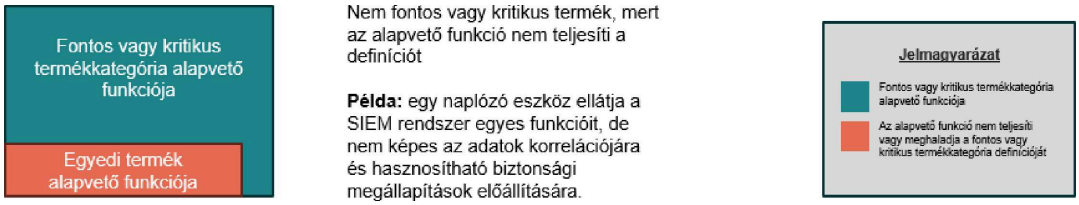
Egy fontos vagy kritikus fontosságú termékkategória fogalommeghatározását jelentősen meghaladó, digitális elemeket tartalmazó termék alapvető funkcióinak szemléltetése



60. példa: Egyes naplózó és naplóvizualizációs eszközök képesek naplóadatok fogadására és a rendszer eseményeit bemutató alapvető áttekintőtáblák megjelenítésére. Bár ezek az eszközök támogathatják a biztonsági megfigyelési tevékenységeket, alapvető funkciójuk elmarad a SIEM-rendszerekétől, mivel nem végeznek adatkorrelációt, és nem nyújtanak hasznosítható biztonsági meglátásokat. Ezért általában nem tekinthető úgy, hogy az ilyen eszközök alapvető funkciója a SIEM-rendszer.

4. ábra:

Egy olyan, digitális elemeket tartalmazó termék alapvető funkcióinak szemléltetése, amelyek jelentősen elmaradnak egy fontos vagy kritikus fontosságú termékkategória meghatározásától

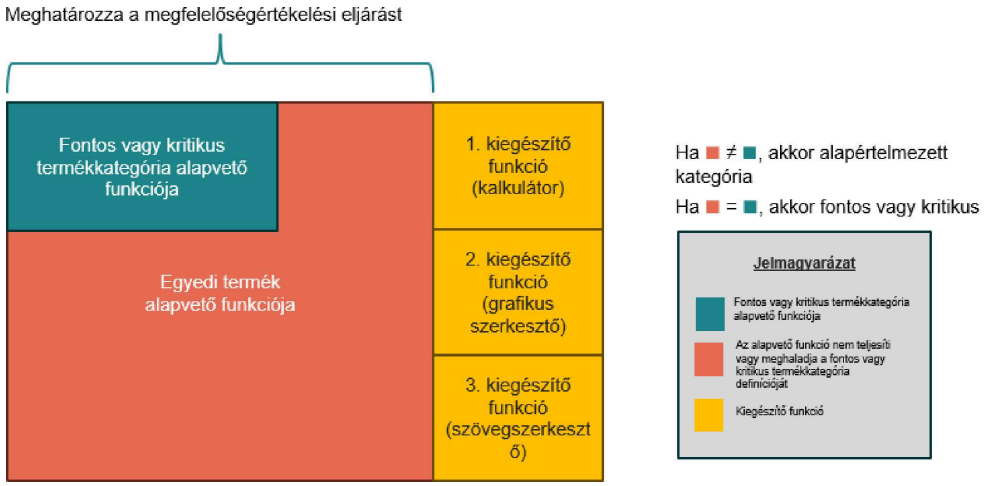


143. A gyártó nem mutathatja be megtévesztő módon a digitális elemeket tartalmazó termékének alapvető funkcióit úgy, hogy kivonja magát a digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékekre alkalmazandó megfelelőségértékelési rendszer alól, például azáltal, hogy túlhangsúlyozza vagy lekicsinyíti bizonyos funkciók szerepét annak érdekében, hogy a termék jelentősen meghaladjon egy adott funkciót, vagy jelentősen elmaradjon attól. Ilyen helyzet adódhat például akkor, ha egyértelmű következetlenségek vannak a promóciós anyagok, a használati utasítások és a műszaki dokumentáció között.

144. A digitális elemeket tartalmazó termék az alkalmazandó megfelelőségértékelési rendszer meghatározása céljából nem rendelkezhet egynél több alapvető funkcióval. A kiberrezilienciáról szóló rendelet VII. mellékletével összhangban a gyártóknak a termék műszaki dokumentációjának részeként ismertetniük kell a digitális elemeket tartalmazó termékük rendeltetését és az általuk követett megfelelőségértékelési eljárást. A termék alapvető funkcióját ezért egyértelműen meg kell határozni. Ez lehetővé teszi az alkalmazandó megfelelőségértékelési rendszer helyes azonosítását, és lehetővé teszi a piacfelügyeleti hatóságok számára, hogy felügyeljék és ellenőrizzék a rendelet helyes alkalmazását.

5. ábra:

Annak szemléltetése, hogy egy digitális elemeket tartalmazó adott termék alapvető funkciója hogyan határozza meg a termékosztályt és ezáltal az alkalmazandó megfelelőségértékelési eljárást



145. Egyes digitális elemeket tartalmazó termékeket digitális elemeket tartalmazó egységes termékként hoznak forgalomba, de különálló, saját funkciókkal rendelkező modulokból állnak. Amennyiben a gyártó ezeket a modulokat külön is forgalmazza, például abban az esetben, ha azokat külön kínálja vásárlásra, hasznosításra vagy előfizetésre, ezek a modulok önálló, digitális elemeket tartalmazó termékeknek minősülnek. Ezért ezeket alapvető funkciójuk alapján kell besorolni (így az egyes modulok alapvető funkciója alapján a vonatkozó megfelelőségértékelési rendszer hatálya alá kell tartozniuk). Ez nem érinti a kizárólag digitális elemeket tartalmazó integrált termék alkotóelemeiként szállított és külön nem rendelkezésre bocsátott modulokat; ilyenkor az alapvető funkciót a digitális elemeket tartalmazó integrált termék szintjén határozzák meg.

61. példa: Egy gyártó egységes biztonsági csomagot hoz forgalomba, amely több modult foglal magában, többek között egy SIEM-et, egy behatolásérzékelő rendszert és egy elemzési modult. A gyártó ezeket a modulokat külön előfizetések keretében is kínálja. Ebben a forgatókönyvben minden modul különálló, digitális elemeket tartalmazó termék, amelyet saját alapvető funkciója alapján sorolnak be. A SIEM modul az I. osztályba tartozó, digitális elemeket tartalmazó fontos termékekre vonatkozó megfelelőségértékelési rendszer hatálya alá tartozik, mivel alapvető funkciója a „Biztonsági információkat és eseményeket kezelő (SIEM) rendszerek”. A behatolásérzékelő rendszer a II. osztályba tartozó, digitális elemeket tartalmazó fontos termékekre vonatkozó megfelelőségértékelési rendszer hatálya alá tartozik, mivel alapvető funkciója a „Tűzfalak, behatolásérzékelő és megelőző rendszerek”. Az analitikai modul a digitális elemeket tartalmazó „alapértelmezett” termékekre vonatkozó megfelelőségértékelési rendszer hatálya alá tartozik, mivel alapvető funkciója nem egyezik meg egy fontos vagy kritikus fontosságú termékkategóriával.

146. A kiberrezilienciáról szóló rendelet 32. cikkében meghatározott kötelezettségek be nem tartása a 64. cikk (3) bekezdésével összhangban közigazgatási bírság kiszabását vonhatja maga után.

6.2. A digitális elemeket tartalmazó fontos és kritikus fontosságú termékek megfelelőségértékelése

147. Miután a gyártó meghatározta a digitális elemeket tartalmazó termékének alapvető funkcióit, el kell végeznie az alkalmazandó megfelelőségértékelési eljárások egyikét. A gyártónak biztosítania kell, hogy a digitális elemeket tartalmazó termék egésze megfeleljen az alapvető követelményeknek, adott esetben figyelembe véve a termékbe integrált alkotóelemek vagy funkciók biztonságát.

148. A II. osztályba tartozó, digitális elemeket tartalmazó fontos termékek (a 32. cikk (5) bekezdésével összhangban szabad és nyílt forráskódú szoftvernek minősülő termékek kivételével) és a digitális elemeket tartalmazó kritikus fontosságú termékek esetében kötelező egy szigorúbb megfelelőségértékelési eljárás harmadik fél bevonásával (a B +C modul, a H modul vagy kiberbiztonsági tanúsítási rendszerek alapján) ([24]). Ezzel szemben az I. osztályba tartozó, digitális elemeket tartalmazó fontos termékeket (a 32. cikk (5) bekezdésével összhangban szabad és nyílt forráskódú szoftvernek minősülő termékek kivételével) csak akkor kell harmadik fél által végzett megfelelőségértékelési eljárásnak alávetni, ha a gyártó nem alkalmazta vagy csak részben alkalmazta az *Európai Unió Hivatalos Lapjában* közzétett hivatkozásokkal rendelkező releváns harmonizált szabványokat (a továbbiakban: harmonizált szabványok), egységes előírásokat vagy legalább „jelentős" megbízhatósági szintű európai kiberbiztonsági tanúsítási rendszereket ([25]).

149. Ezért ahhoz, hogy egy I. osztályba tartozó, digitális elemeket tartalmazó fontos terméknél elvégezhető legyen a belső ellenőrzési eljárás, i. a vonatkozó harmonizált szabvány valamennyi alkalmazandó követelményét alkalmazni kell, és ii. a szabvány alkalmazási körének ki kell terjednie legalább az adott termék alapvető funkciójához kapcsolódó valamennyi kiberbiztonsági kockázatra.

150. A digitális elemeket tartalmazó termék alkalmazási köre szélesebb lehet, mint a vonatkozó harmonizált szabványban előirányzott alkalmazási kör, és az ilyen további funkciók eltérő vagy további kiberbiztonsági kockázatokat jelenthetnek. A gyártónak mindig el kell végeznie a 13. cikk (2) bekezdése szerinti kockázatértékelést, és következésképpen ellenőriznie kell, hogy a harmonizált szabvány végrehajtása kiterjed-e a digitális elemeket tartalmazó termékkel kapcsolatos valamennyi kockázatra. Ha a szabvány végrehajtása nem terjed ki az összes kockázatra, a gyártónak más eszközökkel kell biztosítania, hogy a digitális elemeket tartalmazó terméke megfeleljen az alapvető követelményeknek.

151. Ezért ha az I. osztályba tartozó, digitális elemeket tartalmazó fontos termék gyártója olyan releváns harmonizált szabványt alkalmazott, amely kiterjed a termék alapvető funkciójához kapcsolódó kockázatokra, dönthet úgy, hogy a belső ellenőrzési eljárást alkalmazza a termék megfelelőségének igazolására. Megfelelőségértékelési tevékenységei részeként a gyártónak továbbra is igazolnia kell, hogy a digitális elemeket tartalmazó termékére alkalmazandó valamennyi kockázatot kezeli. Ezért ha eltérés van a harmonizált szabvány hatálya és a digitális elemeket tartalmazó termék egészének alkalmazási köre között, a gyártónak még dokumentálnia kell, hogy milyen további intézkedéseket vezetett be e kockázatok kezelése érdekében.

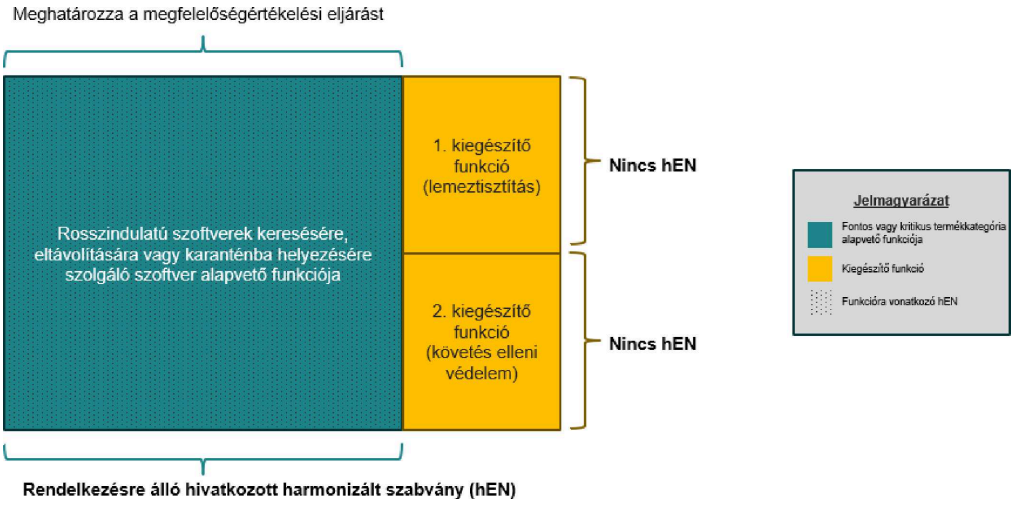
62. példa: Egy vírusirtó szoftver alapvető funkciója az (EU) 2025/2392 végrehajtási rendelet I. mellékletének 4. pontjában leírt, rosszindulatú szoftverek keresésére, eltávolítására vagy karanténba helyezésére szolgáló szoftver. A digitális elemeket tartalmazó termék további jellemzőkkel is rendelkezik, nevezetesen egy lemeztisztítási funkcióval, valamint egy követés elleni funkcióval, amely védi a felhasználót az interneten való navigálás során. A gyártó kockázatértékelést végez a digitális elemeket tartalmazó termék egészére vonatkozóan, beleértve a vírusirtó alapvető funkcióját, a lemeztisztítást és a követés elleni funkciókat is. Harmonizált szabványt alkalmaz, amely kiterjed a vírusirtó alapvető funkciójához kapcsolódó kockázatokra, valamint további intézkedéseket alkalmaz a további funkciókból eredő kockázatok kezelésére. A gyártó a megfelelőségértékeléséhez alkalmazhatja a belső ellenőrzési eljárást, amely a digitális elemeket tartalmazó termék egészére kiterjed, beleértve a lemeztisztítást és a követés elleni funkciókat is.

([24]) Ugyanez a helyzet egy legalább „jelentős" megbízhatósági szintű európai kiberbiztonsági tanúsítási rendszer használata esetén is, mivel szükség van egy harmadik félnek minősülő tanúsító szerv bevonására.

([25]) A tömörség kedvéért e szakasz fennmaradó részében ez csak azokra a harmonizált szabványokra vonatkozik, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*. Ugyanez az iránymutatás vonatkozik azonban a 27. cikk (2) bekezdésével összhangban elfogadott egységes előírásokra és az európai kiberbiztonsági tanúsítási rendszerekre is, ha azokat a Bizottság a 27. cikk (9) bekezdésével összhangban felhatalmazáson alapuló jogi aktusok útján meghatározza.

6. ábra:

Annak szemléltetése, hogy a kizárólag az alapvető funkcióra vonatkozó, hivatkozott harmonizált szabvány használata hogyan határozza meg az alkalmazandó megfelelőségértékelési eljárást



152. Ugyanez a helyzet akkor is, ha a digitális elemeket tartalmazó termék egy olyan további funkciót is integrál, amely maga is egy másik, digitális elemeket tartalmazó fontos vagy kritikus fontosságú termék funkciója. Valójában a digitális elemeket tartalmazó termék egészének alapvető funkciói, nem pedig az egyes integrált alkotóelemek funkciói határozzák meg a digitális elemeket tartalmazó termék fontos vagy kritikus fontosságú termékkategóriába való besorolását, és ennélfogva az alkalmazandó megfelelőségértékelési rendszert. Ha például egy digitális elemeket tartalmazó termék alapvető funkciója szerint az I. osztályba tartozó, digitális elemeket tartalmazó fontos termék, akkor e termék egésze az I. osztályba tartozó, digitális elemeket tartalmazó fontos termékekre alkalmazandó megfelelőségértékelési rendszer hatálya alá tartozik még akkor is, ha olyan alkotóelemet integrál, amely viszont digitális elemeket tartalmazó kritikus fontosságú termék. Ezekben az esetekben, amikor a gyártó olyan harmonizált szabványt alkalmaz, amely kiterjed az adott termék alapvető funkciójához kapcsolódó kockázatokra, megengedett a belső ellenőrzési eljárás alkalmazása.

63. példa: A digitális elemeket tartalmazó hardvertermék alapvető funkciója az (EU) 2025/2392 végrehajtási rendelet I. mellékletének 12. pontjában leírt útvonalválasztó. A digitális elemeket tartalmazó termék további funkciókkal is rendelkezik, beleértve az integrált tűzfal-alkotóelemből adódó tűzfalképességeket is. A gyártó kockázatértékelést végez a digitális elemeket tartalmazó termék egészére vonatkozóan, beleértve az alapvető útvonalválasztó funkciót és a tűzfal funkciót is. Harmonizált szabványt alkalmaz, amely kiterjed az alapvető útvonalválasztó funkcióival kapcsolatos kockázatokra, valamint további intézkedéseket alkalmaz a további funkciókból eredő kockázatok kezelésére. A gyártó például alkalmazhatja a tűzfalakra vonatkozó harmonizált szabványt a tűzfalfunkcióval kapcsolatos kockázatok fedezésére. A gyártó a megfelelőségértékeléséhez alkalmazhatja a belső ellenőrzési eljárást, amely a digitális elemeket tartalmazó termék egészére kiterjed, beleértve a tűzfalfunkciót is.

6.3. A megfelelőség vélelmét érintő szempontok

153. A kiberrezilienciáról szóló rendelet 27. cikkének (1) bekezdése rögzíti, hogy azokról a digitális elemeket tartalmazó termékekről és gyártó által bevezetett eljárásokról, amelyek megfelelnek azon harmonizált szabványoknak, illetve azok egy részének, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*, vélelmezni kell, hogy megfelelnek a kiberrezilienciáról szóló rendelet alapvető kiberbiztonsági követelményeinek, amelyekre az említett

szabványok vagy azok részei vonatkoznak ([26]). A 27. cikk (5) bekezdése kiterjeszti a megfelelőség vélelmét azokra a digitális elemeket tartalmazó termékekre és a gyártó által bevezetett eljárásokra, amelyek megfelelnek a Bizottság által végrehajtási jogi aktusok révén elfogadott egységes előírásoknak, a 27. cikk (8) bekezdése pedig megállapítja a megfelelőség vélelmét a gyártó által bevezetett azon digitális elemeket tartalmazó termékekre és eljárásokra, amelyekre vonatkozóan az (EU) 2019/881 rendelet alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében EU-megfelelőségi nyilatkozatot vagy tanúsítványt állítottak ki, amennyiben ezt a 27. cikk (9) bekezdésével összhangban felhatalmazáson alapuló jogi aktusok útján meghatározták ([27]).

154. Ezért ha a gyártó olyan harmonizált szabványt alkalmazott, amelynek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*, a szabvány hatálya alá tartozó kockázatok tekintetében vélelmezni kell a megfelelőséget. Ilyen helyzet adódhat például akkor, ha a hivatkozott harmonizált szabvány a digitális elemeket tartalmazó termék alapvető funkciójával kapcsolatos valamennyi kockázatra kiterjed, és nincsenek olyan további funkciók, amelyek kiberbiztonsági kockázatot jelentenek. Például az útvonalválasztókra vonatkozó harmonizált szabvány várhatóan kiterjed legalább az e digitális elemeket tartalmazó termékek alapvető funkciójával kapcsolatos kockázatokra. Ha az ilyen termék nem tartalmaz további funkciókat, vagy ha ezek a további funkciók nem jelentenek olyan kockázatot, amelyre a szabvány nem terjed ki, a digitális elemeket tartalmazó termék esetében vélelmezni lehet a megfelelőséget.

155. A 151. és a 152. pontban tárgyalt esetekben a gyártó alkalmazhatja a belső ellenőrzési eljárást, mivel a harmonizált szabvány kiterjed a digitális elemeket tartalmazó termék alapvető funkcióival kapcsolatos kockázatokra. Az említett példákban leírt, digitális elemeket tartalmazó termékek azonban túlterjedhetnek a harmonizált szabványok alkalmazási körén, és további funkcióik olyan kiberbiztonsági kockázatokat jelenthetnek, amelyekre az adott harmonizált szabvány nem terjed ki. Az ilyen digitális elemeket tartalmazó termékek esetében ezért e további funkciók tekintetében a megfelelőség nem vélelmezhető.

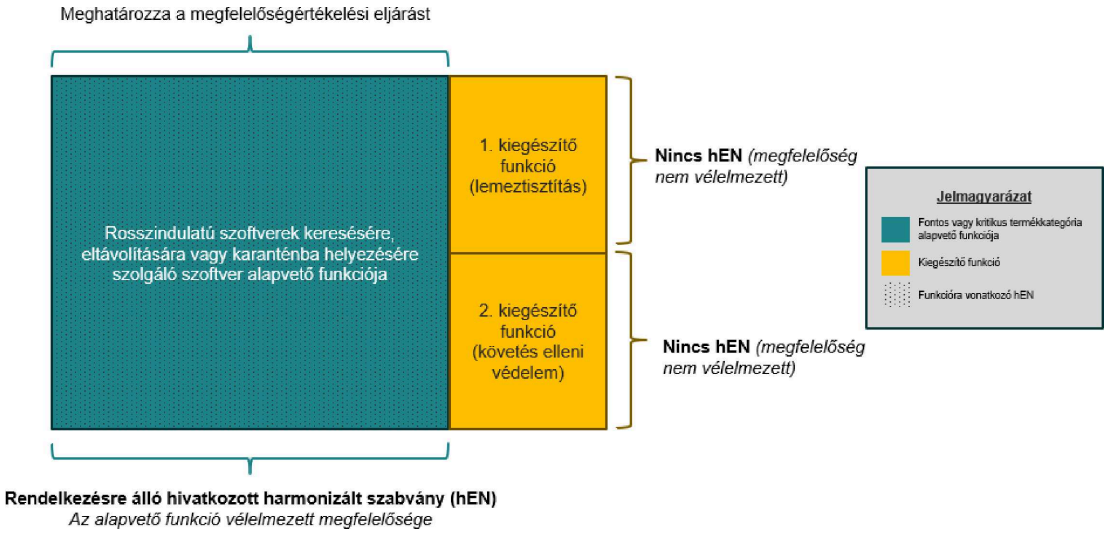
64. példa: Egy vírusirtó szoftver alapvető funkciója rosszindulatú szoftverek keresésére, eltávolítására vagy karanténba helyezésére szolgáló szoftver, és a harmonizált szabvány kiterjed az alapvető funkcióhoz kapcsolódó kockázatokra. Ez a digitális elemeket tartalmazó termék további funkciókat is tartalmaz, nevezetesen egy lemeztisztítási funkciót és egy követés elleni, a felhasználót az internetes navigálás során védő funkciót, amelyek kockázataira a harmonizált szabvány nem terjed ki. A harmonizált szabvány alkalmazása esetén a gyártó belső ellenőrzési eljárást alkalmazhat a megfelelőségértékeléshez. A termék alapvető funkciójához kapcsolódó kockázatok tekintetében a megfelelőség vélelmezhető, a további funkciókhoz kapcsolódó kockázatok tekintetében azonban nem.

([26]) A kék útmutató 4.1.2.2. szakasza egyértelműen kimondja, hogy „[a] kockázattal kapcsolatos harmonizációs jogszabályok esetében […] a gyártó még a harmonizált szabványok – amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában* – alkalmazásakor is teljes felelősséggel tartozik a termékével kapcsolatos kockázatok értékeléséért, amellyel megállapítja, mely alapvető (vagy egyéb) követelmények tekinthetők relevánsnak. Ezen értékelést követően a gyártó dönthet a harmonizált szabványokban – amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában* – foglalt műszaki előírások alkalmazása mellett, hogy végrehajtsa a harmonizált szabványban megállapított »kockázatcsökkentő intézkedéseket«”.

([27]) A fentiekhez hasonlóan e szakasz fennmaradó részében ez csak azokra a harmonizált szabványokra vonatkozik, amelyek hivatkozásait közzétették az *Európai Unió Hivatalos Lapjában*. Ugyanez az iránymutatás azonban az egységes előírásokra és az európai kiberbiztonsági tanúsítási rendszerekre is vonatkozik.

7. ábra:

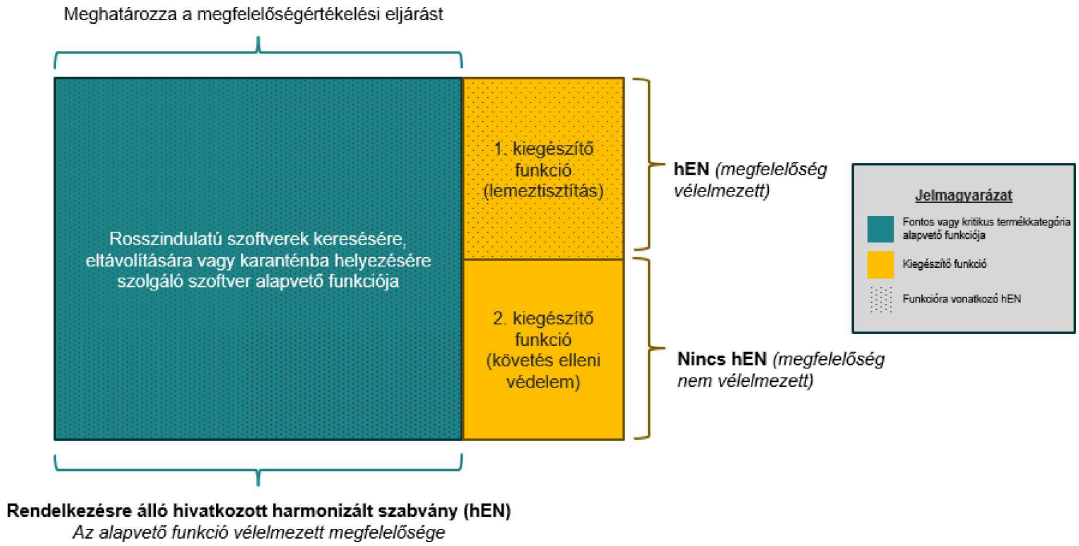
A harmonizált szabvány az alapvető funkciók tekintetében biztosítja a megfelelőség vélelmét (mivel az adott alapvető funkcióval kapcsolatos valamennyi kockázattal foglalkozik), a kiegészítő funkciók tekintetében azonban nem.



65. példa: Az előző példával azonos forgatókönyvben a harmonizált szabványt úgy frissítették, hogy az a további funkciók egyikével – a lemeztisztítási funkcióval – kapcsolatos kockázatokra is kiterjed, a másikkal (a követés elleni funkcióval) kapcsolatos kockázatokra azonban nem. A harmonizált szabvány alkalmazása esetén a gyártó belső ellenőrzési eljárást alkalmazhat a megfelelőségértékeléshez. A termék alapvető funkcióival és a lemeztisztító funkcióval kapcsolatos kockázatok tekintetében a megfelelőség vélelmezhető, a követés elleni funkcióval kapcsolatos kockázatok tekintetében azonban nem.

8. ábra:

A harmonizált szabvány biztosítja a megfelelőség vélelmét az alapvető funkció és az 1. kiegészítő funkció tekintetében, mivel az e két funkcióval kapcsolatos valamennyi kockázatra kiterjed, a 2. kiegészítő funkció tekintetében azonban nem.



7. A DIGITÁLIS ELEMEKET TARTALMAZÓ TERMÉKEK ÉS AZ ALKOTÓELEMEK KIBERBIZTONSÁGI KOCKÁZATÉRTÉKELÉSE ÉS INTEGRÁLÁSA

7.1. A kiberbiztonsági kockázatok értékeléséről és kezeléséről

156. A kiberrezilienciáról szóló rendelet 13. cikkének (2) bekezdésében előírt kiberbiztonsági kockázatértékelés keretében a gyártóknak azonosítaniuk kell a releváns kockázatokat, és értékelniük kell azok lehetséges hatását a digitális elemeket tartalmazó termékre. A gyártóknak továbbá az I. mellékletben foglalt alapvető követelményekkel összhangban megfelelő intézkedéseket kell végrehajtaniuk e kockázatok kezelése érdekében.

157. A szervezeti kockázatkezelésben a kockázatokat általában a szervezet belső célkitűzéseiből vagy kockázatvállalási hajlandóságából levezetett elfogadási kritériumok alapján értékelik. Ezzel szemben a kiberrezilienciáról szóló rendelet értelmében a fennmaradó kiberbiztonsági kockázatot arra a követelményre tekintettel kell értékelni, hogy a forgalomba hozott, digitális elemeket tartalmazó termék a kockázatok alapján – figyelembe véve rendeltetését és észszerűen előre látható használatát – megfelelő szintű kiberbiztonságot biztosítson.

158. Ennek megfelelően a gyártó belső kockázattűrése, kereskedelmi stratégiája vagy pusztán költségszempontjai nem relevánsak annak meghatározása szempontjából, hogy kezelték-e a kockázatokat. A 13. cikk (2) és (3) bekezdésének alkalmazásában a gyártóknak képesnek kell lenniük annak megállapítására, hogy az azonosított kiberbiztonsági kockázatokat megfelelően kezelték-e az I. melléklet I. részében foglalt alapvető követelmények végrehajtása révén, figyelembe véve a rendeltetést, az észszerűen előrelátható használatot és a használati feltételeket, beleértve adott esetben a működési környezetet (például a digitális elemeket tartalmazó termék célfelhasználóit) és a védendő eszközöket, figyelembe véve a digitális elemeket tartalmazó termék használatának várható időtartamát.

159. A fennmaradó kiberbiztonsági kockázat a kockázatértékelés és a kockázatkezelés eredendő eredménye. Elismert tény, hogy a kiberbiztonsági kockázatokat a gyakorlatban nem lehet teljes mértékben kiküszöbölni. A fennmaradó kockázat megléte azonban nem jelenti azt, hogy a gyártó saját belátása szerint bármilyen kockázatot elfogadhat. Digitális elemeket tartalmazó termék csak akkor hozható forgalomba, ha a megfelelő intézkedések meghozatalát követően a fennmaradó kockázatokat az alapvető követelmények végrehajtása révén, a digitális elemeket tartalmazó termék rendeltetésének és észszerűen előrelátható használatának figyelembevételével megfelelően kezelték.

160. Ha kiberbiztonsági kockázatokat azonosítanak, a gyártók a 13. cikk (3) bekezdésével összhangban kötelesek azokat megfelelő intézkedésekkel kezelni, többek között termékszinten is. A körülményektől függően ez magában foglalhatja például a támadási felület csökkentését, műszaki biztonsági elemek bevezetését, a funkciók korlátozását vagy kiigazítását, vagy a digitális elemeket tartalmazó termék rendeltetésének pontosabb meghatározását. A gyártók lépéseket tehetnek a digitális elemeket tartalmazó termék észszerűen előrelátható használatának alakítására is, például kockázati kommunikáció, felhasználói iránymutatás vagy a felhasználói felület kialakítása révén, annak érdekében, hogy a felhasználói magatartást a biztonságos használati minták felé tereljék.

161. A kiberrezilienciáról szóló rendelet nem rendelkezik arról, hogy a kiberbiztonsági kockázat vagy felelősség a felhasználókra vagy harmadik felekre ruházható a terméktervezés hiányosságainak ellensúlyozása vagy annak igazolása érdekében, hogy a kiberbiztonsági kockázatokat miért nem kezelik. A digitális elemeket tartalmazó biztonságos termék forgalomba hozatalára és az alapvető követelményeknek való megfelelés igazolására vonatkozó kötelezettség továbbra is a gyártót terheli.

162. A felhasználóknak nyújtott információk és utasítások felhasználhatók a digitális elemeket tartalmazó termék biztonságos bevezetésének és üzemeltetésének támogatására, beleértve azt az esetet is, amikor a gyártó úgy döntött, hogy a termék rendeltetését megbízható környezetre korlátozza, és tájékoztatja a felhasználókat a fennmaradó kockázatokról, a digitális elemeket tartalmazó termék jellegének és célfelhasználóinak megfelelő módon.

66. példa: Egy gyártó ipari érzékelőt fejleszt ki megbízható környezetben való használatra. Ahhoz, hogy az érzékelő megfelelően el tudja látni a funkcióját, a gyártó nem hajt végre a magát az érzékelőt érő fizikai támadások elleni védelmet célzó intézkedéseket. A kockázatértékelésben azonosított kapcsolódó kockázatok csökkentése érdekében a gyártó az érzékelő rendeltetését kizárólag az olyan megbízható környezetben való használatra korlátozza, amely kiküszöböli a digitális elemeket tartalmazó termékhez való jogosulatlan fizikai hozzáférést. A felhasználóknak szóló információk és utasítások egyértelmű tájékoztatást nyújtanak az érzékelő használatának e korlátairól, a digitális elemeket tartalmazó termék jellegének és célfelhasználóinak megfelelő módon.

67. példa: Egy gyártó menedzselt asztali és mobil eszközökön való professzionális felhasználásra szánt szoftveralkalmazást fejleszt ki. Az alkalmazás helyben tárolt érzékeny adatokat és a felhasználók által generált tartalmakat kezel. A kockázatértékelés során a gyártó a jogosulatlan hozzáférés kockázatát azonosítja akkor, ha az ilyen adatokat egyszerű szöveg formájában tárolják az eszközön. Ahelyett, hogy magán az alkalmazáson belül saját titkosítási mechanizmust tervezne és valósítana meg, a gyártó úgy dönt, hogy az alkalmazás által használni kívánt operációs rendszer által helyben biztosított titkosítási és kulcskezelési funkciókra támaszkodik, mivel az operációs rendszer beépített kriptográfiai szolgáltatásai kiforrottak és rendszeresen karbantartják őket.

163. Ha a kiberbiztonsági kockázatértékelés olyan kockázatokat azonosít, amelyek megfelelő intézkedésekkel nem kezelhetők kielégítően, a kiberrezilienciáról szóló rendeletnek való megfelelés szükségessé teheti a digitális elemeket tartalmazó termék kialakításának, funkcióinak vagy rendeltetésének módosítását. A kizárólag a költségekkel vagy a kereskedelmi megvalósíthatósággal kapcsolatos megfontolások nem elégségesek a kockázatkezelés mellőzésének alátámasztásához, ha emiatt a digitális elemeket tartalmazó termék nem felel meg az alapvető követelményeknek.

7.2. A digitális elemeket tartalmazó termékeknek a kockázatok alapján megfelelő szintű kiberbiztonságot biztosító tervezéséről, fejlesztéséről és gyártásáról

164. A kiberrezilienciáról szóló rendelet I. melléklete I. részének 1. pontjában említett alapvető kiberbiztonsági követelmény előírja, hogy a digitális elemeket tartalmazó termékeket úgy kell megtervezni, fejleszteni és gyártani, hogy a kockázatok alapján megfelelő szintű kiberbiztonságot biztosítsanak.

165. Ez az alapvető követelmény a kiberbiztonsági kockázatértékelés keretében azonosított valamennyi kiberbiztonsági kockázat kezelésére irányul. Ez különösen azokat a kiberbiztonsági kockázatokat foglalja magában, amelyeket az I. melléklet I. részében foglalt, az 1. ponttól eltérő alapvető követelmények végrehajtásának részeként egyébként nem kezelnek megfelelően. Ez az alapvető követelmény eltér a kiberbiztonsági kockázatértékelésnek a 13. cikk (2) bekezdése szerinti elvégzésére vonatkozó jogi kötelezettségtől.

166. Ha a digitális elemeket tartalmazó termékkel kapcsolatos valamennyi releváns kiberbiztonsági kockázatot az 1. ponttól eltérő alkalmazandó alapvető követelmények kezelésére szolgáló megfelelő intézkedések végrehajtásával kezelik, az I. melléklet I. részének 1. pontjában említett alapvető követelményt teljesítettnek kell tekinteni. Ezzel szemben ha a kiberbiztonsági kockázatértékelés olyan további kockázatokat azonosít, amelyeket az ilyen intézkedések nem kezelnek teljes mértékben, az I. melléklet I. részének 1. pontjában említett alapvető követelménynek való megfelelés érdekében a gyártóknak a digitális elemeket tartalmazó termékre vonatkozóan megfelelő intézkedéseket kell végrehajtaniuk e kockázatok kezelésére. A gyakorlatban a legtöbb esetben a többi alapvető követelménynek való megfelelés várhatóan az e követelménynek való megfelelést eredményezi.

7.3. A külső függőségekkel és az integrált alkotóelemekkel kapcsolatos kockázatértékelés és kellő gondosság

167. A kiberrezilienciáról szóló rendelet két különálló, de egymást kiegészítő kötelezettséget állapít meg a gyártók számára a kiberbiztonsági kockázatkezeléssel kapcsolatban. Egyrészt a 13. cikk (2) bekezdése előírja a gyártók számára, hogy végezzenek kiberbiztonsági kockázatértékelést magára a digitális elemeket tartalmazó termékre vonatkozóan. Másrészt a 13. cikk (5) bekezdése előírja, hogy az integrált alkotóelemek tekintetében kellő gondossággal kell eljárni. E két kötelezettség együttesen hivatott biztosítani azt, hogy a digitális elemeket tartalmazó termék biztonságos maradjon, többek között akkor is, ha távoli adatkezelési megoldásokra, távoli szolgáltatásokra vagy harmadik fél által biztosított szoftver- vagy hardver-alkotóelemekre támaszkodik.

168. A kiberbiztonsági kockázatértékelés azon releváns kockázatok azonosítására és kezelésére vonatkozik, amelyek hatással lehetnek a digitális elemeket tartalmazó termékre, beleértve a terméken kívülről eredő kockázatokat, például a külső hálózatokat, a környezeti tényezőket vagy más külső szempontokat, amelyek hatással lehetnek a digitális elemeket tartalmazó termékre, vagy amelyekre a termék támaszkodik. Az ilyen külső kockázatok esetében a kiberrezilienciáról szóló rendelet nem írja elő a gyártók számára a külső környezet ellenőrzését vagy irányítását. Ehelyett a gyártóknak azonosítaniuk kell ezeket a kockázatokat, és azokat magának a digitális elemeket tartalmazó terméknek a tervezése és fejlesztése révén kell csökkenteniük. Ez magában foglalja az I. melléklet I. részében meghatározott megfelelő alapvető követelmények végrehajtását, valamint szükség esetén a felhasználóknak az integrációs vagy telepítési kockázatokkal kapcsolatban adott tájékoztatást és utasításokat.

169. A gyártó például azonosíthatja annak kockázatát, hogy a termék működése során jogosulatlan személyek a digitális elemeket tartalmazó termék részét nem képező háttérendszerekhez hozzáférve megkísérelhetnek rosszindulatú parancsokat küldeni a digitális elemeket tartalmazó terméknek. Az ilyen háttérrendszerek, ha azokat nem a gyártó tervezte és fejlesztette ki, vagy azok nem a gyártó felelősségi körébe tartoznak, vagy ha nem támogatják a digitális elemeket tartalmazó termék valamely funkcióját, nem minősülnek távoli adatkezelési megoldásnak, ennélfogva a kiberrezilienciáról szóló rendelet alkalmazásában nem tartoznak a digitális elemeket tartalmazó termék körébe. Mindazonáltal a kiberrezilienciáról szóló rendelet előírja a gyártó számára, hogy termékszintű intézkedésekkel kezelje az általuk esetlegesen jelentett kockázatot, például a távoli parancsok kriptográfiai hitelesítésének előírásával, a konfigurációváltoztatások integritásának ellenőrzésével, vagy rendellenes viselkedés észlelése esetén biztonsági szempontból releváns naplók vagy riasztások generálásával. Ugyanígy ha a gyártó a külső szolgáltatás elérhetetlenné válásából eredő kockázatot azonosít, például áramkimaradások vagy az infrastruktúra meghibásodása miatt, a kiberrezilienciáról szóló rendelet termékszintű kockázatcsökkentő intézkedéseket írhat elő az ilyen kiberbiztonsági kockázatokkal szemben, például annak biztosítását, hogy az üzemszünet miatt a digitális elemeket tartalmazó termék ne kerüljön bizonytalan állapotba. Ilyenkor a kiberrezilienciáról szóló rendelet szabályozza a digitális elemeket tartalmazó termék reagálását ezekre a külső kockázatokra; viszont nem ír elő kötelezettségeket a háttérinfrastruktúra megszervezésének, személyzettel való ellátásának vagy üzemeltetésének módjára vonatkozóan, és nem kezeli az infrastruktúrát a digitális elemeket tartalmazó termék részeként.

170. A kellő gondosság a digitális elemeket tartalmazó termék részét képező elemekre, különösen a harmadik fél által biztosított integrált szoftver- vagy hardver-alkotóelemekre vonatkozik. A gyártóknak megfelelő intézkedéseket kell hozniuk annak biztosítása érdekében, hogy az ilyen alkotóelemek ne ássák alá a digitális elemeket tartalmazó termék alapvető követelményeknek való megfelelését. Ez csak annak meghatározásával érhető el, hogy a digitális elemeket tartalmazó termék mit igényel alkotóelemeitől a kiberbiztonsági célkitűzéseinek eléréséhez, valamint annak kockázatalapú ellenőrzésével, hogy ezek az alkotóelemek összhangban vannak-e a termék igényeivel, amint azt a (34) preambulumbekezdés is jelzi.

171. Kiberbiztonsági kockázatértékelésével összhangban a gyártónak azonosítania kell azokat a követelményeket, amelyeknek az integrált alkotóelemnek meg kell felelnie. Ha például a digitális elemeket tartalmazó termék valamely alkotóelem által biztosított kriptográfiai funkciókra, frissítési mechanizmusokra vagy biztonságos kommunikációra támaszkodik, a gyártónak a kellő gondosság részeként azonosítania kell ezeket az igényeket, és ellenőriznie kell, hogy az alkotóelem megfelel-e azoknak. Az erre vonatkozó bizonyíték állhat az alkotóelem gyártójától kapott dokumentációból, például műszaki előírásokból, biztonsági dokumentációból vagy a vonatkozó megfelelőségi vagy megbízhatósági dokumentációból. Adott esetben a gyártó teszteket is végezhet annak ellenőrzésére, hogy ezek az alkotóelemek megfelelően ellátják-e a vonatkozó funkciókat. Bár a kellő gondosság külön jogi kötelezettség, támogatja és alátámasztja a gyártó azon képességét, hogy igazolja a digitális elemeket tartalmazó termék egészére vonatkozó alapvető követelményeknek való megfelelést.

172. A digitális elemeket tartalmazó termék egészét érintő kockázatok értékelésekor a kiberbiztonsági kockázatértékelésben figyelembe kell venni a terméken kívüli elemeket, például a környezeti elemeket, a külső infrastruktúrát, más rendszereket vagy hálózatokat, és a kockázatokat adott esetben termékszintű intézkedésekkel kell kezelni annak érdekében, hogy a digitális elemeket tartalmazó termék megfeleljen az alapvető követelményeknek. A kockázatértékelés részeként figyelembe kell venni azokat az alkotóelemeket is, amelyek fizikailag vagy logikailag integrálódnak a digitális elemeket tartalmazó termékbe, de harmadik féltől származnak. A megfelelés érdekében azonban a gyártónak azokat külsőleg szállított alkotóelemekként kell kezelnie, amelyek tulajdonságait az integráláskor kellő gondosság mellett ellenőrizni kell, mivel előfordulhat, hogy a gyártó nem végezte el azok átalakítását vagy újrafejlesztését.

173. Ugyanez a logika alkalmazandó az alkotóelemek fejlesztése és integrálása során. Ha a gyártó maga fejleszt ki funkciókat, közvetlenül kell végrehajtania az alapvető követelményeket. Ha a gyártó mások által kifejlesztett alkotóelemeket integrál, kellő gondossággal biztosítania kell, hogy ezeket az alkotóelemeket olyan módon lehessen használni, amely lehetővé teszi a digitális elemeket tartalmazó termék egészének megfelelését. A célkitűzés mindkét esetben változatlan: a forgalomba hozott, digitális elemeket tartalmazó terméknek a kiberbiztonsági kockázatértékelésben azonosított kockázatokat figyelembe véve el kell érnie a kiberrezilienciáról szóló rendelet által előírt megfelelő kiberbiztonsági szintet.

7.4. **A kockázatértékelések és a megfelelőségi dokumentáció újrafelhasználása digitális elemeket tartalmazó termékcsaládok esetében**

174. A gyártók forgalomba hozhatnak digitális elemeket tartalmazó hasonló termékeket, például ugyanazon termékcsalád különböző változatait, modelljeit vagy konfigurációit. Amennyiben az ilyen, digitális elemeket tartalmazó termékek architektúrája, biztonsági szempontból releváns kialakítása és rendeltetése azonos, és a termékek ugyanazoknak a kiberbiztonsági kockázatoknak vannak kitéve, a kiberrezilienciáról szóló rendelet nem írja elő a gyártók számára, hogy a kockázatértékelés és a megfelelőségértékelés céljából minden egyes változatot digitális elemeket tartalmazó, teljesen különálló termékként kezeljenek.

175. Ilyenkor – feltéve, hogy a releváns kockázatokkal szembeni védelem és az alapvető követelmények teljesítése valamennyi érintett változat esetében megfelelő – a gyártók a következőkre támaszkodhatnak: i. a kiberrezilienciáról szóló rendelet 13. cikkének (2) bekezdésével összhangban elvégzett egyetlen kiberbiztonsági kockázatértékelés, ii. egyetlen műszaki dokumentáció, és iii. egyetlen megfelelőségértékelési eljárás. Ez lehetővé teszi a digitális elemeket tartalmazó termékcsoportra vonatkozó egyetlen EU-megfelelőségi nyilatkozat kiállítását is, ha az egyértelműen azonosítja azokat a termékváltozatokat, amelyekre vonatkozik.

176. A döntő szempont az, hogy a változatok közötti eltérések relevánsak-e a kiberbiztonság szempontjából. Azok az eltérések, amelyek nem befolyásolják a digitális elemeket tartalmazó termék kiberbiztonsági tulajdonságait, például a szín, az alaktényező, a memóriaméret vagy más, a biztonság szempontjából nem releváns jellemzők különbségei, nem igényelnek külön kockázatértékelést vagy megfelelőségértékeléseket. Ezzel szemben egyes esetekben a változatok eltérő módon befolyásolhatják az alapvető követelmények végrehajtását, például különböző kommunikációs interfészek, szoftvercsomagok, frissítési mechanizmusok vagy távoli konnektivitás révén. Ilyenkor ezeknek az eltéréseknek tükröződniük kell a kockázatértékelésben, valamint szükség esetén a megfelelőségértékelésben és a műszaki dokumentációban.

177. A gyártók továbbra is felelősek annak biztosításáért, hogy a kockázatértékelés és a kapcsolódó dokumentáció pontosan tükrözze a forgalomba hozott, digitális elemeket tartalmazó termékeket. Ha egy új változat új kiberbiztonsági kockázatokat eredményez, vagy megváltoztatja az alapvető követelmények végrehajtásának módját, a meglévő kockázatértékelést és megfelelőségi dokumentációt ennek megfelelően aktualizálni kell. Az egyetlen megfelelőségértékelésre való támaszkodás csak annyiban lehetséges, amennyiben a digitális elemeket tartalmazó termékek kiberbiztonsági tulajdonságaik tekintetében nem mutatnak különbségeket.

8. **TÁVOLI ADATKEZELÉS**

178. A kiberrezilienciáról szóló rendelet 3. cikkének 1. pontjában foglalt meghatározás szerint a digitális elemeket tartalmazó termék „szoftver- vagy hardvertermék és annak távoli adatkezelési megoldásai, beleértve a külön forgalomba hozott szoftver- vagy hardver-alkotóelemeket is”. Ennek fényében a gyártónak a digitális elemeket tartalmazó terméket teljes egészében kell figyelembe vennie, annak távoli adatkezelési megoldásaival (RDPS) együtt. Például annak igazolásakor, hogy a digitális elemeket tartalmazó termék megfelel az I. mellékletben meghatározott alapvető követelményeknek, a távoli adatkezelési megoldásokat a kockázatértékeléstől kezdve figyelembe kell venni (13. cikk (2) bekezdés). Ugyanez érvényes az életciklusra vonatkozó kötelezettségek, például az aktívan kihasznált sérülékenységek és súlyos incidensek bejelentése tekintetében (14. cikk).

179. Ezen iránymutatás célja, hogy további támogatást nyújtson a gyártóknak annak meghatározásához, hogy a digitális elemeket tartalmazó termékük rendelkezik-e a kiberrezilienciáról szóló rendeletben meghatározott távoli adatkezelési megoldással, és hogyan teljesítsék az e tekintetben fennálló megfelelési kötelezettségeiket. A kiberrezilienciáról szóló rendeletben meghatározott fogalommeghatározások és preambulumbekezdések első elemzését követően ez az iránymutatás kérdéseket fogalmaz meg a gyártók számára annak tisztázásához, hogy a digitális elemeket tartalmazó termékük tartalmaz-e távoli adatkezelési megoldást – lásd a *8.1.* szakaszt (*What is considered a remote data processing solution for a product with digital elements?*). Ezt követően kifejti a távoli adatkezelési megoldások műszaki vonatkozásait, valamint a kiberrezilienciáról szóló rendeletnek való megfelelés értékelésének módját – lásd a *8.2.* szakaszt (*Practical and technical implications of remote data processing solutions and reliance on third-party solutions*).

180. A 3. cikk 2. pontjában foglalt fogalommeghatározás szerint a távoli adatkezelés „olyan távolról történő adatkezelés, amelyhez a szoftvert a gyártó tervezte és fejlesztette ki, vagy amelyet a gyártó felelőssége mellett terveztek vagy fejlesztettek ki, és amelynek hiánya megakadályozná a digitális elemeket tartalmazó termék valamely funkciójának ellátását". A távoli adatkezelési megoldás tehát a távolról történő adatkezelés szoftveres elemeit jelenti (a 3. cikk 4. pontjában meghatározottak szerint „egy elektronikus információs rendszer számítógépes kódból álló része"). Szándékolt jelentése szerint nem vonja a digitális elemeket tartalmazó termék körébe azt a hardvert, amelyre a távoli adatkezelés támaszkodhat.

181. A (11) és (12) preambulumbekezdés további magyarázattal szolgál a fogalom értelmezéséről. A (11) preambulumbekezdés egyértelművé teszi, hogy a távoli adatkezelési megoldás lefedésének célja, hogy a „termékeket a gyártók teljes egészében megfelelően biztosítsák, függetlenül attól, hogy az adatokat helyben, a felhasználó eszközén kezelik vagy tárolják, vagy távolról a gyártó kezeli vagy tárolja". Kimondja továbbá, hogy „[a]z e rendelet hatálya alá tartozó távoli adatkezelési megoldásokra vonatkozó követelmények ezért nem vonnak maguk után olyan műszaki, operatív vagy szervezeti intézkedéseket, amelyek a gyártó teljes hálózati és információs rendszereinek biztonságát fenyegető kockázatok kezelésére irányulnak".

182. Ezért a (11) preambulumbekezdésből az következik, hogy a kiberrezilienciáról szóló rendeletben előírt követelmények a jogalkotói szándék szerint nem a szervezet teljes informatikai infrastruktúrájára terjednek ki, hanem csak azokra a szoftveres alkotóelemekre, amelyek lehetővé teszik az adatkezelési megoldás végrehajtását. Például a gyártó saját emberi erőforrásaival, bérszámfejtésével, ügyfélkapcsolat-kezelésével, folyamatos integrációs/folyamatos szállítási (CI/CD) folyamatokkal kapcsolatos belső rendszerei nem tekintendők távoli adatkezelési megoldásnak, ahogy a biztonsági frissítések peremterületi terjesztése sem. Ugyanígy az ellenőrzési és tesztelési tevékenységekhez kapcsolódó rendszerek, például a behatolási tesztelés, a fenyegetésvadászat és a „red teaming" kívül esnek a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékek körén. Fontos megjegyezni, hogy bár a digitális elemeket tartalmazó termék biztonságára vonatkozó hatékony és rendszeres tesztek és felülvizsgálatok alkalmazása a kiberrezilienciáról szóló rendelet I. melléklete II. részének 3. pontjában meghatározott alapvető követelmény, ez nem jelenti azt, hogy az ilyen tevékenységeket a digitális elemeket tartalmazó termék tekintetében távoli adatkezelési megoldásnak kell tekinteni.

183. A (12) preambulumbekezdés a felhőszolgáltatásokra összpontosítva részletezi azokat a körülményeket, amelyek mellett a felhőszolgáltatások távoli adatkezelési megoldásnak tekinthetők. A preambulumbekezdés emlékeztet arra, hogy a felhőszolgáltatások és a felhőszolgáltatási modellek az (EU) 2022/2555 irányelv (NIS 2) ([28]) hatálya alá tartoznak, amely kiberbiztonsági kockázatkezelési követelményeket állapít meg a felhőszolgáltatókra vonatkozóan. Ezeket a követelményeket az (EU) 2024/2690 bizottsági végrehajtási rendelet ([29]) határozza meg részletesebben.

8.1. **Mi minősül távoli adatkezelési megoldásnak a digitális elemeket tartalmazó termékek esetében?**

184. A távoli adatkezelésnek a 3. cikk (2) bekezdésében foglalt fogalommeghatározása tehát három elemen alapul: i. az adatkezelés „távolról" történik-e, ii. az ilyen adatkezelés hiánya megakadályozná a digitális elemeket tartalmazó termék valamely funkciójának ellátását, és iii. a szoftvert a gyártó tervezte és fejlesztette-e ki, vagy azt a gyártó felelőssége mellett terveztek vagy fejlesztettek-e ki. A következő három alszakasz részletesebben foglalkozik ezekkel az elemekkel.

([28]) Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o., ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) A Bizottság (EU) 2024/2690 végrehajtási rendelete (2024. október 17.) az (EU) 2022/2555 irányelvnek a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2690, 2024.10.18., ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *A „távolról” fogalma*

185. A 3. cikk (2) bekezdésében említett „távolról” fogalma releváns, de nem elegendő annak meghatározásához, hogy a digitális elemeket tartalmazó termék magában foglal-e távoli adatkezelési megoldást. Tekintettel továbbá azon megoldások sokféleségére, amelyek e fogalom alá tartozhatnak, a „távolról” fogalma nem határozható meg kimerítően. A gyártónak eseti értékelést kell végeznie.

186. A kiberrezilienciáról szóló rendelet (11) preambulumbekezdése két esetet említ: az adatokat „helyben, a felhasználó eszközén” kezelik vagy tárolják, vagy „távolról a gyártó kezeli” vagy tárolja. A távoli adatkezelésre jellemzően a digitális elemeket tartalmazó termék felhasználói környezetén vagy a szervezet működési környezetén kívül kerül sor (foglalkozásszerű felhasználó esetében). Ez azonban nem zárja ki, hogy a feldolgozásra az eszköz közelében („peremterületen”) is sor kerüljön. Az adatátvitel lehet vezetékes (pl. Ethernet kábel) vagy vezeték nélküli (pl. wifi, Bluetooth). A felhőalapú számítástechnika, beleértve a pereminformatikát is, tipikus példája a „távoli” adatkezelésnek. Például egy olyan felhőalapú funkció esetében, amelyhez a felhasználó mobilalkalmazásból fér hozzá, az adatkezelés egy része a felhőben, a felhasználó környezetén kívül történik.

187. Fontos megjegyezni, hogy a távoli adatkezelési megoldást nem feltétlenül működtetik harmadik fél által biztosított felhőinfrastruktúrán. A gyártó telephelyén található helyi szervereken zajló távoli adatkezelés is távoli adatkezelési megoldásnak minősülhet. Más szóval: egy helyszínen és egy magánfelhőben futtatott megoldás ugyanúgy minősülhet távoli adatkezelési megoldásnak, mint egy nyilvános felhőben és a helyszínen kívül futtatott megoldás.

188. Azt a két döntő kérdést, amelyek együttesen meghatározzák, hogy az adatkezelés távoli adatkezelési megoldásként a kiberrezilienciáról szóló rendelet hatálya alá tartozik-e, az alábbi *8.1.2.* és *8.2.* szakasz ismerteti. Ha a válasz mindkét kérdésre igenlő, a távoli adatkezelés távoli adatkezelési megoldásnak minősül.

8.1.2. *Az adatkezelés hiánya megakadályozná-e a digitális elemeket tartalmazó termék valamely funkciójának ellátását?*

189. Amint azt a „távoli adatkezelésnek” a 3. cikk (2) bekezdésében foglalt fogalommeghatározása meghatározza, ahhoz, hogy a távolról történő adatkezelés távoli adatkezelési megoldásnak minősüljön, a hiányának meg kell akadályoznia a digitális elemeket tartalmazó termék valamely funkciójának ellátását. A „funkciók” e fogalommeghatározásban szereplő fogalma nem korlátozódik a digitális elemeket tartalmazó termék „alapvető funkciójára” vagy „rendeltetésére”, mivel a kiberrezilienciáról szóló rendelet nem ír elő ilyen korlátozást. A kiberrezilienciáról szóló rendelet hatálya alá tartozó funkciók egyrészt olyan funkciók, amelyek közvetlenül betöltik a digitális elemeket tartalmazó termék felhasználók által tapasztalt rendeltetését, másrészt olyan funkciók, amelyek támogatják a termék általános teljesítményét.

190. Példák olyan funkciókra, amelyek esetében előfordulhat távolról történő adatkezelés, és ez megakadályozná a digitális elemeket tartalmazó termék valamely funkciójának ellátását: i. parancsok küldése egy eszköznek, ii. fájlok szinkronizálása, iii. a felhasználó bevezetése, iv. konfiguráció (a digitális elemeket tartalmazó termék személyre szabása), v. a frissítések automatizált terjesztése, beleértve a jellemzők frissítését és a biztonsági javításokat is, vi. személyazonosság- és hozzáférés-kezelés.

191. Egyes esetekben a felhasználó a funkciót távolról és manuálisan is használhatja (pl. izzó bekapcsolása alkalmazással vagy manuálisan). Ez a lehetőség nem zárja ki a funkció távoli ellátásával kapcsolatos adatkezelés távoli adatkezelési megoldásként való minősítését. E funkció távolról történő ellátása szintén a digitális elemeket tartalmazó termék által kínált funkciók közé tartozik.

192. Ezzel szemben ha egy bizonyos adatkezelés hiánya nem akadályozza meg a digitális elemeket tartalmazó termék valamely funkciójának ellátását, az adatkezelés nem minősül a kiberrezilienciáról szóló rendelet értelmében vett távoli adatkezelési megoldásnak. Erre példa a kizárólag statisztikai célból gyűjtött telemetriai adatok távoli elemzése vagy a jövőbeli termékfejlesztés.

193. Mindazonáltal, még ha az adatkezelés nem is támogatja a digitális elemeket tartalmazó termék valamely funkcióját, előfordulhat, hogy a gyártóknak a kiberbiztonsági kockázatértékelésük részeként (pl. a termék működési környezetére tekintettel) mérlegelniük kell, hogy ezek a távoli alkotóelemek kockázatot eredményeznek-e a digitális elemeket tartalmazó termékre nézve, és ennek megfelelően csökkenteniük kell ezeket a kockázatokat (pl. termékszintű kockázatcsökkentések révén).

194. A honlapok sajátos esetet képeznek, amely a *2.1. szakaszban* (*Placing on the market*) is kifejtett módon pontosítást igényel. A honlapok nem tartoznak a távoli adatkezelési megoldás körébe, ha a kiberrezilienciáról szóló rendelet (11) preambulumbekezdése kifejtett módon nem támogatják a digitális elemeket tartalmazó termék valamely funkcióját. Ahhoz, hogy a távoli adatkezelési megoldás körébe tartozzon, nem elegendő, ha egy honlap a digitális elemeket tartalmazó termékre vonatkozó információkat tartalmaz, még akkor sem, ha a termék átirányít egy ilyen honlapra. Nem minősül távoli adatkezelési megoldásnak például a felhasználók átirányítása egy olyan külső weboldalra, amely tájékoztatást és utasításokat ad a felhasználóknak. Ezzel szemben egy honlap a távoli adatkezelési megoldás körébe tartozhat akkor, ha lehetővé teszi vagy támogatja a digitális elemeket tartalmazó termék valamely funkcióját. Például a digitális elemeket tartalmazó termék működéséhez szükséges hitelesítő adatokat vagy tokeneket kibocsátó hitelesítési portál távoli adatkezelési megoldásnak minősül (feltéve, hogy a fogalommeghatározás egyéb kritériumai is teljesülnek).

8.1.3. *A szoftvert a gyártó tervezte és fejlesztette ki, vagy azt a gyártó felelőssége mellett tervezték és fejlesztették ki?*

195. A „távoli adatkezelésnek” a kiberrezilienciáról szóló rendelet 3. cikkének 2. pontjában szereplő fogalommeghatározása részletesebben meghatározza, hogy a távolról történő adatkezelés szoftverét a gyártónak kell megterveznie és kifejlesztenie, vagy azt a gyártó felelőssége mellett kell elvégezni. A teljes egészében a gyártó által (házon belül) kifejlesztett és tervezett távoli adatkezelés természetesen távoli adatkezelési megoldásnak minősül. Ez a helyzet akkor is, ha a gyártók külső szolgáltatót vesznek igénybe a megoldás kidolgozásához és megtervezéséhez (ekkor az a „saját felelősségük mellett” történik). A „gyártó felelőssége mellett” kifejezés a gyártóra szabott távoli adatkezelési megoldásokra utal. Ezek olyan esetek, amikor a gyártó nem egyszerűen egy meglévő, digitális elemeket tartalmazó termék vagy szolgáltatás hasznosítását engedélyezi az ügyfeleknek kínálttal azonos vagy kismértékben módosított verziók formájában. „A gyártó felelőssége mellett” azt jelenti, hogy a szoftvert kizárólag a gyártó állítja elő, vagy a nevében eljáró személy a gyártó által rendelkezésre bocsátott tervek és előírások alapján.

196. A távoli adatkezelési megoldás értelmezésében nem döntő szempont, hogy „ki működteti a megoldást”, mivel a kiberrezilienciáról szóló rendeletben foglalt fogalommeghatározás csak a távoli adatkezelési megoldás kialakítását és fejlesztését említi. Ez összhangban van a kiberrezilienciáról szóló rendelet megközelítésével, amely szerint a követelmények és kötelezettségek a gyártókat terhelik, nem pedig a digitális elemeket tartalmazó termék működését. Ha a gyártók olyan megoldásokat terveznek és fejlesztenek ki, amelyeket aztán harmadik fél üzemeltet, továbbra is felelősek maradnak a kiberrezilienciáról szóló rendeletnek az általuk forgalomba hozott, digitális elemeket tartalmazó termékre vonatkozó alapvető követelményeinek való megfelelésért.

197. Különbséget kell tenni azon esetek között, amikor a tervezést és a fejlesztést a gyártók végzik (vagy a gyártók felelőssége mellett végzik), valamint azon esetek között, amikor a gyártók nem az általuk (vagy a felelősségük mellett) tervezett és kifejlesztett, harmadik fél által nyújtott megoldásokra támaszkodnak. Érdemes például figyelembe venni azokat a legelterjedtebb felhőszolgáltatási modelleket, amelyek különböző szintű felhasználói ellenőrzést biztosítanak, és amelyekre a kiberrezilienciáról szóló rendelet (12) preambulumbekezdése is hivatkozik, nevezetesen a szolgáltatott szoftvert (SaaS), a platformszolgáltatást (PaaS) és az infrastruktúra-szolgáltatást (IaaS).

198. Harmadik fél által nyújtott IaaS-megoldás esetében a gyártó nem kezeli vagy ellenőrzi az alapul szolgáló fizikai és virtuális erőforrásokat (például az alapul szolgáló hardvert és a felhőszolgáltató hipervizorát), de képes tetszőleges szoftvereket telepíteni és futtatni az ilyen erőforrások, például operációs rendszerek és alkalmazások felhasználásával. A szoftvert a gyártó tervezte és fejlesztette ki, vagy azt a gyártó felelőssége mellett terveztek vagy fejlesztettek ki, ennélfogva távoli adatkezelési megoldásnak minősülhet (ha megfelel a fogalommeghatározás egyéb elemeinek).

199. Harmadik fél által nyújtott PaaS-megoldás esetében a gyártó saját (önállóan létrehozott vagy beszerzett) alkalmazást telepít a felhőszolgáltató által biztosított programozási nyelvek és futtatási környezetek használatával, és integrálja az alkalmazást a digitális elemeket tartalmazó termékébe. A gyártó ellenőrzi az alkalmazást és adott esetben a futtatási környezet konfigurációs beállításait. Az alkalmazást ezért a gyártó tervezte és fejlesztette ki, vagy azt a gyártó felelőssége mellett terveztek vagy fejlesztettek ki, ennélfogva távoli adatkezelési megoldásnak minősülhet (ha megfelel a fogalommeghatározás egyéb elemeinek).

200. Harmadik fél által nyújtott SaaS-megoldás esetében a SaaS-szolgáltató teljes mértékben kidolgozott alkalmazást kínál a gyártónak a gyártó digitális elemeket tartalmazó termékébe történő integrálásra. A gyártó korlátozottan képes kezelni a felhasználóspecifikus alkalmazáskonfigurációs beállításokat. Az alkalmazást ezért nem a gyártó tervezte és fejlesztette ki, és nem is a gyártó felelőssége mellett tervezték és fejlesztették ki.

201. Mindazonáltal, ha bizonyos elemek nem minősülnek távoli adatkezelési megoldásnak (pl. a hipervizor a harmadik fél által biztosított IaaS-infrastruktúra esetében, az operációs rendszer a harmadik fél által nyújtott PaaS-megoldás esetében, vagy a harmadik fél által biztosított SaaS-alkalmazás), de a digitális elemeket tartalmazó termékbe oly módon vannak integrálva, amely befolyásolja annak biztonságát, az ilyen megoldásokat a harmadik fél által biztosított alkotóelemekhez hasonlónak kell tekinteni. A gyártónak azonosítania és értékelnie kell az említett elemek integrálásával kapcsolatos kockázatokat, és azokat a digitális elemeket tartalmazó termékre vonatkozó alapvető követelmények végrehajtásával kell kezelnie. Ezt adott esetben támogathatják a felhőszolgáltató által a közös felelősségi modelljén keresztül rendelkezésre bocsátott biztonsági funkciók, ha a gyártó ezeket a funkciókat az azonosított kockázatok kezelésére használja vagy konfigurálja. Emellett a gyártónak az ezen alkotóelemek biztonságával kapcsolatos, a 13. cikk (5) bekezdésében említett kellő gondosságra vonatkozó kötelezettséghez hasonló kötelezettséget kell teljesítenie, mégpedig olyan módon, amely arányos azzal a kockázattal, amelyet a távoli megoldás jelent a digitális elemeket tartalmazó termék biztonságára nézve.

202. Összefoglalásképpen:

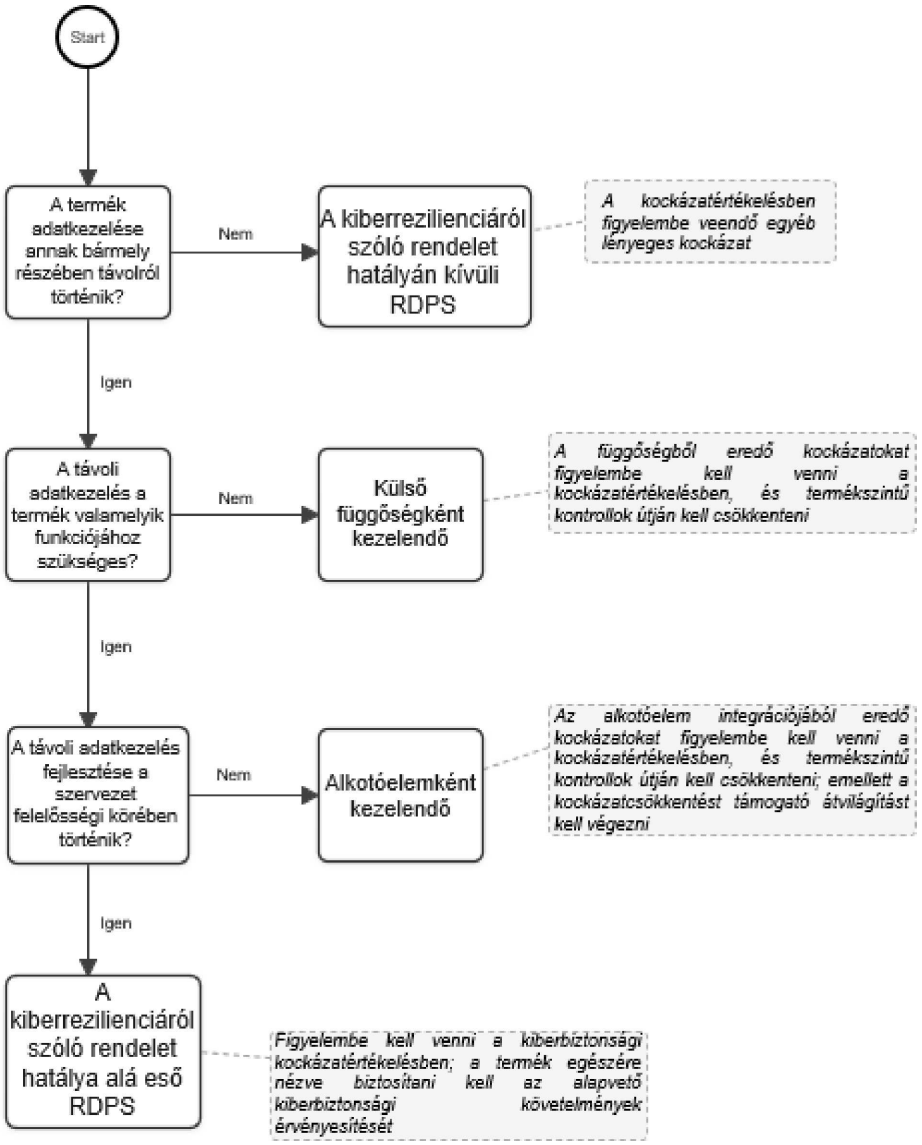
a) Ahhoz, hogy az adatkezelés távoli adatkezelési megoldásnak minősüljön, a *8.1.2.* szakaszban (*Would the absence of such data processing prevent the product with digital elements from performing one of its* functions?) és a *8.1.3.* (*Has the software been designed and developed by the manufacturer, or under its responsibility?*) szakaszban feltett mindkét kérdésre igenlő választ kell adni.

b) Ha a *8.1.2.* szakaszban (*Would the absence of such data processing prevent the product with digital elements from performing one of its* functions?) szereplő kérdésre adott válasz nemleges, a gyártóknak kockázatértékelésük részeként értékelniük kell az ilyen adatkezelés meglétéből eredő kockázatokat.

c) Ha a *8.1.2.* szakaszban (*Would the absence of such data processing prevent the product with digital elements from performing one of its* functions?) szereplő kérdésre adott válasz igenlő, a *8.1.3.* szakaszban (*Has the software been designed and developed by the manufacturer, or under its responsibility?*) szereplő kérdésre adott válasz viszont nemleges, a gyártóknak a harmadik fél által nyújtott megoldást alkotóelemként kell kezelniük. A kockázatértékelés részeként a gyártóknak értékelniük kell az ilyen megoldások integrálásából eredő kockázatokat, és azokat megfelelően csökkenteniük kell. Emellett a gyártóknak kellő gondossággal kell eljárniuk.

9. ábra:

Stilizált folyamatábra annak meghatározásához, hogy egy digitális elemeket tartalmazó termék tartalmaz-e távoli adatkezelési megoldást



8.2. A távoli adatkezelési megoldások gyakorlati és technikai vonatkozásai, a harmadik fél által nyújtott megoldások igénybevétele

203. A kiberrezilienciáról szóló rendelet kockázatalapú megközelítést követ, amelyet a 13. cikk (2) és (3) bekezdése, valamint az I. melléklet I. részének első alapvető követelménye rögzít, amely szerint „a digitális elemeket tartalmazó termékeket úgy kell megtervezni, fejleszteni és gyártani, hogy a kockázatok alapján megfelelő szintű kiberbiztonságot biztosítsanak”. Következésképpen kockázatalapú megközelítést kell alkalmazni a kiberrezilienciáról szóló rendelet távoli adatkezelési megoldásokra vonatkozó követelményeinek alkalmazásakor, valamint a digitális elemeket tartalmazó termékbe integrált, harmadik fél által nyújtott szolgáltatásokból eredő kockázatok kezelésekor.

204. Először is a gyártóknak i. jelezniük kell a műszaki dokumentációban, hogy a digitális elemeket tartalmazó termékük távoli adatkezelési megoldással rendelkezik vagy harmadik fél által nyújtott távoli megoldásokra támaszkodik, és ii. be kell mutatniuk az ilyen megoldásokat. Ha ugyanaz a távoli adatkezelési megoldás több, digitális elemeket tartalmazó terméket támogat, a távoli adatkezelési megoldást minden egyes termék műszaki dokumentációjában fel kell tüntetni. A több, digitális elemeket tartalmazó terméket kiszolgáló távoli adatkezelési megoldásra vonatkozó dokumentáció több eltérő termékmegfelelőség-értékelésre kiterjedően újra felhasználható.

205. A (11) preambulumbekezdésben említettek szerint a digitális elemeket tartalmazó termék részét képező és ezért a termék megfelelőségértékelésének hatálya alá tartozó távoli adatkezelési megoldást azokra a szoftvermodulokra kell korlátozni, amelyek felelősek a digitális elemeket tartalmazó termék funkcióiért, valamint az e modulok által a külső szolgáltatásokkal használt interfészekre. Nem minősülnek távoli adatkezelési megoldásnak azok a további háttérrendszerek, amelyek további feldolgozást végeznek, és amelyekkel a digitális elemeket tartalmazó termék nem lép közvetlen interakcióba.

206. Mindazonáltal ezek a háttérrendszerek továbbra is külső függőségek, amelyeket a kiberbiztonsági kockázatértékelés részeként értékelni kell, és termékszintű intézkedésekkel kell mérsékelni. A gyártó által végzett kockázatértékelésnek a következőket kell figyelembe vennie: i. a távoli adatkezelési megoldással kapcsolatos kockázatok, ii. a harmadik fél által nyújtott távoli megoldások igénybevételével kapcsolatos kockázatok (a harmadik fél által biztosított alkotóelemekhez hasonlóan), és iii. a termékkörnyezettel (pl. a mögöttes hardverrel) kapcsolatos kockázatok. E kockázatok csökkentése érdekében a gyártóknak biztonsági ellenőrzéseket kell végezniük magán a digitális elemeket tartalmazó terméken.

207. Ezenkívül a harmadik fél által nyújtott távoli szolgáltatásokkal kapcsolatos megfelelőségértékelés és/vagy a kellő gondosságra vonatkozó kötelezettségek teljesítésének részeként a megbízhatósági dokumentumok alábbi, nem kimerítő jegyzéke újra felhasználható a gyártó értékelésének alátámasztására:

a) az (EU) 2024/2690 bizottsági végrehajtási rendelet szerinti kötelezettségek teljesítésének igazolása;

b) az (EU) 2022/2554 rendelet (DORA) szerinti kötelezettségek teljesítésének igazolása;

c) az (EU) 2019/881 rendelet (a kiberbiztonsági rendelet) alapján elfogadott európai kiberbiztonsági tanúsítási rendszer keretében szerzett megfelelőségi nyilatkozat vagy tanúsítvány;

d) az ISO/IEC 27017:2015 vagy az ISO/IEC 27001:2022 szabványnak való megfelelés igazolása.

208. Végül a távoli szolgáltatást nyújtó harmadik felekkel folytatott interakcióik során a gyártóknak saját kockázatértékelésük alapján (adott esetben a szolgáltató közös felelősségi modelljére is támaszkodva) a legmegfelelőbb biztonsági intézkedéseket kell végrehajtaniuk. Ezeknek a kockázatcsökkentő intézkedéseknek magukban kell foglalniuk a digitális elemeket tartalmazó termékeik biztonsági ellenőrzését, valamint a harmadik félnek minősülő szolgáltatók által biztosított biztonsági intézkedések ellenőrzését (kellő gondosság). Az ilyen kockázatok csökkentésének egyik eszköze lehet a biztonsági garanciák beépítése a harmadik félnek minősülő szolgáltatókkal kötött, szolgáltatási szintre vonatkozó megállapodásaikba, beleértve az arra vonatkozó biztosítékokat is, hogy a szolgáltatók megfelelően kezelik a sérülékenységeket. A távoli szolgáltatást nyújtó harmadik felek megoldásainak jelentős változtatása nem minősülhet a digitális elemeket tartalmazó termék jelentős módosításának, mivel ezek az elemek nem tartoznak a gyártó felelősségi körébe. A kellő gondosságra vonatkozó kötelezettségeik részeként és a harmadik félnek minősülő szolgáltatók igénybevételéből eredő kockázatok megfelelő csökkentése érdekében azonban a gyártók számára ajánlott gondoskodni arról, hogy harmadik fél felhőszolgáltatóik megfelelően tájékoztassák őket a megoldásaikon végrehajtott változásokról. Előfordulhat, hogy a gyártóknak ezen információk alapján felül kell vizsgálniuk kockázatértékelésüket. Az aktualizált kockázatértékelésnek figyelembe kell vennie, hogy a harmadik félnek minősülő szolgáltatók továbbra is elegendő garanciát nyújtanak-e a kiberbiztonság tekintetében, és hogy a termékszintű biztonsági ellenőrzések továbbra is megfelelőek-e. Egyes esetekben előfordulhat, hogy a gyártóknak módosítaniuk kell ezeket az ellenőrzéseket, vagy harmadik félnek minősülő szolgáltatót kell váltaniuk.

8.3. **A távoli adatkezelési megoldások felhasználási esetei**

A gyártóknak nyújtott további gyakorlati iránymutatásként ez a szakasz egy sor fiktív felhasználási eseten keresztül ismerteti a távoli adatkezelésen alapuló, digitális elemeket tartalmazó termékek alaptípusait, és szemlélteti, hogy az adatkezelés a kiberrezilienciáról szóló rendelet értelmében távoli adatkezelési megoldásnak minősül-e.

8.3.1. *Mobilbanki alkalmazás*

Egy pénzügyi szervezet mobilbanki alkalmazást hoz forgalomba. Az alkalmazás háttérrendszerei támogatják többek között a hitelesítést, az engedélyezést, a számlakezelést és a kifizetéseket. A pénzügyi szervezet az alkalmazás funkcióinak támogatására hibrid stratégiát alkalmaz, amely a házon belüli infrastruktúrára és harmadik felek által nyújtott távoli megoldásokra támaszkodik. Ezek a következők:

A pénzügyi szervezet által kifejlesztett, saját tárhelyen működtetett infrastruktúra:

— Az ügyfél megnyitja a mobil banki alkalmazást, amely az ügyfelet a banki interfészen keresztül hitelesíti. Ez a pénzügyi szervezet által kifejlesztett és annak saját tárhelyén működtetett megoldás, amely fogadja az alkalmazás kéréseit, és ezeknek megfelelő válaszokat ad vissza. A banki interfész a számlakezelő rendszer lekérdezésével ellenőrzi az ügyfél személyazonosságát, és hozzáférést biztosít az alkalmazáshoz.

— Az ügyfél az alkalmazáson keresztül átutalást kezdeményez. Az alkalmazás továbbítja a megbízást a banki interfésznek, amely ennek megfelelő kérést nyújt be a könyvelési rendszerhez.

— A saját tárhelyen működtetett, de a banki interfésztől logikailag elkülönített számlakezelési rendszer és könyvelési rendszer rögzíti a tranzakciót.

— A könyvelési rendszer visszaadja a tranzakció státuszát a banki interfésznek, amely megjeleníti az eredményt az ügyfélnek.

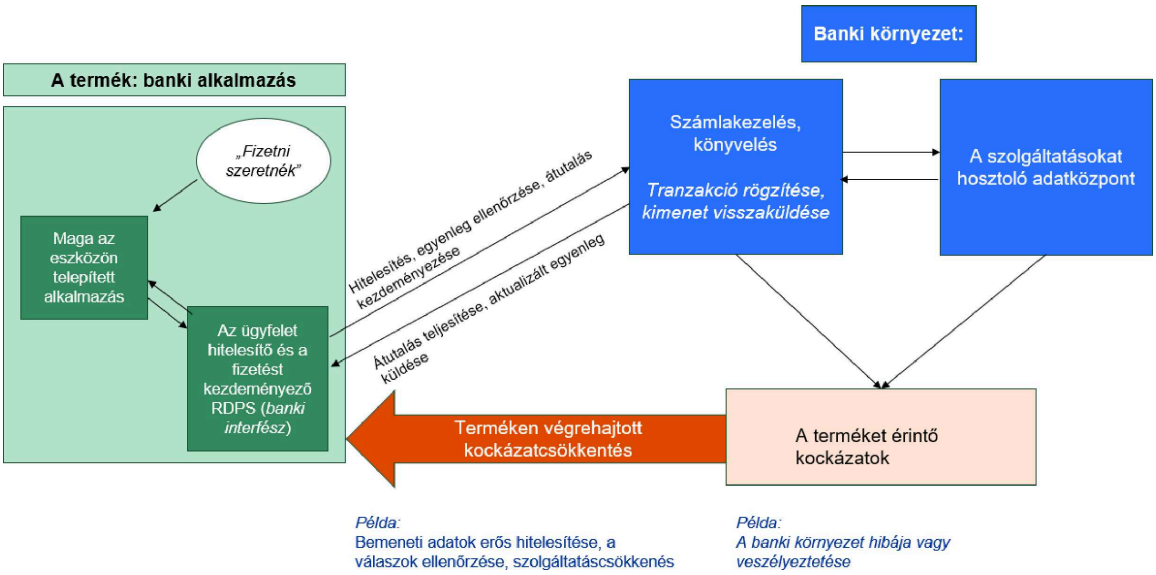
A távoli adatkezelési megoldásokat érintő szempontok:

— A banki interfész szükséges ahhoz, hogy az alkalmazás el tudja látni a funkcióit, nevezetesen az ügyfél hitelesítését, az ügyfél megbízásainak – többek között a fizetési és átutalási megbízások – benyújtását, valamint az eredménystátusz visszaküldését. A banki interfész tervezése és fejlesztése a gyártó felelőssége mellett történik. Mivel a fenti szakaszokban ismertetett mindkét kérdésre adott válasz igenlő, a banki interfészt távoli adatkezelési megoldásnak kell tekinteni. Ennek megfelelően figyelembe kell venni a kiberbiztonsági kockázatértékelésben, valamint a digitális elemeket tartalmazó termék egészére vonatkozó alapvető követelmények érvényesítésében. A benyújtott megbízás későbbi feldolgozását, különösen a tranzakciónak a számlakezelési és könyvelési rendszerekben történő rögzítését, valamint kiegyenlítését és elszámolását olyan rendszerek végzik, amelyekkel az alkalmazás nem áll közvetlen kapcsolatban, ennélfogva nem minősül távoli adatkezelési megoldásnak.

— A számlakezelési rendszer és a könyvelési rendszer a banki alkalmazás tekintetében nem minősül távoli adatkezelési megoldásnak. Az alkalmazás nem áll közvetlen kapcsolatban velük (a banki felülettel lép interakcióba, amely viszont ezekre támaszkodik). Bár ezek rendelkezésre állása szükséges lehet egy funkció elvégzéséhez, a kiberrezilienciáról szóló rendelet hatálya csak a rendszer azon részeire terjed ki, amelyek közvetlenül érintkeznek a digitális elemeket tartalmazó termékkel. Ezért a kiberrezilienciáról szóló rendelet alkalmazásában nem tartoznak a távoli adatkezelési megoldás fogalommeghatározása alá. Ezek a rendszerek azonban továbbra is külső függőségek, amelyek jelentős kiberbiztonsági kockázatokat idézhetnek elő a digitális elemeket tartalmazó termék tekintetében. A könyvelési rendszer feltörése például lehetővé teheti a támadó számára, hogy befolyásolja tranzakciónak az alkalmazásban később megjelenő eredményeit. A gyártónak ezért a kiberbiztonsági kockázatértékelés részeként azonosítania és értékelnie kell ezeket a kockázatokat, és azokat olyan termékszintű intézkedésekkel kell csökkentenie, mint a back-end interfészek erős hitelesítése, a tranzakciós adatok integritásának védelme, a biztonságos kommunikációs csatornák és az alkalmazás által kapott válaszok ellenőrzése.

10. ábra:

Egy távoli adatkezelési megoldáson alapuló banki alkalmazás stilizált ábrázolása



Harmadik fél által nyújtott SaaS ügyfélszolgálati célokra:

— A pénzügyi szervezet egy harmadik félnek minősülő szolgáltató által kifejlesztett és működtetett ügyfélszolgálati csevegőmegoldást integrál az alkalmazásába; a harmadik félnek minősülő szolgáltató megírta a csevegési szolgáltatás szerverkódját, létrehozta a felhasználói felületet, és működteti azt az infrastruktúrát, ahol a csevegőt telepítik (SaaS-modell).

— Amikor az ügyfél támogatási kérést nyújt be, az alkalmazás csevegési munkamenet létrehozása és az üzenetfolyam kezelése érdekében összekapcsolja az ügyfelet a harmadik fél szolgáltatásával, anélkül, hogy hozzáférést biztosítana a harmadik fél számára az alapvető banki rendszerekhez.

A távoli adatkezelési megoldásokat érintő szempontok:

— A támogató csevegési megoldás szükséges ahhoz, hogy a digitális elemeket tartalmazó termék ellássa valamely funkcióját, de azt nem a pénzügyi szervezet tervezte és fejlesztette ki, vagy nem a pénzügyi szervezet felelőssége mellett tervezték és fejlesztették ki; ennélfogva nem minősül távoli adatkezelési megoldásnak. Ugyanakkor harmadik fél által biztosított alkotóelemként kell kezelni. Az e harmadik fél által nyújtott szolgáltatás igénybevétele kiberbiztonsági kockázatot jelenthet a banki alkalmazás számára: például a támadó a csevegőcsatornát arra használhatja, hogy megszemélyesítse a bankot, vagy rosszindulatú tartalmakat továbbítson a felhasználóknak. A pénzügyi szervezetnek figyelembe kell vennie ezeket a kockázatokat kiberbiztonsági kockázatértékelése során, és azokat olyan termékszintű intézkedésekkel kell csökkentenie, mint például a csevegési funkció elkülönítése az alapvető banki jellemzőktől, az adatáramlások ellenőrzése és a tartalom validálása. A SaaS tekintetében is kellő gondossággal kell eljárni.

8.3.2. *Intelligens termosztát*

Az intelligens termosztát lehetővé teszi a felhasználók számára, hogy mobilalkalmazáson keresztül szabályozzák otthonuk hőmérsékletét. A mobilalkalmazás és az intelligens termosztát távoli adatkezelésre támaszkodik az adatcsere (pl. a hőmérséklet növelésére irányuló kérés) és az adatok tárolása (pl. felhasználói preferenciák) során. Ezeket a funkciókat a gyártó felelőssége mellett fejlesztették ki és tervezték meg, de egy harmadik fél által biztosított mögöttes fizikai és virtuális infrastruktúrán futnak (harmadik fél által biztosított IaaS).

Mivel az intelligens termosztát e távoli adatkezelés nélkül nem tudná ellátni intelligens funkcióit, ennek hiánya megakadályozná a digitális elemeket tartalmazó terméket egy vagy több funkciójának ellátásában. Ezenkívül a szoftvert az intelligens termosztát gyártójának felelőssége mellett fejlesztették ki és tervezték meg. Ezért a távoli adatkezelés a kiberrezilienciáról szóló rendelet meghatározása szerinti távoli adatkezelési megoldásnak minősül.

A kiberrezilienciáról szóló rendeletnek való megfelelés céljából az intelligens termosztát gyártójának dokumentálnia kell a távoli adatkezelési megoldást, valamint a digitális elemeket tartalmazó termék műszaki dokumentációjában a harmadik fél által biztosított IaaS igénybevételét, beleértve a szerződéses szolgáltatás részleteit is. A gyártónak figyelembe kell vennie ezeket az elemeket a kockázatértékelésben, amely magában foglalja a digitális elemeket tartalmazó termék rendeltetését és észszerűen előrelátható használatát. A gyártó a kiberrezilienciáról szóló rendelet alapvető követelményeit a távoli adatkezelési megoldással kapcsolatos kockázatok alapján hajtja végre. A harmadik fél által biztosított IaaS esetében a gyártónak gondoskodnia kell arról, hogy a harmadik félnek minősülő szolgáltató által nyújtott biztonsági intézkedések megfelelőek legyenek, és/vagy magának kell meghoznia az infrastruktúrával kapcsolatos megfelelő intézkedéseket. Az előbbi esetében a gyártó például kérheti annak igazolását, hogy a NIS 2 szerinti kötelezettségek teljesültek.

8.3.3. *E-olvasó*

Egy e-olvasó szoftver gyártója harmadik fél által nyújtott SaaS tárolási szolgáltatást használ az ügyfelek által vásárolt elektronikus könyvek tárolására és a könyveikhez való hozzáférés biztosítására. E tárolási szolgáltatás hiánya megakadályozná a digitális elemeket tartalmazó termék valamely funkciójának ellátását, de a harmadik fél által nyújtott SaaS tárolási szolgáltatást nem a gyártó fejleszti vagy nem a gyártó felelősség mellett fejlesztik; a SaaS-szolgáltató minden felhasználási esetben elérhetővé teszi azt az ügyfelek számára.

A SaaS tárolási szolgáltatás nem felel meg a távoli adatkezelési megoldás fogalommeghatározásának. Az e-olvasó gyártója azonban a digitális elemeket tartalmazó terméke működéséhez erre a külső szolgáltatásra támaszkodik, ezért kiberbiztonsági kockázatértékelése során figyelembe kell vennie a kapcsolódó kockázatokat. Az e-olvasó gyártójának a SaaS-t alkotóelemként kell kezelnie. A gyártónak megfelelő termékszintű biztonsági intézkedéseket kell végrehajtania, többek között biztonságos hitelesítést, titkosítást és a tárolási szolgáltatással folytatott kommunikáció integritásának védelmét. A SaaS-szolgáltató kiválasztása és integrálása során gyakorolt kellő gondosság a gyártót az azzal kapcsolatos kötelezettségei tekintetében is támogatni fogja, hogy a digitális elemeket tartalmazó termék egésze megfeleljen az alapvető követelményeknek.

8.3.4. *Ipari robot*

Egy ipari robot feladata, hogy alkatrészeket vegyen fel. A robot a kamerákon keresztül gyűjtött információkat a gyártó által tervezett és kifejlesztett távoli szolgáltatásra küldi. A szolgáltatás egy harmadik fél által biztosított mögöttes fizikai és virtuális infrastruktúrán fut (harmadik fél által biztosított IaaS). A felhőalapú szolgáltatás a kamerajel alapján kiszámítja az alkatrészek helyzetét, és parancsokat küld vissza a robotnak, hogy vegye fel azokat.

Ezen adatkezelés hiánya megakadályozná az ipari robotot abban, hogy alkatrészeket vegyen fel, és ezáltal ellássa egyik funkcióját. Ezenkívül az infrastruktúrán futó szoftvert a gyártó tervezte és fejlesztette ki. A gyártó által tervezett és kifejlesztett szoftver megfelel a távoli adatkezelési megoldás fogalommeghatározásának.

Az ipari robot gyártójának dokumentálnia kell a távoli adatkezelési megoldást, valamint a digitális elemeket tartalmazó termék műszaki dokumentációjában a harmadik fél által biztosított IaaS igénybevételét, beleértve a szerződéses szolgáltatás részleteit is. A gyártónak ezeket az elemeket is figyelembe kell vennie a kockázatértékelésben, amely a digitális elemeket tartalmazó termék rendeltetésére és észszerűen előrelátható használatára is kiterjed. A gyártó a kockázatok alapján végrehajtja a kiberrezilienciáról szóló rendeletnek a digitális elemeket tartalmazó termékre – többek között annak távoli adatkezelési megoldásaira – vonatkozó alapvető követelményeit. Az IaaS-szolgáltató kiválasztása során gyakorolt kellő gondosság a gyártót a kötelezettségei tekintetében is támogatni fogja. A gyártó például kérheti annak igazolását, hogy a NIS 2 szerinti kötelezettségek teljesültek.

8.3.5. *Mobilhálózat*

Az okostelefon 5G hálózaton keresztül biztosít internetkapcsolatot, telefonhívást és üzenetküldést a felhasználók számára (mobil kapcsolat). A mobilhálózatot távközlési szolgáltatók tervezik meg és fejlesztik ki. A hálózat kiscellákból és bázisállomásokból, valamint egyéb hálózati berendezésekből áll.

A digitális elemeket tartalmazó terméknek képesnek kell lennie arra, hogy megfelelően kapcsolódjon a hálózathoz; ez az egyik funkciója. Az azonban, hogy ez a hálózat működik-e vagy sem, nem releváns annak megállapítása szempontjából, hogy a digitális elemeket tartalmazó termék megfelelően működik-e. A hálózat csak kommunikációs csatorna, és nem szükséges ahhoz, hogy a digitális elemeket tartalmazó termék ellássa a „hálózathoz való megfelelő csatlakozás” funkcióját. Ugyanígy az Ethernet kábel, az útvonalválasztó vagy a wifijel a kommunikációt vagy összeköttetést lehetővé tevő eszköz, és nem minősül olyan adatkezelésnek, amelynek hiánya megakadályozná a digitális elemeket tartalmazó terméket valamely funkciójának ellátásában.

Következésképpen a mobilhálózat nem felel meg a távoli adatkezelési megoldás fogalommeghatározásának. A hálózat nem tekintendő harmadik fél által biztosított alkotóelemnek, mivel a digitális elemeket tartalmazó termékbe nem integrálnak szoftvert, a termék csupán igénybe veszi a hálózatot. Ezért nem szükséges, hogy a gyártó kellő gondosságra vonatkozó kötelezettségeket teljesítsen a hálózatszolgáltatóval szemben.

9. **TOVÁBBI ELEMEK**

9.1. **Jelentéstételi kötelezettségek**

209. A kiberrezilienciáról szóló rendelet 14. cikkének (1) és (3) bekezdése értelmében a gyártónak egyidejűleg be kell jelentenie a koordinátorként kijelölt CSIRT-nek és az ENISA-nak i. a digitális elemeket tartalmazó termékében található, aktívan kihasznált sérülékenységeket, amelyről tudomást szerez, és ii. minden olyan súlyos incidenst, amely hatással van a digitális elemeket tartalmazó termék biztonságára, és amelyről tudomást szerez.

210. A 69. cikk (3) bekezdésével és a 71. cikk (2) bekezdésének második mondatával összhangban a 14. cikknek való megfelelés kötelezettsége 2026. szeptember 11-től alkalmazandó a kiberrezilienciáról szóló rendelet hatálya alá tartozó, digitális elemeket tartalmazó valamennyi termékre, beleértve a 2027. december 11. előtt forgalomba hozott, digitális elemeket tartalmazó termékeket is. Továbbá a sérülékenységek kezelésére vonatkozó kötelezettségektől eltérően, amelyek csak a termék támogatási időszakának hosszára vonatkoznak, a jelentéstételi kötelezettségek a digitális elemeket tartalmazó termék támogatásának megszűnését követően is alkalmazandók. Ha a digitális elemeket tartalmazó terméket 2027. december 11. előtt hozták forgalomba, vagy ha támogatási időszaka lejárt, a gyártónak nem kell megfelelnie az I. melléklet II. részében meghatározott sérülékenységkezelési kötelezettségeknek.

211. Emlékeztetni kell arra, hogy az ilyen események bejelentésére vonatkozó kötelezettség akkor alkalmazandó, ha a gyártó tudomást szerez arról, hogy a sérülékenységet aktívan kihasználják, vagy hogy súlyos incidens következett be, és az a digitális elemeket tartalmazó terméke biztonságának veszélyeztetéséhez vezetett. Ezért az arra vonatkozó iránymutatás, hogy a gyártó tudomásszerzése mely időpontban vélelmezendő, bizonyára segíti a gyártókat annak meghatározásában, hogy az alkalmazandó bejelentési határidőket mikortól kell számítani.

212. A gyártókra különböző uniós jogi aktusok alapján hasonló jelentéstételi kötelezettségek vonatkozhatnak. A „tudomásszerzés” fogalmának következetes értelmezése és a gyártók e kötelezettségeknek való könnyebb megfelelése érdekében ez az iránymutatás összhangban van az (EU) 2024/2690 bizottsági végrehajtási rendelet (31) preambulumbekezdésével és az adatvédelmi incidensek általános adatvédelmi rendelet szerinti bejelentéséről szóló 9/2022. sz. iránymutatás II. szakaszának A. pontjával.

213. Egyes esetekben a gyártó észlel gyanús eseményt, vagy egy harmadik fél – magánszemély, ügyfél, szervezet, hatóság, médiaszervezet vagy más forrás – hívja fel a figyelmét egy potenciális incidensre vagy sérülékenységre. Ilyenkor a gyártónak haladéktalanul értékelnie kell a gyanús eseményt annak megállapítása érdekében, hogy az aktívan kihasznált sérülékenységnek vagy a digitális elemeket tartalmazó termék biztonságát érintő súlyos incidensnek minősül-e. Ezért a gyártó tudomásszerzését vélelmezni kell, ha egy ilyen kezdeti értékelést követően észszerű mértékű bizonyossággal rendelkezik arról, hogy i. aktívan kihasználják a digitális elemeket tartalmazó termékében található sérülékenységet, vagy ii. súlyos incidens következett be, amely a digitális elemeket tartalmazó terméke biztonságának veszélyeztetéséhez vezetett.

214. Ezért az az időpont, amikor a gyártó tudomásszerzése vélelmezhető, az adott aktívan kihasznált sérülékenység vagy súlyos incidens körülményeitől függ. Egyes esetekben kezdettől fogva viszonylag egyértelmű, hogy a sérülékenységet aktívan kihasználják, vagy hogy egy súlyos incidens hatással van a digitális elemeket tartalmazó termék biztonságára. Más esetekben időbe telhet annak megállapítása, hogy a digitális elemeket tartalmazó terméket érint-e sérülékenység, és hogy a sérülékenységet rosszindulatú szereplő kihasználja-e, vagy hogy egy incidens hatással van-e a digitális elemeket tartalmazó termék biztonságára. A hangsúlyt azonban az annak megállapítására irányuló kezdeti értékelés azonnali elvégzésére kell helyezni, hogy ezek a feltételek valóban teljesülnek-e, különösen akkor, ha a sérülékenység jelentős kockázatot hordozhat, és ha teljesülnek, a kiberrezilienciáról szóló rendeletnek megfelelően korrekciós intézkedéseket kell hozni és bejelentést kell tenni.

215. Ezenkívül a jelentéstételi kötelezettségek szerkezete megköveteli a gyártóktól, hogy bejelentéseiket a belső vizsgálataik előrehaladásának, valamint az aktívan kihasznált sérülékenység vagy az incidens behatóbb megismerésének megfelelően fokozatosan frissítsék. A gyártóknak indokolatlan késedelem nélkül, de legkésőbb a tudomásszerzéstől számított 24 órán belül korlátozott információtartalmú korai figyelmeztető bejelentést kell tenniük. Ezt követően további információkat kell közölni indokolatlan késedelem nélkül, de legkésőbb a tudomásszerzéstől számított 72 órán belül benyújtandó bejelentés részeként („72 órás bejelentés”). A teljes jelentést az aktívan kihasznált sérülékenységek esetében a korrekciós vagy kockázatcsökkentő intézkedés rendelkezésre állását követő 14 napon belül, súlyos incidensek esetében pedig a 72 órás bejelentést követő egy hónapon belül kell benyújtani.

216. Amint arra a *3.3.1.* szakasz (*Sustained support and ensuring viability of FOSS*) is emlékeztet, a nyílt forráskódú szoftverek támogatóinak a 24. cikk (3) bekezdésével összhangban jelenteniük kell az aktívan kihasznált sérülékenységeket is ([30]). Ez a kötelezettség akkor alkalmazandó, amikor tudomást szereznek egy aktívan kihasznált sérülékenységről, és nem csak akkor, ha sérülékenység áll fenn egy olyan szabad és nyílt forráskódú szoftver kódbázisában, amelynek az adott szervezet a támogatója. A gyakorlatban, mivel a szabad és nyílt forráskódú szoftver-alkotóelemeket a downstream szereplők jellemzően integrálják más, digitális elemeket tartalmazó termékekbe, a támogató az aktív kihasználásról valószínűleg harmadik felek jelentései révén szerez tudomást, amelyek a digitális elemeket tartalmazó más termékekbe integrált szabad és nyílt forráskódú szoftver-alkotóelemek kihasználását azonosítják. Ilyen helyzet adódhat például akkor, amikor a digitális elemeket tartalmazó termék gyártója észleli a saját termékébe integrált szabad és nyílt forráskódú szoftver-alkotóelem aktív kihasználását, és azt jelenti az adott alkotóelem támogatójának; vagy amikor a felhasználó vagy a biztonsági kutató bizonyítékot talál a digitális elemeket tartalmazó termékbe integrált szabad és nyílt forráskódú szoftver-alkotóelem kihasználására, és ezt az aktív kihasználást jelenti az alkotóelem támogatójának.

217. Azt is egyértelművé kell tenni, hogy mivel az aktívan kihasznált sérülékenységek bejelentésére vonatkozó kötelezettség akkor alkalmazandó, amikor a gyártó tudomást szerez az aktív kihasználásról, a gyártó nem köteles bejelenteni azokat a sérülékenységeket, amelyek aktív kihasználásáról már 2026. szeptember 11. (a jelentéstételi kötelezettség alkalmazásának kezdőnapja) előtt tudomást szerzett. A kiberrezilienciáról szóló rendelet ezért nem írja elő az ilyen sérülékenységek visszamenőleges bejelentését. Ezzel szemben fennáll a kötelezettség akkor, ha a gyártónak 2026. szeptember 11. előtt tudomása volt a sérülékenységről, de abban az időpontban nem volt tudomása annak aktív kihasználásáról (akár azért, mert még nem történt ilyen, akár azért, mert a gyártó arról nem szerzett tudomást). Ha később, 2026. szeptember 11. után aktív kihasználásra kerül sor, vagy a gyártó arról tudomást szerez, a sérülékenység a jelentéstételi kötelezettség hatálya alá tartozó, aktívan kihasznált sérülékenységnek minősül.

218. Ugyanígy a gyártónak csak a digitális elemeket tartalmazó termékében található, aktívan kihasznált sérülékenységeket kell bejelentenie. Ha a digitális elemeket tartalmazó termék harmadik fél által biztosított alkotóelemből eredő, aktívan kihasznált sérülékenységet tartalmaz, a digitális elemeket tartalmazó termék gyártója köteles bejelenteni ezt az aktívan kihasznált sérülékenységet. Ha azonban a gyártó tudatában van annak, hogy egy harmadik fél által biztosított alkotóelem sérülékenységet tartalmaz, de i. a sérülékenység nem használható ki a digitális elemeket tartalmazó termékében (pl. mert a sérülékeny kód nem érhető el), vagy ii. a sérülékenységet nem használták ki a digitális elemeket tartalmazó termékében, akkor a sérülékenység nem minősül a digitális elemeket tartalmazó termékében található, aktívan kihasznált sérülékenységnek, ennélfogva nem tartozik az adott gyártóra vonatkozó kötelező jelentéstétel hatálya alá. Az említett gyártó a kiberrezilienciáról szóló rendelet 15. cikkével összhangban önkéntes alapon továbbra is bejelentheti ezt a sérülékenységet. Meg kell felelnie továbbá a kiberrezilienciáról szóló rendelet I. mellékletének II. részében foglalt sérülékenységkezelési követelményeknek, valamint a 13. cikk (6) bekezdésével összhangban és a *9.2.1.* szakaszban (*Reporting upstream and sharing security fixes*) részletesebben kifejtettek szerint jelentenie kell a sérülékenységet az alkotóelemet gyártó vagy karbantartó személynek vagy szervezetnek.

([30]) Amennyiben a támogató részt vesz a digitális elemeket tartalmazó termék fejlesztésében.

219. Miután tudomást szereztek egy aktívan kihasznált sérülékenységről vagy súlyos incidensről, a gyártók a 14. cikk (8) bekezdésével összhangban kötelesek tájékoztatni az érintett felhasználókat és adott esetben valamennyi felhasználót. Amennyiben ezt nem teszik meg időben, a bejelentést fogadó CSIRT-ek átadhatják ezeket az információkat a felhasználóknak, ha ez arányosnak és szükségesnek tekinthető az adott sérülékenység vagy incidens hatásának megelőzéséhez vagy csökkentéséhez.

220. A kiberrezilienciáról szóló rendelet kockázatalapú megközelítésével összhangban a 14. cikk (8) bekezdésében meghatározott, a felhasználók tájékoztatására vonatkozó kötelezettséget kockázatalapú és arányos módon kell alkalmazni. Különösen az aktívan kihasznált sérülékenységre vagy súlyos incidensre vonatkozó információszolgáltatás nem jelenti azt, hogy az ilyen információt megkülönböztetés nélkül nyilvánosságra kell hozni. Adott esetben, valamint a digitális elemeket tartalmazó termék jellegére, az érintett felhasználókra és a sérülékenység vagy az incidens esemény lehetséges hatására tekintettel a gyártók az érintett felhasználókra vagy ügyfelekre korlátozhatják a részletes információk nyilvánosságra hozatalát. Ez különösen igaz az érzékeny vagy alapvető környezetben használt, digitális elemeket tartalmazó termékekre, ahol a műszaki részletek nyilvánosságra hozatala önmagában növelheti a kiberbiztonsági kockázatokat vagy megkönnyítheti a további kihasználást.

221. A sérülékenység megfelelő kezelését vagy csökkentését követően helyénvaló lehet a szélesebb körű nyilvánosságra hozatal. Erről van szó például akkor, ha a nyilvánosságra hozatal hozzájárul az általános tudatosság növeléséhez, vagy lehetővé teszi a felhasználók számára annak ellenőrzését, hogy a digitális elemeket tartalmazó termékeik már nem érintettek. Ilyenkor a szélesebb körű nyilvánosságra hozatal részletességének és időzítésének arányosnak kell maradnia, és figyelembe kell vennie a hasznosítás fennmaradó kockázatait, a digitális elemeket tartalmazó termék jellegét és az érintett felhasználók érdekeit. Ezenkívül az I. melléklet II. részének 4. pontja előírja a gyártók számára, hogy a biztonsági frissítés rendelkezésre bocsátását követően hozzák nyilvánosságra a kijavított sérülékenységekre vonatkozó információkat.

9.2. **Sérülékenységek kezelése**

9.2.1. *Upstream jelentéstétel és a biztonsági javítások megosztása*

222. A kiberrezilienciáról szóló rendelet 13. cikkének (6) bekezdése előírja a gyártók számára, hogy jelentsék az integrált alkotóelemek sérülékenységeit az adott alkotóelemet gyártó vagy karbantartó személynek vagy szervezetnek (a továbbiakban: upstream jelentéstétel).

223. A gyártóknak csak az általuk integrált alkotóelem verziója tekintetében kell upstream jelentést tenniük. Amennyiben az alkotóelemet gyártó vagy karbantartó személy vagy szervezet biztonsági szabályzatokat, összehangolt sérülékenységfeltárási eljárásokat vagy a sérülékenységek bejelentésére kijelölt csatornákat alakított ki, a gyártóknak ezekkel összhangban kell jelentést tenniük, különösen akkor, ha a kijavítatlan sérülékenységek idő előtti nyilvánosságra hozatala növelheti a kiberbiztonsági kockázatokat. Ezenkívül az upstream karbantartók terheinek csökkentése érdekében, különösen a nyílt forráskódú projektek esetében, a gyártók nem kötelesek upstream irányban jelentést tenni, ha meg tudják erősíteni, hogy az alkotóelemet gyártó vagy karbantartó személy vagy szervezet tudatában van a sérülékenység fennállásának. A gyártóknak ajánlott észszerű lépéseket tenniük a párhuzamos jelentések benyújtásának elkerülése érdekében, például azáltal, hogy az upstream irányú jelentéstétel előtt ellenőrzik a nyilvánosan hozzáférhető sérülékenységi adatbázisokat, a projektspecifikus biztonsági tanácsokat vagy a meglévő problémakövető rendszereket.

224. A gyártóknak csak azokról a sérülékenységekről kell upstream jelentést tenniük, amelyek magában az integrált alkotóelemben állnak fenn, azokról a sérülékenységekről azonban nem, amelyek az alkotóelemnek a gyártó által kifejlesztett más kódba való integrálásából vagy más alkotóelemek integrálásából erednek. Mindazonáltal előfordulhatnak olyan helyzetek, amikor valamely alkotóelemnek egy digitális elemeket tartalmazó konkrét termékbe történő integrálása az adott alkotóelem olyan viselkedési formáit, interakcióit vagy biztonsági szempontból releváns jellemzőit fedi fel, amelyek önmagukban nem voltak nyilvánvalóak vagy nem voltak könnyen azonosíthatók. Ilyenkor ajánlott, hogy a gyártók közöljék ezeket az információkat az alkotóelemet gyártó vagy karbantartó személlyel vagy szervezettel a sérülékenység kezelésére irányuló helyes gyakorlatok előmozdítása érdekében, amelyek célja a hatékony helyreállítás megkönnyítése és az alkotóelem-ökoszisztéma általános biztonságának javítása.

225. Végezetül a gyártók nem kötelesek a sérülékenység upstream jelentésére, ha az alkotóelem már nem rendelkezik karbantartóval, vagy ha a gyártó az új verziók vagy biztonsági javítások tekintetében már nem az eredeti karbantartót veszi igénybe. Ilyenkor mindazonáltal ajánlott, hogy a gyártó észszerű alternatív intézkedésekkel tájékoztassa az adott alkotóelem felhasználóit, például a meglévő közösségi mechanizmusokon (levelezőlistákon, jegykezelőkön) vagy a nyilvános sérülékenységi nyilvántartásokon keresztül.

226. Ezenkívül a 13. cikk (6) bekezdése értelmében azok a gyártók, amelyek egy integrált alkotóelem sérülékenységének kezelése érdekében szoftvermódosítást fejlesztettek ki, kötelesek megosztani ezt a szoftvermódosítást (a továbbiakban: biztonsági javítás) az alkotóelemet gyártó vagy karbantartó személlyel vagy szervezettel (a továbbiakban: upstream megosztás).

227. Amennyiben a gyártóknak a 13. cikk (6) bekezdése értelmében biztonsági javítást kell megosztaniuk, a javítást adott esetben géppel olvasható formátumban, az alkotóelemet gyártó vagy karbantartó személy vagy szervezet által könnyen ellenőrizhető és adott esetben integrálható módon kell biztosítani. Szabad és nyílt forráskódú alkotóelem esetén a biztonsági javítást az adott alkotóelem licencével összeegyeztethető módon kell megosztani, például úgy, hogy azt ugyanazon licenc vagy olyan licenc alapján osztják meg, amely lehetővé teszi a karbantartó számára, hogy a javítást saját licence alapján terjessze. Amennyiben az adott alkotóelem karbantartója rendelkezik iránymutatásokkal arra vonatkozóan, hogy a biztonsági javításokat hogyan kell megosztani, a gyártónak követnie kell ezeket az iránymutatásokat.

228. A kiberrezilienciáról szóló rendelet azonban nem írja elő a gyártók számára annak biztosítását, hogy biztonsági javításaikat az alkotóelemet gyártó vagy karbantartó személy vagy szervezet szükségszerűen elfogadja. Azt sem kötelesek biztosítani, hogy ezek a javítások szükségszerűen integrálódjanak az alkotóelem kódtárába, például abban az esetben, ha a karbantartó esetleg más megoldást részesít előnyben a probléma megoldására. Ugyanígy a gyártók nem kötelesek elfogadni az alkotóelem karbantartója által kidolgozott javasolt javítást, és előnyben részesíthetik a probléma más megfelelő módon történő mérséklését.

229. Egyes esetekben előfordulhat, hogy az alkotóelemet gyártó vagy karbantartó személy vagy szervezet már biztosított biztonsági javítást a sérülékenység kezelésére, de a gyártó eltérő kockázatcsökkentési stratégiát hajt végre (például egy másik konfiguráció megváltoztatásával). Ilyenkor a kiberrezilienciáról szóló rendelet nem írja elő a gyártó számára a rendszer egy másik részét érintő módosítás upstream megosztását. Ilyenkor mindazonáltal ajánlott, hogy a gyártó így járjon el, ha ezzel támogatni tudja az alkotóelemet karbantartó személyt vagy szervezetet.

9.2.2. *Ismert kihasználható sérülékenységek*

230. A kiberrezilienciáról szóló rendelet I. melléklete I. részének egyik alapvető követelménye előírja, hogy a 13. cikk (2) bekezdésében említett kiberbiztonsági kockázatértékelés alapján és adott esetben a digitális elemeket tartalmazó termékeket ismert kihasználható sérülékenységek nélkül kell forgalmazni.

231. A 3. cikk 41. pontjában foglalt fogalommeghatározás szerint a kihasználható sérülékenység „olyan sérülékenység, amelyet valamely ellenséges fél a gyakorlati működési feltételek mellett potenciálisan ténylegesen kihasználhat”. Gyakorlati működési feltételek mellett nem minden sérülékenység használható ki, és egyes sérülékenységek csak elméleti feltételek mellett (pl. laboratóriumban vagy szimulációban) és/vagy nem olyan feltételek mellett használhatók ki, amelyek a digitális elemeket tartalmazó termék működési környezetében merülnének fel.

232. A kiberrezilienciáról szóló rendelet előírja a gyártók számára, hogy megfelelő szabályzatokkal és eljárásokkal rendelkezzenek a belső vagy külső forrásokból bejelentett potenciális sérülékenységek kezelésére és orvoslására (13. cikk (8) bekezdés). Nem határozza meg azonban kifejezetten, hogy a kihasználható sérülékenységet mikor kell a gyártó által ismertnek tekinteni, ami azt a kötelezettséget vonja maga után, hogy a forgalomba hozatal időpontjában meg kell felelni ennek az alapvető követelménynek.

233. A sérülékenység akkor tekinthető ismertnek, ha szerepel a releváns, nyilvánosan hozzáférhető sérülékenységi adatbázisokban, például az (EU) 2022/2555 irányelv 12. cikkének (2) bekezdésével létrehozott európai sérülékenységi adatbázisban vagy más kiemelkedő sérülékenységi adatbázisokban.

234. Emellett egy sérülékenység ismert lehet akkor is, ha arról a gyártót nem nyilvános információk – például biztonsági kutató általi összehangolt közlés vagy a gyártó saját belső tesztelése és elemzése – révén tájékoztatták, többek között például mesterséges intelligencián alapuló szolgáltatások igénybevételekor. Ugyanígy egy sérülékenység ismert lehet akkor is, ha arról megbízható médiaorgánumok, többek között kiberbiztonsági szakkiadványok vagy az általános tömegkommunikációs eszközök nyilvánosan és kellő hangsúllyal beszámoltak.

235. Mindazonáltal egy sérülékenység bejelentése vagy észlelése önmagában nem jelenti azt, hogy az a gyakorlatban kihasználható vagy az érintett, digitális elemeket tartalmazó konkrét termékre alkalmazható. A gyártónak meg kell vizsgálnia azt, és meg kell erősítenie az ilyen értesülések helytállóságát és a digitális elemeket tartalmazó saját termék érintettségét. Ennek megfelelően bizonyos idő telhet el a sérülékenység első bejelentése és megerősítése között. A *9.1.* szakaszban (*Reporting obligations*) jelzett módon a hangsúlyt a gyors kivizsgálásra és reagálásra kell helyezni.

236. Ezenkívül a gyártók azon kötelezettsége, hogy megfeleljenek az I. melléklet I. részében meghatározott alapvető követelményeknek, a 13. cikk (1) bekezdésével összhangban a forgalomba hozatal időpontjában alkalmazandó. A gyakorlatban előfordulhat, hogy új, potenciálisan kihasználható sérülékenységeket a digitális elemeket tartalmazó termék fejlesztési életciklusának végső szakaszaiban, többek között röviddel az értékesítési láncba való belépés (így a forgalomba hozatal) előtt fedeznek fel.

237. Mivel a digitális elemeket tartalmazó termékek ismert kihasználható sérülékenységek nélküli forgalomba hozatalára vonatkozó kötelezettség kockázatalapú kötelezettség, a gyártó feladata annak meghatározása, hogy a kiberbiztonsági kockázatértékelés alapján a digitális elemeket tartalmazó termék a kiberrezilienciáról szóló rendeletnek megfelelően biztonságosan forgalomba hozható-e. Alternatív megoldásként a gyártó megállapíthatja, hogy a digitális elemeket tartalmazó termék forgalomba hozatala előtt egy esetlegesen ismertté vált új sérülékenységet ki kell javítani. E megállapítás során a gyártóknak figyelembe kell venniük a sérülékenység súlyosságát, kihasználhatóságát és lehetséges hatását, valamint a használatbavételt követően magával a digitális elemeket tartalmazó termékkel kapcsolatban felmerülő kockázatokat. Figyelembe vehetik annak kockázatait is, hogy a termék kiadását elhalasztják a sérülékenység megszüntetéséig, például azért, mert az új kiadás más kihasználható sérülékenységeket is kezel, vagy mert szükséges a kritikus fontosságú rendszerek folyamatos működésének biztosításához. Mindenesetre a digitális elemeket tartalmazó termék forgalomba hozatalát követően a gyártó továbbra is köteles hatékonyan és az I. melléklet II. részében meghatározott sérülékenységkezelési követelményekkel összhangban kezelni a sérülékenységeket.

9.2.3. *Hatékony és rendszeres tesztelés és felülvizsgálat*

238. Az I. melléklet II. részének 3. pontja előírja a gyártók számára, hogy a támogatási időszak alatt végezzék el a digitális elemeket tartalmazó termék biztonságának hatékony és rendszeres tesztelését és felülvizsgálatát. A rendszeres tesztelés nem ugyanazon tesztelési folyamat meghatározott időközönként történő mechanikus megismétlését követeli meg. Azt jelenti, hogy rendszeresen felül kell vizsgálni, hogy új inputok, például újonnan azonosított fenyegetések vagy újonnan felfedezett sérülékenységek szükségessé teszik-e a meglévő tesztek frissítését, és ennek megfelelően kell végrehajtani a teszteket.

239. A felülvizsgálat gyakoriságának, mélységének és tartalmának arányosnak kell lennie a digitális elemeket tartalmazó termék kiberbiztonsági kockázati profiljával, időbeli alakulásával és a fenyegetettségi helyzettel. Amennyiben a felülvizsgálat a tesztkészletet érintő releváns új inputot azonosít, új vagy módosított teszteket kell kidolgozni és végrehajtani a terméken annak biztosítása érdekében, hogy ne maradjanak kezeletlen sérülékenységek. Ez magában foglalhatja a meglévő tesztek újbóli elvégzését, ha a digitális elemeket tartalmazó termék módosítása indokolttá teszi az ilyen típusú tesztelést, például a regresszióvizsgálatot.

240. Amennyiben a felülvizsgálat nem állapít meg ilyen inputot, nem szükséges további teszteket kidolgozni. Ezzel párhuzamosan továbbra is alkalmazandók a sérülékenységek kezelésére vonatkozó egyéb kötelezettségek, beleértve a felmerülő kockázatokkal kapcsolatos sérülékenységek kezelésére és orvoslására vonatkozó kötelezettségeket is.

9.3. **Egyéb jogszabályokkal való kölcsönhatás**

9.3.1. *Az (EU) 2019/2144 rendelet és a 168/2013/EU rendelet*

241. A kiberrezilienciáról szóló rendelet 2. cikke (2) bekezdésének c) pontja megállapítja, hogy a rendelet nem alkalmazandó az (EU) 2019/2144 rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékekre. Az (EU) 2019/2144 rendelet „az (EU) 2018/858 rendelet 4. cikkében meghatározott, M, N és O kategóriájú járművekre, valamint az ilyen járművekhez tervezett és gyártott rendszerekre, alkotóelemekre és önálló műszaki egységekre” alkalmazandó.

242. Hasonlóképpen a 168/2013/EU rendelet hatálya alá tartozó, digitális elemeket tartalmazó termékeket az (EU) 2025/1535 felhatalmazáson alapuló bizottsági rendelet kizárta a kiberrezilienciáról szóló rendelet hatálya alól. A 168/2013/EU rendelet hatálya az L kategóriájú járművekre, továbbá „az ilyen járművekhez tervezett és gyártott rendszerekre, alkotóelemekre és önálló műszaki egységekre, valamint alkatrészekre és tartozékokra” terjed ki (2. cikk (1) bekezdés).

243. A kiberrezilienciáról szóló rendelet hatálya nem terjed ki az említett rendeletek hatálya alá tartozó járművekre. Ezenkívül további pontosításokra van szükség az ilyen járművekhez tervezett és gyártott azon rendszerekre, alkotóelemekre, önálló műszaki egységekre, alkatrészekre és tartozékokra (e szakasz alkalmazásában a továbbiakban: alkotóelemek) vonatkozó mentesség hatályát illetően, amelyek a kiberrezilienciáról szóló rendelet értelmében digitális elemeket tartalmazó termékeknek minősülnek.

244. Úgy tekinthető, hogy ezek az alkotóelemek nem tartoznak a kiberrezilienciáról szóló rendelet hatálya alá, feltéve, hogy azokat kizárólag az (EU) 2019/2144 és a 168/2013/EU rendelet hatálya alá tartozó járművekbe való integrálásra tervezték és gyártották. Ez attól függetlenül így van, hogy az alkotóelem gyártója közvetlenül a járműgyártónak vagy a gépjárműipari ellátási lánc egy másik gazdasági szereplőjének értékesíti-e azt, ha az alkotóelemet egyértelműen csak az említett járművekbe való végső integrálásra szánták, és csak arra alkalmasak.

245. Ezzel szemben a kiberrezilienciáról szóló rendelet hatálya alá tartozik az a gyártó, amely olyan, digitális elemeket tartalmazó generikus alkotóelemeket értékesít, amelyek különböző terméktípusokba – és nem kizárólag az említett rendeletek hatálya alá tartozó járművekbe – integrálhatók.

246. Annak értékelését, hogy valamely alkotóelem a kiberrezilienciáról szóló rendelet értelmében forgalomba hozottnak minősül-e, azon objektív feltételek alapján kell elvégezni, amelyek mellett azt forgalmazzák. Ha a gyártó a kizárólagosan az említett járművekbe való végső integrálás mellett más célra is alkalmas alkotóelemet kínál a gépjárműipari ellátási láncon kívüli vevők számára nyitva álló értékesítési csatornákon, például általános kiskereskedelmi egységeken vagy a nagyközönség megrendeléseit fogadó online értékesítési csatornákon keresztül, az alkotóelem a rendeltetésére vonatkozó állításoktól függetlenül a kiberrezilienciáról szóló rendelet hatálya alá tartozik. Ilyen körülmények között nem tekinthető úgy, hogy az alkotóelemet kizárólag az (EU) 2019/2144 és a 168/2013/EU rendelet hatálya alá tartozó járművekbe való integrálásra tervezték és gyártották, és a gyártónak meg kell felelnie a kiberrezilienciáról szóló rendeletnek. Ezzel szemben a korlátozott, vállalkozások közötti, a gépjárműipari ellátási láncra korlátozódó értékesítési csatornák használata arra utalhat, hogy azokat kizárólag ilyen integrációra tervezték és gyártották.

9.3.2. *Az EU-típusvizsgálati tanúsítványok érvényessége (69. cikk (1) bekezdés)*

247. A kiberrezilienciáról szóló rendelet 69. cikkének (1) bekezdése kimondja, hogy „[a]z e rendelettől eltérő uniós harmonizációs jogszabályok hatálya alá tartozó, digitális elemeket tartalmazó termékekre vonatkozó kiberbiztonsági követelmények tekintetében kiadott EU-típusvizsgálati tanúsítványok és jóváhagyó határozatok 2028. június 11-ig érvényesek maradnak, kivéve, ha az említett időpont előtt lejárnak, vagy ha az említett más uniós harmonizációs jogszabály másként rendelkezik, amely esetben az említett jogszabályban említett időpontig maradnak érvényesek”.

248. Az ilyen tanúsítványok és jóváhagyó határozatok folyamatos érvényességét úgy kell értelmezni, hogy az azokra a kiberbiztonsági kockázatokra és kapcsolódó követelményekre korlátozódik, amelyek a kiállításuk alapjául szolgáló uniós harmonizációs jogszabályok hatálya alá tartoznak. E kockázatok tekintetében a gyártóknak az általuk 2027. december 11-én vagy azt követően forgalomba hozni kívánt, digitális elemeket tartalmazó termékek esetében a 69. cikk (1) bekezdésében említett érvényességi idő alatt és 2028. június 11-ig nem kell újraértékelniük vagy újból igazolniuk a megfelelést kizárólag a kiberrezilienciáról szóló rendelet alkalmazásában ([31]). Ez a helyzet a kiadott tanúsítványok és jóváhagyó határozatok esetében, ha az alkalmazandó uniós harmonizációs jogszabályok előírják a gyártó számára, hogy a megfelelőségértékelési eljárást egy bejelentett szervezeten keresztül végezze el, valamint ha a gyártó ezt önkéntesen választotta.

249. Ennek megfelelően az egyéb uniós harmonizációs jogszabályok szerinti érvényes tanúsítvány vagy jóváhagyó határozat megléte nem mentesíti a gyártókat a kiberrezilienciáról szóló rendelet szerinti átfogó kiberbiztonsági kockázatértékelés elvégzése (vagy az abban foglalt egyéb kötelezettségek) alól. Azt teszi lehetővé a számukra, hogy megfelelőségértékelési eljárásuk során a megfelelést alátámasztó bizonyítékként használják fel a meglévő tanúsítványokat, amennyiben azok a kapcsolódó kiberbiztonsági kockázatokra már kiterjednek. Ha a tanúsítvány vagy a jóváhagyó határozat más uniós harmonizációs jogszabályok értelmében 2028. június 11. után is érvényes, a gyártó a kiberrezilienciáról szóló rendelet alkalmazásában csak 2028. június 11-ig támaszkodhat az ilyen tanúsítványra vagy határozatra.

250. Ha a 13. cikk (2) bekezdésével összhangban elvégzett kiberbiztonsági kockázatértékelés olyan további kockázatokat azonosít, amelyekre a meglévő tanúsítványt vagy jóváhagyó határozatot alátámasztó kiberbiztonsági követelmények nem terjednek ki, továbbra is a gyártók felelősek e kockázatoknak a kiberrezilienciáról szóló rendelet szerinti kezeléséért. Ilyenkor a megfelelés megköveteli az azonosított hiányosságok értékelését és csökkentését, függetlenül attól, hogy a meglévő bizonyítvány vagy jóváhagyó határozat továbbra is érvényes-e.

251. Ez azon eset figyelembevételével szemléltethető, amikor a digitális elemeket tartalmazó termékre a 2014/53/EU irányelvet kiegészítő (EU) 2022/30 felhatalmazáson alapuló bizottsági rendeletben (a rádióberendezésekről szóló irányelv felhatalmazáson alapuló jogi aktusa) meghatározott kiberbiztonsági követelmények vonatkoznak, és amikor e követelmények alapján EU-típusvizsgálati tanúsítványt vagy jóváhagyó határozatot adtak ki. Ebben az esetben a tanúsítvány vagy határozat a 69. cikk (1) bekezdésével összhangban továbbra is érvényes az említett tanúsítvány hatálya alá tartozó és a 2014/53/EU irányelv (a rádióberendezésekről szóló irányelv) kiberbiztonsági alapvető követelményeihez kapcsolódó kiberbiztonsági kockázatokra.

252. Ilyenkor a gyártók a kiberrezilienciáról szóló rendelet alkalmazásában nem kötelesek újraértékelni vagy ismételten igazolni a megfelelést az említett tanúsítványok szerint már kezelt kockázatok tekintetében mindaddig, amíg a vonatkozó tanúsítvány vagy jóváhagyó határozat érvényes, de legkésőbb 2028. június 11-ig. Ez magában foglalja például a hálózatvédelemmel, a személyes adatok és a magánélet védelmével vagy a csalás megelőzésével kapcsolatos kiberbiztonsági kockázatokat (amennyiben ezek a kockázatok az említett tanúsítvány hatálya alá tartoznak), amelyek a rádióberendezésekről szóló irányelv kiberbiztonsági követelményeihez kapcsolódnak, és tükröződnek a megfelelőségértékelésben.

253. Ha azonban a kiberrezilienciáról szóló rendelet 13. cikkének (2) bekezdésével összhangban elvégzett kiberbiztonsági kockázatértékelés olyan további kiberbiztonsági kockázatokat azonosít, amelyekre az említett tanúsítványok nem terjednek ki, a gyártók továbbra is felelősek e kockázatoknak a kiberrezilienciáról szóló rendelettel összhangban történő kezeléséért. Ez magában foglalhatja például a sérülékenységkezelési eljárásokkal, az adatminimalizálással és a támadási felület csökkentésével kapcsolatos kockázatokat, vagy az említett tanúsítványok által nem érintett vagy a rádióberendezésekről szóló irányelv alapvető kiberbiztonsági követelményeinek hatálya alá nem tartozó egyéb termékspecifikus kiberbiztonsági szempontokat.

254. Ennek megfelelően a rádióberendezésekről szóló irányelv szerinti, a kiberbiztonsággal kapcsolatos alapvető követelményeire vonatkozó érvényes EU-típusvizsgálati tanúsítvány vagy jóváhagyó határozat megléte önmagában nem igazolja a kiberrezilienciáról szóló rendeletnek való teljes megfelelést. Ehelyett lehetővé teszi a gyártók számára, hogy az említett tanúsítványra vagy határozatra támaszkodjanak a kapcsolódó kockázatoknak való megfelelés bizonyítékaként, biztosítva ugyanakkor, hogy a fennmaradó vagy újonnan azonosított kockázatokat a kiberrezilienciáról szóló rendeletnek megfelelően értékeljék és csökkentsék.

([31]) A 2027. december 11. előtt forgalomba hozott, digitális elemeket tartalmazó termékek a forgalomba hozataluk időpontjában alkalmazandó uniós jogszabályok hatálya alá tartoznak, és ha megfelelőek voltak, értékesíthetők és üzembe helyezhetők, kivéve, ha 2027. december 11-én vagy azt követően jelentős módosításokon mennek keresztül. A „forgalomba hozatal” és a „forgalmazás” fogalmát illetően lásd még e dokumentum *2.1.* szakaszát (*Placing on the market*), valamint a kék útmutató 2. fejezetét.

255. Hasonlóképpen, ha a digitális elemeket tartalmazó termékre a 2027. január 20-tól teljeskörűen alkalmazandó (EU) 2023/1230 rendeletben (a gépekről szóló rendelet) meghatározott, kiberbiztonsággal kapcsolatos alapvető egészségvédelmi és biztonsági követelmények vonatkoznak, és ha az említett követelmények alapján EU-típusvizsgálati tanúsítványt vagy jóváhagyó határozatot adtak ki, az említett tanúsítvány vagy jóváhagyó határozat a kiberrezilienciáról szóló rendelet 69. cikkének (1) bekezdésével összhangban továbbra is érvényes a gépekről szóló rendelet hatálya alá tartozó kiberbiztonsági kockázatokra.

256. Ez különösen a korrupció elleni védelemmel, valamint az ellenőrzési rendszerek biztonságával és megbízhatóságával kapcsolatos kiberbiztonsági szempontokat érinti, a gépekről szóló rendelet III. mellékletének 1.1.9. és 1.2.1. szakaszában meghatározottak szerint. E kockázatok tekintetében a gyártók a kiberrezilienciáról szóló rendelet alkalmazásában nem kötelesek újraértékelni vagy ismételten igazolni a megfelelést mindaddig, amíg a vonatkozó tanúsítvány vagy jóváhagyó határozat érvényes, de legkésőbb 2028. június 11-ig. Ez annyiban alkalmazandó, amennyiben ezeket a kockázatokat a gépekről szóló rendelet szerinti megfelelőségértékelés keretében kezelték.

257. A rádióberendezésekről szóló irányelv fent említett alapvető kiberbiztonsági követelményeihez hasonlóan, ha a kiberrezilienciáról szóló rendelet 13. cikkének (2) bekezdése szerint elvégzett kiberbiztonsági kockázatértékelés olyan további kiberbiztonsági kockázatokat azonosít, amelyek nem tartoznak a gépekről szóló rendelet alapján kiállított releváns tanúsítvány hatálya alá, és amelyek kapcsolódnak az említett rendelet kiberbiztonsági követelményeihez, továbbra is a gyártók felelősek e kockázatoknak a kiberrezilienciáról szóló rendelettel összhangban történő kezeléséért.