2025/2392

2025.12.1.

A BIZOTTSÁG (EU) 2025/2392 VÉGREHAJTÁSI RENDELETE

(2025. november 28.)

a digitális elemeket tartalmazó fontos és kritikus fontosságú termékek kategóriáinak az (EU) 2024/2847 európai parlamenti és tanácsi rendelet szerinti műszaki leírásáról

(EGT-vonatkozású szöveg)

AZ EURÓPAI BIZOTTSÁG,

tekintettel az Európai Unió működéséről szóló szerződésre,

tekintettel 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 szóló, 2024. október 23-i (EU) 2024/2847 európai parlamenti és tanácsi rendeletre (a kiberrezilienciáról szóló rendelet) ([1]) és különösen annak 7. cikke (4) bekezdésére,

mivel:

(1) Az (EU) 2024/2847 rendelet meghatározza a digitális elemeket tartalmazó termékek kiberbiztonságára vonatkozó szabályokat. Az említett rendelet III. melléklete meghatározza a digitális elemeket tartalmazó fontos termékek azon kategóriáit, amelyekre a forgalomba hozatalkor a más, digitális elemeket tartalmazó termékekre alkalmazandó eljárásoknál szigorúbb megfelelőségértékelési eljárások vonatkoznak. Az (EU) 2024/2847 rendelet IV. melléklete meghatározza a digitális elemeket tartalmazó kritikus fontosságú termékek azon kategóriáit, amelyek esetében a gyártók számára előírható, hogy az (EU) 2019/881 európai parlamenti és tanácsi rendelet ([2]) szerinti európai kiberbiztonsági tanúsítási rendszer keretében európai kiberbiztonsági tanúsítványt szerezzenek be, vagy amelyeket forgalomba hozatalukkor harmadik fél általi kötelező megfelelőségértékelésnek vetnének alá.

(2) Az (EU) 2024/2847 rendelet 7. cikkének (1) bekezdése és 8. cikkének (1) bekezdése értelmében a digitális elemeket tartalmazó termék alapvető funkciója meghatározza, hogy a digitális elemeket tartalmazó termék megfelel-e a digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékek valamely kategóriájára vonatkozó műszaki leírásnak, és ezért az alkalmazandó megfelelőségértékelési eljárásoknak.

(3) A digitális elemeket tartalmazó termék kifejlesztésekor és a kívánt funkciók elérése érdekében a gyártók jellemzően olyan egyéb alkotóelemeket is integrálnak saját, digitális elemeket tartalmazó termékeikbe, amelyek szintén digitális elemeket tartalmazó termékek, és amelyek megfelelhetnek a fontos vagy kritikus fontosságú termékek valamely kategóriája műszaki leírásának. Az (EU) 2024/2847 rendelet értelmében a digitális elemeket tartalmazó termék a digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékekre alkalmazandó megfelelőségértékelési eljárások hatálya alá tartozik, amennyiben az adott termék egésze az említett rendelet III. és IV. mellékletében meghatározott fontos vagy kritikus fontosságú termék. Például egy beágyazott böngészőnek egy okostelefonokban használt híralkalmazás alkotóelemeként történő integrálása önmagában nem vonja maga után azt, hogy a híralkalmazást az olyan digitális elemeket tartalmazó termékekre alkalmazandó megfelelőségértékelési eljárásnak kelljen alávetni, amelyek alapvető funkciója az „önálló és beágyazott böngészők”. Mindazonáltal az (EU) 2024/2847 rendelettel összhangban a gyártónak biztosítania kell, hogy a digitális elemeket tartalmazó termék egésze megfeleljen az alapvető kiberbiztonsági követelményeknek. Ezért a gyártónak az egész termék biztonságát kell értékelnie, adott esetben figyelembe véve az abba beépített alkotóelemek vagy funkciók biztonságát. Például ahhoz, hogy egy híralkalmazás gyártója bizonyítsa, hogy a digitális elemeket tartalmazó terméke megfelel az (EU) 2024/2847 rendeletnek, az adott gyártónak igazolnia kell, hogy a híralkalmazás egésze megfelel az alkalmazandó követelményeknek, adott esetben figyelembe véve az alkalmazásba integrált beágyazott böngésző biztonságát.

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

([2]) Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Az a tény, hogy a digitális elemeket tartalmazó termék az e rendeletben meghatározott műszaki leírásokban részletezettektől eltérő vagy azokon túlmutató funkciókat lát el, önmagában nem jelenti azt, hogy a digitális elemeket tartalmazó termék nem rendelkezik az (EU) 2024/2847 rendelet III. és IV. mellékletében meghatározott valamely termékkategória alapvető funkcióival. Például az „operációs rendszerek” alapvető funkciójával rendelkező, digitális elemeket tartalmazó termékek gyakran tartalmaznak olyan szoftvereket, például számológépeket vagy egyszerű grafikus szerkesztőket, amelyek az adott termékkategória műszaki leírásában nem szereplő kiegészítő funkciókat látnak el. A digitális elemeket tartalmazó termékek gyakran tartalmaznak olyan alkotóelemeket is, amelyek egy másik, digitális elemeket tartalmazó fontos vagy kritikus fontosságú termék funkcionalitásával rendelkeznek – ilyen például egy böngészőfunkciót magában foglaló operációs rendszer vagy egy tűzfalfunkciót magában foglaló útválasztót (router). Ez azonban önmagában nem jelenti azt, hogy az ilyen, digitális elemeket tartalmazó termékek nem rendelkeznek az „operációs rendszerek”, illetve a „routerek, internetcsatlakozásra szánt modemek és kapcsolók” alapvető funkcióival.

(5) Másfelől az olyan digitális elemeket tartalmazó termék, amely képes ellátni az (EU) 2024/2847 rendelet III. és IV. mellékletében meghatározott termékkategóriák valamelyikének funkcióit, de amelynek alapvető funkcionalitása eltér az adott termékkategóriáétól, nem tekinthető úgy, hogy megfelel az adott termékkategória műszaki leírásának. Például 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 adatokat gyűjtenek, elemzik és biztonsági célokból hasznosítható információként mutatják be azokat. Mivel azonban alapvető funkciója nem egyezik meg a SIEM alapvető funkciójával, egy SOAR szoftver általában nem felel meg a „biztonsági információkat és eseményeket kezelő (SIEM) rendszerek” műszaki leírásának. Hasonlóképpen, egy okostelefon jellemzően olyan alkotóelemeket tartalmaz, amelyek az (EU) 2024/2847 rendelet III. és IV. mellékletében meghatározott termékkategóriák közül több funkcióját is ellátják, például operációs rendszert vagy integrált jelszókezelőt. Mivel azonban az okostelefon alapvető funkciója nem az operációs rendszer vagy a jelszókezelő funkciója, általában nem tekinthető úgy, hogy megfelel az ilyen termékkategóriák műszaki leírásának.

(6) Az (EU) 2024/2847 rendelet 13. cikkének (2) és (3) bekezdése értelmében a digitális elemeket tartalmazó termékek gyártóinak a digitális elemeket tartalmazó termék kockázataival arányos módon kell végrehajtaniuk az (EU) 2024/2847 rendelet I. mellékletének I. részében meghatározott alapvető kiberbiztonsági követelményeket, a digitális elemeket tartalmazó termék rendeltetése és észszerűen előrelátható használata, valamint használati feltételei alapján, figyelembe véve a termék használatának várható időtartamát. Az említett rendelet 13. cikkének (2) és (3) bekezdésével összhangban, és függetlenül attól, hogy a digitális elemeket tartalmazó termék fontos vagy kritikus fontosságú, digitális elemeket tartalmazó terméknek minősül-e, a gyártóknak átfogó kiberbiztonsági kockázatértékelést kell végezniük, és jelezniük kell, hogy a kockázatértékelés alapján hogyan hajtják végre az alapvető kiberbiztonsági követelményeket, beleértve azok tesztelését és megbízhatóságát is. Amennyiben a digitális elemeket tartalmazó termékük alapvető funkciója megfelel valamely digitális elemeket tartalmazó fontos vagy kritikus fontosságú termék műszaki leírásának, a gyártóknak az (EU) 2024/2847 rendelet 32. cikkének (2), (3), (4) és (5) bekezdésében meghatározott konkrét megfelelőségértékelési eljárásokat követve kell igazolniuk a megfelelőséget.

(7) Ez a rendelet példákat tartalmaz azokra a digitális elemeket tartalmazó termékekre, amelyek alapvető funkciója megfelel egyes, digitális elemeket tartalmazó fontos vagy kritikus fontosságú termékek műszaki leírásának. Ezek a példák csak szemléltetési célokat szolgálnak, és nem kimerítő felsorolást tartalmaznak.

(8) A gyártók jogbiztonságának biztosítása érdekében a digitális elemeket tartalmazó termékek azon kategóriáit, amelyek nem manipulálható mikroprocesszorok, nem manipulálható mikrovezérlők, intelligens kártyák és hasonló eszközök, beleértve a biztonságos elemeket is, az azon hibák vagy gyengeségek potenciális kihasználhatóságával szembeni ellenállás szintje alapján kell megkülönböztetni, amelyekre tervezték őket. Az AVA_VAN-szint széles körben használt és szabványosított módszer az ilyen rezisztenciaszint kifejezésére. Az AVA_VAN-szinteket a nyilvánosan hozzáférhető közös kritériumok és közös értékelési módszertani szabványok határozzák meg, amelyek a meglévő, a piacon széles körben elfogadott tanúsítási keretrendszerek, például az (EU) 2024/482 bizottsági végrehajtási

rendelet ([3]) alapjául szolgálnak. Az (EU) 2024/482 végrehajtási rendelet olyan európai kiberbiztonsági tanúsítási rendszert hoz létre, amely a termék egyedi megbízhatósági szinten történő tanúsítására használható. A globális gyakorlatokra építve az (EU) 2024/482 végrehajtási rendelet 2027 végéig lehetőséget biztosít a szabványok régebbi változatain alapuló tanúsítványok kiállítására. Ezért az (EU) 2024/2847 rendelettel összefüggésben helyénvaló lehetővé tenni, hogy az AVA_VAN szinteket az említett szabványok legújabb vagy korábbi változataira való hivatkozással fejezzék ki.

(9) Az e rendeletben előírt intézkedések összhangban vannak az (EU) 2024/2847 rendelet 62. cikkének (1) bekezdésével létrehozott bizottság véleményével,

ELFOGADTA EZT A RENDELETET:

1. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

(1) „közös kritériumok”: az (EU) 2024/482 végrehajtási rendelet 2. cikkének (1) bekezdésében vagy az említett végrehajtási rendelet 3. cikke (2) bekezdésének a) és b) pontjában említett szabványokban meghatározott informatikai biztonságértékelés közös kritériumai;

(2) „közös értékelési módszertan”: az (EU) 2024/482 végrehajtási rendelet 2. cikkének (2) bekezdésében vagy az említett végrehajtási rendelet 3. cikke (2) bekezdésének c) és d) pontjában említett szabványokban meghatározott informatikai biztonságértékelés közös módszertana.

2. cikk

(1) Az (EU) 2024/2847 rendelet III. mellékletében felsorolt I. és II. osztályba tartozó, digitális elemeket tartalmazó termékek kategóriáinak műszaki leírását e rendelet I. melléklete határozza meg.

(2) Az (EU) 2024/2847 rendelet IV. mellékletében felsorolt, digitális elemeket tartalmazó termékek kategóriáinak műszaki leírását e rendelet II. melléklete határozza meg.

3. cikk

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben, 2025. november 28-án.

a Bizottság részéről
az elnök
Ursula VON DER LEYEN

([3]) A Bizottság (EU) 2024/482 végrehajtási rendelete (2024. január 31.) a közös kritériumokon alapuló európai kiberbiztonsági tanúsítási rendszer (EUCC) elfogadása tekintetében az (EU) 2019/881 európai parlamenti és tanácsi rendelet alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/482, 2024.2.7., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

I. MELLÉKLET

DIGITÁLIS ELEMEKET TARTALMAZÓ FONTOS TERMÉKEK

I. osztály

Termékkategória	Műszaki leírás
1. Személyazonosság-kezelő rendszerek és emelt szintű hozzáférést kezelő szoftverek és hardverek, beleértve a hitelesítő és a hozzáférés-ellenőrző leolvasókat, ideértve a biometrikus leolvasókat is	A személyazonosság-kezelő rendszerek olyan, digitális elemeket tartalmazó termékek, amelyek hitelesítési vagy engedélyezési mechanizmusokat biztosítanak, és amelyek természetes személyek, jogi személyek, eszközök vagy rendszerek azonosító okmányainak életciklus-kezelésére vonatkozó mechanizmusokat is biztosíthatnak, például személyazonosság-nyilvántartást, rendelkezést, karbantartást, nyilvántartásból való törlést. Ezek a rendszerek olyan hozzáférés-kezelő rendszereket foglalnak magukban, amelyek természetes személyek, jogi személyek, eszközök vagy rendszerek digitális erőforrásokhoz vagy fizikai helyszínekhez való hozzáférését ellenőrzik. Az emelt szintű hozzáférést kezelő szoftver olyan hozzáférés-kezelő rendszer, amely ellenőrzi és nyomon követi az IT- vagy OT-rendszerekhez és az érzékeny információkhoz való hozzáférési jogokat egy szervezeten belül, beleértve a kiemelt felhasználókra vonatkozó differenciált belépési ellenőrzési politikákat végrehajtó rendszereket is. Ebbe a kategóriába tartoznak többek között a hitelesítést és belépési ellenőrzést végző leolvasók, a biometrikus leolvasók, az egyszeri bejelentkezési szoftverek, az egyesített személyazonosság-kezelő szoftverek, az egyszeri jelszavakat generáló szoftverek, a hardver-hitelesítési eszközök, például a tranzakcióazonosító szám (TAN) generátorai, a hitelesítési szoftverek és a többtényezős hitelesítési szoftverek.
2. Önálló és beágyazott böngészők	Olyan digitális elemeket tartalmazó szoftvertermékek, amelyek lehetővé teszik a végfelhasználók számára a hálózatokhoz, például az internethez kapcsolódó szervereken tárolt webes tartalmak és szolgáltatások elérését, megjelenítését és az azokkal való interakciót. Ezek jellemzően magukban foglalják a jelölőnyelven (pl. HTML) írt tartalmak tolmácsolására és megjelenítésére szolgáló böngészőmotort, a webprotokollok (pl. HTTP, HTTPS) támogatását, a szkriptek végrehajtásának és a felhasználói inputok kezelésének képességét, valamint a weboldalakról származó ideiglenes vagy tartós adatok tárolását (sütik). Ez a kategória magában foglalja többek között a böngészők funkcióit ellátó önálló alkalmazásokat, a más rendszerbe vagy alkalmazásba történő integrálásra szánt beágyazott böngészőket, valamint az integrált MI-ügynökkel rendelkező böngészőket.
3. Jelszókezelők	Digitális elemeket tartalmazó termékek, amelyek jelszavakat tárolnak helyben, egy eszközön, vagy távoli szerveren, beleértve az olyan tevékenységeket, mint a jelszavak létrehozása, valamint a jelszómegosztás és a jelszóhasználatot szolgáló, helyi vagy harmadik féltől származó alkalmazásokkal való integráció. Ebbe a kategóriába tartoznak többek között a helyi jelszókezelők, a böngésző kiterjesztéseként biztosított jelszókezelők, a vállalati jelszókezelők, valamint a hardveralapú jelszókezelők.

Termékkategória	Műszaki leírás
4. Rosszindulatú szoftverek keresésére, eltávolítására vagy karanténba helyezésére szolgáló szoftverek	Digitális elemeket tartalmazó szoftvertermékek, amelyeket jellemzően vírusirtónak vagy rosszindulatú programok elleni védelemnek neveznek, és amelyek rosszindulatú szoftvereket vagy kódokat észlelnek vagy keresnek az eszközökön, vagy eltávolítják vagy karanténba helyezik az ilyen szoftvereket vagy kódokat az ilyen eszközök integritásának, bizalmas jellegének vagy rendelkezésre állásának fenntartása érdekében. Ebben a termékkategóriában a rosszindulatú szoftver olyan rosszindulatú funkciókat vagy képességeket tartalmazó szoftver, amelyek közvetlenül vagy közvetve kárt okozhatnak a felhasználónak és/vagy a számítógépes rendszernek, mint például vírusok, férgek, zsarolóvírusok, kémszoftverek és trójai programok. Ebbe a kategóriába tartoznak többek között azok a szoftverek, amelyek valós időben vagy manuálisan észlelik vagy keresik a rosszindulatú szoftvereket, a rootkit-észlelő és mentési lemezek, amelyek alapvető funkciója a rosszindulatú szoftverek keresése, eltávolítása vagy karanténba helyezése.
5. Virtuális magánhálózat (VPN) funkcióval rendelkező, digitális elemeket tartalmazó termékek	Digitális elemeket tartalmazó termékek, amelyek egy fizikai vagy virtuális hálózat rendszererőforrásaiból épített, titkosított logikai alagutat hoznak létre. Ebbe a kategóriába tartoznak többek között a virtuális magánhálózati ügyfelek, a virtuális magánhálózati szerverek és a virtuális magánhálózati átjárók.
6. Hálózatkezelő rendszerek	Olyan digitális elemeket tartalmazó termékek, amelyek összekapcsolt hálózati elemeket, például szervereket, routereket, kapcsolókat, munkaállomásokat, nyomtatókat vagy mobil eszközöket kezelnek azok nyomon követése, valamint hálózati műveleteik és konfigurációjuk ellenőrzése révén. Ez a kategória magában foglalja többek között a végponttól végpontig terjedő irányítási rendszereket és a dedikált konfigurációkezelő rendszereket, például a szoftveralapú hálózatkezelési vezérlőket.
7. Biztonsági információkat és eseményeket kezelő (SIEM) rendszerek	Digitális elemeket tartalmazó termékek, amelyek több forrásból gyűjtenek adatokat, ezeket elemzik és korrelálják, valamint biztonsággal kapcsolatos célokból – például fenyegetések és biztonsági események észlelése, kriminalisztikai elemzés vagy megfelelés céljából – hasznosítható információként mutatják be.
8. Rendszerbetöltés-vezérlő programok	Digitális elemeket tartalmazó szoftvertermékek, amelyek a bekapcsolás/újraindítás utáni kezdeti rendszerindítás folyamatát kezelik a hardver inicializálásával, a vezérlés operációs rendszerkörnyezetbe vagy rendszererőforrásokba való betöltésével vagy átvitelével, valamint a rendszerindítási lehetőségek kiválasztásával. Ebbe a kategóriába tartoznak többek között az UEFI belső vezérlőprogramok, valamint az egy- és többlépcsős rendszerindító betöltők.
9. Nyilvános kulcsú infrastruktúra és elektronikus tanúsítványok kibocsátására szolgáló szoftverek	A nyilvános kulcsú infrastruktúra (PKI) részeként használt, digitális elemeket tartalmazó termékek, amelyek a digitális tanúsítványok validálását, létrehozását, kiállítását, terjesztését, státuszának közzétételét, megújítását vagy visszavonását, vagy az ilyen digitális tanúsítványokhoz kapcsolódó kriptográfiai kulcsok létrehozását, tárolását, letétét, cseréjét, megsemmisítését vagy rotációját kezelik. Ebbe a kategóriába tartoznak többek között a kulcskezelő rendszerek, a digitális tanúsítványkezelő rendszerek, az online tanúsítványállapot-protokoll-válaszadók és az all-in-one PKI-megoldások.

Termékkategória	Műszaki leírás
10. Fizikai és virtuális hálózati interfészek	A fizikai hálózati interfészek olyan digitális elemeket tartalmazó termékek, amelyek közvetlenül csatlakoztatnak egy eszközt a hálózathoz az interfész-illesztőprogramok által biztosított, jellemzően az adatkapcsolati rétegben működő alkalmazásprogramozási interfészen (API) keresztül, és amelyek hardveradaptereket tartalmaznak a megfelelő belső vezérlőprogrammal rendelkező, jellemzően a fizikai és az adatkapcsolati rétegben működő átviteli adathordozókhoz. A virtuális hálózati interfészek olyan digitális elemeket tartalmazó termékek, amelyek közvetlenül vagy közvetve csatlakoztatnak egy eszközt egy hálózathoz egy olyan API-n keresztül, amely a fizikai hálózati interfészek illesztőprogramjait imitálja, és jellemzően az adatkapcsolati rétegben működik. Ez a kategória magában foglalja többek között a vezetékes és vezeték nélküli hálózati interfész kártyákat, vezérlőket és adaptereket, például Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee vagy Fieldbus esetében, valamint a tisztán virtuális önálló termékeket, például virtuális hálózati interfész kártyákat, konténer hálózati interfészeket és VPN interfészeket.
11. Operációs rendszerek	Digitális elemeket tartalmazó szoftvertermékek, amelyek absztrakt interfészt biztosítanak az alapul szolgáló hardverhez, és ellenőrzik a szoftver végrehajtását, és amelyek olyan szolgáltatásokat nyújthatnak, mint például a számítástechnikai erőforrás-gazdálkodás és -konfiguráció, az ütemezés, a bemeneti-kimeneti vezérlés, az adatok kezelése, valamint olyan interfész biztosítása, amelyen keresztül az alkalmazások kapcsolatba lépnek a rendszer erőforrásaival és perifériáival. Ebbe a kategóriába tartoznak többek között a valós idejű operációs rendszerek, az általános célú és a speciális célú operációs rendszerek.
12. Routerek, internetcsatlakozásra szánt modemek és kapcsolók	Az útvonalválasztók (routerek) olyan digitális elemeket tartalmazó termékek, amelyek létrehozzák és szabályozzák a különböző hálózatok közötti adatáramlást azáltal, hogy útvonalakat választanak ki útvonalválasztási protokollmechanizmusok és algoritmusok segítségével, és amelyek jellemzően a hálózati rétegen működnek. Ebbe a kategóriába tartoznak többek között a vezetékes és vezeték nélküli routerek, a virtuális routerek és a modemekkel vagy anélkül működő routerek.
	Az internethez való csatlakozásra szánt modemek olyan digitális elemeket tartalmazó hardvertermékek, amelyek digitális modulációs és demodulációs technikákat alkalmaznak az analóg jelek digitális jelekből és digitális jelekké történő átalakítására az IP-alapú kommunikáció céljából. Ebbe a kategóriába tartoznak többek között az optikai modemek, a digitális előfizetői vonal (DSL) modemei, a kábelmodemek (DOCSIS), a műholdas modemek és a celluláris modemek.
	A kapcsolók olyan digitális elemeket tartalmazó termékek, amelyek csomagtovábbítási mechanizmusokon keresztül biztosítják a hálózati eszközök közötti kapcsolatot, és amelyek irányítási síkkal rendelkeznek, amelyet jellemzően az adatkapcsolaton vagy a hálózati rétegen hajtanak végre. Ez a kategória magában foglalja többek között az irányított kapcsolókat, az intelligens kapcsolókat, a többrétegű kapcsolókat, a virtuális biztonsági kapcsolókat, a szoftveralapú hálózatépítéshez való programozható kapcsolókat és a hidakat, például a vezeték nélküli hozzáférési pontokat.

Termékkategória	Műszaki leírás
13. Biztonsági funkciókkal rendelkező mikroprocesszorok	Olyan, digitális elemeket tartalmazó termékek, amelyek olyan integrált áramkörök, amelyek külső memórián és periférián alapuló központi feldolgozási funkciókat látnak el, beleértve a mikrokódot és más alacsony szintű belső vezérlőprogramokat is. Emellett biztonsági vonatkozású funkciókat is biztosítanak, például titkosítást, hitelesítést, biztonságos kulcstárolást, véletlenszerű számgenerálást, megbízható végrehajtási környezetet vagy más hardveralapú védelmi mechanizmusokat, amelyek célja a mikroprocesszoron kívüli egyéb termékek, hálózatok vagy szolgáltatások, például biztonságos rendszerindítási lánc, virtualizáció vagy biztonságos kommunikációs interfészek biztosítása.
14. Biztonsági funkciókkal rendelkező mikrovezérlők	Olyan, digitális elemeket tartalmazó termékek, amelyek olyan integrált áramkörök, amelyek memóriát – és jellemzően más perifériákat is, beleértve a mikrokódot és más alacsony szintű belső vezérlőprogramokat is – integráló központi feldolgozási funkciókat látnak el, lehetővé téve a mikrovezérlő programozhatóságát. Emellett biztonsági vonatkozású funkciókat is biztosítanak, például titkosítást, hitelesítést, biztonságos kulcstárolást, véletlenszerű számgenerálást, megbízható végrehajtási környezetet vagy más hardveralapú védelmi mechanizmusokat, amelyek célja a mikrovezérlőn kívüli egyéb termékek, hálózatok vagy szolgáltatások, például biztonságos rendszerindítási lánc, virtualizáció vagy biztonságos kommunikációs interfészek biztosítása.
15. Biztonsági funkciókkal rendelkező, alkalmazásspecifikus integrált áramkörök (ASIC) és a felhasználás helyén programozható logikai kapumátrixok (FPGA)	A biztonsági funkciókkal rendelkező, alkalmazásspecifikus integrált áramkörök (ASIC) olyan, digitális elemeket tartalmazó termékek, amelyek részben vagy egészben egy meghatározott funkció ellátására vagy egy adott alkalmazás végrehajtására tervezett integrált áramkörök, beleértve a mikrokódot és más alacsony szintű belső vezérlőprogramot is. Emellett biztonsági vonatkozású funkciókat is biztosítanak, például titkosítást, hitelesítést, biztonságos kulcstárolást, véletlenszerű számgenerálást, megbízható végrehajtási környezetet vagy más hardveralapú védelmi mechanizmusokat, amelyek célja az ASIC-en kívüli egyéb termékek, hálózatok vagy szolgáltatások, például biztonságos rendszerindítási lánc, virtualizáció vagy biztonságos kommunikációs interfészek biztosítása.
	A biztonsági vonatkozású funkciókkal rendelkező, a felhasználás helyén programozható logikai kapumátrixok (FPGA) olyan, digitális elemeket tartalmazó termékek, amelyek olyan integrált áramkörök, amelyeket konfigurálható logikai blokkok mátrixa jellemez, és amelyeket úgy terveztek, hogy a gyártást követően meghatározott funkció ellátása vagy egy adott alkalmazás – többek között mikrokód és más alacsony szintű belső vezérlőprogram – megvalósítása céljából újraprogramozhatók legyenek. Emellett biztonsági vonatkozású funkciókat is biztosítanak, például titkosítást, hitelesítést, biztonságos kulcstárolást, véletlenszerű számgenerálást, megbízható végrehajtási környezetet vagy más hardveralapú védelmi mechanizmusokat, amelyek célja az FPGA-n kívüli egyéb termékek, hálózatok vagy szolgáltatások, például biztonságos rendszerindítási lánc, virtualizáció vagy biztonságos kommunikációs interfészek biztosítása.
16. Általános célú intelligens otthoni virtuális asszisztensek	Olyan digitális elemeket tartalmazó termékek, amelyek akár közvetlenül, akár más berendezéseken keresztül a nyilvános interneten kommunikálnak, és amelyek természetes nyelvi utasításokon alapuló igényeket, feladatokat vagy kérdéseket dolgoznak fel, például hang- vagy írásbeli bemeneten keresztül, és amelyek ezen igények, feladatok vagy kérdések alapján hozzáférést biztosítanak más szolgáltatásokhoz, vagy lakossági környezetben ellenőrzik a csatlakoztatott eszközök funkcióit. Ebbe a kategóriába tartoznak többek között az integrált virtuális asszisztenssel rendelkező okos hangszórók, valamint az e leírásnak megfelelő önálló virtuális asszisztensek.

Termékkategória	Műszaki leírás
17. Biztonsági funkciókkal rendelkező intelligens otthoni termékek, beleértve az intelligens ajtózárakat, a biztonsági kamerákat, a babafigyelő rendszereket és a riasztórendszereket	Olyan, digitális elemeket tartalmazó termékek, amelyek lakókörnyezetben védik a fogyasztók fizikai biztonságát, és amelyek más rendszerekből, távolról irányíthatók vagy kezelhetők, valamint az ilyen termékeket központilag irányító hardverek és szoftverek. Ebbe a kategóriába tartoznak többek között az okos zárak, a babafigyelő rendszerek, a riasztórendszerek és az otthoni biztonsági kamerák.
18. A 2009/48/EK európai parlamenti és tanácsi irányelv ([1]) hatálya alá tartozó, internetre csatlakoztatott játékok, amelyek szociális interaktív funkciókkal, így például beszéddel vagy videofelvétellel, vagy helymeghatározó funkciókkal rendelkeznek	A szociális interaktív funkciókkal rendelkező, internetre csatlakoztatott játékok a 2009/48/EK irányelv hatálya alá tartozó, digitális elemeket tartalmazó termékek, amelyek akár közvetlenül, akár bármely más berendezésen keresztül a nyilvános interneten kommunikálnak, és amelyek olyan beépített technológiákkal – például billentyűzettel, mikrofonnal, hangszóróval vagy kamerával – rendelkeznek, amelyek lehetővé teszik a bejövő és kimenő kommunikációt.
	A helymeghatározó funkciókkal rendelkező, internethez csatlakoztatott játékok a 2009/48/EK irányelv hatálya alá tartozó, digitális elemeket tartalmazó termékek, amelyek akár közvetlenül, akár bármely más berendezésen keresztül a nyilvános interneten kommunikálnak, és amelyek olyan technológiákkal rendelkeznek, amelyek lehetővé teszik a játék vagy annak felhasználója földrajzi helyének nyomon követését vagy következtetéssel történő megállapítását. Amennyiben a játék csupán érzékelési technológiák alkalmazásával érzékeli a felhasználó vagy más játékok közelségét, a játék nem tekinthető helymeghatározó funkcióval rendelkezőnek.
19. Emberi testen viselhető vagy elhelyezhető, személyes használatra szánt termékek, amelyek egészségügyi megfigyelési, így például nyomkövetési célt szolgálnak, és amelyekre az (EU) 2017/745 ([2]) vagy az (EU) 2017/746 európai parlamenti és tanácsi rendelet ([3]) nem alkalmazandó, vagy a gyermekek általi használatra és gyermekek részére készült, személyes használatra szánt, viselhető termékek	Az emberi testen viselhető vagy elhelyezhető, egészségügyi megfigyelési célt szolgáló, személyes használatra szánt termékek olyan, digitális elemeket tartalmazó termékek, amelyeket közvetlenül a testen, vagy ruházaton vagy kiegészítőkön keresztül viselnek, és amelyek rendszeresen vagy folyamatosan érzékelik és feldolgozzák a felhasználó egészsége szempontjából releváns információkat, beleértve a szervezetre vonatkozó mérőszámokat is, kivéve az (EU) 2017/745 rendelet vagy az (EU) 2017/746 rendelet hatálya alá tartozó termékeket. Ebbe a kategóriába tartoznak többek között az e leírásnak megfelelő fitneszkövetők, okosórák, intelligens kiegészítők, intelligens ruházat és sportruházat.
	A gyermekek általi használatra és gyermekeknek szánt, viselhető személyes termékek olyan, digitális elemeket tartalmazó termékek, amelyeket 14 év alatti személyek közvetlenül a testükön, vagy ruházaton vagy kiegészítőkön keresztül viselhetnek vagy elhelyezhetnek. Ebbe a kategóriába tartoznak többek között a gyermekek biztonsága érdekében viselhető eszközök.

([1]) Az Európai Parlament és a Tanács 2009/48/EK irányelve (2009. június 18.) a játékok biztonságáról (HL L 170., 2009.6.30., 1. o., ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Az Európai Parlament és a Tanács (EU) 2017/745 rendelete (2017. április 5.) az orvostechnikai eszközökről, a 2001/83/EK irányelv, a 178/2002/EK rendelet és az 1223/2009/EK rendelet módosításáról, valamint a 90/385/EGK és a 93/42/EGK tanácsi irányelv hatályon kívül helyezéséről (HL L 117., 2017.5.5., 1. o., ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Az Európai Parlament és a Tanács (EU) 2017/746 rendelete (2017. április 5.) az *in vitro* diagnosztikai orvostechnikai eszközökről, valamint a 98/79/EK irányelv és a 2010/227/EU bizottsági határozat hatályon kívül helyezéséről (HL L 117., 2017.5.5., 176. o., ELI: http://data.europa.eu/eli/reg/2017/746/oj).

II. osztály

Termékkategória	Műszaki leírás
1. Az operációs rendszerek és hasonló környezetek virtualizált végrehajtását támogató hipervizorok és konténeres futtatókörnyezetek	A hipervizorok olyan, digitális elemeket tartalmazó szoftvertermékek, amelyek absztrahálják és/vagy allokálják a számítástechnikai erőforrásokat, és lehetővé teszik az egymástól és/vagy a fizikai hardvertől logikusan elkülönülő virtuális gépek végrehajtását, kezelését és vezénylését. A hipervizorok futhatnak közvetlenül a hardveren (csupasz fémen), az operációs rendszeren vagy egy másik virtuális gépen (beágyazott virtualizáció). E termékkategória összefüggésében a virtuális gép a számítástechnikai környezet szoftveralapú logikai szétválasztása, amely magában foglalja a hardvererőforrások (pl. CPU, memória, tárolás, hálózati interfészek) virtualizált készletét, és jellemzően saját operációs rendszert üzemeltet. Ez a kategória magában foglalja többek között az 1. típusú hipervizorokat (csupasz fém), a 2. típusú hipervizorokat (amelyeket operációs rendszeren helyeznek el) és a hibrid hipervizorokat.
	A konténeres futtatókörnyezetek olyan, digitális elemeket tartalmazó szoftvertermékek, amelyek elszigetelt folyamatokként kezelik az egy gazdagépes operációs rendszeren futó konténerek végrehajtását és életciklusát, elosztják az erőforrásokat, és lehetővé teszik az egyes konténerek kezelését és szervezését. E termékkategóriával összefüggésben a konténer olyan szoftveralapú végrehajtási környezet, amely egy vagy több szoftver alkotóelemét és azok függőségeit egyetlen csomagba foglalja, lehetővé téve számukra, hogy függetlenül és következetesen működjenek.
2. Tűzfalak, behatolásérzékelő és megelőző rendszerek	A tűzfalak olyan, digitális elemeket tartalmazó termékek, amelyek a hálózatra irányuló és onnan kiinduló adatátviteli forgalom nyomon követése és korlátozása révén védik az összekapcsolt hálózatot vagy rendszert a jogosulatlan hozzáféréssel szemben. Ebbe a kategóriába tartoznak többek között a hálózati tűzfalak és az alkalmazásszintű tűzfalak, például webalkalmazások tűzfalai vagy szűrői és a kéretlen üzenetek elleni átjárók.
	A behatolásérzékelő rendszerek olyan, digitális elemeket tartalmazó termékek, amelyek figyelik a forgalmat, miután az gyanús tevékenység céljából belépett a hálózati környezetbe, és észlelik vagy azonosítják, hogy behatolást kíséreltek meg, behatolás történt vagy történik egy csatlakoztatott hálózaton vagy rendszerben. Ebbe a kategóriába tartoznak többek között a hálózatalapú behatolásérzékelő rendszerek és a gazdagépalapú behatolásérzékelő rendszerek.
	A behatolásmegelőzési rendszerek olyan, digitális elemeket tartalmazó termékek, amelyek olyan behatolásérzékelő rendszerből állnak, amely aktívan reagál a csatlakoztatott hálózatba vagy rendszerbe történő behatolásra. Ebbe a kategóriába tartoznak többek között a hálózatalapú behatolásmegelőzési rendszerek és a gazdagépalapú behatolásmegelőzési rendszerek.

Termékkategória	Műszaki leírás
3. Nem manipulálható mikroprocesszorok	Azok a digitális elemeket tartalmazó termékek, amelyek az e melléklet „I. osztály” táblázatának 13. pontjában említett, biztonsági vonatkozású funkciókkal rendelkező mikroprocesszorok, beleértve a manipulálás jelzését, az azzal szembeni ellenállást vagy az arra történő reagálást is, és amelyeket emellett az AVA_VAN 2. vagy 3. szintjének védelmére is terveztek, a közös kritériumokban és a közös értékelési módszertanban meghatározottak szerint.
4. Nem manipulálható mikrovezérlők	Azok a digitális elemeket tartalmazó termékek, amelyek az e melléklet „I. osztály” táblázatának 14. pontjában említett, biztonsági vonatkozású funkciókkal rendelkező mikrovezérlők, beleértve a manipulálás jelzését, az azzal szembeni ellenállást vagy az arra történő reagálást is, és amelyeket emellett az AVA_VAN 2. vagy 3. szintjének védelmére is terveztek, a közös kritériumokban és a közös értékelési módszertanban meghatározottak szerint.

ELI: http://data.europa.eu/eli/reg_impl/2025/2392/oj

II. MELLÉKLET

DIGITÁLIS ELEMEKET TARTALMAZÓ KRITIKUS FONTOSSÁGÚ TERMÉKEK

Termékkategória	Műszaki leírás
1. Biztonsági zárakkal ellátott hardvereszközök	Olyan, digitális elemeket tartalmazó hardvertermékek, amelyek biztonságosan tárolják, feldolgozzák vagy kezelik az érzékeny adatokat, vagy kriptográfiai műveleteket hajtanak végre, és amelyek több különálló alkotóelemből állnak, és tartalmaznak egy olyan fizikai hardverborítékot, amely a fizikai támadásokkal szembeni ellenintézkedésként biztosítja a manipulálás jelzését, az annak való ellenállást vagy az arra adott választ. Ez a kategória magában foglalja többek között a fizikai fizetési terminálokat, a kriptográfiai elemeket létrehozó és kezelő biztonsági hardvermodulokat, valamint a fenti leírásnak megfelelő menetíró készülékeket.
2. Az (EU) 2019/944 európai parlamenti és tanácsi irányelv ([1]) 2. cikkének 23. pontjában foglalt meghatározás szerinti okos mérési rendszereken belüli intelligens fogyasztásmérő átjárók (smart meter gateways), valamint a fejlett biztonsági célokra, többek között biztonságos kriptográfiára szolgáló egyéb biztonságos rejtjelező eszközök	Az intelligens fogyasztásmérő átjárók olyan, digitális elemeket tartalmazó termékek, amelyek ellenőrzik az (EU) 2019/944 irányelv 2. cikkének 23. pontjában meghatározott okos mérési rendszerek alkotóelemei és az engedélyezett harmadik felek, például közüzemi szolgáltatók közötti kommunikációt. Az intelligens fogyasztásmérő átjárók gyűjtik, feldolgozzák és tárolják a fogyasztásmérők adatait vagy a személyes adatokat, védik az adatokat és az információáramlást konkrét kriptográfiai igények – például az adatok titkosítása és dekódolása – támogatása révén, tűzfalfunkciókat foglalnak magukban, és eszközöket biztosítanak más eszközök vezérléséhez. Ez a kategória magában foglalja többek között az (EU) 2019/944 irányelv 2. cikkének 23. pontjában meghatározott, villamos energiát mérő intelligens fogyasztásmérő rendszerekhez kapcsolódó intelligens fogyasztásmérő átjárókat. Ide tartozhatnak az egyéb energiaforrások, például a gáz vagy a hő fogyasztását mérő, más intelligens fogyasztásmérő rendszerekben használt intelligens fogyasztásmérő átjárók is, feltéve, hogy az átjáró megfelel ennek a leírásnak.
3. Intelligens kártyák vagy hasonló eszközök, beleértve a biztonságos elemeket is	A biztonságos elemek olyan mikrovezérlők vagy mikroprocesszorok, amelyek biztonsági vonatkozású funkciókkal rendelkeznek, beleértve a manipulálás jelzését, az annak való ellenállást vagy az arra való reagálást. Jellemzően kriptográfiai műveleteket vagy érzékeny adatokat, például személyazonosító adatokat vagy fizetési hitelesítő adatokat tárolnak, dolgoznak fel vagy kezelnek. A biztonságos elemeket úgy alakították ki, hogy legalább az AVA_VAN.4 védelmét biztosítsák, a közös kritériumokban vagy a közös értékelési módszertanban meghatározottak szerint. Készülhetnek diszkrét szilíciumból vagy lehetnek egylapkás rendszerekbe (SoC) integrálhatók. A biztonságos elemek magukban foglalhatnak alkalmazási környezetet vagy operációs rendszert, és tartalmazhatnak egy vagy több alkalmazást is. Ebbe a kategóriába tartoznak többek között a megbízható platformmodulok (TPM-ek) és a beágyazott univerzális integrált áramköri kártyák (UICC).
	Az okoskártyák vagy hasonló eszközök kártya formájú hordozóanyagba, például műanyagba vagy fába beépített biztonságos elemek, vagy más formájú hordozóanyagokba beépített biztonságos elemek. Ebbe a kategóriába tartoznak többek között a személyazonosító és úti okmányok, a minősített aláírási kártyák, a cserélhető UICC-k, a fizikai fizetési kártyák, a fizikai belépőkártyák, a digitális tachográfkártyák vagy az integrált fizetésbiztonsági elemeket tartalmazó csuklópántok.

([1]) Az Európai Parlament és a Tanács (EU) 2019/944 irányelve (2019. június 5.) a villamos energia belső piacára vonatkozó közös szabályokról és a 2012/27/EU irányelv módosításáról (HL L 158., 2019.6.14., 125. o., ELI: http://data.europa.eu/eli/dir/2019/944/oj).