Úradný vestník
Európskej únie

SK
Séria L

2025/2392

1.12.2025

VYKONÁVACIE NARIADENIE KOMISIE (EÚ) 2025/2392

z 28. novembra 2025

o technickom opise kategórií dôležitých a kritických produktov s digitálnymi prvkami podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2024/2847

(Text s významom pre EHP)

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) ([1]), a najmä na jeho článok 7 ods. 4,

keďže:

(1) V nariadení (EÚ) 2024/2847 sa stanovujú pravidlá kybernetickej bezpečnosti pre produkty s digitálnymi prvkami. Konkrétne v prílohe III k uvedenému nariadeniu sa stanovujú kategórie dôležitých produktov s digitálnymi prvkami, na ktoré sa pri ich uvádzaní na trh vzťahujú postupy posudzovania zhody prísnejšie než postupy uplatniteľné pri iných produktoch s digitálnymi prvkami. V prílohe IV k nariadeniu (EÚ) 2024/2847 sa stanovujú kategórie kritických produktov s digitálnymi prvkami, pri ktorých by mohla pre výrobcov existovať povinnosť získať európsky certifikát kybernetickej bezpečnosti v rámci európskej schémy certifikácie kybernetickej bezpečnosti podľa nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 ([2]) alebo pri ktorých by pri ich uvádzaní na trh mohla existovať povinnosti zadať tretej strane vykonanie posudzovania zhody.

(2) Podľa článku 7 ods. 1 a článku 8 ods. 1 nariadenia (EÚ) 2024/2847 základná funkcia produktu s digitálnymi prvkami určuje, či predmetný produkt s digitálnymi prvkami spĺňa technický opis kategórie dôležitých alebo kritických produktov s digitálnymi prvkami, a teda uplatniteľné postupy posudzovania zhody.

(3) Výrobcovia pri vývoji produktu s digitálnymi prvkami v snahe o želaný súbor funkcií spravidla do svojich vlastných produktov s digitálnymi prvkami integrujú iné komponenty, ktoré sú takisto produktmi s digitálnymi prvkami a ktoré dokážu splniť technický opis kategórie dôležitého alebo kritického produktu. Podľa nariadenia (EÚ) 2024/2847 existuje v prípade produktu s digitálnymi prvkami povinnosť vykonať postup posudzovania zhody uplatniteľný pri dôležitých alebo kritických produktoch s digitálnymi prvkami, ak predmetný produkt ako celok je dôležitým alebo kritickým produktom v zmysle príloh III a IV k uvedenému nariadeniu. Napríklad integrovanie zabudovaného prehliadača ako komponentu spravodajskej aplikácie pre smartfóny ako také neznamená povinnosť vykonať pri danej spravodajskej aplikácii postup posudzovania zhody uplatniteľný na produkty s digitálnymi prvkami so základnou funkciou ako „samostatný a zabudovaný prehliadač“. Výrobca napriek tomu v súlade s nariadením (EÚ) 2024/2847 musí zaručiť, že produkt s digitálnymi prvkami ako celok spĺňa základné požiadavky kybernetickej bezpečnosti. Preto výrobca musí posúdiť bezpečnosť celkového produktu a podľa potreby zvážiť bezpečnosť komponentov alebo funkcií, ktoré sú v ňom integrované. Napríklad ak chce výrobca spravodajskej aplikácie preukázať, že jeho produkt s digitálnymi prvkami je v súlade s nariadením (EÚ) 2024/2847, musí preukázať, že spravodajská aplikácia ako celok spĺňa uplatniteľné požiadavky a podľa potreby zvážiť bezpečnosť zabudovaného prehliadača integrovaného v aplikácii.

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

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (Ú. v. EÚ L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(4) Skutočnosť, že produkt s digitálnymi prvkami vykonáva aj iné alebo dodatočné funkcie, a nie len funkcie rozvedené v technickom opise stanovenom v tomto nariadení, ako taká neznamená, že produkt s digitálnymi prvkami nemá základnú funkciu produktu kategórie stanovenej v prílohách III a IV k nariadeniu (EÚ) 2024/2847. Napríklad produkty s digitálnymi prvkami, ktoré majú základnú funkciu „operačných systémov“, často zahŕňajú softvér, ktorý vykonáva doplnkové funkcie, ktoré nefigurujú v technickom opise danej kategórie produktov, ako napríklad funkcie kalkulačky alebo jednoduchých grafických editorov. Produkty s digitálnymi prvkami takisto často zahŕňajú komponenty s funkciami iného dôležitého alebo kritického produktu s digitálnymi prvkami, ako sú operačné systémy s integrovanou funkciou prehliadača, alebo smerovače s integrovanou funkciou firewallu. Táto skutočnosť ako taká však neznamená, že dané produkty s digitálnymi prvkami nemajú základnú funkciu „operačných systémov“ alebo „smerovače, modemy určené na pripojenie k internetu a prepínače“.

(5) Na druhej strane sa pri produktoch s digitálnymi prvkami, ktoré dokážu vykonávať funkcie kategórie produktov stanovenej v prílohách III a IV k nariadeniu (EÚ) 2024/2847, ale ktorých samotná základná funkcia je iná než základná funkcia produktov danej kategórie, nevychádza z predpokladu, že spĺňajú technický opis predmetnej kategórie produktov. Napríklad softvér orchestrácie, automatizácie a odozvy zabezpečenia (SOAR) často dokáže vykonávať funkcie produktov s digitálnymi prvkami kategórie „systémy riadenia bezpečnostných informácií a udalostí (SIEM)“, t. j. zbierať údaje, analyzovať ich a poskytovať ich ako využiteľné informácie na bezpečnostné účely. Pretože však základnou funkciou softvéru SOAR nie je funkcia SIEM, nemá sa vo všeobecnosti vychádzať z predpokladu, že spĺňa technický opis „systémov riadenia bezpečnostných informácií a udalostí (SIEM)“. Podobne smartfóny spravidla zahŕňajú komponenty vykonávajúce funkcie viacerých kategórií produktov stanovených v prílohách III a IV k nariadeniu (EÚ) 2024/2847, napríklad funkcie ako operačný systém alebo integrovaný správca hesiel. Pretože však základnou funkciou smartfónov nie je funkcia operačného systému ani správcu hesiel, vo všeobecnosti sa nemá vychádzať z predpokladu, že spĺňajú technický opis predmetných kategórií produktov.

(6) Výrobcovia produktov s digitálnymi prvkami sú podľa článku 13 ods. 2 a 3 nariadenia (EÚ) 2024/2847 povinní vykonávať základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I k nariadeniu (EÚ) 2024/2847, a to spôsobom, ktorý je primeraný vzhľadom na riziká spojené s produktom s digitálnymi prvkami na základe zamýšľaného účelu a logicky predvídateľného používania, ako aj podmienok používania produktu s digitálnymi prvkami s ohľadom na dĺžku predpokladaného používania produktu. Výrobcovia sú podľa článku 13 ods. 2 a ods. 3 uvedeného nariadenia a bez ohľadu na to, či sa produkt s digitálnymi prvkami považuje za dôležitý alebo kritický produkt s digitálnymi prvkami, povinní vykonávať komplexné posúdenie kybernetickobezpečnostných rizík a uviesť, ako sa základné požiadavky kybernetickej bezpečnosti podľa údajov z posúdenia rizika vykonávajú vrátane ich testovania a zaručenia. Ak základná funkcia ich produktu s digitálnymi prvkami spĺňa technický opis dôležitého alebo kritického produktu s digitálnymi prvkami, výrobcovia musia preukázať súlad podľa konkrétnych postupov posudzovania zhody stanovených v článku 32 ods. 2, 3, 4 a 5 nariadenia (EÚ) 2024/2847.

(7) Toto nariadenie obsahuje príklady produktov s digitálnymi prvkami, ktorých základné funkcie spĺňajú technický opis určitých dôležitých alebo kritických produktov s digitálnymi prvkami. Príklady slúžia len na ilustráciu a nepredstavujú vyčerpávajúci zoznam.

(8) V snahe poskytnúť výrobcom právnu istotu by sa kategórie produktov s digitálnymi prvkami, ktoré sú mikroprocesormi odolnými proti neoprávnenej manipulácii, mikrokontrolérmi odolnými proti neoprávnenej manipulácii a kartami Smart card a podobnými zariadeniami vrátane bezpečnostných prvkov, mali rozlišovať na základe úrovne odolnosti proti možnému zneužitiu chýb alebo slabých stránok, so zreteľom na ktorú sú koncipované. Úroveň AVA_VAN je rozšírený a štandardizovaný spôsob vyjadrenia danej úrovne odolnosti. Úrovne AVA_VAN sú stanovené vo verejne dostupných normách spoločných kritérií a spoločnej metodiky hodnotenia, ktoré sú základom existujúcich certifikačných rámcov, ktoré sú na trhu vo všeobecnosti prijaté, ako je napríklad

vykonávacie nariadenie Komisie (EÚ) 2024/482 ([3]). Vo vykonávacom nariadení (EÚ) 2024/482 sa stanovuje európska schéma certifikácie kybernetickej bezpečnosti, ktorú možno použiť na certifikovanie produktu ako produktu s konkrétnym stupňom dôveryhodnosti. Vykonávacie nariadenie (EÚ) 2024/482 vychádza z celosvetovej praxe a stanovuje sa v ňom možnosť vydávať certifikáty na základe starších verzií noriem do konca roka 2027. Preto je v kontexte nariadenia (EÚ) 2024/2847 vhodné umožniť vyjadrovať úrovne AVA_VAN odkazom buď na aktuálnu, alebo staršie verzie daných noriem.

(9) Opatrenia stanovené v tomto nariadení sú v súlade so stanoviskom výboru zriadeného článkom 62 ods. 1 nariadenia (EÚ) 2024/2847,

PRIJALA TOTO NARIADENIE:

Článok 1

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1. „spoločné kritériá“ sú spoločné kritériá hodnotenia bezpečnosti informačných technológií, ako sa vymedzujú v článku 2 bode 1 vykonávacieho nariadenia (EU) 2024/482 alebo ako sa stanovujú v normách uvedených v článku 3 ods. 2 písm. a) a b) uvedeného vykonávacieho nariadenia;

2. „spoločná metodika hodnotenia“ je spoločná metodika hodnotenia bezpečnosti informačných technológií, ako sa vymedzuje v článku 2 bode 2 vykonávacieho nariadenia (EU) 2024/482 alebo ako sa stanovuje v normách uvedených v článku 3 ods. 2 písm. c) a d) uvedeného vykonávacieho nariadenia.

Článok 2

1. Technický opis kategórií produktov s digitálnymi prvkami uvedených v triedach I a II v prílohe III k nariadeniu (EÚ) 2024/2847 je opis stanovený v prílohe I k tomuto nariadeniu.

2. Technický opis kategórií produktov s digitálnymi prvkami uvedených v prílohe IV k nariadeniu (EÚ) 2024/2847 je opis stanovený v prílohe II k tomuto nariadeniu.

Článok 3

Toto nariadenie nadobúda účinnosť dvadsiatym dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli 28. novembra 2025

Za Komisiu
predsedníčka
Ursula VON DER LEYEN

([3]) Vykonávacie nariadenie Komisie (EÚ) 2024/482 z 31. januára 2024, ktorým sa stanovujú pravidlá uplatňovania nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881, pokiaľ ide o prijatie európskej schémy certifikácie kybernetickej bezpečnosti založenej na spoločných kritériách (EUCC) (Ú. v. EÚ L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

PRÍLOHA I

DÔLEŽITÉ PRODUKTY S DIGITÁLNYMI PRVKAMI

Trieda I

Kategória produktu	Technický opis
1. Systémy správy identifikačných údajov a softvér a hardvér na správu privilegovaného prístupu vrátane čítačiek na autentifikáciu a kontrolu prístupu vrátane biometrických čítačiek	Systémy správy identifikačných údajov sú produkty s digitálnymi prvkami, ktoré poskytujú mechanizmy na autentifikáciu alebo autorizáciu a ktoré takisto môžu poskytovať mechanizmy na riadenie životného cyklu potvrdzovania identifikačných údajov fyzických osôb, právnických osôb, zariadení alebo systémov, ako je registrácia identity, jej poskytovanie, udržiavanie a zrušenie jej registrácie. Tieto systémy zahŕňajú systémy riadenia prístupu na kontrolu prístupu fyzických osôb, právnických osôb, zariadení alebo systémov k digitálnym zdrojom alebo fyzickým lokalitám. Softvér riadenia privilegovaného prístupu je systém riadenia prístupu na kontrolu a monitorovanie prístupových práv k systémom IT alebo OT a citlivým informáciám v organizácii vrátane systémov na vynucovanie politík diferencovanej kontroly prístupu pre privilegovaných používateľov. Táto kategória zahŕňa okrem iného čítačky na autentifikáciu a kontrolu prístupu, biometrické čítačky, softvér na jediné prihlásenie, federovaný softvér na správu identifikačných údajov, softvér na jednorazové heslá, zariadenia na autentifikáciu hardvéru, ako sú generátory čísel autentifikácie transakcie (transaction authentication number – TAN), softvér na autentifikáciu a softvér na viacfaktorovú autentifikáciu.
2. Samostatné a zabudované prehliadače	Softvérové produkty s digitálnymi prvkami, ktoré umožňujú koncovým používateľom prístup k webovému obsahu a službám na serveroch, ktoré sú pripojené k sieťam, ako je internet, ich vykreslenie a interakciu s nimi. Spravidla zahŕňajú vykresľovacie jadro, ktoré načíta a zobrazí obsah zapísaný v značkovacom jazyku (napr. HTML), podporu pre webové protokoly (HTTP, HTTPS), schopnosť vykonávať skripty a riadiť vstupy používateľov, ako aj ukladanie dočasných alebo trvalých údajov z webových lokalít (súbory cookie). Táto kategória zahŕňa okrem iného samostatné aplikácie, ktoré spĺňajú funkcie prehliadačov, zabudovaných prehliadačov určených na integrovanie do iného systému alebo aplikácie, ako aj prehliadačov s integrovanými AI agentmi.
3. Správcovia hesiel	Produkty s digitálnymi prvkami, ktoré uchovávajú heslá miestne v zariadení alebo na vzdialenom serveri vrátane úkonov, ako je generácia hesiel, ako aj zdieľanie hesiel a ich integrácia do miestnych aplikácií alebo aplikácií tretích strán na používanie hesiel. Táto kategória okrem iného zahŕňa miestnych správcov hesiel, správcov hesiel poskytovaných ako rozšírenie prehliadača, podnikových správcov hesiel, ako aj správcov hesiel založených na hardvéri.

Kategória produktu	Technický opis
4. Softvér na vyhľadávanie, odstraňovanie alebo uzatváranie škodlivého softvéru do karantény	Softvérové produkty s digitálnymi prvkami spravidla nazývané antivírus alebo antimalvér, ktoré odhaľujú alebo vyhľadávajú škodlivý softvér alebo kódy v zariadeniach alebo taký softvér alebo kódy odstraňujú alebo umiestňujú do karantény, aby sa zachovala integrita, dôvernosť alebo dostupnosť predmetných zariadení. V kontexte tejto kategórie produktov škodlivý softvér znamená softvér obsahujúci škodlivé funkcie alebo podmienky, ktoré môžu spôsobiť škody priamo alebo nepriamo používateľovi a/alebo v počítačovom systéme, ako sú napríklad vírusy, červy, ransomvér, špionážny softvér a trójske kone. Táto kategória okrem iného zahŕňa softvér na odhaľovanie alebo vyhľadávanie škodlivého softvéru v reálnom čase alebo manuálne, odhaľovanie rootkitu a záchranné disky so základnou funkciou vyhľadávať škodlivý softvér, odstraňovať ho alebo umiestňovať ho do karantény.
5. Produkty s digitálnymi prvkami s funkciou virtuálnej neverejnej siete (VPN)	Produkty s digitálnymi prvkami, ktoré vytvárajú zašifrovaný logický tunel vybudovaný zo systémových zdrojov fyzickej alebo virtuálnej siete. Táto kategória okrem iného zahŕňa klientov, servery a brány virtuálnych súkromných sietí.
6. Systémy správy sietí	Produkty s digitálnymi prvkami, ktoré riadia spojené prvky sietí, ako sú servery, smerovače, prepínače, pracovné stanice, tlačiarne alebo mobilné zariadenia, prostredníctvom ich monitorovania a regulovania ich sieťových operácií a konfigurácie. Táto kategória okrem iného zahŕňa systémy riadenia medzi koncovými bodmi a špecializované systémy riadenia konfigurácie, ako sú kontroléry softvérovo definovaných sietí.
7. Systémy riadenia bezpečnostných informácií a udalostí (SIEM)	Produkty s digitálnymi prvkami, ktoré zbierajú údaje z viacerých zdrojov, predmetné údaje analyzujú a korelujú a sprístupňujú ako použiteľné informácie na účely súvisiace s bezpečnosťou, ako je odhaľovanie hrozieb a incidentov, forenzná analýza alebo účely dosahovania súladu s predpismi.
8. Správcovia spúšťania	Softvérové produkty s digitálnymi prvkami, ktoré riadia proces prvotného spustenia systému po zapnutí/reštartovaní prostredníctvom inicializácie hardvéru, načítania alebo prenesenia riadenia do prostredia operačného systému alebo na systémové prostriedky a výberom možností spustenia. Táto kategória okrem iného zahŕňa firmvér UEFI, jednostupňové a viacstupňové zavádzače systému.
9. Infraštruktúra verejných kľúčov a softvér na vytváranie elektronických certifikátov	Produkty s digitálnymi prvkami používané ako súčasť infraštruktúry verejného kľúča (PKI), ktoré riadia validáciu, vytváranie, vydávanie, distribúciu, obnovenie, zrušenie digitálnych certifikátov a uverejňovanie ich stavu alebo generovanie, ukladanie, uschovanie, výmenu, zničenie alebo rotáciu kryptografických kľúčov súvisiacich s predmetnými digitálnymi certifikátmi. Táto kategória okrem iného zahŕňa kľúčové systémy riadenia, systémy riadenia digitálnych certifikátov, odpovedače protokolu OCSP (Online Certificate Status Protocol) a riešenia PKI typu všetko v jednom.

Kategória produktu	Technický opis
10. Fyzické a virtuálne sieťové rozhrania	Fyzické sieťové rozhrania sú produkty s digitálnymi prvkami, ktoré priamo spájajú zariadenie so sieťou prostredníctvom aplikačného programovacieho rozhrania (API) poskytovaného ovládačmi rozhrania spravidla fungujúcimi na vrstve dátového spoja, a ktoré sú vybavené hardvérovými adaptérmi na prenosové médiá so zodpovedajúcim firmvérom spravidla fungujúcim na fyzickej vrstve a vrstve dátového spoja. Virtuálne sieťové rozhrania sú produkty s digitálnymi prvkami, ktoré priamo alebo nepriamo spájajú zariadenie so sieťou prostredníctvom API, ktoré emuluje API ovládačov fyzického sieťového rozhrania spravidla fungujúcich na vrstve dátového spoja. Táto kategória okrem iného zahŕňa drôtové a bezdrôtové karty sieťového rozhrania, ovládače a adaptéry napr. na RLAN, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee alebo Fieldbus, ako aj úplne virtuálne samostatné produkty, ako sú virtuálne karty sieťového rozhrania, rozhrania CNI (Container Network Interface) a rozhrania VPN.
11. Operačné systémy	Softvérové produkty s digitálnymi prvkami, ktoré poskytujú abstraktné rozhranie príslušného hardvéru a ovládajú vykonávanie softvéru a ktoré môžu poskytovať služby ako riadenie a konfiguráciu výpočtového zdroja, plánovanie, riadenie vstupov a výstupov, správu údajov a poskytovanie rozhrania, prostredníctvom ktorého aplikácie interagujú so systémovými zdrojmi a periférnymi zariadeniami. Táto kategória okrem iného zahŕňa operačné systémy v reálnom čase, operačné systémy na všeobecné účely a operačné systémy na špeciálne účely.
12. Smerovače, modemy určené na pripojenie k internetu a prepínače	Smerovače sú produkty s digitálnymi prvkami, ktoré vytvárajú a ovládajú tok údajov medzi rôznymi sieťami tak, že vyberajú cesty alebo trasy pomocou mechanizmov a algoritmov smerovacích protokolov, a ktoré spravidla fungujú na sieťovej vrstve. Táto kategória okrem iného zahŕňa drôtové a bezdrôtové smerovače, virtuálne smerovače a smerovače s modemami alebo bez nich.
	Modemy určené na pripojenie k internetu sú hardvérové produkty s digitálnymi prvkami, ktoré využívajú techniky digitálnej modulácie a demodulácie na premenu analógových signálov z digitálnych signálov a naopak na komunikáciu založenú na IP. Táto kategória okrem iného zahŕňa optické modemy, DSL modemy, káblové modemy (DOCSIS), satelitné modemy a celulárne modemy.
	Prepínače sú produkty s digitálnymi prvkami, ktoré poskytujú prepojenie medzi zosieťovanými zariadeniami prostredníctvom mechanizmov presmerovania a ktoré majú rovinu manažmentu, spravidla sa vykonávajú na vrstve dátového spoja alebo sieťovej vrstve. Táto kategória okrem iného zahŕňa riadené prepínače, inteligentné prepínače, viacvrstvové prepínače, virtuálne bezpečnostné prepínače, programovateľné prepínače pre softvérovo definované siete a mosty, ako sú bezdrôtové prístupové body.

Kategória produktu	Technický opis
13. Mikroprocesory s bezpečnostnými funkciami	Produkty s digitálnymi prvkami, ktoré sú integrovanými obvodmi vykonávajúcimi centrálne funkcie procesora založené na externej pamäti a periférnych zariadeniach vrátane mikrokódu a iného nízkoúrovňového firmvéru. Navyše poskytujú funkcie súvisiace s bezpečnosťou, ako je šifrovanie, autentifikácia, uchovávanie bezpečnostného kľúča, generácia náhodných čísel, dôveryhodné vykonávacie prostredie alebo iné ochranné mechanizmy založené na hardvéri, ktorých účelom je zabezpečiť iné produkty, siete alebo služby presahujúce samotný mikroprocesor, ako napríklad zabezpečené poradie spúšťania systému, virtualizácia alebo zabezpečené komunikačné rozhrania.
14. Mikroradiče s bezpečnostnými funkciami	Produkty s digitálnymi prvkami, ktoré sú integrovanými obvodmi vykonávajúcimi základné procesné funkcie integrujúce pamäť, čo umožňuje programovateľnosť mikroradiča (mikrokontroléru) a spravidla aj periférnych zariadení vrátane mikrokódu a iného nízkoúrovňového firmvéru. Navyše poskytujú funkcie súvisiace s bezpečnosťou, ako je šifrovanie, autentifikácia, uchovávanie bezpečnostného kľúča, generácia náhodných čísel, dôveryhodné vykonávacie prostredie alebo iné ochranné mechanizmy založené na hardvéri, ktorých účelom je zabezpečiť iné produkty, siete alebo služby presahujúce samotný mikroradič (mikrokontrolér), ako napríklad zabezpečené poradie spúšťania systému, virtualizácia alebo zabezpečené komunikačné rozhrania.
15. Integrované obvody pre konkrétne aplikácie (ASIC) a logické hradlá programovateľné po výrobe (FPGA) s bezpečnostnými funkciami	Integrované obvody pre konkrétne aplikácie (ASIC) s bezpečnostnými funkciami sú produkty s digitálnymi prvkami, ktoré sú integrovanými obvodmi, ktoré sú úplne alebo čiastočne koncipované na plnenie konkrétnej funkcie alebo vykonávanie konkrétnej aplikácie vrátane mikrokódu a iného nízkoúrovňového firmvéru. Navyše poskytujú funkcie súvisiace s bezpečnosťou, ako je šifrovanie, autentifikácia, uchovávanie bezpečnostného kľúča, generácia náhodných čísel, dôveryhodné vykonávacie prostredie alebo iné ochranné mechanizmy založené na hardvéri, ktorých účelom je zabezpečiť iné produkty, siete alebo služby presahujúce samotný ASIC, ako napríklad zabezpečené poradie spúšťania systému, virtualizácia alebo zabezpečené komunikačné rozhrania.
	Logické hradlá programovateľné po výrobe (FPGA) s bezpečnostnými funkciami sú produkty s digitálnymi prvkami, ktoré sú integrovanými obvodmi, ktoré sa vyznačujú maticou konfigurovateľných logických blokov koncipovaných tak, aby boli po výrobe preprogramovateľné na plnenie konkrétnej funkcie alebo vykonávanie konkrétnej aplikácie vrátane mikrokódu a iného nízkoúrovňového firmvéru. Navyše poskytujú funkcie súvisiace s bezpečnosťou, ako je šifrovanie, autentifikácia, uchovávanie bezpečnostného kľúča, generácia náhodných čísel, dôveryhodné vykonávacie prostredie alebo iné ochranné mechanizmy založené na hardvéri, ktorých účelom je zabezpečiť iné produkty, siete alebo služby presahujúce samotné FPGA, ako napríklad zabezpečené poradie spúšťania systému, virtualizácia alebo zabezpečené komunikačné rozhrania.
16. Virtuálni asistenti pre inteligentné domácnosti na všeobecné účely	Produkty s digitálnymi prvkami, ktoré priamo alebo pomocou iného zariadenia komunikujú na verejnom internete a ktoré spracúvajú pokyny, úlohy alebo otázky na základe príkazov v prirodzenom jazyku (napríklad prostredníctvom audio vstupov alebo písaných vstupov) a ktoré na základe daných pokynov, úloh alebo otázok poskytujú prístup k iným službám alebo ovládajú funkcie pripojených zariadení v obytných priestoroch. Táto kategória okrem iného zahŕňa inteligentné reproduktory s integrovaným virtuálnym asistentom a samostatných virtuálnych asistentov, ktorí spĺňajú tento opis.

Kategória produktu	Technický opis
17. Produkty pre inteligentné domácnosti s bezpečnostnými funkciami vrátane inteligentných zámkov dverí, bezpečnostných kamier, systémov na monitorovanie detí a poplašných systémov	Produkty s digitálnymi prvkami, ktoré chránia fyzickú bezpečnosť spotrebiteľov v obytných budovách a ktoré možno ovládať alebo riadiť na diaľku z iných systémov, ako aj hardvér a softvér, ktoré takéto produkty ovládajú centrálne. Táto kategória okrem iného zahŕňa inteligentné zariadenia na zamykanie dverí, systémy na monitorovanie bábätiek, poplašné systémy a domáce bezpečnostné kamery.
18. Hračky pripojené na internet, na ktoré sa vzťahuje smernica Európskeho parlamentu a Rady 2009/48/ES ([1]) s funkciami na spoločenskú interakciu (napr. hovorenie alebo filmovanie) alebo s funkciami sledovania polohy.	Hračky pripojené na internet s funkciami na spoločenskú interakciu sú produktmi s digitálnymi prvkami, na ktoré sa vzťahuje smernica 2009/48/ES, ktoré priamo alebo pomocou iného zariadenia komunikujú na verejnom internete a ktoré majú zabudované technológie umožňujúce prichádzajúcu aj odchádzajúcu komunikáciu, ako sú klávesnice, mikrofóny, reproduktory alebo kamery.
	Hračky pripojené na internet s funkciami na sledovanie polohy sú produktmi s digitálnymi prvkami, na ktoré sa vzťahuje smernica 2009/48/ES, ktoré priamo alebo pomocou iného zariadenia komunikujú na verejnom internete a ktoré majú technológie umožňujúce sledovanie alebo vyvodenie zemepisnej polohy hračky alebo jej používateľa. Ak hračka pomocou snímacích technológií dokáže len zistiť blízkosť používateľa alebo iných hračiek, nepovažuje sa za hračku s funkciou na sledovanie polohy.
19. Produkty, ktoré sa majú nosiť alebo byť umiestnené na ľudskom tele na účely zdravotného monitorovania (napríklad sledovanie) a na ktoré sa nevzťahuje nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 ([2]) ani (EÚ) 2017/746 ([3]), alebo produkty na nosenie na tele určené na použitie deťmi a pre deti	Osobné produkty, ktoré sa majú nosiť alebo byť umiestnené na ľudskom tele a ktoré slúžia na účely monitorovania zdravotného stavu, sú produktmi s digitálnymi prvkami, ktoré sa nosia priamo na tele alebo na oblečení alebo doplnkoch a ktoré dokážu pravidelne alebo neprerušene snímať a ďalej spracúvať informácie (vrátane metriky tela) relevantné pre zdravie používateľa, s výnimkou produktov patriacich do rozsahu pôsobnosti nariadenia (EÚ) 2017/745 alebo nariadenia (EÚ) 2017/746. Táto kategória okrem iného zahŕňa zariadenia na sledovanie fyzickej kondície, inteligentné hodinky, inteligentné šperky, inteligentné odevy a športové oblečenie, ktoré spĺňajú tento opis.
	Osobné produkty, ktoré sa majú nosiť alebo byť umiestnené na ľudskom tele, určené pre deti sú produkty s digitálnymi prvkami, ktoré možno nosiť na tele alebo umiestniť priamo na telo alebo na oblečenie alebo doplnky, pre osoby mladšie ako 14 rokov. Táto kategória okrem iného zahŕňa detské bezpečnostné produkty, ktoré sa majú nosiť alebo byť umiestnené na ľudskom tele.

([1]) Smernica Európskeho parlamentu a Rady 2009/48/ES z 18. júna 2009 o bezpečnosti hračiek (Ú. v. EÚ L 170, 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS (Ú. v. EÚ L 117, 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach *in vitro* a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ (Ú. v. EÚ L 117, 5.5.2017, s. 176, ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Trieda II

Kategória produktu	Technický opis
1. Hypervízory a kontajnerové systémy režimu runtime, ktoré podporujú virtualizované spúšťanie operačných systémov a podobných prostredí	Hypervízory sú softvérové produkty s digitálnymi prvkami, ktoré odoberajú a/alebo prideľujú výpočtové zdroje a umožňujú vykonávanie, riadenie alebo organizovanie virtuálnych strojov, ktoré sú od seba a/alebo od fyzického hardvéru logicky oddelené. Hypervízory môžu fungovať priamo na hardvéri (čistý počítač), na operačnom systéme alebo v rámci iného virtuálneho stroja (vnorená virtualizácia). V kontexte tejto kategórie produktov je virtuálny stroj softvérovo definované logické oddelenie výpočtového prostredia, ktoré zahŕňa virtualizovaný súbor hardvérových zdrojov (napr. centrálna procesorová jednotka, pamäť, ukladací priestor, rozhrania siete) a spravidla je hostiteľom svojho vlastného operačného systému. Táto kategória okrem iného zahŕňa hypervízory typu 1 (čistý počítač), typu 2 (fungujúci na hostiteľskom operačnom systéme) a hybridné hypervízory.
	Kontajnerové systémy režimu runtime sú softvérové produkty s digitálnymi prvkami, ktoré riadia vykonávanie a životný cyklus kontajnerov fungujúcich na jedinom hostiteľskom operačnom systéme ako izolované procesy a ktoré prideľujú zdroje a umožňujú riadenie a organizovanie jednotlivých kontajnerov. V kontexte tejto kategórie produktov je kontajner vykonávacie prostredie založené na softvéri, ktoré združuje jeden alebo viacero softvérových komponentov a ich závislostí v jednom balíku, čo umožňuje jeho nezávislé a konzistentné fungovanie.
2. Brány firewall, systémy na detekciu a prevenciu narušení	Brány firewall sú produkty s digitálnymi prvkami, ktoré chránia pripojenú sieť alebo systém pred neoprávneným prístupom na základe monitorovania a obmedzovania prenosu dátovej komunikácie z danej siete alebo do nej. Táto kategória okrem iného zahŕňa brány firewall pre siete a aplikácie, ako sú brány firewall pre webové aplikácie alebo filtre a brány proti nevyžiadanej pošte.
	Systémy na detekciu narušení sú produkty s digitálnymi prvkami, ktoré pri prenose v sieti monitorujú podozrivú aktivitu a detegujú alebo identifikujú pokusy o narušenie (neoprávnené vniknutie), či k nemu aktuálne nedochádza alebo k nemu nedošlo v pripojenej sieti alebo systéme. Táto kategória okrem iného zahŕňa systémy na detekciu narušení založené na sieti a systémy na detekciu narušení založené na hostiteľovi.
	Systémy na prevenciu narušení sú produkty s digitálnymi prvkami, ktoré tvorí systém na detekciu narušení, ktorý na narušenie pripojenej siete alebo systému aktívne reaguje. Táto kategória okrem iného zahŕňa systémy na prevenciu narušení založené na sieti a systémy na prevenciu narušení založené na hostiteľovi.

Kategória produktu	Technický opis
3. Mikroprocesory odolné proti neoprávnenej manipulácii	Produkty s digitálnymi prvkami, ktoré sú mikroprocesormi s bezpečnostnými funkciami uvedenými v tabuľke Trieda I bode 13 tejto prílohy vrátane dôkazov o neoprávnenej manipulácii, odolnosti alebo reakcie a ktoré sú navyše koncipované tak, aby poskytovali ochranu AVA_VAN úrovne 2 alebo 3, ako sa stanovuje v spoločných kritériách a spoločnej metodike hodnotenia.
4. Mikroovládače odolné proti neoprávnenej manipulácii	Produkty s digitálnymi prvkami, ktoré sú mikroovládačmi (mikrokontrolérmi) s bezpečnostnými funkciami uvedenými v tabuľke Trieda I bode 14 tejto prílohy vrátane dôkazov o neoprávnenej manipulácii, odolnosti alebo reakcie a ktoré sú navyše koncipované tak, aby poskytovali ochranu AVA_VAN úrovne 2 alebo 3, ako sa stanovuje v spoločných kritériách a spoločnej metodike hodnotenia.

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

PRÍLOHA II

KRITICKÉ PRODUKTY S DIGITÁLNYMI PRVKAMI

Kategória produktu	Technický opis
1. Hardvérové zariadenia s bezpečnostnými schránkami	Hardvérové produkty s digitálnymi prvkami, ktoré bezpečne uchovávajú, spracúvajú alebo spravujú citlivé údaje alebo vykonávajú kryptografické operácie a ktoré pozostávajú z viacerých samostatných komponentov vrátane hardvérového fyzického obalu, ktorý zabezpečuje dôkazy o neoprávnenej manipulácii, odolnosť alebo reakciu ako protiopatrenia proti fyzickým útokom. Táto kategória okrem iného zahŕňa fyzické platobné terminály, hardvérové bezpečnostné moduly, ktoré generujú a riadia kryptografické prvky, a tachografy, ktoré spĺňajú uvedený opis.
2. Prístroje smart meter gateway v inteligentných meracích systémoch vymedzených v článku 2 bode 23 smernice Európskeho parlamentu a Rady (EÚ) 2019/944 ([1]) a iné zariadenia na vyššie bezpečnostné účely vrátane bezpečného kryptografického spracovania.	Prístroje smart meter gateway sú produkty s digitálnymi prvkami, ktoré riadia komunikáciu medzi komponentmi v pripojených alebo inteligentných meracích systémoch, ako sú vymedzené v článku 2 bode 23 smernice (EÚ) 2019/944, a autorizovanými tretími stranami, napríklad poskytovateľmi verejných služieb. Prístroje smart meter gateway zbierajú, spracúvajú a uchovávajú údaje z merania alebo osobné údaje, chránia údaje a informačné toky prostredníctvom podpory osobitných kryptografických potrieb, napríklad šifrovania a dešifrovania údajov, sú v nich zabudované funkcie firewall a poskytujú prostriedky na ovládanie iných zariadení. Táto kategória zahŕňa okrem iného prístroje smart meter gateway súvisiace s inteligentnými meracími systémami merajúcimi elektrinu, ako sú vymedzené v článku 2 bode 23 smernice (EÚ) 2019/944. Takisto môže zahŕňať prístroje smart meter gateway používané v iných inteligentných meracích systémoch merajúcich spotrebu iných zdrojov energie (napr. plynu alebo tepla) za predpokladu, že prístroj spĺňa tento opis.
3. Čipové karty alebo podobné zariadenia s bezpečnostnými prvkami	Bezpečnostné prvky sú mikroradiče (mikrokontroléry) alebo mikroprocesory s bezpečnostnými funkciami vrátane dôkazov o neoprávnenej manipulácii, odolnosti alebo reakcie. Spravidla uchovávajú, spracúvajú alebo riadia kryptografické operácie alebo citlivé údaje, ako sú potvrdenia totožnosti alebo potvrdenia platieb. Úlohou bezpečnostných prvkov je poskytovať ochranu minimálne AVA_VAN úrovne 4, ako sa stanovuje v spoločných kritériách a spoločnej metodike hodnotenia. Môže ísť o diskrétny čip alebo môžu byť integrované do systémov na čipe (SOC). V bezpečnostných prvkoch môže byť zahrnuté prostredie aplikácie alebo operačný systém a takisto môžu zahŕňať jednu alebo viaceré aplikácie. Táto kategória zahŕňa okrem iného moduly dôveryhodnej platformy (TPM) a zabudované univerzálne karty s integrovaným obvodom (UICC).
	Karty Smart card alebo podobné zariadenia sú bezpečnostné prvky integrované do nosného materiálu (napr. plast alebo drevo) v tvare karty alebo bezpečnostné prvky integrované v nosnom materiáli v inom tvare. Táto kategória zahŕňa okrem iného preukazy totožnosti a cestovné doklady, karty na kvalifikované podpisy, nahraditeľné karty UICC, fyzické platobné karty, fyzické prístupové karty, digitálne tachografové karty alebo náramky s integrovanými bezpečnostnými prvkami na platbu.

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2019/944 z 5. júna 2019 o spoločných pravidlách pre vnútorný trh s elektrinou a o zmene smernice 2012/27/EÚ (Ú. v. EÚ L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).