2025/2392

1.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2392

ze dne 28. listopadu 2025

o technickém popisu kategorií důležitých a kritických produktů s digitálními prvky podle nařízení Evropského parlamentu a Rady (EU) 2024/2847

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Evropského parlamentu a Rady (EU) 2024/2847 ze dne 23. října 2024 o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) č. 168/2013 a (EU) 2019/1020 a směrnice (EU) 2020/1828 (akt o kybernetické odolnosti) ([1]), a zejména na čl. 7 odst. 4 uvedeného nařízení,

vzhledem k těmto důvodům:

(1) Nařízení (EU) 2024/2847 stanoví pravidla kybernetické bezpečnosti pro produkty s digitálními prvky. Konkrétně příloha III uvedeného nařízení stanoví kategorie důležitých produktů s digitálními prvky, které při uvedení na trh podléhají postupům posuzování shody, které jsou přísnější než postupy platné pro jiné produkty s digitálními prvky. Příloha IV nařízení (EU) 2024/2847 stanoví kategorie kritických produktů s digitálními prvky, u nichž by výrobci mohli mít povinnost získat evropský certifikát kybernetické bezpečnosti v rámci evropského systému certifikace kybernetické bezpečnosti podle nařízení Evropského parlamentu a Rady (EU) 2019/881 ([2]) nebo které by při uvedení na trh podléhaly povinnému posouzení shody třetí stranou.

(2) Podle čl. 7 odst. 1 a čl. 8 odst. 1 nařízení (EU) 2024/2847 klíčová funkce produktu s digitálními prvky určuje, zda tento produkt s digitálními prvky splňuje technický popis kategorie důležitých nebo kritických produktů s digitálními prvky, a tudíž použitelné postupy posuzování shody.

(3) Při vývoji produktu s digitálními prvky a za účelem dosažení požadovaného souboru funkcí výrobci obvykle integrují do svých vlastních produktů s digitálními prvky další složky, které jsou rovněž produkty s digitálními prvky a které mohou splňovat technický popis kategorie důležitých nebo kritických produktů. Podle nařízení (EU) 2024/2847 podléhá produkt s digitálními prvky postupům posuzování shody použitelným na důležité nebo kritické produkty s digitálními prvky, pokud je tento produkt jako celek důležitým nebo kritickým produktem, jak je stanoveno v přílohách III a IV uvedeného nařízení. Například integrace vestavěného prohlížeče jako součásti zpravodajské aplikace pro použití v chytrých telefonech sama o sobě neznamená, že se na zpravodajskou aplikaci vztahuje postup posuzování shody použitelný na produkty s digitálními prvky, které mají klíčovou funkci „samostatných a vestavěných prohlížečů“. V souladu s nařízením (EU) 2024/2847 však musí výrobce zajistit, aby produkt s digitálními prvky jako celek splňoval základní požadavky na kybernetickou bezpečnost. Výrobce proto musí vyhodnotit bezpečnost celého výrobku a případně zvážit bezpečnost součástí nebo funkcí, které jsou do něj začleněny. Aby například výrobce zpravodajské aplikace prokázal, že jeho produkt s digitálními prvky je v souladu s nařízením (EU) 2024/2847, musí prokázat, že zpravodajská aplikace jako celek splňuje příslušné požadavky, případně s ohledem na bezpečnost vestavěného prohlížeče, který je do jeho aplikace začleněn.

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

([2]) Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

(4) Skutečnost, že produkt s digitálními prvky vykonává i jiné funkce než ty, které jsou podrobně popsány v technických popisech stanovených v tomto nařízení, případně doplňující funkce, sama o sobě neznamená, že produkt s digitálními prvky nemá klíčovou funkci některé kategorie produktů stanovené v přílohách III a IV nařízení (EU) 2024/2847. Například produkty s digitálními prvky, které mají klíčovou funkci jako „operační systémy“, často zahrnují software, který vykonává pomocné funkce, které nejsou zahrnuty v technickém popisu této produktové kategorie, jako jsou kalkulátory nebo jednoduché grafické editory. Produkty s digitálními prvky často obsahují také součásti, které mají funkčnost jiného důležitého nebo kritického produktu s digitálními prvky, jako je operační systém integrující funkci prohlížeče nebo router integrující funkci firewallu. To však samo o sobě neznamená, že takové produkty s digitálními prvky nemají klíčovou funkci jako „operační systémy“ nebo „směrovače, modemy určené pro připojení k internetu a přepínače“.

(5) Na druhé straně produkt s digitálními prvky, který je schopen vykonávat funkce některé kategorie produktů stanovené v přílohách III a IV nařízení (EU) 2024/2847, ale jehož klíčová funkce se sama o sobě liší od funkce této kategorie produktů, se nepovažuje za produkt splňující technický popis této kategorie produktů. Například software pro orchestraci, automatizaci a reakci v oblasti bezpečnosti (SOAR) je často schopen plnit funkce produktů s digitálními prvky v kategorii „systémy řízení bezpečnostních informací a událostí (SIEM)“, tj. shromažďovat údaje, analyzovat je a prezentovat je jako využitelné informace pro bezpečnostní účely. Jelikož však jeho klíčová funkce není funkcí SIEM, nelze mít obecně za to, že software SOAR splňuje technický popis „systémů řízení bezpečnostních informací a událostí (SIEM)“. Podobně chytrý telefon obvykle integruje součásti, které plní funkce několika kategorií produktů stanovených v přílohách III a IV nařízení (EU) 2024/2847, jako je operační systém nebo integrovaný správce hesel. Jelikož však klíčová funkce chytrého telefonu není funkce operačního systému nebo správce hesla, nelze mít obecně za to, že splňuje technický popis těchto kategorií produktů.

(6) Podle čl. 13 odst. 2 a 3 nařízení (EU) 2024/2847 mají výrobci produktů s digitálními prvky uplatňovat základní požadavky na kybernetickou bezpečnost stanovené v části I přílohy I nařízení (EU) 2024/2847 způsobem, který je přiměřený rizikům produktu s digitálními prvky na základě zamýšleného účelu a rozumně předvídatelného použití, jakož i podmínek použití produktu s digitálními prvky, s přihlédnutím k době, po kterou se očekává, že bude produkt používán. V souladu s čl. 13 odst. 2 a 3 uvedeného nařízení a bez ohledu na to, zda je produkt s digitálními prvky považován za důležitý nebo kritický produkt s digitálními prvky, mají výrobci provést komplexní posouzení kybernetických bezpečnostních rizik a uvést, jak jsou základní požadavky na kybernetickou bezpečnost uplatňovány na základě posouzení rizik, včetně jejich testování a záruky. Pokud klíčová funkce jejich produktu s digitálními prvky splňuje technický popis důležitého nebo kritického produktu s digitálními prvky, musí výrobci prokázat shodu zvláštními postupy posuzování shody stanovenými v čl. 32 odst. 2, 3, 4 a 5 nařízení (EU) 2024/2847.

(7) Toto nařízení obsahuje příklady produktů s digitálními prvky, jejichž klíčová funkce splňuje technický popis určitých důležitých nebo kritických produktů s digitálními prvky. Tyto příklady jsou uvedeny pouze pro ilustraci a nejsou vyčerpávajícím výčtem.

(8) Aby byla výrobcům poskytnuta právní jistota, měly by být rozlišeny kategorie produktů s digitálními prvky, jimiž jsou mikroprocesory odolné proti nedovolené manipulaci, mikrořadiče odolné proti nedovolené manipulaci a čipové karty a podobná zařízení, včetně zabezpečených prvků, na základě úrovně odolnosti proti potenciální využitelnosti nedostatků nebo slabých stránek, s přihlédnutím k účelu, pro který jsou navrženy. Úroveň AVA_VAN je široce používaný a standardizovaný způsob vyjádření takové úrovně odolnosti. Úrovně AVA_VAN jsou stanoveny ve veřejně dostupných společných kritériích a společných normách pro metodiku hodnocení, které jsou základem stávajících certifikačních rámců široce přijímaných na trhu, jako je prováděcí nařízení Komise (EU) 2024/482 ([3]).

([3]) Prováděcí nařízení Komise (EU) 2024/482 ze dne 31. ledna 2024, kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o přijetí evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC) (Úř. věst. L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

Prováděcí nařízení (EU) 2024/482 zavádí evropské schéma certifikace kybernetické bezpečnosti, které lze použít k certifikaci produktu na konkrétní úrovni záruky. Na základě celosvětových postupů stanoví prováděcí nařízení (EU) 2024/482 možnost vydávat certifikáty na základě starších verzí norem do konce roku 2027. V souvislosti s nařízením (EU) 2024/2847 je proto vhodné umožnit, aby úrovně AVA_VAN byly vyjádřeny odkazem buď na nejnovější verzi, nebo na starší verze uvedených norem.

(9) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle čl. 62 odst. 1 nařízení (EU) 2024/2847,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Definice

Pro účely tohoto nařízení se rozumí:

1) „společnými kritérii“ společná kritéria pro hodnocení bezpečnosti informačních technologií definovaná v čl. 2 odst. 1 prováděcího nařízení (EU) 2024/482 nebo stanovená v normách uvedených v čl. 3 odst. 2 písm. a) a b) uvedeného prováděcího nařízení;

2) „společnou metodikou hodnocení“ společná metodika pro hodnocení bezpečnosti informačních technologií definovaná v čl. 2 odst. 2 prováděcího nařízení (EU) 2024/482 nebo stanovená v normách uvedených v čl. 3 odst. 2 písm. c) a d) uvedeného prováděcího nařízení.

Článek 2

1. Technický popis kategorií produktů s digitálními prvky spadajících do tříd I a II uvedených v příloze III nařízení (EU) 2024/2847 je stanoven v příloze I tohoto nařízení.

2. Technický popis kategorií produktů s digitálními prvky uvedených v příloze IV nařízení (EU) 2024/2847 je stanoven v příloze II tohoto nařízení.

Článek 3

Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Bruselu dne 28. listopadu 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

DŮLEŽITÉ PRODUKTY S DIGITÁLNÍMI PRVKY

Třída I

Kategorie produktů	Technický popis
1. Software pro systémy správy identity a pro správu privilegovaného přístupu a hardware, včetně čtečky k ověřování totožnosti a ke kontrole přístupu, mj. biometrické čtečky	Systémy správy identity jsou produkty s digitálními prvky, které poskytují mechanismy pro ověřování totožnosti nebo autorizaci a které mohou rovněž poskytovat mechanismy pro správu identifikačních údajů fyzických a právnických osob, zařízení nebo systémů během životního cyklu, jako je registrace totožnosti, poskytování služeb, údržba, zrušení registrace. Tyto systémy zahrnují systémy správy přístupu, které kontrolují přístup fyzických a právnických osob, zařízení nebo systémů k digitálním zdrojům nebo fyzickým umístěním. Software pro správu privilegovaného přístupu je systém správy přístupu, který kontroluje a monitoruje přístupová práva k systémům IT nebo OT a citlivým informacím v rámci organizace, včetně systémů prosazujících diferencované politiky kontroly přístupu pro privilegované uživatele. Tato kategorie zahrnuje mimo jiné čtečky pro ověřování totožnosti a kontrolu přístupu, biometrické čtečky, software pro jednotné přihlašování, federovaný software pro správu identit, software pro jednorázová hesla, hardwarová autentizační zařízení, jako jsou generátory ověřovacích čísel transakce (TAN), autentizační software a multifaktorový autentizační software.
2. Samostatné a vestavěné prohlížeče	Softwarové produkty s digitálními prvky, které umožňují koncovým uživatelům přístup, zobrazování a interakci s webovým obsahem a službami na serverech připojených k sítím, jako je internet. Obvykle zahrnují prohlížeč, který načítá a zobrazuje obsah napsaný ve značkovacím jazyce (např. HTML), podporu webových protokolů (např. HTTP, HTTPS), schopnost spouštět skripty a spravovat uživatelské vstupy, jakož i ukládání dočasných nebo trvalých údajů z internetových stránek (cookies). Tato kategorie zahrnuje mimo jiné samostatné aplikace, které plní funkce prohlížečů, vestavěné prohlížeče určené k integraci do jiného systému nebo aplikace, jakož i prohlížeče s integrovanými agenty umělé inteligence.
3. Správci hesel	Produkty s digitálními prvky, které ukládají hesla, a to lokálně na zařízení nebo na vzdáleném serveru, včetně činností, jako je generování hesel, jakož i sdílení hesel a integrace s místními aplikacemi nebo aplikacemi třetích stran pro používání hesel. Tato kategorie zahrnuje mimo jiné místní správce hesel, správce hesel poskytované jako rozšíření prohlížeče, podnikové správce hesel a správce hesel založených na hardwaru.

Kategorie produktů	Technický popis
4. Software, který vyhledává škodlivé programy, odstraňuje je nebo je dává do karantény	Softwarové produkty s digitálními prvky, obvykle označované jako antivirus nebo antimalware, které na zařízeních odhalují nebo vyhledávají škodlivé programy nebo kód nebo tyto programy nebo kód odstraňují nebo je umísťují do karantény, aby byla zachována integrita, důvěrnost nebo dostupnost daných zařízení. V souvislosti s touto kategorií produktů se škodlivými programy rozumí programy obsahující škodlivé prvky nebo schopnosti, které mohou přímo či nepřímo poškodit uživatele a/nebo počítačový systém, jako jsou viry, počítačoví červi, ransomware, špionážní software a trojské koně. Tato kategorie zahrnuje mimo jiné software pro detekci nebo vyhledávání škodlivého softwaru v reálném čase nebo ručně, detekci rootkitů a záchranné disky s klíčovou funkcí vyhledávání škodlivých programů, jejich odstraňování nebo umísťování do karantény.
5. Produkty s digitálními prvky s funkcí virtuální soukromé sítě (VPN)	Produkty s digitálními prvky, které vytvářejí zašifrovaný logický tunel, který je vybudován ze systémových zdrojů fyzické nebo virtuální sítě. Tato kategorie zahrnuje mimo jiné klienty, servery a brány virtuálních soukromých sítí.
6. Systémy řízení sítě	Produkty s digitálními prvky, které spravují připojené síťové prvky, jako jsou servery, směrovače, přepínače, pracovní stanice, tiskárny nebo mobilní zařízení, tím, že je monitorují a řídí jejich provoz a konfiguraci sítě. Tato kategorie zahrnuje mimo jiné systémy řízení mezi koncovými body a specializované systémy řízení konfigurace, jako jsou řídicí jednotky pro softwarově definované sítě.
7. Systémy řízení bezpečnostních informací a událostí	Produkty s digitálními prvky, které shromažďují údaje z více zdrojů, analyzují a korelují tyto údaje a prezentují je jako využitelné informace pro účely související s bezpečností, jako je odhalování hrozeb a incidentů, forenzní analýza nebo dodržování předpisů.
8. Boot manageři	Softwarové produkty s digitálními prvky, které řídí proces počátečního spuštění systému po zapnutí / opětovném spuštění inicializací hardwaru, načtením nebo přenosem řízení do prostředí operačního systému nebo systémových zdrojů a výběrem možností spuštění. Do této kategorie patří mimo jiné firmware UEFI, jednostupňové a vícestupňové zavaděče.
9. Infrastruktura veřejných klíčů a software k vydávání digitálních certifikátů	Produkty s digitálními prvky používané jako součást infrastruktury veřejných klíčů (PKI), které spravují validaci, vytváření, vydávání, distribuci, zveřejňování statusu, obnovu nebo zrušení digitálních certifikátů nebo vytváření, ukládání, umisťování, výměnu, zničení nebo rotaci kryptografických klíčů spojených s těmito digitálními certifikáty. Tato kategorie zahrnuje mimo jiné systémy správy klíčů, digitální systémy správy certifikátů, odpovídače protokolu OCSP (Online Certificate Status Protocol) a řešení PKI „vše v jednom“.

Kategorie produktů	Technický popis
10. Fyzická a virtuální síťová rozhraní	Fyzická síťová rozhraní jsou produkty s digitálními prvky, které přímo propojují zařízení se sítí prostřednictvím aplikačního programovacího rozhraní (API) poskytovaného ovladačem rozhraní. Obvykle pracují na vrstvě datového spoje a jsou vybaveny hardwarovými adaptéry pro přenosová média s odpovídajícím firmwarem, který obvykle pracuje na vrstvě datového spoje. Virtuální síťová rozhraní jsou produkty s digitálními prvky, které přímo nebo nepřímo připojují zařízení k síti prostřednictvím API, které napodobuje rozhraní ovladačů fyzických síťových rozhraní, obvykle pracujících na vrstvě datového spoje. Tato kategorie zahrnuje mimo jiné karty pevného a bezdrátového síťového rozhraní, řídicí jednotky a adaptéry, jako jsou Wi-Fi, Ethernet, IrDA, USB, Bluetooth, NearLink, Zigbee nebo Fieldbus, jakož i čistě virtuální samostatné produkty, jako jsou karty virtuálního síťového rozhraní, rozhraní CNI (Container Network Interface) a rozhraní VPN.
11. Operační systémy	Softwarové produkty s digitálními prvky, které poskytují abstraktní rozhraní základního hardwaru a ovládají provádění softwaru a mohou poskytovat služby, jako je řízení a konfigurace výpočetních zdrojů, plánování, řízení vstupů a výstupů, správa dat a poskytování rozhraní, jehož prostřednictvím aplikace komunikují se systémovými zdroji a periferními zařízeními. Tato kategorie zahrnuje mimo jiné operační systémy v reálném čase, operační systémy pro všeobecné účely a operační systémy pro speciální účely.
12. Směrovače, modemy určené pro připojení k internetu a přepínače	Směrovače jsou produkty s digitálními prvky, které vytvářejí a řídí tok dat mezi různými sítěmi výběrem tras za použití mechanismů a algoritmů směrovacích protokolů, které obvykle pracují na síťové vrstvě. Tato kategorie zahrnuje mimo jiné drátové a bezdrátové směrovače, virtuální směrovače a směrovače s modemy nebo bez nich.
	Modemy určené pro připojení k internetu jsou hardwarové produkty s digitálními prvky, které používají digitální modulační a demodulační techniky k převodu analogových signálů z digitálních (a naopak) pro komunikaci prostřednictvím IP. Tato kategorie zahrnuje mimo jiné optické modemy, digitální předplatitelskou linku (DSL), kabelové modemy (DOCSIS), satelitní modemy a buňkové modemy.
	Přepínače jsou produkty s digitálními prvky, které zajišťují propojení mezi síťovými zařízeními prostřednictvím mechanismů přesměrování a které mají řídicí rovinu, obvykle implementovanou na datové nebo síťové vrstvě. Tato kategorie zahrnuje mimo jiné řízené přepínače, inteligentní přepínače, vícevrstvé přepínače, virtuální bezpečnostní přepínače, programovatelné přepínače pro softwarově definované sítě a mosty, jako jsou bezdrátové přístupové body.

Kategorie produktů	Technický popis
13. Mikroprocesory s bezpečnostními funkcemi	Produkty s digitálními prvky, které jsou integrovanými obvody vykonávajícími funkce centrálního procesoru založené na externí paměti a periferních zařízeních, včetně mikrokódu a jiného firmwaru nízké úrovně. Kromě toho poskytují bezpečnostní funkce, jako je šifrování, autentizace, bezpečné ukládání klíčů, generování náhodných čísel, důvěryhodné realizační prostředí nebo jiné hardwarové ochranné mechanismy, jejichž cílem je zabezpečit jiné produkty, sítě nebo služby nad rámec samotného mikroprocesoru, jako je bezpečné spouštění systému, virtualizace nebo bezpečná komunikační rozhraní.
14. Mikrořadiče s bezpečnostními funkcemi	Produkty s digitálními prvky, které jsou integrovanými obvody vykonávajícími základní zpracovatelské funkce integrující paměť, umožňující programovatelnost mikrořadiče a zpravidla dalších periferních zařízení, včetně mikrokódu a jiného nízkoúrovňového firmwaru. Kromě toho poskytují bezpečnostní funkce, jako je šifrování, autentizace, bezpečné ukládání klíčů, generování náhodných čísel, důvěryhodné realizační prostředí nebo jiné hardwarové ochranné mechanismy, jejichž cílem je zabezpečit jiné produkty, sítě nebo služby nad rámec samotného mikrořadiče, jako je bezpečné spouštění systému, virtualizace nebo bezpečná komunikační rozhraní.
15. Aplikačně specifické integrované obvody (ASIC) a programovatelná hradlová pole (FPGA) s bezpečnostními funkcemi	Aplikačně specifické integrované obvody (ASIC) s funkcemi souvisejícími s bezpečností jsou produkty s digitálními prvky, které jsou integrovanými obvody, které jsou navrženy zcela nebo částečně na míru tak, aby plnily konkrétní funkci nebo zavedly konkrétní aplikaci, včetně mikrokódu a jiného firmwaru nízké úrovně. Kromě toho poskytují bezpečnostní funkce, jako je šifrování, autentizace, bezpečné ukládání klíčů, generování náhodných čísel, důvěryhodné realizační prostředí nebo jiné hardwarové ochranné mechanismy, jejichž cílem je zabezpečit jiné produkty, sítě nebo služby nad rámec samotných ASIC, jako je bezpečné spouštění systému, virtualizace nebo bezpečná komunikační rozhraní.
	Programovatelná hradlová pole (FPGA) s funkcemi souvisejícími s bezpečností jsou produkty s digitálními prvky, které jsou integrovanými obvody charakterizovanými maticí konfigurovatelných logických bloků navržených tak, aby byly po výrobě přeprogramovatelné pro výkon konkrétní funkce nebo aplikace, včetně mikrokódu a jiného firmwaru nízké úrovně. Kromě toho poskytují bezpečnostní funkce, jako je šifrování, autentizace, bezpečné ukládání klíčů, generování náhodných čísel, důvěryhodné realizační prostředí nebo jiné hardwarové ochranné mechanismy, jejichž cílem je zabezpečit jiné produkty, sítě nebo služby nad rámec samotného FPGA, jako je bezpečné spouštění systému, virtualizace nebo bezpečná komunikační rozhraní.
16. Obecní virtuální asistenti pro chytré domácnosti	Produkty s digitálními prvky, které komunikují na veřejném internetu, ať už přímo, nebo prostřednictvím jiného zařízení, které zpracovávají požadavky, úkoly nebo otázky založené na výzvách v přirozeném jazyce, například prostřednictvím zvukových nebo písemných vstupů, a které na základě těchto požadavků, úkolů nebo otázek poskytují přístup k jiným službám nebo kontrolují funkce připojených zařízení v obytných budovách. Tato kategorie zahrnuje mimo jiné inteligentní reproduktory s integrovanými virtuálními asistenty a samostatné virtuální asistenty, kteří odpovídají tomuto popisu.

Kategorie produktů	Technický popis
17. Produkty pro chytré domácnosti s bezpečnostními funkcemi, včetně chytrých dveřních zámků, bezpečnostních kamer, systémů pro monitorování dětí (dětských chůviček) a poplašných systémů	Produkty s digitálními prvky, které chrání fyzickou bezpečnost spotřebitelů v obytných budovách a které lze dálkově ovládat nebo spravovat z jiných systémů, jakož i hardware a software, který tyto produkty centrálně řídí. Tato kategorie zahrnuje mimo jiné chytré dveřní zámky, systémy pro sledování dětí (dětské chůvičky), poplašné systémy a domácí bezpečnostní kamery.
18. Hračky připojené k internetu, na které se vztahuje směrnice Evropského parlamentu a Rady 2009/48/ES ([1]) a které mají sociální interaktivní funkce (např. k mluvení nebo natáčení) nebo funkce ke sledování polohy	Hračky připojené k internetu, které mají sociální interaktivní funkce, jsou produkty s digitálními prvky, na něž se vztahuje směrnice 2009/48/ES, které komunikují na veřejném internetu, ať už přímo, nebo prostřednictvím jakéhokoli jiného zařízení, a které mají vestavěné technologie, které umožňují příchozí a odchozí komunikaci, jako je klávesnice, mikrofon, reproduktor nebo kamera.
	Hračky připojené k internetu, které mají funkce ke sledování polohy, jsou produkty s digitálními prvky, na které se vztahuje směrnice 2009/48/ES, které komunikují přímo nebo prostřednictvím jiného zařízení na veřejné internetové síti a jsou vybaveny technologiemi, které umožňují sledování nebo vyhledávání geografické polohy hračky nebo jejího uživatele. Pokud hračka dokáže pomocí senzorových technologií detekovat pouze blízkost uživatele nebo jiných hraček, nepovažuje se za hračku s funkcí sledování polohy.
19. Osobní výrobky k nošení, které se nosí nebo umísťují na lidské tělo, jejichž účelem je sledovat zdravotní stav a na něž se nevztahuje nařízení Evropského parlamentu a Rady (EU) 2017/745 ([2]) ani (EU) 2017/746 ([3]), nebo osobní výrobky k nošení, které jsou určeny pro děti a k používání u dětí	Osobní výrobky k nošení, které mají být nošeny nebo umístěny na lidském těle a jejichž účelem je monitorování zdraví, jsou produkty s digitálními prvky nošené na těle přímo nebo prostřednictvím oděvů či doplňků, které mohou pravidelně nebo nepřetržitě snímat a dále zpracovávat informace, včetně tělesných metrik, relevantní pro zdraví uživatele, s výjimkou výrobků, které spadají do oblasti působnosti nařízení (EU) 2017/745 nebo nařízení (EU) 2017/746. Do této kategorie patří mimo jiné fitness sledovací přístroje, chytré hodinky, inteligentní šperky, inteligentní oděvy a sportovní oděvy, které odpovídají tomuto popisu.
	Osobní výrobky k nošení, které jsou určeny k použití dětmi a pro děti, jsou produkty s digitálními prvky, které mohou být nošeny nebo umístěny na těle, přímo nebo prostřednictvím oděvů či doplňků, osob mladších 14 let. Do této kategorie patří mimo jiné výrobky pro bezpečnost dětí, které jsou určeny k nošení nebo umístění na lidském těle.

([1]) Směrnice Evropského parlamentu a Rady 2009/48/ES ze dne 18. června 2009 o bezpečnosti hraček (Úř. věst. L 170, 30.6.2009, s. 1, ELI: http://data.europa.eu/eli/dir/2009/48/oj).

([2]) Nařízení Evropského parlamentu a Rady (EU) 2017/745 ze dne 5. dubna 2017 o zdravotnických prostředcích, změně směrnice 2001/83/ES, nařízení (ES) č. 178/2002 a nařízení (ES) č. 1223/2009 a o zrušení směrnic Rady 90/385/EHS a 93/42/EHS (Úř. věst. L 117, 5.5.2017, s. 1, ELI: http://data.europa.eu/eli/reg/2017/745/oj).

([3]) Nařízení Evropského parlamentu a Rady (EU) 2017/746 ze dne 5. dubna 2017 o diagnostických zdravotnických prostředcích *in vitro* a o zrušení směrnice 98/79/ES a rozhodnutí Komise 2010/227/EU (Úř. věst. L 117, 5.5.2017, s. 176. ELI: http://data.europa.eu/eli/reg/2017/746/oj).

Třída II

Kategorie produktů	Technický popis
1. Hypervizory a systémy runtime kontejnerů, které podporují virtualizované provedení operačních systémů a podobných prostředí	Hypervizory jsou softwarové produkty s digitálními prvky, které přidělují a/nebo přiřazují výpočetní zdroje a umožňují spouštění, správu nebo organizaci virtuálních strojů, které jsou logicky odděleny od sebe navzájem a/nebo od fyzického hardwaru. Hypervizory mohou běžet přímo na hardwaru (bare metal), na operačním systému nebo v rámci jiného virtuálního stroje (vnořená virtualizace). V kontextu této kategorie produktů je virtuální stroj softwarově definované logické oddělení výpočetního prostředí, které zahrnuje virtualizovaný soubor hardwarových zdrojů (např. centrální procesorová jednotka, paměť, úložiště, síťová rozhraní) a obvykle je hostitelem vlastního operačního systému. Do této kategorie patří mimo jiné hypervizory typu 1 (bare metal), hypervizory typu 2 (fungující na hostitelském operačním systému) a hybridní hypervizory.
	Systémy runtime kontejnerů jsou softwarové produkty s digitálními prvky, které řídí provádění a životní cyklus kontejnerů provozovaných v jediném operačním systému jako izolované procesy a které přidělují zdroje a umožňují správu a organizaci jednotlivých kontejnerů. V souvislosti s touto kategorií produktů je kontejner softwarovým realizačním prostředím, které sdružuje jednu nebo více softwarových součástí a jejich závislosti do jediného balíčku, což mu umožňuje fungovat nezávisle a konzistentně.
2. Firewally, systémy detekce narušení a prevence	Firewally jsou produkty s digitálními prvky, které chrání připojenou síť nebo systém před neoprávněným přístupem sledováním a omezováním přenosu dat do této sítě a z ní. Tato kategorie zahrnuje mimo jiné síťové firewally a aplikační firewally, jako jsou firewally nebo filtry pro webové aplikace a antispamové brány.
	Systémy detekce narušení jsou produkty s digitálními prvky, které sledují, zda v provozu po vstupu do síťového prostředí nedochází k podezřelé činnosti a odhalují nebo identifikují, že došlo k pokusu o vniknutí do propojené sítě nebo systému nebo že k němu došlo v připojené síti nebo systému. Tato kategorie zahrnuje mimo jiné síťové systémy detekce narušení a systémy detekce narušení na bázi hostitele.
	Systémy prevence narušení jsou produkty s digitálními prvky složenými ze systému detekce narušení, který aktivně reaguje na vniknutí do připojené sítě nebo systému. Tato kategorie zahrnuje mimo jiné síťové systémy prevence narušení a systémy prevence narušení na bázi hostitele.

Kategorie produktů	Technický popis
3. Mikroprocesory odolné proti manipulaci	Produkty s digitálními prvky, které jsou mikroprocesory s bezpečnostními funkcemi uvedenými v tabulce „Třída I“ v bodě 13 této přílohy, včetně dokazování nedovolené manipulace, odolnosti nebo reakce, a které jsou navíc navrženy tak, aby poskytovaly ochranu úrovně 2 nebo 3 AVA_VAN, jak je stanoveno ve společných kritériích a společné metodice hodnocení.
4. Mikrořadiče odolné proti manipulaci	Produkty s digitálními prvky, které jsou mikrořadiče s bezpečnostními funkcemi uvedenými v tabulce „Třída I“ v bodě 14 této přílohy, včetně dokazování nedovolené manipulace, odolnosti nebo reakce, a které jsou navíc navrženy tak, aby poskytovaly ochranu úrovně 2 nebo 3 AVA_VAN, jak je stanoveno ve společných kritériích a společné metodice hodnocení.

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

PŘÍLOHA II

KRITICKÉ PRODUKTY S DIGITÁLNÍMI PRVKY

Kategorie produktů	Technický popis
1. Hardwarová zařízení s bezpečnostními schránkami	Hardwarové produkty s digitálními prvky, které bezpečně ukládají, zpracovávají nebo spravují citlivé údaje nebo provádějí kryptografické operace a které sestávají z více samostatných součástí a obsahují hardwarovou fyzickou obálku zajišťující dokazování nedovolené manipulaci, odolnost nebo reakci jako protiopatření proti fyzickým útokům. Tato kategorie zahrnuje mimo jiné fyzické platební terminály, hardwarové bezpečnostní moduly, které generují a spravují šifrovací prvky, a tachografy, které odpovídají výše uvedenému popisu.
2. Přístroje Smart meter gateway v rámci inteligentních měřicích systémů vymezených v čl. 2 bodu 23 směrnice Evropského parlamentu a Rady (EU) 2019/944 ([1]) a další přístroje pro účely zajištění větší bezpečnosti, mj. pro bezpečné přijímání plateb v kryptoměně.	Přístroje Smart meter gateway jsou produkty s digitálními prvky, které řídí komunikaci mezi součástmi v inteligentních měřicích systémech ve smyslu čl. 2 bodu 23 směrnice (EU) 2019/944 nebo k nim připojenými, a oprávněnými třetími stranami, jako jsou poskytovatelé veřejných služeb. Přístroje Smart meter gateway shromažďují, zpracovávají a ukládají naměřená data nebo osobní údaje, chrání data a toky informací podporou specifických kryptografických požadavků, jako je šifrování a dešifrování dat, mají vestavěné funkce brány firewall a poskytují prostředky pro ovládání jiných zařízení. Tato kategorie zahrnuje mimo jiné přístroje Smart meter gateway související s inteligentními měřicími systémy měřícími elektřinu ve smyslu čl. 2 bodu 23 směrnice (EU) 2019/944. Může rovněž zahrnovat přístroje Smart meter gateway používané v jiných inteligentních měřicích systémech měřících spotřebu jiných zdrojů energie, jako je plyn nebo teplo, za předpokladu, že brána odpovídá tomuto popisu.
3. Čipové karty nebo podobná zařízení, včetně zabezpečených prvků	Zabezpečenými prvky jsou mikrořadiče nebo mikroprocesory s funkcemi souvisejícími s bezpečností, včetně důkazů o nedovolené manipulaci, odolnosti nebo reakci. Obvykle ukládají, zpracovávají nebo spravují kryptografické operace nebo citlivé údaje, jako jsou údaje o totožnosti nebo platební údaje. Zabezpečené prvky jsou navrženy tak, aby poskytovaly ochranu alespoň AVA_VAN.4, jak je stanoveno ve společných kritériích nebo společné metodice hodnocení. Mohou mít podobu samostatného čipu nebo být integrovány do systémů na čipu (SoC). Zabezpečené prvky mohou zahrnovat aplikační prostředí nebo operační systém a mohou zahrnovat jednu nebo více aplikací. Tato kategorie zahrnuje mimo jiné moduly důvěryhodných platforem (TPM) a zabudované univerzální integrované obvodové karty (UICC).
	Čipové karty nebo podobná zařízení jsou zabezpečené prvky začleněné do nosného materiálu, jako je plast nebo dřevo, ve tvaru karty nebo zabezpečené prvky integrované do nosných materiálů jiných tvarů. Tato kategorie zahrnuje mimo jiné doklady totožnosti a cestovní doklady, kvalifikované podpisové karty, vyměnitelné karty UICC, fyzické platební karty, fyzické přístupové karty, karty digitálního tachografu nebo náramky s integrovanými platebními zabezpečenými prvky.

([1]) Směrnice Evropského parlamentu a Rady (EU) 2019/944 ze dne 5. června 2019 o společných pravidlech pro vnitřní trh s elektřinou a o změně směrnice 2012/27/EU (Úř. věst. L 158, 14.6.2019, s. 125, ELI: http://data.europa.eu/eli/dir/2019/944/oj).