2024/3144

19.12.2024

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2024/3144

ze dne 18. prosince 2024,

kterým se mění prováděcí nařízení (EU) 2024/482, pokud jde o použitelné mezinárodní normy, a kterým se uvedené prováděcí nařízení opravuje

(Text s významem pro EHP)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na 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“) ([1]), a zejména na čl. 49 odst. 7 tohoto nařízení,

vzhledem k těmto důvodům:

(1) Prováděcí nařízení Komise (EU) 2024/482 ([2]) v souladu s evropským rámcem pro certifikaci kybernetické bezpečnosti stanoveným v nařízení (EU) 2019/881 vymezuje úlohy, pravidla a povinnosti, jakož i strukturu evropského systému certifikace kybernetické bezpečnosti založeného na společných kritériích (EUCC).

(2) Prováděcí nařízení (EU) 2024/482 vychází ze zavedených mezinárodních norem, které jsou společnými kritérii a společnou metodikou hodnocení, které spravuje Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC). Prováděcí nařízení (EU) 2024/482 odkazuje na normy ISO/IEC, ale nespecifikuje příslušnou verzi těchto norem. Proto by mělo být upřesněno, která verze norem se vztahuje na certifikáty vydané v rámci EUCC.

(3) Vládní organizace, které přispěly k vypracování společných kritérií a společné metodiky hodnocení prostřednictvím dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT (Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security – CRRA), jsou spolu s ISO/IEC spoluvlastníky autorských práv. Tyto vládní organizace si ponechávají právo je používat. Vzhledem k významu těchto dokumentů, které vycházejí z CCRA, by tyto dokumenty měly být rovněž základem pro certifikaci v rámci EUCC.

(4) Společná kritéria a společné normy metodiky hodnocení podléhají interpretacím ze strany CCRA, které usnadňují jejich provádění a které mohou být zohledněny zařízeními pro hodnocení bezpečnosti informačních technologií (ITSEF) a certifikačními orgány.

(5) Mezinárodní normy týkající se společných kritérií mohou podléhat aktualizacím. Aby byl zajištěn řádný a včasný přechod, je vhodné definovat přechodná pravidla, aby prodejci, zařízení ITSEF a certifikační subjekty a další příslušné subjekty měli dostatek času na nezbytné úpravy. Tato přechodná pravidla by měla být v přiměřeném rozsahu sladěna s globálními postupy, jako jsou postupy stanovené v CCRA.

([1]) Úř. věst. L 151, 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) 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).

(6) Prováděcí nařízení (EU) 2024/482 neupřesňuje, do kdy může být certifikace produktu IKT založena na předchozích verzích společných kritérií a společných norem metodiky hodnocení. Technické oblasti a profily ochrany uvedené v přílohách I, II a III uvedeného prováděcího nařízení vycházejí z předchozích verzí norem ISO/IEC 15408 a 18045. Prováděcí nařízení (EU) 2024/482 by proto mělo upřesnit, za jakých okolností se stále uplatňuje předchozí verze společných kritérií a společné metodiky hodnocení a jak bude fungovat přechod na nejnovější verzi mezinárodních norem.

(7) Během přechodného období by pro příslušné zúčastněné strany mělo být prioritou aktualizovat příslušné technické oblasti a profily ochrany. Prováděcí nařízení (EU) 2024/482 by mělo stanovit, že bezpečnostní cíle založené na předchozí verzi norem budou přijímány do 31. prosince 2027 v souladu s politikou přechodu přijatou CCRA. Je však třeba poznamenat, že politika přechodu CCRA zahrnuje počáteční hodnocení produktů a profilů ochrany, která byla zahájena nejpozději 30. června 2024, což je datum, kdy EUCC ještě nebyl použitelný. Kromě toho by v souladu s politikou přechodu CCRA mělo prováděcí nařízení (EU) 2024/482 stanovit, že bezpečnostní cíle, které jsou v souladu s uvedeným prováděcím nařízením a požadují soulad s profily ochrany na základě předchozí verze norem, budou přijímány do 31. prosince 2027. Navíc, pokud je nový certifikát vydaný podle prováděcího nařízení (EU) 2024/482 v souvislosti s procesem přezkumu vnitrostátního certifikátu, který začíná do dvou let od vydání původního certifikátu, mělo by být možné použít předchozí verzi norem. To by nebylo relevantní pro proces přezkumu, který nevyžaduje vydání nového certifikátu podle prováděcího nařízení (EU) 2024/482, a pokud osvědčení zůstává v platnosti.

(8) S cílem zajistit řádný přechod na nejnovější verzi norem by prováděcí nařízení (EU) 2024/482 mělo stanovit zvláštní přechodná pravidla a i nadále umožňovat vydávání certifikátů podle uvedeného prováděcího nařízení, které uvádějí shodu s profily ochrany, které vycházejí z předchozích verzí norem zveřejněných CCRA, pokud je použití těchto profilů ochrany vyžadováno právními předpisy Unie. Tak je tomu v případě prováděcího nařízení Komise (EU) 2016/799 ([3]), jakož i nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ([4]) a prováděcího rozhodnutí Komise (EU) 2016/650 ([5]).

(9) Příloha I prováděcího nařízení (EU) 2024/482 uvádí použitelné přehledy aktuálních certifikačních postupů pro hodnocení produktů IKT a profilů ochrany. Neupřesňuje však verzi dokumentů. Proto by mělo být upřesněno, která verze dokumentů se vztahuje na certifikáty vydané v rámci EUCC. Tyto verze vycházejí z dokumentů schválených Evropskou skupinou pro certifikaci kybernetické bezpečnosti (ECCG), přičemž pro účely jejich začlenění do EUCC prošly dalším přezkumem. Kromě toho by příloha I měla být změněna tak, aby zahrnovala aktualizované a nové přehledy aktuálních certifikačních postupů po jejich schválení Evropskou skupinou pro certifikaci kybernetické bezpečnosti, čímž se zajistí jednotná akreditace subjektů posuzování shody v rámci EUCC. Požadavky na akreditaci zařízení ITSEF by měly být aktualizovány, aby se vyjasnilo uplatňování kritérií nezávislosti a nestrannosti, a pro akreditaci certifikačních orgánů by měl být vytvořen nový přehled aktuálních certifikačních postupů.

(10) Přehledy aktuálních certifikačních postupů mohou být do systému EUCC doplněny nebo by mohly být aktualizovány v souvislosti s jeho údržbou. U nových nebo aktualizovaných přehledů aktuálních certifikačních postupů může být nutné stanovit vhodná přechodná pravidla, aby prodejci, zařízení ITSEF, certifikační orgány a další zúčastněné strany mohli provést nezbytné úpravy. Pro účely aktualizace přehledu aktuálních certifikačních postupů týkajícího se akreditace zařízení ITSEF by se aktualizovaný dokument měl vztahovat na akreditace vydané před 8. červencem 2025 pouze při jejich přezkumu, například v souvislosti s postupem hodnocení nebo opětovného hodnocení. Aktualizovaný dokument by se dále měl vztahovat na všechny akreditace zařízení ITSEF vydané po 8. červenci 2025.

([3]) Prováděcí nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí (Úř. věst. L 139, 26.5.2016, s. 1, ELI:. http://data.europa.eu/eli/reg_impl/2016/799/oj).

([4]) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

([5]) Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 109, 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Další opravy článků 5, 8, 16, 29 a 44 a přílohy IV prováděcího nařízení (EU) 2024/482 přispívají k zajištění jednotného znění a jasného právního výkladu.

(12) Pravidla pro oznamování subjektů posuzování shody by měla být stanovena horizontálně pro všechny systémy v rámci evropského rámce pro certifikaci kybernetické bezpečnosti. Na taková pravidla oznamování se vztahuje prováděcí nařízení Komise (EU) 2024/3143 ([6]). Články 23 a 24 prováděcího nařízení (EU) 2024/482 by proto měly být zrušeny ode dne, kdy se začne uplatňovat prováděcí nařízení (EU) 2024/3143.

(13) Prováděcí nařízení (EU) 2024/482 by proto mělo být odpovídajícím způsobem změněno a opraveno.

(14) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem výboru zřízeného podle článku 66 nařízení (EU) 2019/881,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Prováděcí nařízení (EU) 2024/482 se mění takto:

1) v článku 2 se body 1) a 2) nahrazují tímto:

„1) „společnými kritérii“ se rozumí společná kritéria pro hodnocení bezpečnosti informačních technologií, jak jsou stanovena v normách ISO/IEC 15408–1:2022, ISO/IEC 15408–2:2022, ISO/IEC 15408–3:2022, ISO/IEC 15408–4:2022 nebo ISO/IEC 15408–5:2022 nebo ve společných kritériích pro hodnocení bezpečnosti informačních technologií, verze CC:2022, části 1 až 5, zveřejněných účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT;

2) „společnou metodikou hodnocení“ se rozumí společná metodika hodnocení bezpečnosti informačních technologií, jak je stanovena v normě ISO/IEC 18045:2022, nebo společná metodika pro hodnocení bezpečnosti informačních technologií, verze CEM:2022, zveřejněná účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT;“;

2) článek 3 se nahrazuje tímto:

„*Článek 3*

Normy pro hodnocení

1. Na hodnocení prováděná v rámci EUCC se vztahují následující normy:

a) společná kritéria;

b) společná metodika hodnocení.

2. Do 31. prosince 2027 lze vydávat certifikáty v rámci systému EUCC, přičemž se uplatní některá z těchto norem:

a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 nebo ISO/IEC 15408-3:2008;

b) společná kritéria pro hodnocení bezpečnosti informačních technologií, verze 3.1, revize 5, zveřejněná účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT;

([6]) Prováděcí nařízení Komise (EU) 2024/3143 ze dne 18. prosince 2024, kterým se stanoví okolnosti, formáty a postupy pro oznámení podle čl. 61 odst. 5 nařízení Evropského parlamentu a Rady (EU) 2019/881 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“) a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií (Úř. věst. L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

c) ISO/IEC 18045:2008;

d) společná metodika pro hodnocení bezpečnosti informačních technologií, revize 5, verze 3.1, zveřejněná účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT.

3. Do 31. prosince 2027 lze v rámci systému EUCC podle norem uvedených v odstavci 1 vydávat certifikáty, kterými se potvrzuje shoda s profilem ochrany, který odpovídá normám uvedeným v odstavci 2.

4. Certifikát podle norem uvedených v odstavci 1 může být rovněž vydán v rámci systému EUCC za účelem uplatnění shody s profilem ochrany, který odpovídá některé z následujících norem, za předpokladu, že použití tohoto profilu ochrany je vyžadováno prováděcím nařízením Komise (EU) 2016/799 (*), nařízením Evropského parlamentu a Rady (EU) č. 910/2014 (**)nebo prováděcím rozhodnutím Komise (EU) 2016/650 (***):

a) společná kritéria hodnocení bezpečnosti informačních technologií, verze 3.1, revize 1 až 4, zveřejněná účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT;

b) společná metodika hodnocení bezpečnosti informačních technologií, verze 3.1, revize 1 až 4, zveřejněná účastníky dohody o uznávání certifikátů o společných kritériích v oblasti bezpečnosti IT.

_____

(*) Prováděcí nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014, kterým se stanoví požadavky na konstrukci, zkoušení, montáž, provoz a opravy tachografů a jejich součástí (Úř. věst. L 139, 26.5.2016, s. 1, ELI:. http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu (Úř. věst. L 109, 26.4.2016, s. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).“;

3) v kapitole IV se vkládá nový článek 20a, který zní:

„*Článek 20a*

Specifikace požadavků na akreditaci subjektů posuzování shody

Akreditace subjektů posuzování shody zohlední specifikaci požadavků na akreditaci certifikačních subjektů a zařízení ITSEF, jak je stanoveno v použitelných přehledech aktuálních certifikačních postupů uvedených v bodě 2 přílohy I.“;

4) články 23 a 24 se zrušují;

5) v článku 48 se doplňuje nový odstavec 4, který zní:

„4. Není-li v příloze I nebo II stanoveno jinak, použijí se přehledy aktuálních certifikačních postupů ode dne použitelnosti pozměňujícího aktu, kterým byly začleněny do přílohy I nebo II.“;

6) v článku 49 se doplňuje nový odstavec 4, který zní:

„4. Při provádění přezkumu uvedeného v odstavci 3 do dvou let od vydání původního certifikátu a v případě, že takový přezkum vede k vydání nového certifikátu v souladu s tímto nařízením, lze použít normy uvedené v čl. 3 odst. 2. Datem vydání původního certifikátu se rozumí datum vydání posledního certifikátu pro produkt IKT nebo profil ochrany, na němž je stávající certifikace založena.“;

7) příloha I se nahrazuje zněním uvedeným v příloze I tohoto nařízení;

8) příloha IV se mění v souladu s přílohou II tohoto nařízení.

Článek 2

Prováděcí nařízení (EU) 2024/482 se opravuje takto:

1) v čl. 5 odst. 1 se písmeno b) nahrazuje tímto:

„b) tvrzení o shodě s certifikovaným profilem ochrany jako součásti procesu IKT, pokud produkt IKT spadá do kategorie produktů IKT, na které se tento profil ochrany vztahuje.“;

2) článek 8 se opravuje takto:

a) název se nahrazuje tímto:

„Informace nezbytné pro certifikaci a hodnocení“;

b) odstavec 1 se nahrazuje tímto:

„1. Žadatel o certifikaci podle systému EUCC poskytne nebo jinak zpřístupní certifikačnímu subjektu a zařízení ITSEF veškeré informace nezbytné pro certifikační a hodnoticí činnosti.“;

3) článek 16 se nahrazuje tímto:

„*Článek 16*

Informace nezbytné pro certifikaci a hodnocení profilů ochrany

Žadatel o certifikaci profilu ochrany poskytne nebo jinak zpřístupní certifikačnímu subjektu a zařízení ITSEF veškeré informace nezbytné pro certifikační a hodnoticí činnosti v úplné a správné formě. Ustanovení čl. 8 odst. 2, 3, 4 a 7 se použijí obdobně.“;

4) v článku 17 se zrušuje odstavec 1;

5) v článku 29 se odstavec 2 nahrazuje tímto:

„2. Pokud držitel certifikátu EUCC ve lhůtě uvedené v odstavci 1 nenavrhne vhodné nápravné opatření, platnost certifikátu se pozastaví v souladu s článkem 30 nebo se zruší v souladu s článkem 14 nebo 20.“.

Článek 3

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

Ustanovení čl. 1 odst. 4 se použije ode dne 8. ledna 2025.

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

V Bruselu dne 18. prosince 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

„„PŘÍLOHA I

Přehledy aktuálních certifikačních postupů pro technické oblasti a další přehledy aktuálních certifikačních postupů

1. Přehledy aktuálních certifikačních postupů pro technické oblasti na úrovni AVA_VAN úroveň 4 nebo 5:

   a) následující dokumenty týkající se harmonizovaného hodnocení technické oblasti „čipové karty a podobná zařízení“:

      1) „Minimální požadavky na bezpečnostní hodnocení čipových karet a podobných zařízení vůči zařízením ITSEF“, verze 1.1;

      2) „Minimální bezpečnostní požadavky na lokalitu“, verze 1.1;

      3) „Použití společných kritérií na integrované obvody“, verze 1.1;

      4) „Požadavky na bezpečnostní architekturu (ADV_ARC) pro čipové karty a podobná zařízení“, verze 1.1;

      5) „Certifikace produktů „otevřených“ čipových karet“, verze 1.1;

      6) „Hodnocení složených produktů pro čipové karty a podobná zařízení“, verze 1.1;

      7) „Uplatnění potenciálu útoku na čipové karty a podobná zařízení“, verze 1.2.

   b) následující dokumenty týkající se harmonizovaného hodnocení technické oblasti „hardwarová zařízení s bezpečnostními schránkami“:

      1) „Minimální požadavky na bezpečnostní hodnocení hardwarových zařízení s bezpečnostními schránkami vůči zařízením ITSEF“, verze 1.1;

      2) „Minimální bezpečnostní požadavky na lokalitu“, verze 1.1;

      3) „Uplatnění potenciálu útoku na hardwarová zařízení s bezpečnostními schránkami“, verze 1.2.

2. Přehledy aktuálních certifikačních postupů týkající se harmonizované akreditace subjektů posuzování shody:

   a) „Akreditace zařízení ITSEF pro systém EUCC“, verze 1.1 pro akreditace vydané před 8. červencem 2025;

   b) „Akreditace zařízení ITSEF pro systém EUCC“, verze 1.6c pro akreditace, které jsou nově vydané nebo přezkoumané po 8. červenci 2025;

   c) „Akreditace certifikačních subjektů pro systém EUCC“, verze 1.6b.““

PŘÍLOHA II

V příloze IV prováděcího nařízení (EU) 2024/482, oddíle IV.3, se body 5 a 6 nahrazují tímto:

„5. Pokud certifikační subjekt potvrdí, že změny jsou drobné, vydá se pro upravený produkt IKT nový certifikát a vypracuje se zpráva o údržbě k původní zprávě o certifikaci.

Zpráva o údržbě je součástí dílčí zprávy o analýze dopadů a obsahuje tyto oddíly:

a) úvod;

b) popis změn;

c) dotčené důkazy od vývojáře.

6. Zpráva o údržbě uvedená v bodě 5 se poskytne agentuře ENISA pro zveřejnění na jejích internetových stránkách věnovaných certifikaci kybernetické bezpečnosti.“