2024/482

7.2.2024

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)

(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) Toto nařízení 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). Systém EUCC vychází z dohody o vzájemném uznávání osvědčení o bezpečnosti informačních technologií skupiny vyšších úředníků pro bezpečnost informačních systémů ([2]) (dále jen „SOG-IS“), která používá společná kritéria, včetně postupů a dokumentů této skupiny.

(2) Tento systém by měl být založen na zavedených mezinárodních normách. „Společná kritéria“ je mezinárodní norma pro hodnocení bezpečnosti informací zveřejněná například jako ISO/IEC 15408 – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT. Je založena na hodnocení třetí stranou a předpokládá sedm úrovní záruky hodnocení (*Evaluation Assurance Levels*, „EAL“). Společná kritéria doprovází společná metodika hodnocení, která byla zveřejněna například jako ISO/IEC 18045 – Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Kritéria pro hodnocení bezpečnosti IT – Metodika pro hodnocení bezpečnosti IT. Specifikace a dokumenty, které uplatňují ustanovení tohoto nařízení, se mohou vztahovat k veřejně dostupné normě, která odráží normu použitou při certifikaci podle tohoto nařízení, jako jsou společná kritéria pro hodnocení bezpečnosti informačních technologií a společná metodika pro hodnocení bezpečnosti informačních technologií.

(3) Systém EUCC používá skupinu posouzení zranitelnosti podle společných kritérií (AVA_VAN), složky 1 až 5. Těchto pět složek poskytuje všechny hlavní determinanty a závislosti pro analýzu zranitelnosti produktů IKT. Vzhledem k tomu, že tyto složky odpovídají úrovním záruky uvedeným v tomto nařízení, umožňují informovaný výběr záruky na základě provedených hodnocení bezpečnostních požadavků a rizika spojeného se zamýšleným použitím produktu IKT. Žadatel o certifikát EUCC by měl poskytnout dokumentaci týkající se zamýšleného použití produktu IKT a analýzu úrovní rizik spojených s tímto použitím, aby subjekt posuzování shody mohl zhodnotit vhodnost zvolené úrovně záruky. Pokud hodnotící a certifikační činnosti provádí stejný subjekt posuzování shody, měl by žadatel předložit požadované informace pouze jednou.

(4) Technickou oblastí se rozumí referenční rámec, který zahrnuje skupinu produktů IKT, které mají specifické a podobné bezpečnostní funkce, jež zmírňují útoky, jejichž charakteristiky jsou společné pro danou úroveň záruky. Technická oblast uvádí v přehledech aktuálních certifikačních postupů konkrétní bezpečnostní požadavky, jakož i další metody, techniky a nástroje hodnocení, které se týkají certifikace produktů IKT, na něž se tato technická oblast vztahuje. Technická oblast proto také podporuje harmonizaci hodnocení produktů IKT, na které se vztahuje.

([1]) Úř. věst. L 151, 7.6.2019, s. 15.

([2]) Dohoda o vzájemném uznávání osvědčení o hodnocení bezpečnosti informačních technologií, verze 3.0 z ledna 2010, dostupná na sogis.eu, schválená skupinou vyšších úředníků pro bezpečnost informačních systémů Evropské komise v reakci na bod 3 doporučení Rady 95/144/ES ze dne 7. dubna 1995 o obecných kritériích pro hodnocení bezpečnosti informačních technologií (Úř. věst. L 93, 26.4.1995, s. 27).

V současné době se pro certifikaci na úrovních AVA_VAN.4 a AVA_VAN.5 běžně používají dvě technické oblasti. První technickou oblastí je technická oblast „čipové karty a podobná zařízení“, kde významná část požadovaných bezpečnostních funkcí závisí na specifických, přizpůsobených a často oddělitelných hardwarových prvcích (např. hardware čipových karet, integrované obvody, složené produkty s čipovou kartou, moduly důvěryhodné platformy používané v důvěryhodných počítačových systémech nebo karty digitálních tachografů). Druhou technickou oblastí jsou „hardwarová zařízení s bezpečnostními schránkami“, kde významná část požadovaných bezpečnostních funkcí závisí na hardwarovém fyzickém obalu (označovaném jako „bezpečnostní schránka“), který je navržen tak, aby odolal přímým útokům, např. platební terminály, tachografy ve vozidlech, inteligentní měřiče, terminály kontroly přístupu a hardwarové bezpečnostní moduly).

(5) Při podání žádosti o certifikaci by měl žadatel uvést důvody pro výběr úrovně záruky do souvislosti s cíli stanovenými v článku 51 nařízení (EU) 2019/881 a s výběrem složek z katalogu funkčních požadavků na bezpečnost a požadavků na bezpečnostní záruku obsažených ve společných kritériích. Certifikační subjekty by měly posoudit vhodnost zvolené úrovně záruky a zajistit, aby zvolená úroveň odpovídala úrovni rizika spojeného se zamýšleným použitím produktu IKT.

(6) Podle společných kritérií se certifikace provádí na základě bezpečnostního cíle, který zahrnuje definici bezpečnostního problému produktu IKT a bezpečnostních cílů, které tento problém řeší. Bezpečnostní problém obsahuje podrobnosti o zamýšleném použití produktu IKT a rizicích spojených s tímto použitím. Vybraný soubor bezpečnostních požadavků odpovídá jak bezpečnostnímu problému, tak bezpečnostním cílům produktu IKT.

(7) Profily ochrany jsou účinným prostředkem pro předběžné stanovení společných kritérií, která se týkají dané kategorie produktů IKT, a proto jsou také základním prvkem v procesu certifikace produktů IKT, na které se profil ochrany vztahuje. Profil ochrany se používá k posouzení budoucích bezpečnostních cílů, které spadají do dané kategorie produktů IKT, jimiž se daný profil ochrany zabývá. Profily ochrany dále zefektivňují a zvyšují účinnost procesu certifikace produktů IKT a pomáhají uživatelům správně a efektivně specifikovat funkčnost produktů IKT. Proto by profily ochrany měly být považovány za nedílnou součást procesu IKT vedoucího k certifikaci produktů IKT.

(8) Aby profily ochrany mohly plnit úlohu v procesu IKT podporujícím vývoj a dodání certifikovaného produktu IKT, mělo by být možné tyto profily certifikovat nezávisle na certifikaci konkrétního produktu IKT, který spadá pod příslušný profil ochrany. Proto je pro zajištění vysoké úrovně kybernetické bezpečnosti nezbytné uplatňovat na profily ochrany přinejmenším stejnou úroveň monitorování jako na bezpečnostní cíle. Profily ochrany by měly být zhodnoceny a certifikovány odděleně od souvisejícího produktu IKT a výhradně za použití třídy záruky pro profily ochrany (APE) a případně pro konfigurace profilů ochrany (ACE) podle společných kritérií a společné metodiky hodnocení. Vzhledem k jejich důležité a citlivé roli jako referenční hodnoty při certifikaci produktů IKT by je měly certifikovat pouze veřejné subjekty nebo certifikační subjekt, který získal předchozí schválení pro konkrétní profil ochrany od vnitrostátního orgánu certifikace kybernetické bezpečnosti. Vzhledem k jejich zásadní úloze při certifikaci na úrovni záruky „vysoká“, zejména mimo technické oblasti, by měly být profily ochrany vypracovány jako přehledy aktuálních certifikačních postupů, které by měla schválit Evropská skupina pro certifikaci kybernetické bezpečnosti.

(9) Certifikované profily ochrany by měly být zahrnuty do monitorování shody a souladu se systémem EUCC vnitrostátními orgány certifikace kybernetické bezpečnosti. Pokud jsou pro konkrétní certifikované profily ochrany k dispozici metodika, nástroje a dovednosti používané v rámci přístupů k hodnocení produktů IKT, mohou být technické oblasti založeny na těchto konkrétních profilech ochrany.

(10) V zájmu dosažení vysoké úrovně důvěryhodnosti a záruky u certifikovaných produktů IKT by podle tohoto nařízení nemělo být povoleno sebehodnocení. Mělo by být povoleno pouze posuzování shody zařízením ITSEF a certifikačními subjekty třetí strany.

(11) Společenství SOG-IS poskytlo společné výklady a přístupy k uplatňování společných kritérií a společné metodiky hodnocení při certifikaci, zejména pro úroveň záruky „vysoká“, o niž usilují technické oblasti „čipové karty a podobná zařízení“ a „hardwarová zařízení s bezpečnostními schránkami“. Opětovné použití těchto podpůrných dokumentů v systému EUCC zajistí hladký přechod z vnitrostátních systémů SOG-IS na harmonizovaný systém EUCC. Proto by měly být do tohoto nařízení zahrnuty harmonizované metodiky hodnocení, které mají obecný význam pro všechny certifikační činnosti. Kromě toho by Komise měla mít možnost požádat Evropskou skupinu pro certifikaci kybernetické bezpečnosti, aby přijala stanovisko, v němž schválí a doporučí použití metodik pro hodnocení uvedených v přehledech aktuálních certifikačních postupů pro certifikaci produktu IKT nebo profilu ochrany v rámci systému EUCC. Toto nařízení proto v příloze I uvádí přehledy aktuálních certifikačních postupů pro hodnotící činnosti prováděné subjekty posuzování shody. Evropská skupina pro certifikaci kybernetické bezpečnosti by měla schvalovat a udržovat přehledy aktuálních certifikačních postupů. Přehledy aktuálních certifikačních postupů by se měly používat při certifikaci. Pouze ve výjimečných a řádně odůvodněných případech je subjekt posuzování shody nesmí použít, a to za zvláštních podmínek, zejména po schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti.

(12) Certifikace produktů IKT na úrovni AVA_VAN 4 nebo 5 by měla být možná pouze za zvláštních podmínek a v případě, že je k dispozici specifická metodika hodnocení. Tato specifická metodika hodnocení může být zakotvena v přehledech aktuálních certifikačních postupů příslušných pro danou technickou oblast nebo ve specifických profilech ochrany přijatých jako přehled aktuálních certifikačních postupů, které jsou relevantní pro danou kategorii produktů. Pouze ve výjimečných a řádně odůvodněných případech by měla být možná certifikace na těchto úrovních záruky, a to za zvláštních podmínek, zejména po schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti, včetně příslušné metodiky hodnocení. Takové výjimečné a řádně odůvodněné případy mohou existovat, pokud právní předpisy Unie nebo vnitrostátní právní předpisy vyžadují certifikaci produktu IKT na úrovni AVA_VAN 4 nebo 5. Podobně lze ve výjimečných a řádně odůvodněných případech certifikovat profily ochrany bez použití příslušných přehledů aktuálních certifikačních postupů, a to za zvláštních podmínek, zejména po schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti, včetně příslušné metodiky hodnocení.

(13) Cílem označení a štítků používaných podle EUCC je viditelně prokázat uživatelům důvěryhodnost certifikovaného produktu IKT a umožnit jim informovaný výběr při nákupu produktů IKT. Používání označení a štítků by mělo rovněž podléhat pravidlům a podmínkám stanoveným v normě ISO/IEC 17065 a případně v normě ISO/IEC 17030 s příslušnými pokyny.

(14) Certifikační subjekty by měly rozhodnout o době platnosti certifikátů s ohledem na životní cyklus dotčeného produktu IKT. Doba platnosti by neměla přesáhnout pět let. Vnitrostátní orgány certifikace kybernetické bezpečnosti by měly pracovat na harmonizaci doby platnosti v Unii.

(15) Pokud se rozsah stávajícího certifikátu EUCC sníží, certifikát se zruší a vydá se nový certifikát s novým rozsahem, aby byli uživatelé jasně informováni o aktuálním rozsahu a úrovni záruky certifikátu daného produktu IKT.

(16) Certifikace profilů ochrany se liší od certifikace produktů IKT, protože se týká procesu IKT. Vzhledem k tomu, že profil ochrany zahrnuje kategorii produktů IKT, nelze jeho hodnocení a certifikaci provádět na základě jediného produktu IKT. Vzhledem k tomu, že profil ochrany sjednocuje obecné bezpečnostní požadavky týkající se kategorie produktů IKT, a nezávisle na tom, jak se na produktu IKT projevuje jeho prodejce, měla by doba platnosti certifikátu EUCC pro profil ochrany v zásadě trvat minimálně pět let a může být prodloužena až na dobu životnosti profilu ochrany.

(17) Subjekt posuzování shody je definován jako subjekt, který provádí činnosti posuzování shody, včetně kalibrace, zkoušení, certifikace a inspekce. V zájmu zajištění vysoké kvality služeb toto nařízení stanoví, že činnosti zkoušení na jedné straně a činnosti certifikace a inspekce na straně druhé by měly provádět subjekty, které působí nezávisle na sobě, a to zařízení pro hodnocení bezpečnosti informačních technologií („zařízení ITSEF“) a certifikační subjekty. Oba typy subjektů posuzování shody by měly být akreditovány a v určitých situacích autorizovány.

(18) Certifikační subjekt by měl být akreditován v souladu s normou ISO/IEC 17065 vnitrostátním akreditačním orgánem pro úroveň záruky „významná“ a „vysoká“. Kromě akreditace podle nařízení (EU) 2019/881 ve spojení s nařízením (ES) č. 765/2008 by měly subjekty posuzování shody splňovat zvláštní požadavky, aby byla zaručena jejich odborná způsobilost k hodnocení požadavků na kybernetickou bezpečnost v rámci úrovně záruky „vysoká“ podle EUCC, která je potvrzena „autorizací“. Na podporu autorizačního procesu je třeba vypracovat příslušné přehledy aktuálních certifikačních postupů, které agentura ENISA zveřejní po schválení Evropskou skupinou pro certifikaci kybernetické bezpečnosti.

(19) Odborná způsobilost zařízení ITSEF by měla být posuzována prostřednictvím akreditace zkušební laboratoře v souladu s normou ISO/IEC 17025 a doplněna normou ISO/IEC 23532-1 pro celý soubor hodnotících činností, které jsou relevantní pro úroveň záruky a jsou specifikovány v normě ISO/IEC 18045 ve spojení s normou ISO/IEC 15408. Certifikační subjekt i zařízení ITSEF by měly zavést a udržovat vhodný systém řízení způsobilosti personálu, který vychází z normy ISO/IEC 19896-1 pro prvky a úrovně způsobilosti a pro posouzení způsobilosti. Pro úroveň znalostí, dovedností, zkušeností a vzdělání by měly být použitelné požadavky na hodnotitele převzaty z normy ISO/IEC 19896-3. V souladu s cíli systému by měla být prokázána rovnocenná ustanovení a opatření týkající se odchylek od těchto systémů řízení způsobilosti.

(20) Aby mohlo být zařízení ITSEF autorizováno, mělo by prokázat svou schopnost určit neexistenci známých zranitelností, správné a důsledné zavádění nejmodernějších bezpečnostních funkcí pro danou technologii a odolnost cílového produktu IKT vůči zkušeným útočníkům. Pro autorizace v technické oblasti „čipových karet a podobných zařízení“ by mělo zařízení ITSEF navíc prokázat technické schopnosti nezbytné pro hodnotící činnosti a související úkoly, jak je definováno v podpůrném dokumentu v rámci společných kritérií „Minimální požadavky na bezpečnostní hodnocení čipových karet a podobných zařízení vůči zařízením ITSEF“ ([3]). Pro získání autorizace v technické oblasti „hardwarová zařízení s bezpečnostními schránkami“ by mělo zařízení ITSEF navíc prokázat minimální technické požadavky nezbytné pro provádění hodnotících činností a souvisejících úkolů u hardwarových zařízení s bezpečnostními schránkami, jak doporučuje Evropská skupina pro certifikaci kybernetické bezpečnosti. V kontextu minimálních požadavků by zařízení ITSEF mělo být schopno provádět různé typy útoků uvedené v podpůrném dokumentu v rámci společných kritérií „Uplatnění potenciálu útoku na hardwarová zařízení s bezpečnostními schránkami“. Tyto schopnosti zahrnují znalosti a dovednosti hodnotitele a vybavení a metody hodnocení potřebné k určení a posouzení různých typů útoků.

(21) Vnitrostátní orgán certifikace kybernetické bezpečnosti by měl monitorovat soulad certifikačních subjektů, zařízení ITSEF a držitelů certifikátů s povinnostmi vyplývajícími z tohoto nařízení a nařízení (EU) 2019/881. Vnitrostátní orgán certifikace kybernetické bezpečnosti by měl za tímto účelem využívat všechny vhodné zdroje informací, včetně informací získaných od účastníků certifikačního procesu a z vlastních šetření.

(22) Certifikační subjekty by měly spolupracovat s příslušnými orgány dozoru nad trhem a zohlednit veškeré informace o zranitelnosti, které by mohly být relevantní pro produkty IKT, pro něž vydaly certifikáty. Certifikační subjekty by měly monitorovat profily ochrany, které certifikovaly, aby zjistily, zda bezpečnostní požadavky stanovené pro danou kategorii produktů IKT nadále odrážejí nejnovější vývoj v oblasti hrozeb.

(23) Na podporu monitorování souladu by měly vnitrostátní orgány certifikace kybernetické bezpečnosti spolupracovat s příslušnými orgány dozoru nad trhem v souladu s článkem 58 nařízení Evropského parlamentu a Rady (EU) 2019/881 a nařízením Evropského parlamentu a Rady (EU) 2019/1020 ([4]). Hospodářské subjekty v Unii jsou podle čl. 4 odst. 3 nařízení 2019/1020 povinny sdílet informace a spolupracovat s orgány dozoru nad trhem.

([3]) Společná interpretační knihovna: Minimální požadavky na bezpečnostní hodnocení čipových karet a podobných zařízení vůči zařízením ITSEF, verze 2.1 z února 2020, k dispozici na sogis.eu.

([4]) Nařízení Evropského parlamentu a Rady (EU) 2019/1020 ze dne 20. června 2019 o dozoru nad trhem a souladu výrobků s předpisy a o změně směrnice 2004/42/ES a nařízení (ES) č. 765/2008 a (EU) č. 305/2011 (Úř. věst. L 169, 25.6.2019, s. 1).

(24) Certifikační subjekty by měly monitorovat soulad držitelů certifikátu a shodu všech certifikátů vydaných podle EUCC. Monitorování by mělo zajistit, aby všechny hodnotící zprávy poskytované zařízením ITSEF a závěry v nich přijaté, jakož i kritéria a metody hodnocení byly důsledně a správně uplatňovány ve všech certifikačních činnostech.

(25) Pokud jsou zjištěny potenciální problémy s nesouladem, které se týkají certifikovaného produktu IKT, je důležité zajistit přiměřenou reakci. Platnost certifikátů proto může být pozastavena. Pozastavení by mělo znamenat určitá omezení týkající se propagace a používání daného produktu IKT, ale nemělo by mít vliv na platnost certifikátu. Pozastavení by měl držitel certifikátu EU oznámit kupujícím dotčených produktů IKT, zatímco příslušný vnitrostátní orgán certifikace kybernetické bezpečnosti by měl informovat příslušné orgány dozoru nad trhem. Za účelem informování veřejnosti by agentura ENISA měla informace o pozastavení zveřejnit na vyhrazených internetových stránkách.

(26) Držitel certifikátu EUCC by měl zavést nezbytné postupy pro řízení zranitelností a zajistit, aby tyto postupy byly zakotveny v jeho organizaci. Pokud se držitel certifikátu EUCC dozví o potenciální zranitelnosti, měl by provést analýzu dopadu zranitelností. Pokud analýza dopadu zranitelností potvrdí, že zranitelnost lze zneužít, měl by držitel certifikátu zaslat zprávu o posouzení certifikačnímu subjektu, který by měl následně informovat vnitrostátní orgán certifikace kybernetické bezpečnosti. Zpráva by měla informovat o dopadu zranitelností, potřebných změnách nebo nápravných řešeních, včetně možných širších důsledků zranitelnosti a nápravných řešení pro další produkty. V případě potřeby by měla postup zveřejňování informací o zranitelnostech doplnit norma EN ISO/IEC 29147.

(27) Pro účely certifikace získávají subjekty posuzování shody a vnitrostátní orgány certifikace kybernetické bezpečnosti důvěrné a citlivé údaje a obchodní tajemství, které se týkají také duševního vlastnictví nebo monitorování souladu a jež vyžadují odpovídající ochranu. Měly by proto mít potřebnou odbornou způsobilost a znalosti a měly by zavést systémy ochrany informací. Požadavky a podmínky ochrany informací by měly být splněny jak pro akreditaci, tak pro autorizaci.

(28) Agentura ENISA by měla v souladu s nařízením (EU) 2019/881 na svých internetových stránkách věnovaných certifikaci kybernetické bezpečnosti poskytnout seznam certifikovaných profilů ochrany a uvést jejich status.

(29) Toto nařízení stanoví podmínky pro dohody o vzájemném uznávání se třetími zeměmi. Tyto dohody o vzájemném uznávání mohou být dvoustranné nebo vícestranné a měly by nahradit podobné existující dohody. S ohledem na usnadnění hladkého přechodu k těmto dohodám o vzájemném uznávání mohou členské státy po omezenou dobu pokračovat v provádění stávajících ujednání o spolupráci se třetími zeměmi.

(30) Certifikační subjekty vydávající certifikáty EUCC na úrovni záruky „vysoká“, jakož i příslušná související zařízení ITSEF, by měly být podrobeny vzájemnému hodnocení. Cílem vzájemného hodnocení by mělo být určení trvalého souladu stanov a postupů vzájemně hodnoceného certifikačního subjektu s požadavky systému EUCC. Vzájemné hodnocení se liší od vzájemného hodnocení mezi vnitrostátními orgány certifikace kybernetické bezpečnosti, jak je stanoveno v článku 59 nařízení (EU) 2019/881. Vzájemná hodnocení by měla zajistit, aby certifikační subjekty pracovaly harmonizovaným způsobem a vydávaly certifikáty stejné kvality, a měla by identifikovat případné silné nebo slabé stránky ve výkonu certifikačních subjektů, a to i s ohledem na sdílení osvědčených postupů. Vzhledem k tomu, že existují různé typy certifikačních subjektů, měly by být povoleny různé typy vzájemného hodnocení. Ve složitějších případech, jako jsou certifikační subjekty vydávající certifikáty na různých úrovních AVA_VAN, lze použít různé typy vzájemného hodnocení za předpokladu, že jsou splněny všechny požadavky.

(31) Evropská skupina pro certifikaci kybernetické bezpečnosti by měla hrát důležitou roli při udržování tohoto systému. Mělo by to být mimo jiné prováděno prostřednictvím spolupráce se soukromým sektorem, vytvořením specializovaných podskupin a příslušnými přípravnými pracemi a pomocí, o kterou požádá Komise. Evropská skupina pro certifikaci kybernetické bezpečnosti hraje důležitou roli při schvalování přehledů aktuálních certifikačních postupů. Při schvalování a přijímání přehledů aktuálních certifikačních postupů by měly být náležitě zohledněny prvky uvedené v čl. 54 odst. 1 písm. c) nařízení (EU) 2019/881. Technické oblasti a přehledy aktuálních

certifikačních postupů by měly být zveřejněny v příloze I tohoto nařízení. Profily ochrany, které byly přijaty jako přehledy aktuálních certifikačních postupů, by měly být zveřejněny v příloze II. Aby byla zajištěna dynamika těchto příloh, může je Komise měnit v souladu s postupem stanoveným v čl. 66 odst. 2 nařízení (EU) 2019/881 a s ohledem na stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti. Příloha III obsahuje doporučené profily ochrany, které v době vstupu tohoto nařízení v platnost nejsou přehledy aktuálních certifikačních postupů. Měly by být zveřejněny na internetových stránkách agentury ENISA uvedených v čl. 50 odst. 1 nařízení (EU) 2019/881.

(32) Toto nařízení by se mělo začít používat 12 měsíců po vstupu v platnost. Požadavky kapitoly IV a přílohy V nevyžadují přechodné období, a měly by se proto použít od vstupu tohoto nařízení v platnost.

(33) Opatření stanovená tímto nařízením jsou v souladu se stanoviskem Evropského výboru pro certifikaci kybernetické bezpečnosti zřízeného článkem 66 nařízení (EU) 2019/881,

PŘIJALA TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět a rozsah působnosti

Toto nařízení stanoví evropský systém certifikace kybernetické bezpečnosti založený na společných kritériích (EUCC).

Toto nařízení se vztahuje na všechny produkty informačních a komunikačních technologií (dále jen „IKT“) včetně jejich dokumentace, které jsou předkládány k certifikaci podle EUCC, a na všechny profily ochrany, které jsou předkládány k certifikaci v rámci procesu IKT vedoucího k certifikaci produktů IKT.

Článek 2

Definice

Pro účely tohoto nařízení se použijí následující definice:

1) „společnými kritérii“ se rozumí společná kritéria pro hodnocení bezpečnosti informačních technologií, jak jsou stanovena v normě ISO/IEC 15408;

2) „společnou metodikou hodnocení“ se rozumí společná metodika hodnocení bezpečnosti informačních technologií, jak je stanovena v normě ISO/IEC 18045;

3) „cílem hodnocení“ se rozumí produkt IKT nebo jeho část nebo profil ochrany jako součást procesu IKT, který je podroben hodnocení kybernetické bezpečnosti za účelem získání certifikace v rámci EUCC;

4) „bezpečnostním cílem“ se rozumí tvrzení o bezpečnostních požadavcích závislých na zavedení pro konkrétní produkt IKT;

5) „profilem ochrany“ se rozumí proces IKT, který stanoví bezpečnostní požadavky pro určitou kategorii produktů IKT, který řeší potřeby v oblasti bezpečnosti nezávislé na zavedení a který lze použít k posouzení produktů IKT spadajících do této konkrétní kategorie pro účely jejich certifikace;

6) „hodnotící technickou zprávou“ se rozumí dokument vypracovaný zařízením ITSEF, v němž jsou uvedena zjištění, závěry a odůvodnění získané během hodnocení produktu IKT nebo profilu ochrany v souladu s pravidly a povinnostmi stanovenými v tomto nařízení;

7) „zařízením ITSEF“ se rozumí zařízení pro hodnocení bezpečnosti informačních technologií, což je subjekt posuzování shody podle definice v čl. 2 bodě 13 nařízení (ES) č. 765/2008, který provádí úkoly v oblasti hodnocení;

8) „úrovní AVA_VAN“ se rozumí úroveň záruky analýzy zranitelnosti, která označuje stupeň hodnotících činností ve věci kybernetické bezpečnosti provedených za účelem stanovení úrovně odolnosti proti potenciální zneužitelnosti chyb nebo slabin v cíli hodnocení v jeho provozním prostředí, jak je stanoveno ve společných kritériích;

9) „certifikátem EUCC“ se rozumí certifikát kybernetické bezpečnosti vydaný podle systému EUCC pro produkty IKT nebo pro profily ochrany, které lze použít výhradně v procesu certifikace produktů IKT;

10) „složeným produktem“ se rozumí produkt IKT, který je hodnocen společně s jiným základním produktem IKT, který již obdržel certifikát EUCC a na jehož bezpečnostní funkci složený produkt IKT závisí;

11) „vnitrostátním orgánem certifikace kybernetické bezpečnosti“ se rozumí orgán určený členským státem podle čl. 58 odst. 1 nařízení (EU) 2019/881;

12) „certifikačním subjektem“ se rozumí subjekt posuzování shody podle definice v čl. 2 bodě 13 nařízení (ES) č. 765/2008, který provádí certifikační činnosti;

13) „technickou oblastí“ se rozumí společný technický rámec související s určitou technologií pro harmonizovanou certifikaci se souborem charakteristických bezpečnostních požadavků;

14) „přehledem aktuálních certifikačních postupů“ se rozumí dokument, který specifikuje metody, techniky a nástroje hodnocení, které se vztahují na certifikaci produktů IKT nebo na bezpečnostní požadavky kategorie obecných produktů IKT nebo jakékoli jiné požadavky nezbytné pro certifikaci s cílem harmonizovat hodnocení, a to zejména technických oblastí nebo profilů ochrany;

15) „orgánem dozoru nad trhem“ se rozumí orgán definovaný v čl. 3 odst. 4 nařízení (EU) 2019/1020.

Článek 3

Normy pro hodnocení

Na hodnocení prováděná v rámci systému EUCC se vztahují následující normy:

a) společná kritéria;

b) společná metodika hodnocení.

Článek 4

Úrovně záruky

1. Certifikační subjekty vydávají certifikáty EUCC na úrovni záruky „významná“ nebo „vysoká“.

2. Certifikáty EUCC na úrovni záruky „významná“ odpovídají certifikátům, které pokrývají úroveň AVA_VAN 1 nebo 2.

3. Certifikáty EUCC na úrovni záruky „vysoká“ odpovídají certifikátům, které pokrývají úroveň AVA_VAN 3, 4 nebo 5.

4. Úroveň záruky potvrzená v certifikátu EUCC rozlišuje mezi shodným a rozšířeným použitím složek záruky, jak je uvedeno ve společných kritériích v souladu s přílohou VIII.

5. Subjekty posuzování shody použijí ty složky záruky, na nichž závisí zvolená úroveň AVA_VAN v souladu s normami uvedenými v článku 3.

Článek 5

Metody certifikace produktů IKT

1. Certifikace produktu IKT se provádí na základě jeho bezpečnostního cíle:

a) podle definice žadatele, nebo

b) začlenění certifikovaného profilu ochrany jako součásti procesu IKT, pokud produkt IKT spadá do kategorie produktů IKT, na které se tento profil ochrany vztahuje.

2. Profily ochrany se certifikují výhradně pro účely certifikace produktů IKT spadajících do konkrétní kategorie produktů IKT, na které se profil ochrany vztahuje.

Článek 6

Vlastní posuzování shody

Vlastní posuzování shody ve smyslu článku 53 nařízení (EU) 2019/881 není povoleno.

KAPITOLA II

CERTIFIKACE PRODUKTŮ IKT

ODDÍL I

Zvláštní hodnotící normy a požadavky

Článek 7

Kritéria a metody hodnocení produktů IKT

1. Produkt IKT předložený k certifikaci musí být hodnocen minimálně podle následujících kritérií:

a) použitelné prvky norem uvedených v článku 3;

b) třídy požadavků na bezpečnostní záruku pro posouzení zranitelnosti a nezávislé testování funkčnosti, jak je stanoveno v hodnotících normách uvedených v článku 3;

c) úroveň rizika spojeného se zamýšleným použitím dotčených produktů IKT podle článku 52 nařízení (EU) 2019/881 a jejich bezpečnostní funkce, které podporují bezpečnostní cíle stanovené v článku 51 nařízení (EU) 2019/881;

d) příslušné přehledy aktuálních certifikačních postupů uvedené v příloze I a

e) příslušné certifikované profily ochrany uvedené v příloze II.

2. Ve výjimečných a řádně odůvodněných případech může subjekt posuzování shody požádat, aby se nepoužil příslušný přehled aktuálních certifikačních postupů. V takových případech subjekt posuzování shody informuje vnitrostátní orgán certifikace kybernetické bezpečnosti a svou žádost řádně odůvodní. Vnitrostátní orgán certifikace kybernetické bezpečnosti posoudí odůvodnění výjimky a v oprávněných případech ji schválí. Do přijetí rozhodnutí vnitrostátního orgánu certifikace kybernetické bezpečnosti subjekt posuzování shody nevydá žádný certifikát. Vnitrostátní orgán

certifikace kybernetické bezpečnosti schválenou výjimku bez zbytečného odkladu oznámí Evropské skupině pro certifikaci kybernetické bezpečnosti, která může vydat stanovisko. Vnitrostátní orgán certifikace kybernetické bezpečnosti v co největší míře zohlední stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti.

3. Certifikace produktů IKT na úrovni AVA_VAN 4 nebo 5 je možná pouze v těchto případech:

a) pokud se na produkt IKT vztahuje některá z technických oblastí uvedených v příloze I, hodnotí se v souladu s příslušnými přehledy aktuálních certifikačních postupů těchto technických oblastí;

b) pokud produkt IKT spadá do kategorie produktů IKT, na něž se vztahuje certifikovaný profil ochrany, který zahrnuje úrovně AVA_VAN 4 nebo 5 a který byl uveden jako aktuální profil ochrany v příloze II, hodnotí se v souladu s metodikou hodnocení stanovenou pro tento profil ochrany;

c) pokud se nepoužijí písmena a) a b) tohoto odstavce a pokud je zařazení technické oblasti do přílohy I nebo certifikovaného profilu ochrany do přílohy II v dohledné době nepravděpodobné, a pouze ve výjimečných a řádně odůvodněných případech za podmínek stanovených v odstavci 4.

4. Pokud se subjekt posuzování shody domnívá, že se jedná o výjimečný a řádně odůvodněný případ uvedený v odst. 3 písm. c), oznámí zamýšlenou certifikaci vnitrostátnímu orgánu certifikace kybernetické bezpečnosti s odůvodněním a návrhem metodiky hodnocení. Vnitrostátní orgán certifikace kybernetické bezpečnosti posoudí oprávněnost výjimky a v odůvodněných případech schválí nebo změní metodiku hodnocení, kterou má subjekt posuzování shody použít. Do přijetí rozhodnutí vnitrostátního orgánu certifikace kybernetické bezpečnosti subjekt posuzování shody nevydá žádný certifikát. Vnitrostátní orgán certifikace kybernetické bezpečnosti zamýšlenou certifikaci bez zbytečného odkladu oznámí Evropské skupině pro certifikaci kybernetické bezpečnosti, která může vydat stanovisko. Vnitrostátní orgán certifikace kybernetické bezpečnosti v co největší míře zohlední stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti.

5. V případě, že je produkt IKT hodnocen jako složený produkt v souladu s příslušnými přehledy aktuálních certifikačních postupů, sdílí zařízení ITSEF, které provedlo hodnocení základního produktu IKT, příslušné informace se zařízením ITSEF, které provádí hodnocení složeného produktu IKT.

ODDÍL II

Vydávání, obnovování a zrušení certifikátů eucc

Článek 8

Informace nezbytné pro certifikaci

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

2. Informace uvedené v odstavci 1 obsahují všechny relevantní důkazy v souladu s oddíly „Prvky činnosti vývojáře“ v příslušném formátu, jak je stanoveno v oddílech „Obsah a prezentace prvku důkazů“ společných kritérií a společné metodiky hodnocení pro zvolenou úroveň záruky a související požadavky na bezpečnostní záruku. Důkazy v případě potřeby obsahují podrobnosti o produktu IKT a jeho zdrojovém kódu v souladu s tímto nařízením, s výhradou ochranných opatření proti neoprávněnému zveřejnění.

3. Žadatelé o certifikaci mohou certifikačnímu subjektu a zařízení ITSEF předložit příslušné výsledky hodnocení z předchozí certifikace podle:

a) tohoto nařízení;

b) jiného evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881;

c) vnitrostátního systému uvedeného v článku 49 tohoto nařízení.

4. Pokud jsou výsledky hodnocení relevantní pro jeho úkoly, může zařízení ITSEF tyto výsledky hodnocení opětovně použít za předpokladu, že odpovídají platným požadavkům a je potvrzena jejich pravost.

5. Pokud certifikační subjekt povolí certifikaci složeného produktu, žadatel o certifikaci zpřístupní certifikačnímu subjektu a zařízení ITSEF všechny nezbytné prvky, případně v souladu s přehledem aktuálních certifikačních postupů.

6. Žadatelé o certifikaci rovněž poskytnou certifikačnímu subjektu a zařízení ITSEF následující informace:

a) odkaz na své internetové stránky obsahující doplňující informace o kybernetické bezpečnosti uvedené v článku 55 nařízení (EU) 2019/881;

b) popis postupů žadatele pro řízení zranitelností a jejich zveřejňování.

7. Veškerou příslušnou dokumentaci uvedenou v tomto článku uchovává certifikační subjekt, zařízení ITSEF a žadatel po dobu pěti let po pozbytí platnosti certifikátu.

Článek 9

Podmínky pro vydání certifikátu EUCC

1. Certifikační subjekty vydají certifikát EUCC, pokud jsou splněny všechny následující podmínky:

a) kategorie produktu IKT spadá do oblasti působnosti akreditace a případně autorizace certifikačního subjektu a zařízení ITSEF zapojených do certifikace;

b) žadatel o certifikaci podepsal prohlášení, že přijímá všechny závazky uvedené v odstavci 2;

c) zařízení ITSEF ukončilo hodnocení bez námitek v souladu s hodnotícími normami, kritérii a metodami uvedenými v článcích 3 a 7;

d) certifikační subjekt ukončil přezkum výsledků hodnocení bez námitek;

e) certifikační subjekt ověřil, že hodnotící technické zprávy poskytnuté zařízením ITSEF jsou v souladu s poskytnutými důkazy a že byly správně použity normy, kritéria a metody hodnocení uvedené v článcích 3 a 7.

2. Žadatel o certifikaci přijímá následující závazky:

a) poskytnout certifikačnímu subjektu a zařízení ITSEF všechny nezbytné úplné a správné informace a na požádání poskytnout další potřebné informace;

b) nepropagovat produkt IKT jako certifikovaný podle EUCC před vydáním certifikátu EUCC;

c) propagovat produkt IKT jako certifikovaný pouze s ohledem na rozsah uvedený v certifikátu EUCC;

d) v případě pozastavení, zrušení nebo pozbytí platnosti certifikátu EUCC okamžitě přestat propagovat produkt IKT jako certifikovaný;

e) zajistit, aby produkty IKT prodávané s odkazem na certifikát EUCC byly zcela totožné s produktem IKT, který je předmětem certifikace;

f) dodržovat pravidla používání označení a štítku stanovená pro certifikát EUCC v souladu s článkem 11.

3. V případě, že je produkt IKT certifikován jako složený produkt v souladu s příslušnými přehledy aktuálních certifikačních postupů, sdílí certifikační subjekt, který provedl certifikaci základního produktu IKT, příslušné informace s certifikačním subjektem, který provádí certifikaci složeného produktu IKT.

Článek 10

Obsah a formát certifikátu EUCC

1. Certifikát EUCC musí obsahovat alespoň informace uvedené v příloze VII.

2. Certifikát EUCC nebo zpráva o certifikaci musí jednoznačně specifikovat rozsah a hranice certifikovaného produktu IKT a uvádět, zda byl certifikován celý produkt IKT, nebo pouze jeho části.

3. Certifikační subjekt poskytne žadateli certifikát EUCC alespoň v elektronické podobě.

4. Certifikační subjekt vypracuje zprávu o certifikaci v souladu s přílohou V pro každý certifikát EUCC, který vydá. Zpráva o certifikaci vychází z hodnotící technické zprávy vydané zařízením ITSEF. V hodnotící technické zprávě a ve zprávě o certifikaci se uvedou konkrétní kritéria hodnocení a metody uvedené v článku 7 použité pro hodnocení.

5. Certifikační subjekt poskytne vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a agentuře ENISA každý certifikát EUCC a každou zprávu o certifikaci v elektronické podobě.

Článek 11

Označení a štítek

1. Držitel certifikátu může certifikovaný produkt IKT opatřit označením a štítkem. Označení a štítek prokazují, že produkt IKT byl certifikován v souladu s tímto nařízením. Označení a štítek se připojí v souladu s tímto článkem a s přílohou IX.

2. Označení a štítek musí být viditelně, čitelně a nesmazatelně umístěny na certifikovaném produktu IKT nebo na jeho výrobním štítku. Pokud to vzhledem k povaze produktu není možné nebo odůvodněné, umístí se na obal a průvodní doklady. Pokud se certifikovaný produkt IKT dodává jako software, musí být označení a štítek viditelně, čitelně a nesmazatelně uvedeny v jeho průvodní dokumentaci nebo musí být tato dokumentace snadno a přímo přístupná uživatelům prostřednictvím internetových stránek.

3. Označení a štítek jsou uvedeny v příloze IX a obsahují:

a) úroveň záruky a úroveň AVA_VAN certifikovaného produktu IKT;

b) jedinečnou identifikaci certifikátu, která se skládá z:

   1) názvu systému;

   2) názvu a referenčního čísla akreditace certifikačního subjektu, který certifikát vydal;

   3) roku a měsíce vydání;

   4) identifikačního čísla přiděleného certifikačním subjektem, který certifikát vydal.

4. Označení a štítek musí být doplněny QR kódem s odkazem na internetovou stránku, která obsahuje alespoň:

a) informace o platnosti certifikátu,

b) nezbytné certifikační údaje uvedené v přílohách V a VII;

c) informace, které má držitel certifikátu zveřejnit v souladu s článkem 55 nařízení (EU) 2019/881 a

d) případně historické informace týkající se specifické certifikace nebo certifikací produktu IKT, aby byla umožněna sledovatelnost.

Článek 12

Doba platnosti certifikátu EUCC

1. Certifikační subjekt stanoví dobu platnosti každého vydaného certifikátu EUCC s ohledem na vlastnosti certifikovaného produktu IKT.

2. Doba platnosti certifikátu EUCC nesmí překročit pět let.

3. Odchylně od odstavce 2 smí tato doba přesáhnout pět let, a to po předchozím schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti. Vnitrostátní orgán certifikace kybernetické bezpečnosti oznámí Evropské skupině pro certifikaci kybernetické bezpečnosti udělené schválení bez zbytečného odkladu.

Článek 13

Přezkum certifikátu EUCC

1. Na žádost držitele certifikátu nebo z jiných oprávněných důvodů může certifikační subjekt rozhodnout o přezkumu certifikátu EUCC pro produkt IKT. Přezkum se provádí v souladu s přílohou IV. Rozsah přezkumu určí certifikační subjekt. Je-li to pro přezkum nezbytné, certifikační subjekt požádá zařízení ITSEF o provedení přehodnocení certifikovaného produktu IKT.

2. Na základě výsledků přezkumu a případného přehodnocení certifikační subjekt:

a) potvrdí certifikát EUCC;

b) zruší certifikát EUCC v souladu s článkem 14;

c) zruší certifikát EUCC v souladu s článkem 14 a vydá nový certifikát EUCC se stejným rozsahem a prodlouženou dobou platnosti nebo

d) zruší certifikát EUCC v souladu s článkem 14 a vydá nový certifikát EUCC s jiným rozsahem.

3. Certifikační subjekt může bez zbytečného odkladu rozhodnout o pozastavení platnosti certifikátu EUCC podle článku 30, dokud držitel certifikátu EUCC neučiní nápravná opatření.

Článek 14

Zrušení certifikátu EUCC

1. Aniž je dotčen čl. 58 odst. 8 písm. e) nařízení (EU) 2019/881, certifikát EUCC zruší certifikační subjekt, který jej vydal.

2. Certifikační subjekt uvedený v odstavci 1 oznámí zrušení certifikátu vnitrostátnímu orgánu certifikace kybernetické bezpečnosti. Toto zrušení oznámí rovněž agentuře ENISA s cílem usnadnit plnění jejího úkolu podle článku 50 nařízení (EU) 2019/881. Vnitrostátní orgán certifikace kybernetické bezpečnosti informuje ostatní příslušné orgány dozoru nad trhem.

3. Držitel certifikátu EUCC může požádat o zrušení certifikátu.

KAPITOLA III

CERTIFIKACE PROFILŮ OCHRANY

ODDÍL I

Zvláštní hodnotící normy a požadavky

Článek 15

Kritéria a metody hodnocení

1. Profil ochrany se vyhodnocuje minimálně podle následujících kritérií:

a) použitelné prvky norem uvedených v článku 3;

b) úroveň rizika spojeného se zamýšleným použitím dotčených produktů IKT podle článku 52 nařízení (EU) 2019/881 a jejich bezpečnostní funkce, které podporují bezpečnostní cíle stanovené v článku 51 tohoto nařízení; a

c) příslušné přehledy aktuálních certifikačních postupů uvedené v příloze I. Profil ochrany, na který se vztahuje technická oblast, se certifikuje podle požadavků stanovených v této technické oblasti.

2. Ve výjimečných a řádně odůvodněných případech může subjekt posuzování shody certifikovat profil ochrany, aniž by použil příslušné přehledy aktuálních certifikačních postupů. V takových případech informuje příslušný vnitrostátní orgán certifikace kybernetické bezpečnosti a poskytne odůvodnění pro zamýšlenou certifikaci bez použití příslušných přehledů aktuálních certifikačních postupů, jakož i navrhované metodiky hodnocení. Vnitrostátní orgán certifikace kybernetické bezpečnosti posoudí odůvodnění a v oprávněných případech schválí nepoužití příslušných přehledů aktuálních certifikačních postupů a případně schválí nebo změní metodiku hodnocení, kterou má subjekt posuzování shody použít. Do přijetí rozhodnutí vnitrostátního orgánu certifikace kybernetické bezpečnosti subjekt posuzování shody nevydá žádný certifikát pro profil ochrany. Vnitrostátní orgán certifikace kybernetické bezpečnosti bez zbytečného odkladu oznámí schválené nepoužití příslušných přehledů aktuálních certifikačních postupů Evropské skupině pro certifikaci kybernetické bezpečnosti, která může vydat stanovisko. Vnitrostátní orgán certifikace kybernetické bezpečnosti v co největší míře zohlední stanovisko Evropské skupiny pro certifikaci kybernetické bezpečnosti.

ODDÍL II

Vydávání, obnovování a zrušení certifikátů eucc pro profily ochrany

Článek 16

Informace nezbytné pro certifikaci profilů ochrany

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

Článek 17

Vydávání certifikátů EUCC pro profily ochrany

1. Žadatel o certifikaci poskytne certifikačnímu subjektu a zařízení ITSEF všechny potřebné úplné a správné informace.

2. Články 9 a 10 se použijí obdobně.

3. Zařízení ITSEF vyhodnotí, zda je profil ochrany úplný, konzistentní, technicky správný a účinný pro zamýšlené použití a bezpečnostní cíle kategorie produktů IKT, na které se daný profil ochrany vztahuje.

4. Profil ochrany certifikuje výhradně:

a) vnitrostátní orgán certifikace kybernetické bezpečnosti nebo jiný veřejný subjekt akreditovaný jako certifikační subjekt nebo

b) certifikační subjekt po předchozím schválení vnitrostátním orgánem certifikace kybernetické bezpečnosti pro každý jednotlivý profil ochrany.

Článek 18

Doba platnosti certifikátu EUCC pro profily ochrany

1. Certifikační subjekt stanoví dobu platnosti každého certifikátu EUCC.

2. Doba platnosti může být až do konce životnosti příslušného profilu ochrany.

Článek 19

Přezkum certifikátu EUCC pro profily ochrany

1. Na žádost držitele certifikátu nebo z jiných oprávněných důvodů může certifikační subjekt rozhodnout o přezkumu certifikátu EUCC pro profil ochrany. Přezkum se provádí za podmínek stanovených v článku 15. Rozsah přezkumu určí certifikační subjekt. Je-li to pro přezkum nezbytné, certifikační subjekt požádá zařízení ITSEF o provedení přehodnocení certifikovaného profilu ochrany.

2. Na základě výsledků přezkumu a případného přehodnocení certifikační subjekt provede jednu z následujících činností:

a) potvrdí certifikát EUCC;

b) zruší certifikát EUCC v souladu s článkem 20;

c) zruší certifikát EUCC v souladu s článkem 20 a vydá nový certifikát EUCC se stejným rozsahem a prodlouženou dobou platnosti

d) zruší certifikát EUCC v souladu s článkem 20 a vydá nový certifikát EUCC s jiným rozsahem.

Článek 20

Zrušení certifikátu EUCC pro profil ochrany

1. Aniž je dotčen čl. 58 odst. 8 písm. e) nařízení (EU) 2019/881, certifikát EUCC pro profil ochrany zruší certifikační subjekt, který jej vydal. Článek 14 se použije obdobně.

2. Certifikát pro profil ochrany vydaný v souladu s čl. 17 odst. 4 písm. b) zruší vnitrostátní orgán certifikace kybernetické bezpečnosti, který tento certifikát schválil.

KAPITOLA IV

SUBJEKTY POSUZOVÁNÍ SHODY

Článek 21

Další nebo zvláštní požadavky na certifikační subjekt

1. Certifikační subjekt je vnitrostátním orgánem certifikace kybernetické bezpečnosti autorizován vydávat certifikáty EUCC na úrovni záruky „vysoká“, pokud tento subjekt kromě splnění požadavků stanovených v čl. 60 odst. 1 a v příloze nařízení (EU) 2019/881 o akreditaci subjektů posuzování shody prokáže následující skutečnosti:

a) má odborné znalosti a kompetence požadované pro rozhodnutí o certifikaci na úrovni záruky „vysoká“;

b) provádí své certifikační činnosti ve spolupráci se zařízením ITSEF autorizovaným v souladu s článkem 22 a

c) má požadované kompetence a kromě požadavků stanovených v článku 43 zavedlo vhodná technická a provozní opatření k účinné ochraně důvěrných a citlivých informací pro úroveň záruky „vysoká“.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti posoudí, zda certifikační subjekt splňuje všechny požadavky stanovené v odstavci 1. Uvedené posouzení zahrnuje alespoň strukturované rozhovory a přezkum nejméně jedné pilotní certifikace provedené certifikačním subjektem v souladu s tímto nařízením.

Vnitrostátní orgán certifikace kybernetické bezpečnosti může v rámci svého posuzování opětovně použít veškeré vhodné důkazy z předchozí autorizace nebo podobných činností udělených podle:

a) tohoto nařízení;

b) jiného evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881;

c) vnitrostátního systému uvedeného v článku 49 tohoto nařízení.

3. Vnitrostátní orgán certifikace kybernetické bezpečnosti vypracuje zprávu o autorizaci, která podléhá vzájemnému hodnocení v souladu s čl. 59 odst. 3 písm. d) nařízení (EU) 2019/881.

4. Vnitrostátní orgán certifikace kybernetické bezpečnosti určí kategorie produktů IKT a profily ochrany, na které se autorizace vztahuje. Autorizace je platná po dobu, která není delší než doba platnosti akreditace. Může být na žádost obnovena, pokud certifikační subjekt stále splňuje požadavky stanovené v tomto článku. Pro obnovení autorizace se nevyžaduje žádné pilotní hodnocení.

5. Vnitrostátní orgán certifikace kybernetické bezpečnosti zruší certifikačnímu subjektu autorizaci, pokud již nesplňuje podmínky stanovené v tomto článku. Po zrušení autorizace se certifikační subjekt přestane okamžitě propagovat jako autorizovaný certifikační subjekt.

Článek 22

Další nebo zvláštní požadavky na zařízení ITSEF

1. Zařízení ITSEF je vnitrostátním orgánem certifikace kybernetické bezpečnosti autorizováno k provádění hodnocení produktů IKT, které podléhají certifikaci na úrovni záruky „vysoká“, pokud zařízení ITSEF kromě splnění požadavků stanovených v čl. 60 odst. 1 a v příloze nařízení (EU) 2019/881 o akreditaci subjektů posuzování shody prokáže splnění všech následujících podmínek:

a) má odborné znalosti nezbytné k provádění hodnotících činností pro určení odolnosti vůči nejmodernějším kybernetickým útokům prováděným subjekty se značnými dovednostmi a zdroji;

b) pro technické oblasti a profily ochrany, které jsou součástí procesu IKT pro tyto produkty IKT, má:

1) odborné znalosti k provádění specifických hodnotících činností nezbytných k metodickému určení odolnosti hodnoceného cíle proti zkušeným útočníkům v jeho provozním prostředí za předpokladu „středního“ nebo „vysokého“ potenciálu útoku, jak je stanoveno v normách uvedených v článku 3;

2) odbornou způsobilost podle přehledů aktuálních certifikačních postupů uvedených v příloze I;

c) má požadované kompetence a kromě požadavků stanovených v článku 43 zavedlo vhodná technická a provozní opatření k účinné ochraně důvěrných a citlivých informací pro úroveň záruky „vysoká“.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti posoudí, zda zařízení ITSEF splňuje všechny požadavky stanovené v odstavci 1. Uvedené posouzení zahrnuje alespoň strukturované rozhovory a přezkum nejméně jednoho pilotního hodnocení provedeného zařízením ITSEF v souladu s tímto nařízením.

3. Vnitrostátní orgán certifikace kybernetické bezpečnosti může v rámci svého posuzování opětovně použít veškeré vhodné důkazy z předchozí autorizace nebo podobných činností udělených podle:

a) tohoto nařízení;

b) jiného evropského systému certifikace kybernetické bezpečnosti přijatého podle článku 49 nařízení (EU) 2019/881;

c) vnitrostátního systému uvedeného v článku 49 tohoto nařízení.

4. Vnitrostátní orgán certifikace kybernetické bezpečnosti vypracuje zprávu o autorizaci, která podléhá vzájemnému hodnocení v souladu s čl. 59 odst. 3 písm. d) nařízení (EU) 2019/881.

5. Vnitrostátní orgán certifikace kybernetické bezpečnosti určí kategorie produktů IKT a profily ochrany, na které se autorizace vztahuje. Autorizace platí po dobu, která není delší než doba platnosti akreditace. Může být na žádost obnoveno, pokud zařízení ITSEF stále splňuje požadavky stanovené v tomto článku. Pro obnovení autorizace by nemělo být vyžadováno žádné pilotní hodnocení.

6. Vnitrostátní orgán certifikace kybernetické bezpečnosti zruší zařízení ITSEF autorizaci, pokud již nesplňuje podmínky stanovené v tomto článku. Po zrušení autorizace se zařízení ITSEF přestane propagovat jako autorizované zařízení ITSEF.

Článek 23

Oznámení certifikačních subjektů

1. Vnitrostátní orgán certifikace kybernetické bezpečnosti oznámí Komisi certifikační subjekty na svém území, které jsou na základě své akreditace způsobilé k certifikaci na úrovni záruky „významná“.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti oznámí Komisi certifikační subjekty na svém území, které jsou na základě své akreditace a rozhodnutí o autorizaci způsobilé k certifikaci na úrovni záruky „vysoká“.

3. Vnitrostátní orgán certifikace kybernetické bezpečnosti poskytne při oznámení certifikačních subjektů Komisi alespoň tyto informace:

a) úroveň nebo úrovně záruky, pro které je certifikační subjekt oprávněn vydávat certifikáty EUCC;

b) následující informace týkající se akreditace:

1) datum akreditace;

2) název a adresa certifikačního subjektu;

3) země registrace certifikačního subjektu;

4) referenční číslo akreditace;

5) rozsah a doba platnosti akreditace;

6) adresa, umístění a odkaz na příslušné internetové stránky vnitrostátního akreditačního orgánu a

c) následující informace týkající se autorizace pro úroveň „vysoká“:

1) datum autorizace;

2) referenční číslo autorizace;

3) doba platnosti autorizace;

4) rozsah autorizace včetně nejvyšší úrovně AVA_VAN a případně zahrnuté technické oblasti.

4. Vnitrostátní orgán certifikace kybernetické bezpečnosti zašle agentuře ENISA kopii oznámení uvedeného v odstavcích 1 a 2 za účelem zveřejnění přesných informací o způsobilosti certifikačních subjektů na internetových stránkách věnovaných certifikaci kybernetické bezpečnosti.

5. Vnitrostátní orgán certifikace kybernetické bezpečnosti bez zbytečného odkladu přezkoumá veškeré informace týkající se změny stavu akreditace poskytnuté vnitrostátním akreditačním orgánem. Pokud byly akreditace nebo autorizace zrušeny, vnitrostátní orgán certifikace kybernetické bezpečnosti o tom informuje Komisi a může jí předložit žádost v souladu s čl. 61 odst. 4 nařízení (EU) 2019/881.

Článek 24

Oznámení zařízení ITSEF

Oznamovací povinnosti vnitrostátních orgánů certifikace kybernetické bezpečnosti stanovené v článku 23 se vztahují rovněž na zařízení ITSEF. Oznámení musí obsahovat adresu zařízení ITSEF, platnou akreditaci a případně platnou autorizaci tohoto zařízení ITSEF.

KAPITOLA V

MONITOROVÁNÍ, NESHODA A NESOULAD

ODDÍL I

Monitorování souladu

Článek 25

Monitorovací činnosti vnitrostátního orgánu certifikace kybernetické bezpečnosti

1. Aniž je dotčen čl. 58 odst. 7 nařízení (EU) 2019/881, vnitrostátní orgán certifikace kybernetické bezpečnosti sleduje soulad:

a) certifikačního subjektu a zařízení ITSEF s povinnostmi podle tohoto nařízení a nařízení (EU) 2019/881;

b) držitelů certifikátu EUCC s povinnostmi podle tohoto nařízení a nařízení (EU) 2019/881;

c) certifikovaných produktů IKT s požadavky stanovenými v systému EUCC;

d) záruky vyjádřené v certifikátu EUCC, která se týká vyvíjejících se typů hrozeb.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti provádí své monitorovací činnosti zejména na základě:

a) informací od certifikačních subjektů, vnitrostátních akreditačních orgánů a příslušných orgánů dozoru nad trhem;

b) informací vyplývajících z vlastních nebo cizích auditů a šetření;

c) odběru vzorků provedeného v souladu s odstavcem 3;

d) obdržených stížností.

3. Vnitrostátní orgán certifikace kybernetické bezpečnosti ve spolupráci s ostatními orgány dozoru nad trhem odebere každoročně vzorek alespoň 4 % certifikátů EUCC, jak je stanoveno na základě posouzení rizik. Certifikační subjekty a v případě potřeby i zařízení ITSEF jsou na žádost a jménem příslušného vnitrostátního orgánu certifikace kybernetické bezpečnosti tomuto orgánu nápomocny při monitorování souladu.

4. Vnitrostátní orgán certifikace kybernetické bezpečnosti vybere vzorek certifikovaných produktů IKT ke kontrole na základě objektivních kritérií, včetně:

a) kategorie produktů;

b) úrovní záruky produktů;

c) držitele certifikátu;

d) certifikačního subjektu a případně subdodavatelského zařízení ITSEF;

e) veškerých dalších informací, na které byl orgán upozorněn.

5. Vnitrostátní orgán certifikace kybernetické bezpečnosti informuje držitele certifikátu EUCC o vybraných produktech IKT a kritériích výběru.

6. Certifikační subjekt, který certifikoval produkt IKT zařazený do vzorku, provede na žádost vnitrostátního orgánu certifikace kybernetické bezpečnosti s pomocí příslušného zařízení ITSEF dodatečný přezkum v souladu s postupem stanoveným v oddíle IV.2 přílohy IV a o výsledcích informuje vnitrostátní orgán certifikace kybernetické bezpečnosti.

7. Pokud má vnitrostátní orgán certifikace kybernetické bezpečnosti dostatečný důvod domnívat se, že certifikovaný produkt IKT již není v souladu s tímto nařízením nebo nařízením (EU) 2019/881, může provést šetření nebo využít jakékoli jiné monitorovací pravomoci stanovené v čl. 58 odst. 8 nařízení (EU) 2019/881.

8. Vnitrostátní orgán certifikace kybernetické bezpečnosti informuje certifikační subjekt a příslušné zařízení ITSEF o probíhajících šetřeních týkajících se vybraných produktů IKT.

9. Pokud vnitrostátní orgán certifikace kybernetické bezpečnosti zjistí, že probíhající šetření se týká produktů IKT, které jsou certifikovány certifikačními subjekty usazenými v jiných členských státech, informuje o tom vnitrostátní orgány certifikace kybernetické bezpečnosti příslušných členských států, aby případně spolupracovaly při šetření. Tento vnitrostátní orgán certifikace kybernetické bezpečnosti rovněž informuje Evropskou skupinu pro certifikaci kybernetické bezpečnosti o přeshraničních šetřeních a jejich výsledcích.

Článek 26

Monitorovací činnosti certifikačního subjektu

1. Certifikační subjekt monitoruje:

a) dodržování povinností podle tohoto nařízení a nařízení (EU) 2019/881 ve vztahu k certifikátu EUCC, který vydal certifikační subjekt, držiteli certifikátu;

b) soulad produktů IKT, které certifikoval, s příslušnými bezpečnostními požadavky;

c) záruky vyjádřené v certifikovaných profilech ochrany.

2. Certifikační subjekt provádí své monitorovací činnosti na základě:

a) informací poskytnutých na základě závazků žadatele o certifikát podle čl. 9 odst. 2;

b) informací vyplývajících z činností jiných příslušných orgánů dozoru nad trhem;

c) obdržených stížností;

d) informací o zranitelnostech, které by mohly mít dopad na produkty IKT, které certifikoval.

3. Vnitrostátní orgán certifikace kybernetické bezpečnosti může vypracovat pravidla pro pravidelný dialog mezi certifikačními subjekty a držiteli certifikátů EUCC s cílem ověřit soulad se závazky přijatými podle čl. 9 odst. 2 a podat o něm zprávu, aniž jsou dotčeny činnosti související s jinými příslušnými orgány dozoru nad trhem.

Článek 27

Monitorovací činnosti prováděné držitelem certifikátu

1. Držitel certifikátu EUCC provádí následující úkoly, aby monitoroval shodu certifikovaného produktu IKT s bezpečnostními požadavky na něj:

a) monitoruje informace o zranitelnostech certifikovaného produktu IKT, včetně známých závislostí, vlastními prostředky, ale také s ohledem na:

   1) zveřejnění nebo podání informací o zranitelnostech uživatelem nebo výzkumným pracovníkem v oblasti bezpečnosti podle čl. 55 odst. 1 písm. c) nařízení (EU) 2019/881;

   2) podání z jakéhokoli jiného zdroje;

b) monitoruje záruky uvedené v certifikátu EUCC.

2. Držitel certifikátu EUCC spolupracuje s certifikačním subjektem, zařízením ITSEF a případně s vnitrostátním orgánem certifikace kybernetické bezpečnosti, aby podpořil jejich monitorovací činnosti.

ODDÍL II

Shoda a soulad

Článek 28

Důsledky neshody certifikovaného produktu IKT nebo profilu ochrany

1. Pokud certifikovaný produkt IKT nebo profil ochrany nesplňuje požadavky stanovené v tomto nařízení a v nařízení (EU) 2019/881, certifikační subjekt informuje držitele certifikátu EUCC o zjištěné neshodě a požádá ho o nápravná opatření.

2. Pokud by případ neshody s ustanoveními tohoto nařízení mohl ovlivnit soulad s jinými příslušnými právními předpisy Unie, které stanoví možnost prokázat předpoklad shody s požadavky daného právního aktu pomocí certifikátu EUCC, certifikační subjekt o tom neprodleně informuje vnitrostátní orgán certifikace kybernetické bezpečnosti. Vnitrostátní orgán certifikace kybernetické bezpečnosti neprodleně informuje orgán dozoru nad trhem odpovědný za jiné příslušné právní předpisy Unie o zjištěném případu neshody.

3. Po obdržení informací uvedených v odstavci 1 navrhne držitel certifikátu EUCC ve lhůtě stanovené certifikačním subjektem, která nesmí být delší než 30 dnů, certifikačnímu subjektu nápravné opatření nezbytné k odstranění neshody.

4. Certifikační subjekt může bez zbytečného odkladu pozastavit platnost certifikátu EUCC v souladu s článkem 30 v případě nouze nebo v případě, že držitel certifikátu EUCC s certifikačním subjektem řádně nespolupracuje.

5. Certifikační subjekt provede přezkum v souladu s články 13 a 19 a posoudí, zda nápravné opatření řeší neshodu.

6. Pokud držitel certifikátu EUCC během období uvedeného v odstavci 3 nenavrhne vhodné nápravné opatření, platnost certifikátu se pozastaví v souladu s článkem 30 nebo se zruší v souladu s články 14 nebo 20.

7. Tento článek se nevztahuje na případy zranitelností, které mají vliv na certifikovaný produkt IKT a které se řeší v souladu s kapitolou VI.

Článek 29

Důsledky nesouladu ze strany držitele certifikátu

1. Pokud certifikační subjekt zjistí, že:

a) držitel certifikátu EUCC nebo žadatel o certifikát neplní své závazky a povinnosti stanovené v čl. 9 odst. 2, čl. 17 odst. 2, článku 27 a článku 41 nebo

b) držitel certifikátu EUCC nesplňuje požadavky čl. 56 odst. 8 nařízení (EU) 2019/881 nebo kapitoly VI tohoto nařízení;

stanoví lhůtu nejvýše 30 dnů, ve které držitel certifikátu EUCC přijme nápravné opatření.

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 a 20.

3. Pokračující nebo opakované porušování povinností uvedených v odstavci 1 ze strany držitele certifikátu EUCC vede ke zrušení certifikátu EUCC v souladu s článkem 14 nebo 20.

4. Certifikační subjekt informuje vnitrostátní orgán certifikace kybernetické bezpečnosti o zjištěních uvedených v odstavci 1. Pokud má zjištěný případ nesouladu vliv na soulad s jinými příslušnými právními předpisy Unie, vnitrostátní orgán certifikace kybernetické bezpečnosti neprodleně informuje orgán dozoru nad trhem odpovědný za tyto jiné příslušné právní předpisy Unie o zjištěném případu nesouladu.

Článek 30

Pozastavení platnosti certifikátu EUCC

1. Pokud toto nařízení odkazuje na pozastavení platnosti certifikátu EUCC, certifikační subjekt pozastaví platnost dotčeného certifikátu EUCC na dobu odpovídající okolnostem, které vedly k pozastavení platnosti, jež nepřesáhne 42 dnů. Doba pozastavení začíná dnem následujícím po dni rozhodnutí certifikačního subjektu. Pozastavení nemá vliv na platnost certifikátu.

2. Certifikační subjekt bez zbytečného odkladu oznámí pozastavení držiteli certifikátu a vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a uvede důvody pozastavení, požadovaná opatření, která mají být přijata, a dobu pozastavení.

3. Držitelé certifikace informují kupující dotčených produktů IKT o pozastavení a o důvodech, které certifikační subjekt uvedl pro pozastavení, s výjimkou těch částí důvodů, jejichž sdílení by představovalo bezpečnostní riziko nebo které obsahují citlivé informace. Tyto informace držitel certifikátu rovněž zveřejní.

4. Pokud jiné příslušné právní předpisy Unie stanoví předpoklad shody na základě certifikátů vydaných podle ustanovení tohoto nařízení, vnitrostátní orgán certifikace kybernetické bezpečnosti informuje o pozastavení orgán dozoru nad trhem odpovědný za tyto jiné příslušné právní předpisy Unie.

5. Pozastavení platnosti certifikátu se agentuře ENISA oznámí v souladu s čl. 42 odst. 3.

6. V řádně odůvodněných případech může vnitrostátní orgán certifikace kybernetické bezpečnosti povolit prodloužení doby pozastavení platnosti certifikátu EUCC. Celková doba pozastavení nesmí překročit jeden rok.

Článek 31

Důsledky nesouladu ze strany subjektu posuzování shody

1. V případě nesouladu certifikačního subjektu s jeho povinnostmi nebo příslušného certifikačního subjektu v případě zjištění nesouladu ze strany zařízení ITSEF vnitrostátní orgán certifikace kybernetické bezpečnosti bez zbytečného odkladu:

a) s podporou dotčeného zařízení ITSEF identifikuje potenciálně dotčené certifikáty EUCC;

b) v případě potřeby požádá buď zařízení ITSEF, které hodnocení provedlo, nebo jakékoli jiné akreditované a případně autorizované zařízení ITSEF, které může být v lepším technickém postavení, aby tuto identifikaci podpořilo, o provedení hodnotících činností pro jeden nebo více produktů IKT nebo profilů ochrany;

c) analyzuje dopady nesouladu;

d) informuje držitele certifikátu EUCC, kterého se nesoulad týká.

2. Na základě opatření uvedených v odstavci 1 přijme certifikační subjekt pro každý dotčený certifikát EUCC jedno z následujících rozhodnutí:

a) zachovat certifikát EUCC v nezměněné podobě;

b) zrušit certifikát EUCC v souladu s článkem 14 nebo 20 a v případě potřeby vydat nový certifikát EUCC.

3. Na základě opatření uvedených v odstavci 1 vnitrostátní orgán certifikace kybernetické bezpečnosti:

a) v případě potřeby nahlásí nesoulad certifikačního subjektu nebo souvisejícího zařízení ITSEF vnitrostátnímu akreditačnímu orgánu;

b) případně posoudí možný dopad na autorizaci.

KAPITOLA VI

ŘÍZENÍ A ZVEŘEJŇOVÁNÍ ZRANITELNOSTÍ

Článek 32

Rozsah řízení zranitelností

Tato kapitola se vztahuje na produkty IKT, pro které byl vydán certifikát EUCC.

ODDÍL I

Řízení zranitelností

Článek 33

Postupy řízení zranitelností

1. Držitel certifikátu EUCC zavede a udržuje všechny nezbytné postupy řízení zranitelností v souladu s pravidly stanovenými v tomto oddíle, v případě potřeby doplněné postupy stanovenými v normě EN ISO/IEC 30111.

2. Držitel certifikátu EUCC musí udržovat a zveřejňovat vhodné metody pro získávání informací o zranitelnostech týkajících se jeho produktů z externích zdrojů, včetně uživatelů, certifikačních subjektů a výzkumných pracovníků v oblasti bezpečnosti.

3. Pokud držitel certifikátu EUCC zjistí nebo obdrží informace o potenciální zranitelnosti, která se týká certifikovaného produktu IKT, zaznamená je a provede analýzu dopadu zranitelností.

4. Pokud má potenciální zranitelnost dopad na složený produkt, držitel certifikátu EUCC informuje držitele závislých certifikátů EUCC o potenciální zranitelnosti.

5. Na základě odůvodněné žádosti certifikačního subjektu, který certifikát vydal, předá držitel certifikátu EUCC tomuto certifikačnímu subjektu veškeré příslušné informace o možných zranitelnostech.

Článek 34

Analýza dopadu zranitelností

1. Analýza dopadu zranitelností se vztahuje na cíl hodnocení a prohlášení o záruce obsažená v certifikátu. Analýza dopadu zranitelností se provádí ve lhůtě odpovídající zneužitelnosti a kritičnosti potenciální zranitelnosti certifikovaného produktu IKT.

2. V příslušných případech se provede výpočet potenciálu útoku v souladu s příslušnou metodikou obsaženou v normách uvedených v článku 3 a v příslušných přehledech aktuálních certifikačních postupů uvedených v příloze I, aby se určila zneužitelnost zranitelnosti. V úvahu se bere úroveň AVA_VAN certifikátu EUCC.

Článek 35

Zpráva o analýze dopadu zranitelností

1. Držitel vypracuje zprávu o analýze dopadu zranitelností, pokud analýza dopadu prokáže, že zranitelnost má pravděpodobný dopad na shodu produktu IKT s jeho certifikátem.

2. Zpráva o analýze dopadu zranitelností musí obsahovat posouzení následujících prvků:

a) dopad zranitelnosti na certifikovaný produkt IKT;

b) možná rizika spojená s blízkostí nebo dostupností útoku;

c) zda lze zranitelnost odstranit;

d) kde lze zranitelnost odstranit, možná řešení zranitelnosti.

3. Zpráva o analýze dopadu zranitelností musí případně obsahovat podrobnosti o možných způsobech zneužití zranitelnosti. S informacemi týkajícími se možných způsobů zneužití zranitelnosti se nakládá v souladu s vhodnými bezpečnostními opatřeními na ochranu jejich důvěrnosti a v případě potřeby se zajistí jejich omezené šíření.

4. Držitel certifikátu EUCC předloží bez zbytečného odkladu certifikačnímu subjektu nebo vnitrostátnímu orgánu certifikace kybernetické bezpečnosti zprávu o analýze dopadu zranitelností v souladu s čl. 56 odst. 8 nařízení (EU) 2019/881.

5. Pokud zpráva o analýze dopadu zranitelností stanoví, že zranitelnost není zbytková ve smyslu norem uvedených v článku 3 a že ji lze odstranit, použije se článek 36.

6. Pokud zpráva o analýze dopadu zranitelností stanoví, že zranitelnost není zbytková a že ji nelze odstranit, certifikát EUCC se zruší v souladu s článkem 14.

7. Držitel certifikátu EUCC sleduje všechny zbytkové zranitelnosti, aby zajistil, že nemohou být zneužity v případě změn v provozním prostředí.

Článek 36

Odstranění zranitelností

Držitel certifikátu EUCC předloží certifikačnímu subjektu návrh vhodného nápravného opatření. Certifikační subjekt přezkoumá certifikát v souladu s článkem 13. Rozsah přezkumu se určí podle navrhovaného odstranění zranitelnosti.

ODDÍL II

Zveřejňování zranitelností

Článek 37

Informace sdílené s vnitrostátním orgánem certifikace kybernetické bezpečnosti

1. Informace, které certifikační subjekt poskytne vnitrostátnímu orgánu certifikace kybernetické bezpečnosti, musí zahrnovat všechny prvky nezbytné k tomu, aby vnitrostátní orgán certifikace kybernetické bezpečnosti pochopil dopad zranitelnosti, změny, které je třeba provést na produktu IKT, a případně veškeré informace certifikačního subjektu o širších důsledcích zranitelnosti pro další certifikované produkty IKT.

2. Informace poskytnuté podle odstavce 1 nesmí obsahovat podrobnosti o způsobech zneužití zranitelnosti. Tímto ustanovením nejsou dotčeny vyšetřovací pravomoci vnitrostátního orgánu certifikace kybernetické bezpečnosti.

Článek 38

Spolupráce s ostatními vnitrostátními orgány certifikace kybernetické bezpečnosti

1. Vnitrostátní orgán certifikace kybernetické bezpečnosti sdílí příslušné informace získané v souladu s článkem 37 s ostatními vnitrostátními orgány certifikace kybernetické bezpečnosti a agenturou ENISA.

2. Ostatní vnitrostátní orgány certifikace kybernetické bezpečnosti se mohou rozhodnout zranitelnost dále analyzovat nebo po informování držitele certifikátu EUCC požádat příslušné certifikační subjekty, aby posoudily, zda zranitelnost může mít vliv na další certifikované produkty IKT.

Článek 39

Zveřejnění zranitelnosti

Po zrušení certifikátu držitel certifikátu EUCC zveřejní a zaznamená všechny veřejně známé a odstraněné zranitelnosti produktu IKT v Evropské databázi zranitelností zřízené v souladu s článkem 12 směrnice Evropského parlamentu a Rady

(EU) 2022/2555 ([5]) nebo v jiných online úložištích uvedených v čl. 55 odst. 1 písm. d) nařízení (EU) 2019/881.

KAPITOLA VII

UCHOVÁVÁNÍ, ZVEŘEJŇOVÁNÍ A OCHRANA INFORMACÍ

Článek 40

Uchovávání záznamů certifikačními subjekty a zařízeními ITSEF

1. Zařízení ITSEF a certifikační subjekty vedou systém záznamů, který obsahuje všechny dokumenty vytvořené v souvislosti s každým hodnocením a certifikací, které provádějí.

2. Certifikační subjekty a zařízení ITSEF ukládají záznamy bezpečným způsobem a uchovávají je po dobu nezbytnou pro účely tohoto nařízení a nejméně pět let po zrušení příslušného certifikátu EUCC. Pokud certifikační subjekt vydal nový certifikát EUCC v souladu s čl. 13 odst. 2 písm. c), uchovává dokumentaci ke zrušenému certifikátu EUCC společně s novým certifikátem EUCC a po dobu platnosti tohoto nového certifikátu.

Článek 41

Informace zpřístupněné držitelem certifikátu

1. Informace uvedené v článku 55 nařízení (EU) 2019/881 jsou k dispozici v jazyce, který je pro uživatele snadno přístupný.

2. Držitel certifikátu EUCC bezpečně uchovává následující údaje po dobu nezbytnou pro účely tohoto nařízení a nejméně pět let po zrušení příslušného certifikátu EUCC:

a) záznamy o informacích poskytnutých certifikačnímu subjektu a zařízení ITSEF během certifikačního procesu

b) vzorek certifikovaného produktu IKT.

3. Pokud certifikační subjekt vydal nový certifikát EUCC v souladu s čl. 13 odst. 2 písm. c), držitel uchovává dokumentaci ke zrušenému certifikátu EUCC společně s novým certifikátem EUCC a po dobu platnosti tohoto nového certifikátu.

4. Držitel certifikátu EUCC na žádost certifikačního subjektu nebo vnitrostátního orgánu certifikace kybernetické bezpečnosti zpřístupní záznamy a kopie uvedené v odstavci 2.

Článek 42

Informace, které má agentura ENISA zpřístupnit

1. Agentura ENISA zveřejní na internetových stránkách uvedených v čl. 50 odst. 1 nařízení (EU) 2019/881 tyto informace:

a) všechny certifikáty EUCC;

b) informace o statusu certifikátu EUCC, zejména zda je platný, pozastavený, zrušený nebo zda jeho platnost vypršela;

c) zprávy o certifikaci odpovídající každému certifikátu EUCC;

([5]) Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (Úř. věst. L 333, 27.12.2022, s. 80).

d) seznam akreditovaných subjektů posuzování shody;

e) seznam autorizovaných subjektů posuzování shody;

f) přehledy aktuálních certifikačních postupů uvedené v příloze I;

g) stanoviska Evropské skupiny pro certifikaci kybernetické bezpečnosti uvedená v čl. 62 odst. 4 písm. c) nařízení (EU) 2019/881;

h) zprávy o vzájemném hodnocení vydané v souladu s článkem 47.

2. Informace uvedené v odstavci 1 jsou k dispozici alespoň v angličtině.

3. Certifikační subjekty a případně vnitrostátní orgány certifikace kybernetické bezpečnosti neprodleně informují agenturu ENISA o svých rozhodnutích, která mají vliv na obsah nebo status certifikátu EUCC uvedeného v odst. 1 písm. b).

4. Agentura ENISA zajistí, aby informace zveřejněné v souladu s odst. 1 písm. a), b) a c) jasně identifikovaly verze certifikovaného produktu IKT, na které se vztahuje certifikát EUCC.

Článek 43

Ochrana informací

Subjekty posuzování shody, vnitrostátní orgány certifikace kybernetické bezpečnosti, Evropská skupina pro certifikaci kybernetické bezpečnosti, agentura ENISA, Komise a všechny ostatní strany zajistí bezpečnost a ochranu obchodních tajemství a jiných důvěrných informací, včetně obchodního tajemství, jakož i zachování práv duševního vlastnictví, a přijmou nezbytná a vhodná technická a organizační opatření.

KAPITOLA VIII

DOHODY O VZÁJEMNÉM UZNÁVÁNÍ SE TŘETÍMI ZEMĚMI

Článek 44

Podmínky

1. Třetí země, které jsou ochotny certifikovat své produkty v souladu s tímto nařízením a které si přejí, aby byla tato certifikace v Unii uznána, uzavřou s Unií dohodu o vzájemném uznávání.

2. Dohoda o vzájemném uznávání se vztahuje na příslušné úrovně záruky pro certifikované produkty IKT a případně na profily ochrany.

3. Dohody o vzájemném uznávání uvedené v odstavci 1 lze uzavřít pouze se třetími zeměmi, které splňují tyto podmínky:

a) mají orgán, který:

   1) je veřejným subjektem, jenž je z hlediska organizační a právní struktury, financování a rozhodování nezávislý na subjektech, na něž dohlíží a které monitoruje;

   2) má příslušné monitorovací a dohlížecí pravomoci k provádění šetření a je oprávněn přijímat vhodná nápravná opatření k zajištění souladu;

   3) má účinný, přiměřený a odrazující systém sankcí, který zajišťuje soulad;

   4) souhlasí s tím, že bude spolupracovat s Evropskou skupinou pro certifikaci kybernetické bezpečnosti a agenturou ENISA na výměně osvědčených postupů a příslušného vývoje v oblasti certifikace kybernetické bezpečnosti a bude usilovat o jednotný výklad v současnosti platných kritérií a metod hodnocení, mimo jiné uplatňováním harmonizované dokumentace, která odpovídá přehledům aktuálních certifikačních postupů uvedeným v příloze I;

b) mají nezávislý akreditační orgán, který provádí akreditace za použití norem rovnocenných normám uvedeným v nařízení (ES) č. 765/2008;

c) zavazují se, že procesy a postupy hodnocení a certifikace budou prováděny řádně profesionálním způsobem s přihlédnutím k souladu s mezinárodními normami uvedenými v tomto nařízení, zejména v článku 3;

d) mají schopnost hlásit dosud nezjištěné zranitelnosti a zavedený odpovídající postup pro řízení a zveřejňování zranitelností;

e) mají zavedeny postupy, které jim umožňují účinně podávat a vyřizovat stížnosti a poskytovat stěžovateli účinnou právní ochranu;

f) zřídí mechanismus spolupráce s ostatními subjekty Unie a členských států, které jsou relevantní pro certifikaci kybernetické bezpečnosti podle tohoto nařízení, včetně sdílení informací o případném nesouladu certifikátů, monitorování příslušného vývoje v oblasti certifikace a zajištění společného přístupu k zachování a přezkumu certifikace.

4. Kromě podmínek stanovených v odstavci 3 může být dohoda o vzájemném uznávání uvedená v odstavci 1, která se vztahuje na úroveň záruky „vysoká“, uzavřena se třetími zeměmi pouze tehdy, jsou-li splněny i tyto podmínky:

a) třetí země má nezávislý a veřejný orgán certifikace kybernetické bezpečnosti, který provádí nebo svěřuje hodnotící činnosti nezbytné pro certifikaci na úrovni záruky „vysoká“, jež jsou rovnocenné požadavkům a postupům stanoveným pro vnitrostátní orgány pro kybernetickou bezpečnost v tomto nařízení a v nařízení (EU) 2019/881;

b) dohoda o vzájemném uznávání zavádí společný mechanismus rovnocenný vzájemnému hodnocení pro certifikaci v rámci EUCC s cílem posílit výměnu postupů a společně řešit problémy v oblasti hodnocení a certifikace.

KAPITOLA IX

VZÁJEMNÉ HODNOCENÍ CERTIFIKAČNÍCH SUBJEKTŮ

Článek 45

Postup vzájemného hodnocení

1. Certifikační subjekt, který vydává certifikáty EUCC na úrovni záruky „vysoká“, se pravidelně, nejméně však jednou za pět let, podrobuje vzájemnému hodnocení. Různé typy vzájemného hodnocení jsou uvedeny v příloze VI.

2. Evropská skupina pro certifikaci kybernetické bezpečnosti vypracuje a udržuje harmonogram vzájemných hodnocení, který zajistí dodržování této periodicity. S výjimkou řádně odůvodněných případů se vzájemné hodnocení provádí na místě.

3. Vzájemné hodnocení se může opírat o důkazy shromážděné v průběhu předchozích vzájemných hodnocení nebo rovnocenných postupů vzájemně hodnoceného certifikačního subjektu nebo vnitrostátního orgánu certifikace kybernetické bezpečnosti za předpokladu, že:

a) výsledky nejsou starší než pět let;

b) výsledky jsou doplněny popisem postupů vzájemného hodnocení stanovených pro tento systém, pokud se vztahují ke vzájemnému hodnocení provedenému v rámci jiného certifikačního systému;

c) zpráva o vzájemném hodnocení podle článku 47 uvádí, které výsledky byly znovu použity s dalším hodnocením nebo bez něj.

4. Pokud se vzájemné hodnocení vztahuje na technickou oblast, posuzuje se také příslušné zařízení ITSEF.

5. Certifikační subjekt, který je vzájemně hodnocen, a v případě potřeby vnitrostátní orgán certifikace kybernetické bezpečnosti zajistí, aby byly týmu provádějícímu vzájemné hodnocení zpřístupněny všechny relevantní informace.

6. Vzájemné hodnocení provádí tým pro vzájemné hodnocení sestavený v souladu s přílohou VI.

Článek 46

Fáze vzájemného hodnocení

1. Během přípravné fáze členové týmu pro vzájemné hodnocení přezkoumají dokumentaci certifikačního subjektu, která zahrnuje jeho politiky a postupy, včetně používání přehledů aktuálních certifikačních postupů.

2. Během fáze návštěvy na místě tým pro vzájemné hodnocení posuzuje odbornou způsobilost subjektu a případně způsobilost zařízení ITSEF, které provedlo alespoň jedno hodnocení produktu IKT, jehož se vzájemné hodnocení týká.

3. Doba trvání fáze návštěvy na místě může být prodloužena nebo zkrácena v závislosti na takových faktorech, jako je možnost opětovného použití stávajících důkazů a výsledků vzájemného hodnocení nebo počet zařízení ITSEF a technických oblastí, pro které certifikační subjekt vydává certifikáty.

4. Tým pro vzájemné hodnocení případně určí odbornou způsobilost každého zařízení ITSEF návštěvou jeho technické laboratoře nebo laboratoří a rozhovorem s jeho hodnotiteli, pokud jde o technickou oblast a související specifické metody útoku.

5. Ve fázi podávání zpráv zdokumentuje hodnotící tým svá zjištění ve zprávě o vzájemném hodnocení, která obsahuje závěr a případně seznam zjištěných neshod, přičemž každá z nich je odstupňována podle úrovně kritičnosti.

6. Zpráva o vzájemném hodnocení musí být nejprve projednána s certifikačním subjektem, který je vzájemně hodnocen. Po těchto diskusích stanoví vzájemně hodnocený certifikační subjekt harmonogram opatření, která mají být přijata k řešení zjištění.

Článek 47

Zpráva o vzájemném hodnocení

1. Tým pro vzájemné hodnocení poskytne certifikačnímu subjektu, který je vzájemně hodnocen, návrh zprávy o vzájemném hodnocení.

2. Vzájemně hodnocený certifikační subjekt předloží týmu vzájemného hodnocení připomínky ke zjištěním a seznam závazků k odstranění nedostatků určených v návrhu zprávy o vzájemném hodnocení.

3. Tým pro vzájemné hodnocení předloží Evropské skupině pro certifikaci kybernetické bezpečnosti závěrečnou zprávu o vzájemném hodnocení, která obsahuje také připomínky a závazky přijaté certifikačním subjektem, který byl podroben vzájemnému hodnocení. Tým pro vzájemné hodnocení rovněž uvede své stanovisko k připomínkám a k tomu, zda jsou tyto závazky dostatečné k odstranění zjištěných nedostatků.

4. Pokud jsou ve zprávě o vzájemném hodnocení zjištěny neshody, může Evropská skupina pro certifikaci kybernetické bezpečnosti stanovit vzájemně hodnocenému certifikačnímu subjektu přiměřenou lhůtu k jejich odstranění.

5. Evropská skupina pro certifikaci kybernetické bezpečnosti přijme stanovisko ke zprávě o vzájemném hodnocení:

a) pokud zpráva o vzájemném hodnocení nezjistí neshody nebo pokud byly neshody certifikačním subjektem, který byl podroben vzájemnému hodnocení, náležitě vyřešeny, může Evropská skupina pro certifikaci kybernetické bezpečnosti vydat kladné stanovisko a všechny příslušné dokumenty se zveřejní na internetových stránkách o certifikaci agentury ENISA;

b) pokud certifikační subjekt, který byl podroben vzájemnému hodnocení, neshody ve stanovené lhůtě řádně nevyřeší, může Evropská skupina pro certifikaci kybernetické bezpečnosti vydat negativní stanovisko, které se zveřejní na internetových stránkách o certifikaci agentury ENISA, včetně zprávy o vzájemném hodnocení a všech příslušných dokumentů.

6. Před zveřejněním stanoviska musí být ze zveřejněných dokumentů odstraněny všechny citlivé, osobní nebo chráněné obchodní informace.

KAPITOLA X

UDRŽOVÁNÍ SYSTÉMU

Článek 48

Udržování systému EUCC

1. Komise může požádat Evropskou skupinu pro certifikaci kybernetické bezpečnosti, aby přijala stanovisko za účelem udržování systému EUCC a aby provedla nezbytné přípravné práce.

2. Evropská skupina pro certifikaci kybernetické bezpečnosti může přijmout stanovisko ke schválení přehledů aktuálních certifikačních postupů.

3. Přehledy aktuálních certifikačních postupů, které byly schváleny Evropskou skupinou pro certifikaci kybernetické bezpečnosti, zveřejňuje agentura ENISA.

KAPITOLA XI

ZÁVĚREČNÁ USTANOVENÍ

Článek 49

Vnitrostátní systémy, na které se vztahuje systém EUCC

1. V souladu s čl. 57 odst. 1 nařízení (EU) 2019/881 a aniž je dotčen čl. 57 odst. 3 uvedeného nařízení, všechny vnitrostátní systémy certifikace kybernetické bezpečnosti a související postupy pro produkty IKT a procesy IKT, na které se vztahuje systém EUCC, pozbývají účinnosti 12 měsíců po vstupu tohoto nařízení v platnost.

2. Odchylně od článku 50 může být proces certifikace zahájen v rámci vnitrostátního systému certifikace kybernetické bezpečnosti do 12 měsíců ode dne vstupu tohoto nařízení v platnost za předpokladu, že proces certifikace bude dokončen nejpozději do 24 měsíců od vstupu tohoto nařízení v platnost.

3. Certifikáty vydané v rámci vnitrostátních systémů certifikace kybernetické bezpečnosti mohou podléhat přezkumu. Nové certifikáty, které nahrazují přezkoumané certifikáty, se vydávají v souladu s tímto nařízením.

Článek 50

Vstup v platnost

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

Použije se ode dne 27. února 2025.

Kapitola IV a příloha V se použijí ode dne vstupu tohoto nařízení v platnost.

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

V Bruselu dne 31. ledna 2024.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

Technické oblasti a přehledy aktuálních certifikačních postupů

1. Technické oblasti na úrovni AVA_VAN 4 nebo 5:

   a) dokumenty týkající se harmonizovaného hodnocení technické oblasti „čipové karty a podobná zařízení“, a zejména tyto dokumenty v jejich příslušném znění v platnosti dne [datum vstupu v platnost]:

      1) „Minimální požadavky na bezpečnostní hodnocení čipových karet a podobných zařízení vůči zařízením ITSEF“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      2) „Minimální bezpečnostní požadavky na internetové stránky“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      3) „Použití společných kritérií na integrované obvody“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      4) „Požadavky na bezpečnostní architekturu (ADV_ARC) pro čipové karty a podobná zařízení“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      5) „Certifikace produktů „otevřených“ čipových karet“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      6) „Hodnocení složených produktů pro čipové karty a podobná zařízení“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      7) „Uplatnění potenciálu útoku na čipové karty“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

   b) dokumenty týkající se harmonizovaného hodnocení technické oblasti „hardwarová zařízení s bezpečnostními schránkami“, a zejména tyto dokumenty v jejich příslušném znění v platnosti dne [datum vstupu v platnost]:

      1) „Minimální požadavky na bezpečnostní hodnocení hardwarových zařízení s bezpečnostními schránkami vůči zařízením ITSEF“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      2) „Minimální bezpečnostní požadavky na internetové stránky“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023;

      3) „Uplatnění potenciálu útoku na hardwarová zařízení s bezpečnostními schránkami“, původně schválené Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023.

2. Přehledy aktuálních certifikačních postupů v jejich příslušném znění v platnosti dne [datum vstupu v platnost]:

   a) dokument týkající se harmonizované akreditace subjektů posuzování shody: „Akreditace zařízení ITSEF pro systém EUCC“, původně schválený Evropskou skupinou pro certifikaci kybernetické bezpečnosti dne 20. října 2023.

PŘÍLOHA II

Profily ochrany certifikované na úrovni AVA_VAN 4 nebo 5

1. Pro kategorii prostředků pro vytváření kvalifikovaných podpisů a pečetí na dálku:

1) EN 419241-2:2019 – Důvěryhodné systémy podporující podpisový server – Část 2: Profil ochrany pro zařízení QSCD pro serverový podpis;

2) EN 419221-5:2018 – Profily ochrany pro TSP kryptografické moduly – Část 5: Kryptografický modul pro důvěryhodné služby

2. Profily ochrany, které byly přijaty jako přehledy aktuálních certifikačních postupů:

[PRÁZDNÉ]

PŘÍLOHA III

Doporučené profily ochrany (pro ilustraci technických oblastí z přílohy I)

Profily ochrany používané při certifikaci produktů IKT spadajících do níže uvedené kategorie produktů IKT:

a) pro kategorii strojově čitelných cestovních dokladů:

   1) profil ochrany pro strojově čitelný cestovní doklad s použitím standardního kontrolního postupu s PACE, BSI-CC-PP-0068-V2-2011-MA-01;

   2) profil ochrany pro strojově čitelný cestovní doklad s rozšířenou kontrolou přístupu „aplikace ICAO“, BSI-CC-PP-0056-2009;

   3) profil ochrany pro strojově čitelný cestovní doklad s rozšířenou kontrolou přístupu „aplikace ICAO“ s PACE, BSI-CC-PP-0056-V2-2012-MA-02;

   4) profil ochrany pro strojově čitelný cestovní doklad se základní kontrolou přístupu „aplikace ICAO“, BSI-CC-PP-0055-2009;

b) pro kategorii zařízení vytvářejících bezpečný podpis:

   1) EN 419211-1:2014 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 1: Přehled

   2) EN 419211-2:2013 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 2: Přístroje na generování klíče;

   3) EN 419211-3:2013 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 3: Přístroje na přenos klíče;

   4) EN 419211-4:2013 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 4: Rozšíření pro zařízení na generování klíče a spolehlivá komunikace s aplikací generování certifikátu;

   5) EN 419211-5:2013 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 5: Rozšíření pro zařízení na generování klíče a spolehlivá komunikace s aplikací vytvářející podpis;

   6) EN 419211-6:2014 – Profil ochrany pro zařízení vytvářející bezpečný podpis – část 6: Rozšíření pro zařízení pro importování klíče a důvěryhodná komunikace s aplikací vytvářející podpis;

c) pro kategorii digitálních tachografů:

   1) digitální tachograf – karta tachografu, jak je uvedeno v prováděcím nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení (EU) č. 165/2014 (příloha 1C);

   2) digitální tachograf – celek ve vozidle uvedený v příloze IB nařízení Komise (ES) č. 1360/2002 určený k montáži do silničních vozidel;

   3) digitální tachograf – vnější zařízení GNSS (profil ochrany EGF), jak je uvedeno v příloze 1C prováděcího nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014;

   4) digitální tachograf – snímač pohybu (profil ochrany MS), jak je uvedeno v příloze 1C prováděcího nařízení Komise (EU) 2016/799 ze dne 18. března 2016, kterým se provádí nařízení Evropského parlamentu a Rady (EU) č. 165/2014;

d) pro kategorii bezpečných integrovaných obvodů, čipových karet a souvisejících zařízení:

   1) profil ochrany pro bezpečnostní platformu IC, BSI-CC-PP-0084-2014;

   2) systém Java Card – otevřená konfigurace, V3.0.5 BSI-CC-PP-0099-2017;

   3) systém Java Card – uzavřená konfigurace, BSI-CC-PP-0101-2017;

   4) profil ochrany pro PC rodinu klientských modulů důvěryhodné platformy 2.0 úroveň 0 revize 1.16, ANSSI-CC-PP-2015/07;

5) univerzální karta SIM, PU-2009-RT-79, ANSSI-CC-PP-2010/04;

6) vestavěné UICC (eUICC) pro zařízení pro komunikaci strojů, BSI-CC-PP-0089-2015;

e) pro kategorii bodů (platební) interakce a platebních terminálů:

1) bod interakce „POI-CHIP-ONLY“, ANSSI-CC-PP-2015/01;

2) bod interakce „POI-CHIP-ONLY and Open Protocol Package“, ANSSI-CC-PP-2015/02;

3) bod interakce „POI-COMPREHENSIVE“, ANSSI-CC-PP-2015/03;

4) bod interakce „POI-COMPREHENSIVE and Open Protocol Package“, ANSSI-CC-PP-2015/04;

5) bod interakce „POI-PED-ONLY“, ANSSI-CC-PP-2015/05;

6) bod interakce „POI-PED-ONLY and Open Protocol Package“, ANSSI-CC-PP-2015/06;

f) pro kategorii hardwarových zařízení s bezpečnostními schránkami:

1) kryptografický modul pro podpisové operace CSP se zálohováním – profil ochrany CMCSOB, profil ochrany HSM CMCSOB 14167-2, ANSSI-CC-PP-2015/08;

2) kryptografický modul pro služby generování klíčů CSP – profil ochrany CMCKG, profil ochrany HSM CMCKG 14167-3, ANSSI-CC-PP-2015/09;

3) kryptografický modul pro podpisové operace CSP bez zálohování – profil ochrany CMCSO, profil ochrany HSM CMCKG 14167-4, ANSSI-CC-PP-2015/10.

PŘÍLOHA IV

Kontinuita záruky a přezkum certifikátu

IV.1 **Kontinuita záruky: rozsah**

1. Následující požadavky na kontinuitu záruky se vztahují na činnosti udržování týkající se:

   a) přehodnocení, zda nezměněný certifikovaný produkt IKT stále splňuje bezpečnostní požadavky;

   b) hodnocení dopadů změn certifikovaného produktu IKT na jeho certifikaci;

   c) pokud je součástí certifikace, použití oprav v souladu s vyhodnoceným procesem správy oprav;

   d) pokud je zahrnut, přezkum řízení životního cyklu nebo výrobních procesů držitele certifikátu.

2. Držitel certifikátu EUCC může požádat o přezkum certifikátu v následujících případech:

   a) platnost certifikátu EUCC vyprší do devíti měsíců;

   b) došlo ke změně certifikovaného produktu IKT nebo jiného faktoru, který by mohl ovlivnit jeho bezpečnostní funkce;

   c) držitel certifikátu požaduje, aby bylo znovu provedeno posouzení zranitelností za účelem opětovného potvrzení záruky certifikátu EUCC týkající se odolnosti produktu IKT proti současným kybernetickým útokům.

IV.2 **Přehodnocení**

1. Pokud je třeba posoudit dopad změn v prostředí hrozeb pro nezměněný certifikovaný produkt IKT, musí být certifikačnímu subjektu předložena žádost o přehodnocení.

2. Přehodnocení provede stejné zařízení ITSEF, které se podílelo na předchozím hodnocení, a znovu použije všechny své výsledky, které jsou stále platné. Hodnocení se zaměří na činnosti záruky, které jsou potenciálně ovlivněny změněným prostředím hrozeb pro certifikovaný produkt IKT, zejména na příslušnou skupinu AVA_VAN a navíc na skupinu životního cyklu záruky (ALC), kde se opět shromáždí dostatečné důkazy o údržbě vývojového prostředí.

3. Zařízení ITSEF popíše změny a podrobně popíše výsledky přehodnocení s aktualizací předchozí hodnotící technické zprávy.

4. Certifikační subjekt přezkoumá aktualizovanou hodnotící technickou zprávu a vypracuje zprávu o přehodnocení. Status původního certifikátu se poté změní v souladu s článkem 13.

5. Zpráva o přehodnocení a aktualizovaný certifikát se poskytnou vnitrostátnímu orgánu certifikace kybernetické bezpečnosti a agentuře ENISA ke zveřejnění na jejích internetových stránkách věnovaných certifikaci kybernetické bezpečnosti.

IV.3 **Změny certifikovaného produktu IKT**

1. Pokud byl certifikovaný produkt IKT předmětem změn, držitel certifikátu, který si přeje certifikát zachovat, předloží certifikačnímu subjektu zprávu o analýze dopadů.

2. Zpráva o analýze dopadů obsahuje tyto prvky:

   a) úvod obsahující nezbytné informace k identifikaci zprávy o analýze dopadů a cíle hodnocení, který podléhá změnám;

b) popis změn produktu;

c) identifikaci ovlivněných důkazů od vývojáře;

d) popis úprav důkazů od vývojáře;

e) zjištění a závěry týkající se dopadu na záruku pro každou změnu.

3. Certifikační subjekt přezkoumá změny popsané ve zprávě o analýze dopadů, aby ověřil jejich dopad na záruku certifikovaného cíle hodnocení, jak je navrženo v závěrech zprávy o analýze dopadů.

4. Po přezkoumání certifikační subjekt určí rozsah změny jako drobný nebo velký podle jejího dopadu.

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 za následujících podmínek:

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

1) úvod;

2) popis změn;

3) ovlivněné důkazy od vývojáře;

b) datum platnosti nového certifikátu nepřekročí datum původního certifikátu.

6. Nový certifikát včetně zprávy o údržbě se poskytne agentuře ENISA ke zveřejnění na jejích internetových stránkách věnovaných certifikaci kybernetické bezpečnosti.

7. Pokud se potvrdí, že změny jsou velké, provede se přehodnocení v kontextu předchozího hodnocení a znovu se použijí všechny výsledky předchozího hodnocení, které jsou stále platné.

8. Po dokončení hodnocení změněného cíle hodnocení vypracuje zařízení ITSEF novou hodnotící technickou zprávu. Certifikační subjekt přezkoumá aktualizovanou hodnotící technickou zprávu a případně vydá nový certifikát s novou zprávou o certifikaci.

9. Nový certifikát a zpráva o certifikaci se předají agentuře ENISA ke zveřejnění.

IV.4 **Správa oprav**

1. Postup správy oprav zajišťuje strukturovaný proces aktualizace certifikovaného produktu IKT. Postup správy oprav včetně mechanismu, který žadatel o certifikaci zavedl do produktu IKT, lze použít po certifikaci produktu IKT na odpovědnost subjektu posuzování shody.

2. Žadatel o certifikaci může do certifikace produktu IKT zahrnout opravný mechanismus jako součást certifikovaného postupu řízení zavedeného do produktu IKT za jedné z následujících podmínek:

a) funkce ovlivněné opravou se nacházejí mimo cíl hodnocení certifikovaného produktu IKT;

b) oprava se týká předem stanovené drobné změny certifikovaného produktu IKT;

c) oprava se týká potvrzené zranitelnosti s kritickým dopadem na bezpečnost certifikovaného produktu IKT.

3. Pokud se oprava týká velké změny cíle hodnocení certifikovaného produktu IKT v souvislosti s dříve nezjištěnou zranitelností, která nemá kritický dopad na bezpečnost produktu IKT, použijí se ustanovení článku 13.

4. Postup správy oprav pro produkt IKT se skládá z následujících prvků:

   a) proces vývoje a vydání opravy pro produkt IKT;

   b) technický mechanismus a funkce pro přijetí opravy do produktu IKT;

   c) soubor hodnotících činností týkajících se účinnosti a výkonnosti technického mechanismu.

5. Během certifikace produktu IKT:

   a) žadatel o certifikaci produktu IKT poskytne popis postupu správy oprav;

   b) zařízení ITSEF ověří následující prvky:

      1) vývojář zavedl opravné mechanismy do produktu IKT v souladu s postupem správy oprav, který byl předložen k certifikaci;

      2) meze cíle hodnocení jsou odděleny tak, aby změny provedené v oddělených procesech neovlivnily bezpečnost cíle hodnocení;

      3) technický opravný mechanismus funguje v souladu s ustanoveními tohoto oddílu a tvrzeními žadatele;

   c) certifikační subjekt zahrne do zprávy o certifikaci výsledek posuzovaného postupu správy oprav.

6. Držitel certifikátu může přistoupit k aplikaci opravy vytvořené v souladu s certifikovaným postupem správy oprav dotčeného certifikovaného produktu IKT a v následujících případech musí do 5 pracovních dnů podniknout tyto kroky:

   a) v případě uvedeném v bodě 2 písm. a) nahlásit příslušnou opravu certifikačnímu subjektu, který nezmění odpovídající certifikát EUCC;

   b) v případě uvedeném v bodě 2 písm. b) předložit příslušnou opravu zařízení ITSEF k přezkoumání. Zařízení ITSEF po obdržení opravy informuje certifikační subjekt, který přijme příslušná opatření k vydání nové verze příslušného certifikátu EUCC a k aktualizaci zprávy o certifikaci;

   c) v případě uvedeném v bodě 2 písm. c) předložit dotčenou opravu zařízení ITSEF k nezbytnému přehodnocení, ale může opravu nasadit souběžně. Zařízení ITSEF informuje certifikační subjekt, který poté zahájí související certifikační činnosti.

PŘÍLOHA V

Obsah zprávy o certifikaci

V.1 **Zpráva o certifikaci**

1. Na základě hodnotících technických zpráv poskytnutých zařízením ITSEF vypracuje certifikační subjekt zprávu o certifikaci, kterou zveřejní spolu s příslušným certifikátem EUCC.

2. Zpráva o certifikaci je zdrojem podrobných a praktických informací o produktu IKT nebo kategorii produktů IKT a o bezpečném nasazení produktu IKT, a proto musí obsahovat všechny veřejně dostupné informace, které lze sdílet a jež jsou důležité pro uživatele a zúčastněné strany. Veřejně dostupné informace, které lze sdílet, mohou být uvedeny ve zprávě o certifikaci.

3. Zpráva o certifikaci musí obsahovat alespoň tyto oddíly:

   a) shrnutí;

   b) identifikace produktu IKT nebo kategorie produktu IKT pro profily ochrany;

   c) bezpečnostní služby;

   d) předpoklady a vyjasnění oblasti působnosti;

   e) architektonické informace;

   f) případné doplňující informace o kybernetické bezpečnosti;

   g) testování produktu IKT, pokud bylo provedeno;

   h) v příslušných případech identifikaci procesů řízení životního cyklu a výrobních zařízení držitele certifikátu;

   i) výsledky hodnocení a informace o certifikátu;

   j) shrnutí bezpečnostního cíle produktu IKT předloženého k certifikaci;

   k) označení nebo štítek přiřazené k systému, pokud je k dispozici;

   l) bibliografie.

4. Shrnutí je stručným shrnutím celé zprávy o certifikaci. Shrnutí poskytuje jasný a stručný přehled výsledků hodnocení a obsahuje následující informace:

   a) název hodnoceného produktu IKT, výčet součástí produktu, které jsou součástí hodnocení, a verze produktu IKT;

   b) název zařízení ITSEF, které hodnocení provedlo, a případně seznam subdodavatelů;

   c) datum ukončení hodnocení;

   d) odkaz na hodnotící technickou zprávu vypracovanou zařízením ITSEF;

   e) stručný popis výsledků zprávy o certifikaci, včetně:

      1) verze a případně vydání společných kritérií, která se na hodnocení vztahují;

      2) balíčku záruk podle společných kritérií a složek záruky bezpečnosti včetně úrovně AVA_VAN použité při hodnocení a odpovídající úrovně záruky podle článku 52 nařízení (EU) 2019/881, na které se certifikát EUCC vztahuje;

      3) bezpečnostní funkce hodnoceného produktu IKT;

      4) shrnutí hrozeb a bezpečnostních politik organizace, které hodnocený produkt IKT řeší;

5) zvláštních požadavků na konfiguraci;

6) předpokladů o provozním prostředí;

7) případně přítomnosti schváleného postupu správy oprav v souladu s oddílem IV.4 přílohy IV;

8) prohlášení o vyloučení odpovědnosti.

5. Hodnocený produkt IKT je jasně označen a obsahuje tyto informace:

a) název hodnoceného produktu IKT;

b) výčet součástí produktu IKT, které jsou součástí hodnocení;

c) číslo verze součástí produktu IKT;

d) identifikace dodatečných požadavků na provozní prostředí certifikovaného produktu IKT;

e) jméno a kontaktní údaje držitele certifikátu EUCC;

f) případně postup správy oprav, který je součástí certifikátu;

g) odkaz na internetové stránky držitele certifikátu EUCC, kde jsou uvedeny doplňující informace o kybernetické bezpečnosti certifikovaného produktu IKT v souladu s článkem 55 nařízení (EU) 2019/881.

6. Informace obsažené v tomto oddíle jsou co nejpřesnější, aby byla zajištěna úplná a přesná reprezentace produktu IKT, kterou lze znovu použít při budoucích hodnoceních.

7. Oddíl o bezpečnostní politice obsahuje popis bezpečnostní politiky produktu IKT a strategie nebo pravidla, která hodnocený produkt IKT prosazuje nebo dodržuje. Musí obsahovat odkaz a popis následujících strategií:

a) strategie nakládání se zranitelnostmi držitele certifikátu;

b) strategie kontinuity záruky držitele certifikátu.

8. V případě potřeby mohou strategie zahrnovat podmínky týkající se používání postupu správy oprav během platnosti certifikátu.

9. Oddíl pro předpoklady a vyjasnění oblasti působnosti obsahuje vyčerpávající informace o okolnostech a cílech souvisejících se zamýšleným použitím produktu, jak je uvedeno v čl. 7 odst. 1 písm. c). Informace obsahují:

a) předpoklady o použití a nasazení produktu IKT v podobě minimálních požadavků, jako je správná instalace a konfigurace a splnění požadavků na hardware;

b) předpoklady o prostředí pro vyhovující provoz produktu IKT.

10. Informace uvedené v bodě 9 musí být co nejsrozumitelnější, aby uživatelé certifikovaného produktu IKT mohli činit informovaná rozhodnutí o rizicích spojených s jeho používáním.

11. Oddíl s informacemi o architektuře obsahuje popis produktu IKT a jeho hlavních součástí na vysoké úrovni v souladu s návrhem subsystémů ADV_TDS podle společných kritérií.

12. Úplný seznam doplňujících informací o kybernetické bezpečnosti produktu IKT se poskytuje v souladu s článkem 55 nařízení (EU) 2019/881. Veškerá příslušná dokumentace se označuje čísly verzí.

13. Oddíl o zkoušení produktů IKT obsahuje tyto informace:

    a) název a kontaktní místo orgánu nebo subjektu, který certifikát vydal, včetně odpovědného vnitrostátního orgánu certifikace kybernetické bezpečnosti;

    b) název zařízení ITSEF, které provedlo hodnocení, pokud se liší od certifikačního subjektu;

    c) identifikace použitých složek záruky z norem uvedených v článku 3;

    d) verze přehledu aktuálních certifikačních postupů a další kritéria hodnocení bezpečnosti použitá při hodnocení;

    e) úplné a přesné nastavení a konfigurace produktu IKT během hodnocení, včetně provozních poznámek a pozorování, pokud jsou k dispozici;

    f) jakýkoli použitý profil ochrany, včetně následujících informací:

        1) autor profilu ochrany;

        2) název a identifikátor profilu ochrany;

        3) identifikátor certifikátu profilu ochrany;

        4) název a kontaktní údaje certifikačního subjektu a zařízení ITSEF, které se podílí na hodnocení profilu ochrany;

        5) balíček (balíčky) záruk požadovaných pro produkt, který je ve shodě s profilem ochrany.

14. Výsledky hodnocení a informace týkající se oddílu o certifikátu obsahují tyto informace:

    a) potvrzení o dosažené úrovni záruky podle článku 4 tohoto nařízení a článku 52 nařízení (EU) 2019/881;

    b) požadavky na záruku z norem uvedených v článku 3, které produkt IKT nebo profil ochrany skutečně splňuje, včetně úrovně AVA_VAN;

    c) podrobný popis požadavků na záruku a také podrobnosti o tom, jak produkt splňuje jednotlivé požadavky;

    d) datum vydání a doba platnosti certifikátu;

    e) jedinečný identifikátor certifikátu.

15. Bezpečnostní cíl se zahrne do zprávy o certifikaci nebo se na něj ve zprávě o certifikaci odkáže a shrne se a pro účely zveřejnění se k němu připojí zpráva o certifikaci.

16. Bezpečnostní cíl může být sanitizován v souladu s oddílem VI.2.

17. Označení nebo štítek spojené se systémem EUCC mohou být vloženy do zprávy o certifikaci v souladu s pravidly a postupy stanovenými v článku 11.

18. Oddíl bibliografie obsahuje odkazy na všechny dokumenty použité při sestavování zprávy o certifikaci. Tyto informace obsahují alespoň tyto údaje:

    a) kritéria hodnocení bezpečnosti, přehledy aktuálních certifikačních postupů a další použité příslušné specifikace a jejich verze;

    b) hodnotící technická zpráva;

    c) případně hodnotící technická zpráva pro složené hodnocení;

    d) technická referenční dokumentace;

    e) dokumentace vývojáře použitá při hodnocení.

19. Aby byla zaručena reprodukovatelnost hodnocení, musí být veškerá dokumentace, na kterou se odkazuje, jednoznačně identifikována správným datem vydání a správným číslem verze.

V.2 **Sanitizace bezpečnostního cíle pro zveřejnění**

1. Bezpečnostní cíl, který má být zahrnut do zprávy o certifikaci podle bodu 1 oddílu VI.1 nebo na nějž tato zpráva odkazuje, může být sanitizován odstraněním nebo parafrázováním technických informací, které jsou předmětem ochrany.

2. Výsledný sanitizovaný bezpečnostní cíl musí být skutečnou reprezentací své úplné původní verze. To znamená, že sanitizovaný bezpečnostní cíl nesmí vynechat informace, které jsou nezbytné pro pochopení bezpečnostních vlastností cíle hodnocení a rozsahu hodnocení.

3. Obsah sanitizovaného bezpečnostního cíle splňuje následující minimální požadavky:

   a) jeho úvod se nesanitizuje, protože obecně neobsahuje žádné informace, které by byly předmětem ochrany;

   b) sanitizovaný bezpečnostní cíl musí mít jedinečný identifikátor, který je odlišný od jeho úplné původní verze;

   c) popis cíle hodnocení může být redukován, protože může obsahovat chráněné a podrobné informace o návrhu cíli hodnocení, které by neměly být zveřejněny;

   d) popis bezpečnostního prostředí cíle hodnocení (předpoklady, hrozby, organizační bezpečnostní politiky) se neredukuje, pokud jsou uvedené informace nezbytné pro pochopení rozsahu hodnocení;

   e) bezpečnostní cíle se neredukují, protože je třeba zveřejnit všechny informace, aby bylo možné pochopit záměr bezpečnostního cíle a cíle hodnocení;

   f) všechny bezpečnostní požadavky se zveřejní. V aplikačních poznámkách mohou být uvedeny informace o tom, jak byly funkční požadavky společných kritérií uvedené v článku 3 použity k pochopení bezpečnostního cíle;

   g) souhrnná specifikace cíle hodnocení obsahuje všechny bezpečnostní funkce cíle hodnocení, ale další informace, které jsou předmětem ochrany, mohou být sanitizovány;

   h) odkazy na profily ochrany použité na cíl hodnocení;

   i) zdůvodnění může být sanitizováno tak, aby byly odstraněny informace, které jsou předmětem ochrany.

4. I v případě, že sanitizovaný bezpečnostní cíl není formálně hodnocen v souladu s hodnotícími normami uvedenými v článku 3, certifikační subjekt zajistí, aby byl v souladu s úplným a hodnoceným bezpečnostním cílem, a ve zprávě o certifikaci uvede odkaz na úplný i sanitizovaný bezpečnostní cíl.

PŘÍLOHA VI

Rozsah vzájemného hodnocení a složení týmu pro vzájemné hodnocení

VI.1 **Rozsah vzájemného hodnocení**

1. Jsou zahrnuty tyto typy vzájemného hodnocení:

   a) typ 1: pokud certifikační subjekt provádí certifikační činnosti na úrovni AVA_VAN.3;

   b) typ 2: pokud certifikační subjekt provádí certifikační činnosti související s technickou oblastí uvedenou v příloze I jako přehledy aktuálních certifikačních postupů;

   c) typ 3: pokud certifikační subjekt provádí certifikační činnosti nad úrovní AVA_VAN.3 s využitím profilu ochrany uvedeného jako přehled aktuálních certifikačních postupů v příloze II nebo III.

2. Certifikační subjekt, který je podroben vzájemnému hodnocení, předloží seznam certifikovaných produktů IKT, které mohou být kandidátem na přezkoumání týmem pro vzájemné hodnocení, v souladu s následujícími pravidly:

   a) kandidátské produkty pokrývají technický rozsah autorizace certifikačního subjektu, přičemž nejméně dvě různá hodnocení produktů na úrovni záruky „vysoká“ budou analyzována prostřednictvím vzájemného hodnocení, a jeden profil ochrany, pokud certifikační subjekt vydal certifikát na úrovni záruky „vysoká“;

   b) pro vzájemné hodnocení typu 2 předloží certifikační subjekt alespoň jeden produkt za každou technickou oblast a za každé dotčené zařízení ITSEF;

   c) pro vzájemné hodnocení typu 3 je alespoň jeden kandidátský produkt hodnocen v souladu s použitelnými a relevantními profily ochrany.

VI.2 **Tým pro vzájemné hodnocení**

1. Hodnotící tým se skládá nejméně ze dvou odborníků, přičemž každý je vybrán z různých certifikačních subjektů, které vydávají certifikáty s úrovní záruky „vysoká“, a z různých členských států. Odborníci by měli prokázat příslušné odborné znalosti v oblasti norem uvedených v článku 3 a v oblasti přehledů aktuálních certifikačních postupů, které jsou předmětem vzájemného hodnocení.

2. V případě pověření vydáním certifikátu nebo předchozího schválení certifikátů podle čl. 56 odst. 6 nařízení (EU) 2019/881 musí být členem týmu odborníků vybraných podle odstavce 1 tohoto oddílu navíc odborník z vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je ve spojení s dotčeným certifikačním subjektem.

3. Pro vzájemné hodnocení typu 2 jsou členové týmu vybráni z certifikačních subjektů, které jsou autorizovány pro danou technickou oblast.

4. Každý člen hodnotícího týmu má nejméně dvouletou zkušenost s prováděním certifikačních činností v certifikačním subjektu.

5. Pro vzájemné hodnocení typu 2 nebo 3 má každý člen hodnotícího týmu alespoň dvouletou zkušenost s prováděním certifikačních činností v příslušné technické oblasti nebo profilu ochrany a prokázané odborné znalosti a účast na autorizaci zařízení ITSEF.

6. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který monitoruje vzájemně hodnocený certifikační subjekt a dohlíží na něj, a alespoň jeden vnitrostátní orgán certifikace kybernetické bezpečnosti, jehož certifikační subjekt není předmětem vzájemného hodnocení, se vzájemného hodnocení účastní jako pozorovatel. Agentura ENISA se může vzájemného hodnocení účastnit také jako pozorovatel.

7. Certifikačnímu subjektu, který je podroben vzájemnému hodnocení, je předloženo složení týmu pro vzájemné hodnocení. V odůvodněných případech může složení týmu pro vzájemné hodnocení zpochybnit a požádat o jeho přezkoumání.

PŘÍLOHA VII

Obsah certifikátu EUCC

Certifikát EUCC musí obsahovat alespoň:

a) jedinečný identifikátor stanovený certifikačním subjektem vydávajícím certifikát;

b) informace týkající se certifikovaného produktu IKT nebo profilu ochrany a držitele certifikátu, včetně:

   1) názvu produktu IKT nebo profilu ochrany a případně cíle hodnocení;

   2) typu produktu IKT nebo profilu ochrany a případně cíle hodnocení;

   3) verze produktu IKT nebo profilu ochrany;

   4) jména, adresy a kontaktních údajů držitele certifikátu;

   5) odkazu na internetové stránky držitele certifikátu obsahující doplňující informace o kybernetické bezpečnosti uvedené v článku 55 nařízení (EU) 2019/881;

c) informace týkající se hodnocení a certifikace produktu IKT nebo profilu ochrany, včetně:

   1) názvu, adresy a kontaktních údajů certifikačního subjektu, který certifikát vydal;

   2) pokud se liší od certifikačního subjektu, názvu zařízení ITSEF, které provedlo hodnocení;

   3) názvu příslušného vnitrostátního orgánu certifikace kybernetické bezpečnosti;

   4) odkazu na toto nařízení;

   5) odkazu na zprávu o certifikaci spojenou s certifikátem uvedeným v příloze V;

   6) příslušné úrovně záruky v souladu s článkem 4;

   7) odkazu na verzi norem použitou pro hodnocení podle článku 3;

   8) identifikace úrovně záruky nebo balíčku záruk specifikovaných v normách uvedených v článku 3 a v souladu s přílohou VIII, včetně použitých složek záruky a úrovně AVA_VAN, na kterou se vztahuje;

   9) případně odkazu na jeden nebo více profilů ochrany, kterým produkt IKT nebo profil ochrany vyhovuje;

   10) data vydání;

   11) doby platnosti certifikátu;

d) označení a štítek spojené s certifikátem v souladu s článkem 11.

PŘÍLOHA VIII

Prohlášení o balíčku záruk

1. Rozšíření, na rozdíl od definic ve společných kritériích:

a) se neoznačuje zkratkou „+“;

b) je podrobně popsáno seznamem všech dotčených složek;

c) je podrobně popsáno ve zprávě o certifikaci.

2. Úroveň záruky potvrzená v certifikátu EUCC může být doplněna úrovní záruky hodnocení podle článku 3 tohoto nařízení.

3. Pokud se úroveň záruky potvrzená v certifikátu EUCC nevztahuje na rozšíření, uvede se v certifikátu EUCC jeden z následujících balíčků:

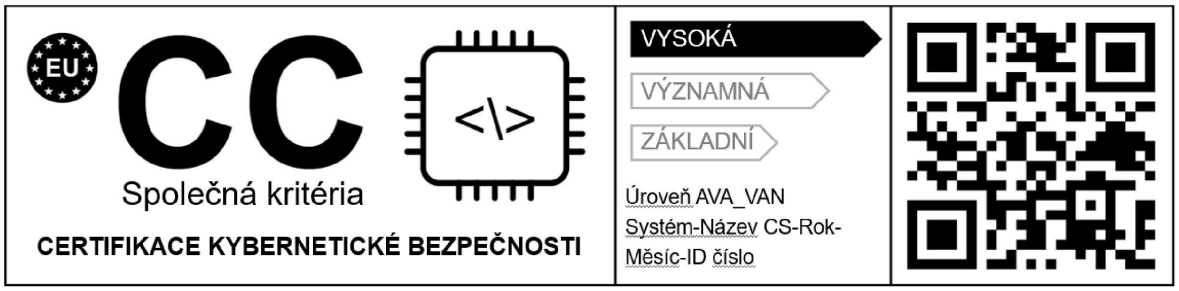
a) „balíček specifických záruk“;

b) „balíček záruk odpovídající profilu ochrany“ v případě odkazu na profil ochrany bez úrovně záruky hodnocení.

PŘÍLOHA IX

Označení a štítek

1. Podoba označení a štítku:



2. Pokud jsou označení a štítek zmenšeny nebo zvětšeny, musí být dodrženy proporce zobrazené ve výše uvedeném výkresu.

3. Pokud jsou fyzicky přítomny, musí být označení a štítek vysoké nejméně 5 mm.