Úřední věstník
Evropské unie

CS
Řada L

2025/2540

12.12.2025

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2025/2540

ze dne 9. prosince 2025,

kterým se stanoví prováděcí pravidla k nařízení Evropského parlamentu a Rady (EU) 2019/881, pokud jde o stanovení plánu vzájemného hodnocení

(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. 59 odst. 5 tohoto nařízení,

vzhledem k těmto důvodům:

(1) Podle čl. 59 odst. 4 nařízení (EU) 2019/881 mají vzájemná hodnocení vnitrostátních orgánů certifikace kybernetické bezpečnosti provádět dva vnitrostátní orgány certifikace kybernetické bezpečnosti jiných členských států a Komise. V zájmu dosažení rovnocenných norem, pokud jde o evropské certifikáty kybernetické bezpečnosti a EU prohlášení o shodě, by Komise měla sledovat aspekty související s dodržováním tohoto nařízení a zajistit, aby vzájemná hodnocení byla v celé Unii prováděna jednotným způsobem. S cílem pomoci určit osvědčené postupy, výzvy a poznatky získané při provádění evropských schémat certifikace kybernetické bezpečnosti by Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) měla mít možnost účastnit se vzájemných hodnocení jako pozorovatel. Agentuře ENISA by ve spolupráci s Komisí a Evropskou skupinou pro certifikaci kybernetické bezpečnosti (ECCG) mělo být rovněž na podporu harmonizovaného provádění ustanovení tohoto nařízení umožněno vypracovat vzory.

(2) Aby bylo zajištěno předvídatelné plánování a účinné přidělování zdrojů, měla by být vzájemná hodnocení každého vnitrostátního orgánu certifikace kybernetické bezpečnosti prováděna podle stanoveného harmonogramu. Vnitrostátní orgán certifikace kybernetické bezpečnosti by měl mít za výjimečných okolností, jako je neočekávaný nedostatek zaměstnanců nebo případy vyšší moci, možnost požádat o odklad vzájemného hodnocení. Za tímto účelem je nezbytné stanovit ujednání pro posouzení takové žádosti a zajistit, aby byl zastřešující harmonogram zachován a nebyly ohroženy cíle mechanismu vzájemného hodnocení.

(3) Aby se zajistilo, že k provádění mechanismu vzájemného hodnocení přispějí všechny členské státy a že budou moci využívat vzájemného učení, měly by vnitrostátní orgány certifikace kybernetické bezpečnosti každého členského státu provádět dvě vzájemná hodnocení během pětiletého období. Měl by být proto zaveden rotační systém, který vnitrostátním orgánům certifikace kybernetické bezpečnosti všech členských států umožní plánovat svou účast. Je rovněž nezbytné stanovit kritéria, která by vnitrostátní orgány certifikace kybernetické bezpečnosti měly zohlednit při výběru zástupců k provádění vzájemných hodnocení s cílem zajistit odpovídající odborné znalosti a způsobilost. Vnitrostátním orgánům certifikace kybernetické bezpečnosti by rovněž mělo být umožněno účastnit se vzájemných hodnocení jako pozorovatelé, aby mohli tento proces monitorovat a učit se z něj. V takových případech by se nemělo požadovat, aby jejich zástupce měl stejné odborné znalosti a způsobilost, jaké se očekávají od zástupců vnitrostátních orgánů certifikace kybernetické bezpečnosti provádějících vzájemná hodnocení.

(4) Aby se zajistilo, že vnitrostátní orgán certifikace kybernetické bezpečnosti bude podroben vzájemnému hodnocení alespoň jedním vnitrostátním orgánem certifikace kybernetické bezpečnosti, který používá stejný přístup k vydávání certifikátů s úrovní „vysoká“, měla by agentura ENISA při výzvě vnitrostátních orgánů úrovni k vyjádření jejich zájmu o vzájemné hodnocení uvést, zda vzájemně hodnocený vnitrostátní orgán certifikace kybernetické bezpečnosti přímo vydává certifikáty s úrovní „vysoká“ nebo zda používá model předchozího schválení uvedený v čl. 56 odst. 6 písm. a) nařízení (EU) 2019/881, uděluje obecné pověření v souladu s písmenem b) uvedeného odstavce nebo používá kombinaci těchto přístupů.

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

(5) Aby byla zajištěna společná hodnotící kritéria a postupy pro provádění vzájemných hodnocení v celé Unii, mělo by každé z těchto hodnocení vždy zahrnovat dotazník pro sebehodnocení, přezkum dokumentace a návštěvu na místě spolu s dotazováním. Po návštěvě na místě by tým pro vzájemné hodnocení měl zjištění projednat s vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, vypracovat návrh zprávy a předložit jej hodnocenému vnitrostátnímu orgánu certifikace kybernetické bezpečnosti k vyjádření, aby byl pokud možno zajištěn konsensus. Tým pro vzájemné hodnocení by měl skupině ECCG předložit závěrečnou zprávu, která může obsahovat pokyny nebo doporučení, na jejichž základě se může vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, zlepšit. Skupina ECCG by měla na návrh týmu pro vzájemné hodnocení rovněž schválit souhrnnou zprávu, která má být zveřejněna.

(6) Aby bylo zajištěno, že s informacemi získanými v rámci procesu vzájemného hodnocení bude nakládáno bezpečným způsobem, měl by tým pro vzájemné hodnocení zajistit používání bezpečných komunikačních kanálů, jako je zabezpečená platforma pro uchovávání a sdílení dokumentů, a používání vhodných záruk pro důvěrné údaje sdílené mezi členy týmu pro vzájemné hodnocení. Agentura ENISA by s přihlédnutím ke stávajícím osvědčeným postupům vnitrostátních orgánů certifikace kybernetické bezpečnosti měla mít rovněž možnost vypracovat pokyny ohledně zajištění bezpečné komunikace, a to zejména s cílem zajistit, aby úroveň bezpečnosti uplatňovaná týmem pro vzájemné hodnocení při shromažďování, sdílení a zpracovávání informací odpovídala bezpečnostním potřebám hodnoceného vnitrostátního orgánu certifikace kybernetické bezpečnosti.

(7) V zájmu usnadnění spolupráce a účinné výměny informací mezi vnitrostátními orgány certifikace kybernetické bezpečnosti by skupina ECCG, zejména její podskupina pro vzájemné hodnocení, měla přispět k vypracování vzorů a pomáhat Komisi při provádění tohoto nařízení.

(8) Mechanismus vzájemného hodnocení představuje transevropskou digitální veřejnou službu ve smyslu nařízení Evropského parlamentu a Rady (EU) 2024/903 ([2]). Toto nařízení zavádí nové závazné požadavky týkající se této služby, a jako takové podléhá povinnosti posouzení interoperability podle článku 3 nařízení (EU) 2024/903. Provádí se proto posouzení interoperability a výsledná zpráva bude zveřejněna na portálu Interoperabilní Evropa.

(9) Při vypracovávání tohoto nařízení vzala Komise v úvahu názory skupiny ECCG, včetně její podskupiny pro vzájemné hodnocení.

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

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Harmonogram vzájemných hodnocení, jejich četnost a náklady s nimi spojené

1. Vzájemná hodnocení vnitrostátních orgánů certifikace kybernetické bezpečnosti se budou provádět v souladu s harmonogramem stanoveným v příloze I. Každé vzájemné hodnocení bude dokončeno do data uvedeného v tomto harmonogramu a poté se bude provádět každých pět let.

2. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, může za výjimečných okolností Komisi požádat, aby jeho vzájemné hodnocení posunula na pozdější datum, než je uvedeno v harmonogramu stanoveném v příloze I. Komise ve spolupráci s Evropskou skupinou pro certifikaci kybernetické bezpečnosti (ECCG) zřízenou článkem 62 nařízení (EU) 2019/881 žádost posoudí a všechny příslušné strany o výsledku včas informuje.

([2]) Nařízení Evropského parlamentu a Rady (EU) 2024/903 ze dne 13. března 2024, kterým se stanoví opatření pro vysokou úroveň interoperability veřejného sektoru v celé Unii (nařízení o interoperabilní Evropě) (Úř. věst. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. Pokud členský stát v souladu s čl. 58 odst. 1 nařízení (EU) 2019/881 určil:

a) více než jeden vnitrostátní orgán certifikace kybernetické bezpečnosti na svém území, všechny vnitrostátní orgány certifikace kybernetické bezpečnosti tohoto členského státu jsou podrobeny vzájemnému hodnocení souběžně;

b) vnitrostátní orgán certifikace kybernetické bezpečnosti nebo vnitrostátní orgány certifikace kybernetické bezpečnosti jiného členského státu, tento orgán nebo tyto orgány mohou být vzájemně hodnoceny v souladu s harmonogramem stanoveným buď pro určující členský stát, nebo pro členský stát určeného vnitrostátního orgánu certifikace kybernetické bezpečnosti nebo vnitrostátních orgánů certifikace kybernetické bezpečnosti, pokud jde o úkoly v oblasti dohledu prováděné v určujícím členském státě.

4. Agentura Evropské unie pro kybernetickou bezpečnost (ENISA) zveřejní na internetových stránkách o evropských schématech certifikace kybernetické bezpečnosti vytvořených podle článku 50 nařízení (EU) 2019/881:

a) informace o harmonogramu stanoveném v příloze I;

b) seznam vnitrostátních orgánů certifikace kybernetické bezpečnosti provádějících vzájemné hodnocení vedený podle čl. 2 odst. 5.

5. Každý vnitrostátní orgán certifikace kybernetické bezpečnosti, který se účastní procesu vzájemného hodnocení, nese vlastní náklady na účast.

Článek 2

Rotační systém pro vnitrostátní orgány certifikace kybernetické bezpečnosti, které provádějí vzájemné hodnocení

1. V souladu s čl. 59 odst. 4 nařízení (EU) 2019/881 mají každé vzájemné hodnocení provádět dva vnitrostátní orgány certifikace kybernetické bezpečnosti jiných členských států, které provádějí vzájemné hodnocení, a Komise. Vnitrostátní orgány certifikace kybernetické bezpečnosti každého členského státu se během každého období stanoveného v příloze I zúčastní vzájemného hodnocení alespoň dvou vnitrostátních orgánů certifikace kybernetické bezpečnosti.

2. Vnitrostátní orgány certifikace kybernetické bezpečnosti jiných členských států se mohou účastnit vzájemného hodnocení jako pozorovatelé s jedním nebo více zástupci, a to se souhlasem vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, vnitrostátního orgánu certifikace kybernetické bezpečnosti, který vzájemné hodnocení provádí, a Komise.

3. Vzájemného hodnocení se může jako pozorovatel zúčastnit jeden zástupce agentury ENISA. Se souhlasem vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, vnitrostátního orgánu certifikace kybernetické bezpečnosti, který vzájemné hodnocení provádí, a Komise se mohou rovněž účastnit další zástupci.

4. Pozorovatelé mají přístup ke stejným informacím jako ostatní členové týmu pro vzájemné hodnocení, ale neplní úkoly související s prováděním vzájemného hodnocení.

5. Agentura ENISA ve spolupráci s Komisí a skupinou ECCG navrhne a vede seznam vnitrostátních orgánů certifikace kybernetické bezpečnosti, které provádějí vzájemné hodnocení, jež mají vypracovat harmonogram stanovený v příloze I. Agentura ENISA ve spolupráci s Komisí během daného roku vnitrostátní orgány certifikace kybernetické bezpečnosti požádá, aby vyjádřily svůj zájem o provedení vzájemných hodnocení vnitrostátních orgánů certifikace kybernetické bezpečnosti podle harmonogramu v příloze I na následující rok nebo o účast v roli pozorovatele.

6. Pokud o provedení vzájemného hodnocení téhož vnitrostátního orgánu certifikace kybernetické bezpečnosti vyjádří zájem více než dva vnitrostátní orgány certifikace kybernetické bezpečnosti, Komise a agentura ENISA zúčastněné vnitrostátní orgány certifikace kybernetické bezpečnosti konzultují a rozhodnou o účastnících vzájemného hodnocení.

7. Pokud v daném roce není dostatek vnitrostátních orgánů certifikace kybernetické bezpečnosti, které mají provádět vzájemné hodnocení, jež vyjádří svůj zájem o provedení vzájemných hodnocení, Komise po konzultaci se skupinou ECCG vybere vnitrostátní orgány certifikace kybernetické bezpečnosti, které vzájemné hodnocení provedou. Komise při svém výběru zohlední povinnost vnitrostátních orgánů certifikace kybernetické bezpečnosti každého členského státu zúčastnit se vzájemného hodnocení alespoň dvou vnitrostátních orgánů certifikace kybernetické bezpečnosti uvedenou v odstavci 1.

Článek 3

Kritéria týkající se složení týmu pro vzájemné hodnocení

1. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který provádí vzájemné hodnocení, v dostatečném předstihu před zahájením vzájemného hodnocení určí jednoho zástupce, který vzájemné hodnocení provede. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který provádí vzájemné hodnocení, může jmenovat více než jednoho zástupce, je-li to nezbytné k zajištění toho, aby měl tým pro vzájemné hodnocení nezbytné kompetence k provedení vzájemného hodnocení.

2. Zástupce vnitrostátního orgánu certifikace kybernetické bezpečnosti, který provádí vzájemné hodnocení, s výjimkou zástupců vnitrostátního orgánu certifikace kybernetické bezpečnosti, kteří se účastní jako pozorovatelé, musí splňovat tato kritéria:

a) mít nejméně dvouletou zkušenost s prací pro vnitrostátní orgán certifikace kybernetické bezpečnosti, který provádí vzájemné hodnocení, nebo mít za sebou účast alespoň na dvou vzájemných hodnocení v roli pozorovatele;

b) mít dostatečné znalosti rámce pro certifikaci kybernetické bezpečnosti stanoveného nařízením (EU) 2019/881;

c) mít dobrou pracovní znalost angličtiny a pokud možno jednoho nebo více jazyků, jimiž se hovoří v členském státě vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení;

d) fungovat nezávisle na vnitrostátním orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení.

3. Vnitrostátní orgány certifikace kybernetické bezpečnosti, které vzájemné hodnocení provádějí, zajistí, aby před zahájením procesu vzájemného hodnocení bylo ostatním vnitrostátním orgánům certifikace kybernetické bezpečnosti, Komisi a agentuře ENISA sděleno jakékoli riziko střetu zájmů týkající se určených zástupců. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, může proti jmenování konkrétních zástupců v souladu s odstavcem 5 vznést námitku.

4. Vnitrostátní orgány certifikace kybernetické bezpečnosti, které provádějí vzájemné hodnocení, si ze svých řad vyberou jednoho zástupce (dále jen „vedoucí týmu“), který bude vzájemné hodnocení koordinovat.

5. Před zahájením procesu vzájemného hodnocení poskytne Komise vnitrostátnímu orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, jména a kontaktní údaje zástupců vnitrostátních orgánů certifikace kybernetické bezpečnosti, které vzájemné hodnocení provádějí. Pokud si vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, přeje vznést námitku proti jmenování jednoho nebo více zástupců, poskytne do dvou týdnů Komisi jasné odůvodnění, informuje agenturu ENISA a skupinu ECCG a požádá je, aby vnitrostátní orgán certifikace kybernetické bezpečnosti, který vzájemné hodnocení provádí, jmenoval jiného zástupce.

6. Pokud postup stanovený v odstavci 5 způsobí z důvodu výjimečných okolností zbytečné prodlevy při zahájení vzájemného hodnocení, rozhodne o složení týmu pro vzájemné hodnocení Komise po konzultaci s agenturou ENISA a skupinou ECCG.

Článek 4

Metodika vzájemného hodnocení

1. Vzájemné hodnocení posoudí aspekty uvedené v příloze II v souladu s čl. 59 odst. 3 nařízení (EU) 2019/881.

2. Agentura ENISA může ve spolupráci se skupinou ECCG a Komisí vypracovat vzory pro posuzování procesů stanovených vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení.

3. Vzájemné hodnocení se zaměří na:

a) dotazník se sebehodnocením;

b) posouzení příslušné dokumentace;

c) online nebo fyzické dotazování nebo obojí;

d) návštěvu na místě.

4. Délka vzájemného hodnocení může být mezi týmem pro vzájemné hodnocení a vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, předem dohodnuta v závislosti na rozsahu a složitosti činností vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení. Návštěva na místě nesmí trvat déle než tři pracovní dny.

5. Nedohodnou-li se tým pro vzájemné hodnocení, vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, a Komise jinak, je jazykem spolupráce angličtina. Zpráva o vzájemném hodnocení uvedená v článku 5 se vypracuje alespoň v angličtině.

6. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, musí spolupracovat a týmu pro vzájemné hodnocení poskytnout přístup k informacím a dokumentům, které jsou k provedení vzájemného hodnocení nezbytné. Vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, předloží alespoň 21 dnů před datem návštěvy na místě dotazník se sebehodnocením a poslední každoroční souhrnnou zprávu přijatou v souladu s čl. 58 odst. 7 písm. g) nařízení (EU) 2019/881. Další dokumenty se na žádost týmu pro vzájemné hodnocení předkládají do sedmi dnů od obdržení těchto žádostí.

7. Dokumenty se poskytují v angličtině, není-li podle odstavce 5 dohodnuto jinak. Nejsou-li dokumenty poskytnuty v angličtině, může tým pro vzájemné hodnocení požádat, aby byly dokumenty nezbytné k provedení vzájemného hodnocení přeloženy do angličtiny.

8. Před vypracováním zprávy o vzájemném hodnocení v souladu s článkem 5 projedná tým pro vzájemné hodnocení předběžná zjištění s vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení.

Článek 5

Zpráva o vzájemném hodnocení

1. Tým pro vzájemné hodnocení vypracuje do 21 dnů od provedení tohoto hodnocení návrh zprávy o vzájemném hodnocení, která obsahuje podrobnosti o členském státě vnitrostátního orgánu certifikace kybernetické bezpečnosti, který byl předmětem vzájemného hodnocení, o vnitrostátních orgánech certifikace kybernetické bezpečnosti, které hodnocení provedly, o Komisi a jakémkoliv pozorovateli, jakož i zjištění a závěry vzájemného hodnocení. V případě potřeby obsahují zprávy doporučení, jejichž cílem je dosáhnout zlepšení v aspektech, jichž se vzájemné hodnocení týká.

2. Agentura ENISA může ve spolupráci s Komisí a skupinou ECCG vypracovat vzor pro zprávu o vzájemném hodnocení.

3. Po vypracování návrhu zprávy o vzájemném hodnocení v souladu s odstavcem 1 jej tým pro vzájemné hodnocení poskytne vnitrostátnímu orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, aby se k němu do 14 dnů vyjádřil. Tým pro vzájemné hodnocení tyto připomínky vyhodnotí a pokud možno je začlení do závěrečné zprávy s cílem zajistit konsensus. V případě neshody se odpověď vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, připojí k závěrečné zprávě.

4. Závěrečná zpráva se zašle skupině ECCG do dvou měsíců od provedení vzájemného hodnocení, včetně shrnutí určeného ke zveřejnění. V souladu s čl. 59 odst. 6 nařízení (EU) 2019/881 skupina ECCG zprávu posoudí a schválí její shrnutí, které se zveřejní na internetových stránkách o evropských schématech certifikace kybernetické bezpečnosti vytvořených podle článku 50 nařízení (EU) 2019/881. Po dohodě s vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, zahrnuje shrnutí rovněž jeho odpověď nebo její části.

5. Před tím, než tým pro vzájemné hodnocení rozešle zprávu o vzájemném hodnocení mimo tento tým, anonymizuje osobní údaje, které během vzájemného hodnocení případně shromáždil.

Článek 6

Důvěrnost informací

1. Všechny strany, které se podílejí na vzájemném hodnocení, zachovávají důvěrnost informací a údajů, jež získají při provádění svých úkolů a činnosti, takovým způsobem, aby chránily zejména:

a) práva duševního vlastnictví a důvěrné obchodní informace nebo obchodní tajemství fyzických nebo právnických osob, včetně zdrojového kódu, s výjimkou případů, na které se vztahuje článek 5 směrnice Evropského parlamentu a Rady (EU) 2016/943 ([3]),

b) účinné provádění tohoto nařízení,

c) veřejné a národní bezpečnostní zájmy,

d) integritu trestního nebo správního řízení.

2. Tým pro vzájemné hodnocení zajistí, aby s veškerými informacemi získanými v rámci procesu vzájemného hodnocení bylo nakládáno bezpečně. Po vypracování závěrečné zprávy a shrnutí podle čl. 5 odst. 4 tým pro vzájemné hodnocení, včetně případného pozorovatele, vymaže nebo zničí všechny dokumenty, které byly v rámci procesu vzájemného hodnocení shromážděny nebo vytvořeny, kromě závěrečné zprávy a shrnutí.

3. Agentura ENISA může s přihlédnutím ke stávajícím osvědčeným postupům vnitrostátních orgánů certifikace kybernetické bezpečnosti ve spolupráci se skupinou ECCG vypracovat pokyny pro bezpečnou a důvěrnou komunikaci.

([3]) Směrnice Evropského parlamentu a Rady (EU) 2016/943 ze dne 8. června 2016 o ochraně nezveřejněného know-how a obchodních informací (obchodního tajemství) před jejich neoprávněným získáním, využitím a zpřístupněním (Úř. věst. L 157, 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Článek 7

Budování kapacit

Agentura ENISA analyzuje souhrnné výsledky vzájemných hodnocení a zdůrazní získané zkušenosti a osvědčené postupy s cílem přispět k budování kapacit vnitrostátních orgánů certifikace kybernetické bezpečnosti a k udržování evropských schémat certifikace kybernetické bezpečnosti. Tato analýza může případně zahrnovat odbornou přípravu a další pokyny pro vnitrostátní orgány certifikace kybernetické bezpečnosti vypracované ve spolupráci se skupinou ECCG.

Článek 8

Vstup v platnost

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

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

V Bruselu dne 9. prosince 2025.

Za Komisi
předsedkyně
Ursula VON DER LEYEN

PŘÍLOHA I

Harmonogram vnitrostátních orgánů certifikace kybernetické bezpečnosti, které jsou předmětem vzájemného hodnocení

Vnitrostátní orgány certifikace kybernetické bezpečnosti níže uvedených členských států budou předmětem vzájemného hodnocení do 31. prosince 2026 a poté každých pět let:

Švédsko, Belgie, Slovensko, Německo, Malta, Česko

Vnitrostátní orgány certifikace kybernetické bezpečnosti níže uvedených členských států budou předmětem vzájemného hodnocení do 31. prosince 2027 a poté každých pět let:

Maďarsko, Řecko, Estonsko, Slovinsko, Nizozemsko, Itálie

Vnitrostátní orgány certifikace kybernetické bezpečnosti níže uvedených členských států budou předmětem vzájemného hodnocení do 31. prosince 2028 a poté každých pět let:

Chorvatsko, Dánsko, Litva, Španělsko, Bulharsko, Irsko

Vnitrostátní orgány certifikace kybernetické bezpečnosti níže uvedených členských států budou předmětem vzájemného hodnocení do 31. prosince 2029 a poté každých pět let:

Finsko, Rakousko, Rumunsko, Lucembursko, Lotyšsko, Polsko

Vnitrostátní orgány certifikace kybernetické bezpečnosti níže uvedených členských států a zemí ESVO, které jsou členy EHP, budou předmětem vzájemného hodnocení do 31. prosince 2030 a poté každých pět let:

Kypr, Francie, Portugalsko, Lichtenštejnsko, Norsko, Island

PŘÍLOHA II

Metodika vzájemného hodnocení

II.1 **Oddělení činností souvisejících s certifikací od činností dozoru**

Při posuzování oddělení činností vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, souvisejících s certifikací od činností dozoru podle čl. 59 odst. 3 písm. a) nařízení (EU) 2019/881 se v rámci vzájemného hodnocení posoudí alespoň tyto aspekty:

a) podrobný popis fungování vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, s jasným uvedením různých subjektů a/nebo útvarů zapojených do provádění nařízení (EU) 2019/881;

b) mapování činností vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, ve srovnání s činnostmi uvedenými v čl. 58 odst. 7 nařízení (EU) 2019/881;

c) pokud vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, vydává certifikáty, vysvětlení prokazující, že mezi jeho činnostmi souvisejícími s certifikací a činnostmi dozoru uvedenými v písmenu b) nedochází k žádnému prolínání.

II.2 **Dohled nad pravidly pro monitorování souladu certifikáty a jejich vymáhání**

Při posuzování postupů vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, spojených s dohledem nad pravidly pro monitorování souladu produktů, služeb a procesů IKT a řízených bezpečnostních služeb s evropskými certifikáty kybernetické bezpečnosti uvedenými v čl. 59 odst. 3 písm. b) nařízení (EU) 2019/881 a vymáháním těchto pravidel se v rámci vzájemného hodnocení posoudí alespoň tyto aspekty:

a) kvalita a úroveň podrobného popisu těchto procesů a postupů a rozsah, v jakém jsou zdokumentovány;

b) zda a do jaké míry se tyto procesy a postupy vztahují na příslušná evropská schémata certifikace kybernetické bezpečnosti;

c) zda je vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, účinně zmocněn kontrolovat subjekty posuzování shody, které vydávají certifikáty, a v případě potřeby vymáhat odejmutí certifikátů;

d) rozsah spolupráce vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, s příslušnými orgány dozoru nad trhem;

e) zda má vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, mechanismus pro řešení stížností fyzických nebo právnických osob požadovaný podle čl. 58 odst. 7 písm. f) nařízení (EU) 2019/881, včetně důkazů o tom, zda mají fyzické a právnické osoby právo podat stížnost a získat účinný soudní prostředek nápravy v souladu s články 63 a 64 uvedeného nařízení.

II.3 **Sledování povinností výrobců nebo poskytovatelů a jejich vymáhání**

Při posuzování postupů vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, spojených se sledováním povinností výrobců nebo poskytovatelů, kteří provádějí vlastní posuzování shody, podle čl. 59 odst. 3 písm. c) nařízení (EU) 2019/881, a vymáháním těchto povinností se v rámci vzájemného hodnocení posoudí alespoň tyto aspekty:

a) zda vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, tyto postupy zavedl a do jaké míry jsou zdokumentovány, zejména zda zavedl mechanismus pro přijímání a zpracovávání informací z externích zdrojů;

b) zda a do jaké míry se tyto postupy vztahují na příslušná evropská schémata certifikace kybernetické bezpečnosti;

c) zda a do jaké míry vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, provádí svá vlastní šetření a zda rozsah šetření zahrnuje povinnosti výrobců stanovené v čl. 53 odst. 2 a 3 nařízení (EU) 2019/881 a v odpovídajících evropských schématech certifikace kybernetické bezpečnosti;

d) zda existuje postup pro výměnu informací mezi činnostmi souvisejícími s certifikací a činnostmi dozoru vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, které jsou relevantní pro sledování povinností výrobců nebo poskytovatelů a jejich vymáhání.

II.4 **Sledování a autorizace subjektů posuzování shody a dohled nad nimi**

Při posuzování postupů vnitrostátního orgánu certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, pro sledování a autorizaci činností subjektů posuzování shody a pro dohled nad nimi podle čl. 59 odst. 3 písm. d) nařízení (EU) 2019/881 se v rámci vzájemného hodnocení posoudí alespoň tyto aspekty:

a) kvalita a úroveň podrobného popisu těchto postupů a rozsah, v jakém jsou zdokumentovány, a to i pro účely spolupráce s vnitrostátním akreditačním orgánem;

b) klíčové statistiky o počtu udělených, pozastavených nebo zrušených povolení, celkovém počtu aktivních subjektů posuzování shody, počtu vydaných certifikátů a počtu nápravných opatření přijatých vnitrostátním orgánem certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení;

c) pokud vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, umožňuje po předchozím schválení nebo na základě obecného pověření úkolem podle čl. 56 odst. 6 nařízení (EU) 2019/881 vydávání evropských certifikátů kybernetické bezpečnosti na úrovni „vysoká“, odborné znalosti pracovníků a postupy, jejichž prostřednictvím vnitrostátní orgán certifikace kybernetické bezpečnosti, který je předmětem vzájemného hodnocení, sleduje činnosti subjektů posuzování shody a dohlíží na ně.