ROZHODNUTÍ KOMISE (EU, Euratom) 2018/559

ze dne 6. dubna 2018,

kterým se stanoví prováděcí pravidla pro článek 6 rozhodnutí (EU, Euratom) 2017/46 o bezpečnosti komunikačních a informačních systémů v Evropské komisi

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 249 této smlouvy,

s ohledem na Smlouvu o založení Evropského společenství pro atomovou energii,

s ohledem na rozhodnutí Komise (EU, Euratom) 2017/46 ze dne 10. ledna 2017 o bezpečnosti komunikačních a informačních systémů v Evropské komisi ([1]), a zejména na článek 6 uvedeného rozhodnutí,

vzhledem k těmto důvodům:

(1) V souvislosti s přijetím rozhodnutí (EU, Euratom) 2017/46 musí Komise přezkoumat, aktualizovat a konsolidovat prováděcí pravidla spojená se zrušeným rozhodnutím Komise C(2006) 3602 o bezpečnosti komunikačních a informačních systémů používaných Komisí.

(2) Člen Komise odpovědný za bezpečnost byl v plném souladu s vnitřním jednacím řádem zmocněn, aby stanovil prováděcí pravidla v souladu s článkem 13 rozhodnutí (EU, Euratom) 2017/46 ([2]).

(3) Prováděcí pravidla rozhodnutí C(2006) 3602 by proto měla být zrušena,

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA 1

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Předmět a oblast působnosti tohoto rozhodnutí jsou uvedeny v článku 1 rozhodnutí (EU, Euratom) 2017/46.

2. Ustanovení tohoto rozhodnutí se týkají všech komunikačních a informačních systémů (CIS). Odpovědnosti vymezené v tomto rozhodnutí se však netýkají CIS zpracovávajících utajované informace EU. Příslušné odpovědnosti pro tyto systémy určí vlastník systémů a bezpečnostní orgán Komise v souladu s rozhodnutím Komise (EU, Euratom) 2015/444 ([3]).

3. V kapitole 2 tohoto rozhodnutí je uveden přehled praktického provádění organizace a odpovědností souvisejících s bezpečností IT. V kapitole 3 tohoto rozhodnutí je uveden přehled postupů podle článku 6 rozhodnutí (EU, Euratom) 2017/46.

Článek 2

Definice

Pro toto rozhodnutí se použijí definice uvedené v článku 2 rozhodnutí (EU, Euratom) 2017/46. Pro účely tohoto rozhodnutí se dále rozumí:

1. „schvalovacím orgánem pro kryptografickou ochranu“ (CAA) funkce vykonávaná bezpečnostním orgánem Komise, který spadá pod vedení Generálního ředitelství pro lidské zdroje a bezpečnost;

([1]) Úř. věst. L 6, 11.1.2017, s. 40.
([2]) Rozhodnutí Komise C(2017) 7428 final ze dne 8. listopadu 2017, kterým se uděluje zmocnění k přijetí prováděcích pravidel, norem a pokynů týkajících se bezpečnosti komunikačních a informačních systémů v Evropské komisi.
([3]) Rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU (Úř. věst. L 72, 17.3.2015, s. 53).

2. „vnějším připojením k síti“ jakékoliv propojení elektronické komunikace mezi vnitřní sítí Komise a jakoukoli jinou sítí, včetně internetu. Tato definice nezahrnuje sítě třetích stran, které jsou poskytovány na základě smlouvy jako součást vnitřní sítě Komise;

3. „úschovou klíče u třetí strany“ postup pro uchovávání kopií kryptografických klíčů u jedné nebo více samostatných stran při zajištění oddělení funkcí, aby bylo umožněno jejich obnovení v případě ztráty provozního klíče. Klíče mohou být rozděleny do dvou nebo více částí, přičemž každá z nich je uložena u jiné strany, aby bylo zajištěno, že žádná jednotlivá strana nemá k dispozici celý klíč.

4. výrazem „RASCI“ zkratka pro přidělení odpovědnosti na základě těchto atributů, kterými se rozumí:

   a) „odpovědným“ („*responsible*“–R) mající povinnost jednat a přijímat rozhodnutí k dosažení požadovaných výsledků;

   b) „ručícím“ („*accountable*“–A) nesoucí zodpovědnost za kroky, rozhodnutí a plnění;

   c) „podporujícím“ („*supports*“–S) mající povinnost spolupracovat s odpovědnou osobu na splnění úkolu;

   d) „konzultovaným“ („*consulted*“–C) kontaktovaný pro radu nebo stanovisko;

   e) „informovaným“ („*informed*“–I) dostávající aktuální příslušné informace.

KAPITOLA 2

ORGANIZACE A ODPOVĚDNOST

Článek 3

Úlohy a odpovědnosti

Úlohy a odpovědnosti v souvislosti s články 4 až 8 tohoto rozhodnutí jsou vymezeny v příloze v souladu s modelem RASCI.

Článek 4

Sladění s politikou Komise v oblasti bezpečnosti informačních systémů

1. Generální ředitelství pro lidské zdroje a bezpečnost provádí přezkum politiky Komise v oblasti bezpečnosti IT a souvisejících norem a pokynů, aby bylo zajištěno, že jsou v souladu s obecnými bezpečnostními politikami Komise, zejména s rozhodnutím Komise (EU, Euratom) 2015/443 ([1]) a rozhodnutím (EU, Euratom) 2015/444.

2. Na žádost jiných útvarů Komise může Generální ředitelství pro lidské zdroje a bezpečnost provést přezkum jejich politik v oblasti bezpečnosti IT nebo jiné dokumentace v oblasti bezpečnosti IT, aby byl zajištěn jejich soulad s politikou Komise v oblasti bezpečnosti informačních systémů. Vedoucí dotčeného útvaru Komise zajistí, aby všechny nesrovnalosti byly řešeny.

3. Generální ředitelství pro lidské zdroje a bezpečnost v rámci své odpovědnosti za bezpečnost informací spolupracuje s Generálním ředitelstvím pro informatiku, aby bylo zajištěno, že postupy v oblasti bezpečnosti IT plně zohledňují klasifikaci a zásady bezpečnosti stanovené v rozhodnutí (EU, Euratom) 2015/443, zejména v článcích 3 a 9.

KAPITOLA 3

POSTUPY V OBLASTI BEZPEČNOSTI IT

Článek 5

Šifrovací technologie

1. Použití šifrovacích technologií pro ochranu utajovaných informací EU („*EU classified information*“ – EUCI) musí být v souladu s rozhodnutím (EU, Euratom) 2015/444.

2. Rozhodnutí o použití šifrovacích technologií pro ochranu jiných informací než EUCI musí být přijato vlastníkem každého komunikačního a informačního systému s přihlédnutím jak k rizikům, která mají být šifrováním zmírněna, tak k rizikům, která to přináší.

3. Jakékoli použití šifrovacích technologií vyžaduje předchozí schválení ze strany CAA s výjimkou případu, kdy je šifrování použito pouze pro ochranu důvěrnosti jiných informací než EUCI během přenosu a používá standardní síťové komunikační protokoly.

([1]) Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (Úř. věst. L 72, 17.3.2015, s. 41).

4. S výjimkou uvedenou v odstavci 3 tohoto článku útvary Komise zajistí, aby zálohy všech dešifrovacích klíčů byly uloženy v úschově u třetí strany za účelem obnovení uložených údajů v případě, že dešifrovací klíč nebude k dispozici. Obnovení zašifrovaných údajů pomocí záloh dešifrovacích klíčů se smí provést pouze na základě autorizace v souladu s normou definovanou ze strany CAA.

5. Žádosti o schválení použití šifrovacích technologií musí být formálně doloženy a musí obsahovat podrobnosti o příslušném komunikačním a informačním systému a o údajích, které mají být chráněny, technologiích, které mají být použity, a souvisejících bezpečnostních provozních postupech. Tyto žádosti o schválení podepisuje vlastník systému.

6. Žádosti o schválení použití šifrovacích technologií posuzuje CAA v souladu se zveřejněnými normami a požadavky.

Článek 6

Bezpečnostní kontroly IT

1. Generální ředitelství pro lidské zdroje a bezpečnost provádí bezpečnostní kontroly IT s cílem ověřit, zda jsou opatření pro bezpečnost IT v souladu s politikami Komise v oblasti bezpečnosti IT, a zkontrolovat integritu těchto kontrolních opatření.

2. Generální ředitelství pro lidské zdroje a bezpečnost může bezpečnostní kontrolu IT provést:

a) z vlastního podnětu;

b) na žádost Rady pro řízení informační bezpečnosti (ISSB);

c) na žádost vlastníka systému;

d) v případě bezpečnostního incidentu nebo

e) v případě zjištění vysokého rizika pro určitý systém.

3. Vlastníci údajů mohou o bezpečnostní kontrolu IT požádat před uložením svých informací v komunikačním a informačním systému.

4. Výsledky kontroly musí být doloženy v oficiální zprávě pro vlastníka systému, která obsahuje zjištění a doporučení ke zlepšení souladu komunikačního a informačního systému s politikou v oblasti bezpečnosti IT, s kopií odeslanou úředníkovi pro bezpečnost informatiky na místní úrovni (LISO). Generální ředitelství pro lidské zdroje a bezpečnost informuje o závažných problémech a doporučeních ISSB.

5. Generální ředitelství pro lidské zdroje a bezpečnost sleduje provádění doporučení.

6. Bezpečnostní kontroly IT musí v příslušných případech zahrnovat kontrolu služeb, prostor a vybavení poskytnutých vlastníkovi systému, včetně interních i externích poskytovatelů služeb.

Článek 7

Přístup z vnějších sítí

1. Generální ředitelství pro lidské zdroje a bezpečnost stanoví pravidla v normě o autorizaci přístupu mezi komunikačními a informačními systémy Komise a vnějšími sítěmi.

2. Pravidla musí rozlišovat mezi různými druhy vnějších připojení k síti a pro každý druh připojení stanovit vhodná bezpečnostní pravidla, včetně stanovení, zda je pro dané připojení vyžadována předchozí autorizace příslušného orgánu, jak je uvedeno v odstavci 4 tohoto článku.

3. V případě potřeby se autorizace udělí na základě oficiální žádosti a schvalovacího postupu. Schválení je platné po určenou dobu a musí být získáno před aktivací připojení.

4. Generální ředitelství pro lidské zdroje a bezpečnost má celkovou odpovědnost za autorizaci žádostí, ale může odpovědnost za autorizaci některých druhů připojení na základě vlastního uvážení přenést na jiný útvar v souladu s čl. 17 odst. 3 rozhodnutí (EU, Euratom) 2015/443 a za podmínek stanovených v odstavci 8.

5. Subjekt udělující autorizaci může jako podmínku pro schválení za účelem ochrany komunikačních a informačních systémů a sítí Komise před riziky neoprávněného přístupu nebo jiného narušení bezpečnosti stanovit další bezpečnostní požadavky.

6. Standardním poskytovatelem síťových služeb pro Komisi je generální ředitelství pro informatiku. Jakýkoli jiný útvar Komise provozující síť, jíž neposkytuje generální ředitelství pro informatiku, musí nejprve získat souhlas ISSB. Příslušný útvar Komise doloží opodstatnění žádosti a prokáže, že kontroly sítě jsou dostatečné pro splnění požadavků na kontrolu příchozích a odchozích toků informací.

7. Vlastník komunikačního a informačního systému určí bezpečnostní požadavky pro vnější přístup do tohoto systému a s podporou úředníka pro bezpečnost informatiky na místní úrovni zajistí zavedení vhodných opatření na ochranu bezpečnosti CIS.

8. Ochranná opatření zavedená pro vnější připojení k síti musí vycházet ze zásad „vědět jen to nejnutnější“ a „co nejomezenějších práv“, které zajišťují, že jednotlivci obdrží pouze ty informace a přístupová práva, které potřebují k výkonu svých funkcí pro Komisi.

9. Všechna vnější připojení k síti musí být filtrována a sledována, aby se odhalila možná narušení bezpečnosti.

10. V případě, že jsou připojení zřízena proto, aby umožnila externí zajištění komunikačního a informačního systému, je autorizace podmíněna úspěšným dokončením postupu popsaného v článku 8.

Článek 8

Externí zajišťování komunikačních a informačních systémů (CIS)

1. Pro účely tohoto rozhodnutí se CIS považuje za externě zajišťovaný, jestliže je zajišťován na základě smlouvy uzavřené s dodavatelem, kterým je třetí strana, a podle uvedené smlouvy je CIS umístěn v prostorách mimo Komisi. To zahrnuje externí zajištění služeb nebo činností jednoho nebo více CIS nebo jiných služeb IT, datových center v prostorách mimo Komisi a zpracování datových souborů Komise externími službami.

2. Externí zajištění služeb nebo činností CIS musí zohledňovat citlivost nebo stupeň utajení zpracovávaných informací takto:

a) CIS zpracovávající utajované informace EU musí být akreditován v souladu s rozhodnutím (EU, Euratom) 2015/444, přičemž musí být předem konzultován orgán pro bezpečnostní akreditaci (SAA) Komise. Systémy zpracovávající utajované informace EU nesmí být zajišťovány externě.

b) Vlastník komunikačního a informačního systému zpracovávajícího jiné informace než EUCI musí zavést přiměřená opatření k řešení potřeb v oblasti bezpečnosti v souladu s příslušnými právními povinnostmi nebo citlivostí informací s přihlédnutím k rizikům externího zajištění služeb nebo činností. Generální ředitelství pro lidské zdroje a bezpečnost může stanovit další požadavky.

c) Externě zajišťované vývojové projekty musí zohlednit citlivost vyvíjeného kódu a veškerých údajů ze zkoušek použitých během vývoje.

3. Pro externě zajišťované komunikační a informační systémy platí kromě zásad stanovených v článku 3 rozhodnutí (EU, Euratom) 2017/46 tyto zásady:

a) podmínky externího zajištění služeb nebo činností těchto systémů musí být navrženy tak, aby nevedly k závislosti na konkrétních dodavatelích;

b) podmínky bezpečnosti externího zajištění služeb nebo činností musí minimalizovat možnosti přístupu k informacím Komise nebo úpravy informací Komise pro pracovníky třetích stran;

c) pracovníci třetích stran, kteří mají přístup k externě zajišťovanému CIS, musí podepsat dohody o zachování důvěrnosti;

d) externí zajištění služeb nebo činností CIS musí být uvedeno v evidenci komunikačních a informačních systémů.

4. Vlastník systému za účasti vlastníka údajů musí:

a) posoudit a zdokumentovat rizika spojená s externím zajištěním služeb nebo činností;

b) stanovit příslušné bezpečnostní požadavky;

c) provádět konzultace s vlastníky všech dalších připojených CIS, aby bylo zajištěno začlenění jejich bezpečnostních požadavků;

d) zajistit zahrnutí příslušných bezpečnostních požadavků a práv do smlouvy o externím zajištění služeb nebo činností;

e) splnit veškeré další požadavky stanovené v podrobném postupu podle odstavce 8 tohoto článku.

Tyto úkony musí být dokončeny před podpisem smlouvy nebo jiné dohody za účelem externího zajištění služeb nebo činností jednoho nebo více CIS.

5. Vlastníci systémů musí řídit rizika spojená s externím zajištěním služeb nebo činností po celou dobu životnosti CIS tak, aby byly splněny stanovené bezpečnostní požadavky.

6. Vlastníci systémů zajistí, aby dodavatelé, kterými jsou třetí strany, byli povinni okamžitě informovat Komisi o všech incidentech v oblasti bezpečnosti IT týkajících se externě zajišťovaného CIS Komise.

7. Vlastník systému je odpovědný za zajištění souladu komunikačního a informačního systému, smlouvy o externím zajištění služeb nebo činností a bezpečnostních opatření s pravidly Komise pro bezpečnost informací a IT.

8. Generální ředitelství pro lidské zdroje a bezpečnost stanoví podrobnou normu týkající se odpovědností a činností stanovených v odstavcích 1 až 7 v souladu s níže uvedeným článkem 10.

KAPITOLA 4

RŮZNÁ A ZÁVĚREČNÁ USTANOVENÍ

Článek 9

Transparentnost

Toto rozhodnutí se dá na vědomí zaměstnancům Komise a všem osobám, na které se vztahuje, a zveřejní se v *Úředním věstníku Evropské unie*.

Článek 10

Normy

1. Ustanovení tohoto rozhodnutí se v případě potřeby podrobněji rozpracují do norem a/nebo pokynů, které mají být přijaty v souladu s rozhodnutím (EU, Euratom) 2017/46 a rozhodnutím C(2017) 7428. Normy a pokyny v oblasti bezpečnosti IT poskytnou další podrobnosti k těmto prováděcím pravidlům a rozhodnutí (EU, Euratom) 2017/46 pro konkrétní oblasti bezpečnosti podle normy ISO 27001:2013 přílohy A. Tyto normy a pokyny jsou založeny na osvědčených postupech a jsou vybrány tak, aby vyhovovaly IT prostředí Komise.

2. Normy se v případě potřeby vypracují podle normy ISO 27001:2013 přílohy A v těchto oblastech:

1) Organizace bezpečnosti informací;

2) Bezpečnost lidských zdrojů;

3) Řízení aktiv;

4) Řízení přístupu;

5) Kryptografie;

6) Fyzická bezpečnost a bezpečnost prostředí;

7) Bezpečnost provozu;

8) Bezpečnost komunikací;

9) Akvizice, vývoj a údržba systémů;

10) Dodavatelské vztahy;

11) Řízení incidentů bezpečnosti informací;

12) Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací;

13) Soulad s požadavky.

3. Normy uvedené v odstavcích 1 a 2 tohoto článku schvaluje před jejich přijetím Rada pro řízení informační bezpečnosti.

4. Zrušují se prováděcí pravidla k rozhodnutí C(2006) 3602 týkající se oblasti působnosti tohoto rozhodnutí.

5. Normy a pokyny přijaté podle rozhodnutí C(2006) 3602 ze dne 16. srpna 2006 zůstávají v platnosti, pokud nejsou v rozporu s těmito prováděcími předpisy, až do jejich zrušení nebo nahrazení normami nebo pokyny, které mají být přijaty podle článku 13 rozhodnutí (EU, Euratom) 2017/46.

Článek 11

Vstup v platnost

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

V Bruselu dne 6. dubna 2018.

Za Komisi,
jménem předsedy,
Günther OETTINGER
člen Komise

PŘÍLOHA

ÚLOHY A ODPOVĚDNOSTI (RASCI)

Model RASCI přiděluje subjektům úlohy s použitím těchto zkratek:

a) R – odpovědný

b) A – ručící

c) S – podporující

d) C – konzultovaný

e) I – informovaný

Úloha / Proces	ISSB	HR (DS)	Útvary Komise	Vlastník systémů	Vlastník údajů	LISO	DIGIT	Dodavatelé
Sladění s politikou Komise v oblasti bezpečnosti informačních systémů		**R/A**	**S**				**S**	
Šifrovací technologie		**C**	**A**	**R**	**I**	**C**		
Bezpečnostní kontroly IT	**I**	**A/R**		**S**	**I**	**I**	**S**	
Přístup z vnějších sítí	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externí zajišťování komunikačních a informačních systémů (CIS)		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Konzultace s ISSB se provádí v souvislosti s provozováním vnitřních sítí kterýmkoli útvarem Komise kromě Generálního ředitelství pro informatiku.

[2] Vlastník CIS, jehož činnosti nebo služby jsou zajišťovány externě, je odpovědný, a vlastník jakéhokoli jiného CIS, se kterým je externě zajišťovaný CIS propojen, je konzultován.