ROZHODNUTIE KOMISIE (EÚ, Euratom) 2018/559

zo 6. apríla 2018,

ktorým sa stanovujú vykonávacie predpisy k článku 6 rozhodnutia (EÚ, Euratom) 2017/46 o bezpečnosti komunikačných a informačných systémov v Európskej komisii

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 249,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu,

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2017/46 z 10. januára 2017 o bezpečnosti komunikačných a informačných systémov v Európskej komisii ([1]), a najmä na jeho článok 6,

keďže:

(1) S prijatím rozhodnutia (EÚ, Euratom) 2017/46 vznikla potreba, aby Komisia preskúmala, aktualizovala a konsolidovala vykonávacie predpisy súvisiace so zrušeným rozhodnutím Komisie K(2006) 3602 o bezpečnosti komunikačných a informačných systémov používaných v rámci Komisie.

(2) V súlade s článkom 13 rozhodnutia (EÚ, Euratom) 2017/46 ([2]) bol člen Komisie zodpovedný za bezpečnosť v plnom súlade s vnútorným rokovacím poriadkom splnomocnený stanoviť vykonávacie predpisy.

(3) Vykonávacie predpisy rozhodnutia K(2006) 3602 by sa preto mali zrušiť,

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA 1

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. Predmet úpravy a rozsah pôsobnosti tohto rozhodnutia sú stanovené v článku 1 rozhodnutia (EÚ, Euratom) 2017/46.

2. Ustanovenia tohto rozhodnutia sa uplatňujú na všetky komunikačné a informačné systémy (CIS). Zodpovednosti vymedzené v tomto rozhodnutí sa však nevzťahujú na komunikačné a informačné systémy, ktoré spracúvajú utajované informácie EÚ. Príslušné zodpovednosti súvisiace s týmito systémami určuje vlastník systému a bezpečnostný orgán Komisie v súlade s rozhodnutím Komisie (EÚ, Euratom) 2015/444 ([3]).

3. Kapitolu 2 tohto rozhodnutia tvorí prehľad praktického vykonávania organizácie a zodpovedností súvisiacich s bezpečnosťou informačných technológií. Kapitolu 3 tohto rozhodnutia tvorí prehľad procesov súvisiacich s článkom 6 rozhodnutia (EÚ, Euratom) 2017/46.

Článok 2

Vymedzenie pojmov

Na toto rozhodnutie sa uplatňuje vymedzenie pojmov v článku 2 rozhodnutia (EÚ, Euratom) 2017/46. Na účely tohto rozhodnutia sa uplatňuje aj toto vymedzenie pojmov:

1. „kryptografický schvaľovací orgán“ (CAA) je funkcia, ktorú vykonáva bezpečnostný orgán Komisie a ktorá spadá do právomoci generálneho riaditeľa pre ľudské zdroje a bezpečnosť;

([1]) Ú. v. EÚ L 6, 11.1.2017, s. 40.
([2]) Rozhodnutie Komisie C(2017) 7428 final z 8. novembra 2017, ktorým sa udeľuje splnomocnenie prijímať vykonávacie predpisy, normy a usmernenia týkajúce sa bezpečnosti komunikačných a informačných systémov v Európskej komisii.
([3]) Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

2. „externé sieťové pripojenie“ je akékoľvek elektronické komunikačné spojenie medzi internou sieťou Komisie a akoukoľvek inou sieťou vrátane internetu. Toto vymedzenie vylučuje siete tretích strán, ktoré sú poskytované na základe zmluvy ako súčasť internej siete Komisie;

3. „úschova kľúčov“ je postup ukladania kópií kryptografických kľúčov u jednej alebo viacerých samostatných strán, pričom sa zabezpečí oddelenie úloh, aby sa umožnilo ich obnovenie v prípade straty prevádzkovej kópie. Kľúče možno rozdeliť na dve alebo viaceré časti, z ktorých každá sa uloží u inej strany, aby sa zabezpečilo, že žiadna strana nebude vlastniť celý kľúč;

4. „RASCI“ je skratka na pridelenie zodpovednosti na základe týchto ukazovateľov prideľovania:

   a) „zodpovednosť“ (responsible, R) je povinnosť konať a prijímať rozhodnutia s cieľom dosiahnuť požadované výsledky;

   b) „zodpovedný“ (accountable, A) je niekto, kto nesie zodpovednosť za kroky, rozhodnutia a výkon;

   c) „podporujúci“ (supports, S) je byť povinný spolupracovať s osobou, ktorá nesie zodpovednosť, s cieľom splniť úlohu;

   d) „poskytujúci konzultácie“ (consulted, C) je subjekt požiadaný o poradenstvo alebo stanovisko;

   e) „informovaný“ (informed, I) je niekto, kto má aktuálne relevantné informácie.

KAPITOLA 2

ORGANIZÁCIA A ZODPOVEDNOSTI

Článok 3

Úlohy a zodpovednosti

Úlohy a zodpovednosti súvisiace s článkami 4 až 8 tohto rozhodnutia sú vymedzené v prílohe v súlade so vzorom RASCI.

Článok 4

Súlad s politikou Komisie v oblasti informačnej bezpečnosti

1. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť preskúma politiku Komisie v oblasti bezpečnosti informačných technológií a súvisiace normy a usmernenia s cieľom zabezpečiť, aby boli v súlade so všeobecnými bezpečnostnými politikami Komisie, najmä s rozhodnutím Komisie (EÚ, Euratom) 2015/443 ([1]) a rozhodnutím (EÚ, Euratom) 2015/444.

2. Na žiadosť iných oddelení Komisie môže Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť preskúmať ich politiky v oblasti bezpečnosti informačných technológií alebo inú dokumentáciu o bezpečnosti informačných technológií s cieľom zabezpečiť ich súlad s politikou Komisie v oblasti informačnej bezpečnosti. Vedúci príslušného oddelenia Komisie zabezpečí, aby sa všetky nezrovnalosti riešili.

3. V rámci svojej zodpovednosti za bezpečnosť informácií zabezpečuje Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť v spolupráci s Generálnym riaditeľstvom pre informatiku, aby sa v procesoch v oblasti bezpečnosti informačných technológií v plnej miere zohľadňovala klasifikácia a zásady bezpečnosti stanovené v rozhodnutí (EÚ, Euratom) 2015/443, najmä v jeho článkoch 3 a 9.

KAPITOLA 3

PROCESY V OBLASTI BEZPEČNOSTI INFORMAČNÝCH TECHNOLÓGIÍ

Článok 5

Šifrovacie technológie

1. Šifrovacie technológie na ochranu utajovaných informácií EÚ (EUCI) sa používajú v súlade s rozhodnutím (EÚ, Euratom) 2015/444.

2. Rozhodnutia o používaní šifrovacích technológií na ochranu údajov, ktoré nie sú utajovanými informáciami EÚ, prijíma vlastník každého komunikačného a informačného systému, pričom zohľadňuje riziká, ktoré sa majú pomocou šifrovania zmierňovať, ako aj riziká, ktoré takéto šifrovanie predstavuje.

3. Každé použitie šifrovacích technológií si vyžaduje predchádzajúce schválenie kryptografického schvaľovacieho orgánu, pokiaľ sa šifrovanie nepoužíva len na ochranu dôvernosti údajov v tranzite, ktoré nie sú utajovanými informáciami EÚ, a nevyužíva štandardné sieťové komunikačné protokoly.

([1]) Rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii (Ú. v. EÚ L 72, 17.3.2015, s. 41).

4. S výnimkou uvedenou v odseku 3 tohto článku oddelenia Komisie zabezpečujú, aby sa zálohovania všetkých dešifrovacích kľúčov ukladali do úschovy kľúčov na účely obnovenia uložených údajov v prípade, že dešifrovací kľúč nie je k dispozícii. Obnovenie šifrovaných údajov pomocou zálohovania dešifrovacích kľúčov sa vykonáva len vtedy, ak je povolené v súlade s normou vymedzenou kryptografickým schvaľovacím orgánom.

5. Žiadosti o schválenie použitia šifrovacích technológií sa formálne zdokumentujú a sú v nich zahrnuté podrobné informácie o komunikačnom a informačnom systéme a údajoch, ktoré majú byť chránené, technológiách, ktoré majú byť použité, ako aj o súvisiacich operačných bezpečnostných postupoch. Tieto žiadosti o schválenie podpisuje vlastník systému.

6. Žiadosti o schválenie použitia šifrovacích technológií hodnotí kryptografický schvaľovací orgán v súlade s uverejnenými normami a požiadavkami.

Článok 6

Kontroly bezpečnosti informačných technológií

1. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť vykonáva kontroly bezpečnosti informačných technológií s cieľom overiť, či sú bezpečnostné opatrenia v oblasti informačných technológií v súlade s politikami Komisie v oblasti bezpečnosti informačných technológií, a skontrolovať integritu týchto kontrolných opatrení.

2. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť môže vykonávať kontroly bezpečnosti informačných technológií:

a) z vlastnej iniciatívy;

b) na žiadosť Riadiaceho výboru pre informačnú bezpečnosť (ISSB);

c) na žiadosť vlastníka systému;

d) v nadväznosti na incident v oblasti bezpečnosti informačných technológií alebo

e) v nadväznosti na zistenie vysokého rizika pre konkrétny systém.

3. Vlastníci údajov môžu požiadať o kontrolu bezpečnosti informačných technológií pred uložením svojich informácií v komunikačnom a informačnom systéme.

4. Výsledky kontroly sa zdokumentujú vo forme formálnej správy, ktorá sa zašle vlastníkovi systému a ktorá zahŕňa zistenia a odporúčania na zlepšenie súladu komunikačného a informačného systému s politikou bezpečnosti informačných technológií. Kópia sa zašle miestnemu úradníkovi informačnej bezpečnosti (LISO). Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť informuje o závažných problémoch a odporúčaniach Riadiaci výbor pre informačnú bezpečnosť.

5. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť monitoruje vykonávanie odporúčaní.

6. V prípade potreby zahŕňajú kontroly bezpečnosti informačných technológií aj kontroly služieb, priestorov a zariadení poskytnutých vlastníkovi systému vrátane interných a externých poskytovateľov služieb.

Článok 7

Prístup z externých sietí

1. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť stanoví pravidlá v norme o povolení prístupu medzi komunikačnými a informačnými systémami Komisie a externými sieťami.

2. V týchto pravidlách sa rozlišujú rôzne typy externých sieťových pripojení a pre každý druh pripojenia sa stanovujú príslušné bezpečnostné predpisy vrátane stanovenia, či sa od príslušného orgánu vyžaduje predchádzajúce povolenie na pripojenie, ako sa uvádza v odseku 4 tohto článku.

3. Ak sa to vyžaduje, povolenie sa udelí na základe formálnej žiadosti a schvaľovacieho procesu. Schválenie je platné na určité obdobie a musí sa získať pred aktiváciou pripojenia.

4. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť má celkovú zodpovednosť za schvaľovanie žiadostí, môže však delegovať zodpovednosť za povoľovanie niektorých typov pripojenia podľa vlastného uváženia v súlade s článkom 17 ods. 3 rozhodnutia (EÚ, Euratom) 2015/443 a za podmienok stanovených v odseku 8.

5. Povoľujúci subjekt môže ako podmienku na schválenie stanoviť ďalšie bezpečnostné požiadavky v záujme ochrany komunikačného a informačného systému a sietí Komisie pred rizikami neoprávneného prístupu alebo iných prípadov narušenia bezpečnosti.

6. Generálne riaditeľstvo pre informatiku je štandardným poskytovateľom sieťových služieb pre Komisiu. Každé iné oddelenie Komisie prevádzkujúce sieť, ktorú neposkytuje Generálne riaditeľstvo pre informatiku, musí najskôr získať súhlas Riadiaceho výboru pre informačnú bezpečnosť. Oddelenie Komisie doloží obchodné odôvodnenie žiadosti a preukáže, že kontroly siete sú dostatočné na to, aby spĺňali požiadavky na kontrolu prichádzajúcich a odchádzajúcich informácií.

7. Vlastník komunikačného a informačného systému stanoví bezpečnostné požiadavky pre externý prístup do uvedeného komunikačného a informačného systému a zabezpečí uplatňovanie primeraných opatrení zameraných na ochranu jeho bezpečnosti s podporou miestneho úradníka informačnej bezpečnosti.

8. Bezpečnostné opatrenia vykonávané v súvislosti s externými sieťovými pripojeniami sú založené na zásade potreby poznať a zásade najnižších práv, ktorými sa zabezpečuje, že jednotlivci dostávajú len tie informácie a prístupové práva, ktoré potrebujú na plnenie svojich služobných povinností pre Komisiu.

9. Všetky externé sieťové pripojenia sa filtrujú a monitorujú s cieľom zistiť prípadné narušenie bezpečnosti.

10. V prípade zriadenia pripojení na účel externého obstarania komunikačných a informačných systémov je povolenie podmienené úspešným ukončením postupu opísaného v článku 8.

Článok 8

Externé obstaranie komunikačných a informačných systémov

1. Na účely tohto rozhodnutia sa komunikačný a informačný systém pokladá za externe obstaraný vtedy, ak sa poskytuje na základe zmluvy s poskytovateľom, ktorý je treťou stranou, a podľa tejto zmluvy je komunikačný a informačný systém umiestnený v priestoroch mimo Komisie. Zahŕňa to externé obstaranie jedného alebo viacerých komunikačných a informačných systémov alebo iných IT služieb, dátových centier v priestoroch mimo Komisie, ako aj súborov údajov Komisie zo strany externých poskytovateľov služieb.

2. Pri externom obstaraní komunikačných a informačných systémov sa musí zohľadňovať citlivosť alebo stupeň utajenia informácií, s ktorými sa zaobchádza, takto:

a) Komunikačné a informačné systémy, ktoré spracúvajú utajované informácie EÚ, sa schvaľujú v súlade s rozhodnutím (EÚ, Euratom) 2015/444 a pred týmto schválením sa musí konzultovať s bezpečnostným akreditačným orgánom Komisie. Systémy, ktoré spracúvajú utajované informácie EÚ, nesmú byť predmetom externého obstarania.

b) Vlastník komunikačného a informačného systému spracúvajúci informácie, ktoré nie sú utajovanými informáciami EÚ, zavedie primerané opatrenia na riešenie potrieb v oblasti bezpečnosti v súlade s príslušnými právnymi záväzkami alebo v závislosti od citlivosti informácií, pričom zohľadní riziká spojené s externým obstaraním. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť môže uložiť dodatočné požiadavky.

c) Pri externe obstaraných vývojových projektoch sa musí zohľadňovať citlivosť vyvinutého kódu a všetkých údajov z testovania používaných počas vývoja.

3. Okrem zásad stanovených v článku 3 rozhodnutia (EÚ, Euratom) 2017/46 sa na externe obstarané komunikačné a informačné systémy vzťahujú tieto zásady:

a) podmienky externého obstarania sa vypracujú tak, aby sa zabránilo závislosti od konkrétnych dodávateľov;

b) podmienky externého obstarania minimalizujú možnosti prístupu k informáciám Komisie alebo ich úpravy pre pracovníkov tretích strán;

c) pracovníci tretích strán, ktorí majú prístup k externe obstaranému komunikačnému a informačnému systému, musia podpísať dohody o zachovaní dôvernosti;

d) externé obstaranie komunikačného a informačného systému sa uvedie v inventári komunikačných a informačných systémov.

4. Vlastník systému musí za účasti vlastníka údajov:

a) posúdiť a zdokumentovať riziká súvisiace s externým obstaraním;

b) stanoviť príslušné bezpečnostné požiadavky;

c) konzultovať s vlastníkmi všetkých ostatných prepojených komunikačných a informačných systémov, aby sa zabezpečilo zahrnutie ich bezpečnostných požiadaviek;

d) zabezpečiť, aby boli v zmluve o externom obstaraní zahrnuté vhodné bezpečnostné požiadavky a práva;

e) plniť všetky ostatné požiadavky stanovené v podrobnom postupe, ako sa uvádza v odseku 8 tohto článku.

Tieto činnosti musia byť ukončené pred podpísaním zmluvy alebo inej dohody o externom obstaraní jedného alebo viacerých komunikačných a informačných systémov.

5. Vlastníci systémov riadia riziká súvisiace s externým obstaraním počas životného cyklu komunikačného a informačného systému, aby splnili vymedzené bezpečnostné požiadavky.

6. Vlastníci systému zabezpečia, aby dodávatelia, ktorými sú tretie strany, boli povinní bezodkladne informovať Komisiu o všetkých incidentoch v oblasti bezpečnosti informačných technológií, ktoré majú vplyv na externé obstaranie komunikačného a informačného systému.

7. Vlastník systému je zodpovedný za zabezpečenie súladu komunikačného a informačného systému, zmluvy o externom obstaraní a bezpečnostných opatrení s pravidlami Komisie o informačnej bezpečnosti a bezpečnosti informačných technológií.

8. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť stanoví podrobnú normu týkajúcu sa zodpovedností a činností stanovených v odsekoch 1 až 7 v súlade s nižšie uvedeným článkom 10.

KAPITOLA 4

RÔZNE A ZÁVEREČNÉ USTANOVENIA

Článok 9

Transparentnosť

Toto rozhodnutie sa oznámi zamestnancom Komisie a všetkým osobám, ktorých sa týka, a uverejní sa v *Úradnom vestníku Európskej únie*.

Článok 10

Normy

1. Ustanovenia tohto rozhodnutia sa v prípade potreby podrobnejšie rozpracujú v normách a/alebo usmerneniach, ktoré sa majú prijať v súlade s rozhodnutím (EÚ, Euratom) 2017/46 a rozhodnutím C(2017) 7428. Normy v oblasti bezpečnosti informačných technológií a príslušné usmernenia poskytnú ďalšie podrobnosti o týchto vykonávacích predpisoch a o rozhodnutí (EÚ, Euratom) 2017/46, pokiaľ ide o konkrétne oblasti bezpečnosti podľa normy ISO 27001:2013 prílohy A. Tieto normy a usmernenia sú založené na najlepších postupoch daného odvetvia a boli vybrané tak, aby vyhovovali IT prostrediu Komisie.

2. Normy sa v prípade potreby vypracujú podľa normy ISO 27001:2013 prílohy A v týchto oblastiach:

1. organizácia informačnej bezpečnosti;
2. bezpečnosť ľudských zdrojov;
3. riadenie aktív;
4. riadenie prístupov;
5. šifrovanie, kryptografia;
6. fyzická bezpečnosť a bezpečnosť prostredia;
7. prevádzková bezpečnosť;
8. komunikačná bezpečnosť;
9. kúpa, vývoj a údržba systémov;
10. vzťahy s dodávateľmi;
11. riadenie incidentov informačnej bezpečnosti;
12. aspekty informačnej bezpečnosti v riadení obchodnej kontinuity;
13. súlad.

3. Riadiaci výbor pre informačnú bezpečnosť schváli normy uvedené v odsekoch 1 a 2 tohto článku pred ich prijatím.

4. Vykonávacie predpisy k rozhodnutiu K(2006) 3602, ktoré sa týkajú rozsahu pôsobnosti tohto rozhodnutia, sa týmto zrušujú.

5. Normy a usmernenia prijaté v zmysle rozhodnutia K(2006) 3602 zo 16. augusta 2006 zostávajú účinné, pokiaľ nie sú v rozpore s týmito vykonávacími predpismi, až kým nebudú zrušené alebo nahradené normami alebo usmerneniami, ktoré sa majú prijať v zmysle článku 13 rozhodnutia (EÚ, Euratom) 2017/46.

Článok 11

Nadobudnutie účinnosti

Toto rozhodnutie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 6. apríla 2018

Za Komisiu
v mene predsedu
Günther OETTINGER
člen Komisie

PRÍLOHA

ÚLOHY A ZODPOVEDNOSTI (RASCI)

Vzor RASCI prideľuje úlohy subjektom pomocou týchto skratiek:

a) R – zodpovednosť (responsible)

b) A – zodpovedný (accountable)

c) S – podporujúci (supporting)

d) C – poskytujúci konzultácie (consulted)

e) I – informovaný (informed)

Úloha / Proces	ISSB	HR (DS)	Oddelenia Komisie	Vlastník systému	Vlastník údajov	LISO	DIGIT	Dodávatelia
Súlad s politikou Komisie v oblasti informačnej bezpečnosti		**R/A**	**S**				**S**	
Šifrovacie technológie		**C**	**A**	**R**	**I**	**C**		
Kontroly bezpečnosti informačných technológií	**I**	**A/R**		**S**	**I**	**I**	**S**	
Prístup z externých sietí	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Externé obstaranie komunikačných a informačných systémov		**S/C**	**A**	**C** [2]	**S**	**C**		**S**

[1] S ISSB konzultuje v súvislosti s prevádzkou interných sietí ktorékoľvek oddelenie Komisie okrem Generálneho riaditeľstva pre informatiku.

[2] Vlastník externe obstaraného komunikačného a informačného systému nesie zodpovednosť a vlastník akéhokoľvek iného komunikačného a informačného systému, s ktorým je externe obstaraný komunikačný a informačný systém prepojený, poskytuje konzultácie.