ROZHODNUTÍ

ROZHODNUTÍ KOMISE (EU, Euratom) 2017/46

ze dne 10. ledna 2017

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,

vzhledem k těmto důvodům:

(1) Komunikační a informační systémy Komise jsou nedílnou součástí fungování Komise a incidenty v oblasti bezpečnosti IT mohou mít vážný dopad na činnost Komise i třetích stran, jako jsou například jednotlivci, podniky či členské státy.

(2) Existuje mnoho hrozeb, které mohou narušit důvěrnost, integritu nebo dostupnost komunikačních a informačních systémů Komise a jimi zpracovávaných informací. Patří mezi ně nepředvídané události, chyby, záměrné útoky a přírodní jevy, které je třeba identifikovat jako provozní rizika.

(3) Komunikačním a informačním systémům je nutné poskytnout úroveň ochrany odpovídající pravděpodobnosti, dopadu a povaze rizik, kterým jsou vystaveny.

(4) Bezpečnost IT v Komisi by měla zajišťovat, že komunikační a informační systémy Komise ochrání informace, které zpracovávají, a budou fungovat, jak bude třeba a kdy bude třeba, a to pod kontrolou oprávněných uživatelů.

(5) Politiku Komise pro bezpečnost IT je třeba provádět konzistentně s politikami bezpečnosti v rámci Komise.

(6) Obecně za bezpečnost v Komisi odpovídá Ředitelství pro bezpečnost pod Generálním ředitelstvím pro lidské zdroje a bezpečnost, které podléhá vedení a spadá do odpovědnosti člena Komise odpovědného za bezpečnost.

(7) Přístup Komise by měl rovněž zohledňovat politické iniciativy a právní předpisy EU týkající se bezpečnosti sítí a informací, bezpečnostních norem a osvědčených postupů, aby byly dodrženy všechny příslušné právní předpisy a umožněna interoperabilita a kompatibilita.

(8) K zajištění účinnosti a účelnosti je třeba, aby útvary Komise odpovědné za komunikační a informační systémy vypracovaly a provedly vhodná opatření a aby byla koordinována opatření pro bezpečnost IT za účelem ochrany komunikačních a informačních systémů v rámci celé Komise.

(9) Pravidla a postupy pro přístup k informacím v kontextu bezpečnosti IT včetně řešení bezpečnostních incidentů v oblasti IT by měly být úměrné hrozbě pro Komisi a její zaměstnance a měly by odpovídat zásadám vymezeným v nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ([1]) o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Unie a o volném pohybu těchto údajů a zohledňovat zásadu profesního tajemství, jak stanovuje článek 339 SFEU.

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

(10) Politiky a pravidla pro komunikační a informační systémy zpracovávající utajované informace EU, citlivé neutajované informace a neutajované informace mají být plně v souladu s rozhodnutími Komise (EU, Euratom) 2015/443 ([1]) a (EU, Euratom) 2015/444 ([2]).

(11) Je třeba, aby Komise přezkoumala a aktualizovala ustanovení týkající se bezpečnosti komunikačních a informačních systémů využívaných Komisí.

(12) Rozhodnutí Komise C(2006) 3602 by proto mělo být zrušeno,

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA 1

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Toto rozhodnutí se týká všech komunikačních a informačních systémů, které jsou vlastněny, opatřovány, spravovány či provozovány Komisí nebo jejím jménem, a veškerého použití těchto systémů Komisí.

2. Toto rozhodnutí vymezuje základní zásady, cíle, organizaci a odpovědnost v souvislosti s bezpečností těchto systémů, zejména pak pro útvary Komise, které je vlastní, opatřují, spravují či provozují, a také pro komunikační a informační systémy poskytované interním poskytovatelem služeb IT. V případě, že je komunikační a informační systém poskytován, vlastněn, spravován či provozován externě na základě bilaterální dohody či smlouvy s Komisí, jsou podmínky takovéto dohody či smlouvy v souladu s tímto rozhodnutím.

3. Toto rozhodnutí platí pro všechny útvary Komise a výkonné agentury. V případě, že komunikační a informační systém Komise využívají jiné orgány a instituce na základě bilaterální dohody s Komisí, jsou podmínky takovéto dohody v souladu s tímto rozhodnutím.

4. Bez ohledu na případné zvláštní údaje ohledně konkrétních skupin zaměstnanců se toto rozhodnutí týká všech členů Komise, zaměstnanců Komise spadajících pod služební řád úředníků Evropské unie („služební řád“) a pod pracovní řád ostatních zaměstnanců Evropské unie ([3]), národních odborníků vyslaných ke Komisi ([4]), externích poskytovatelů služeb a jejich zaměstnanců, stážistů a každého s přístupem ke komunikačnímu a informačnímu systému v působnosti tohoto rozhodnutí.

5. Toto rozhodnutí se vztahuje na Evropský úřad pro boj proti podvodům (OLAF), je-li to slučitelné s právními předpisy Unie a rozhodnutím Komise 1999/352/ES, ESUO, Euratom ([5]). Opatření stanovená tímto rozhodnutím včetně pokynů, kontrol, šetření a obdobných opatření se nemusejí vztahovat na komunikační a informační systém úřadu, zejména pokud jsou neslučitelná s nezávislostí vyšetřovací funkce úřadu či s důvěrností informací získaných úřadem při plnění této funkce.

Článek 2

Definice

Pro účely tohoto rozhodnutí se použijí tyto definice:

1) „Ručícím“ se rozumí ten, kdo nese zodpovědnost za kroky, rozhodnutí a plnění.

([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).

([2]) 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).

([3]) Stanoveno nařízením Rady (EHS, Euratom, ESUO) č. 259/68 ze dne 29. února 1968, kterým se stanoví služební řád úředníků Evropských společenství a pracovní řád ostatních zaměstnanců Evropských společenství a kterým se stanoví zvláštní opatření dočasně použitelná na úředníky Komise (pracovní řád ostatních zaměstnanců) (Úř. věst. L 56, 4.3.1968, s. 1).

([4]) *Commission Decision of 12. Listopadu 2008 laying down rules on the secondment to the Commission of national experts and national experts in professional training* (rozhodnutí Komise ze dne 12. listopadu 2008, kterým se stanoví pravidla pro vysílání národních odborníků a odborné stáže u Komise [C(2008) 6866 final]).

([5]) Rozhodnutí Komise 1999/352/ES, ESUO, Euratom ze dne 28. dubna 1999 o zřízení Evropského úřadu pro boj proti podvodům (OLAF) (Úř. věst. L 136, 31.5.1999, s. 20).

2) „CERT-EU“ je skupina pro reakci na počítačové hrozby pro orgány a agentury EU. Jejím úkolem je podporovat evropské orgány při jejich ochraně proti záměrným a zlovolným útokům s potenciálem narušit integritu jejich prostředků IT a poškodit zájmy EU. Rozsah činností CERT-EU zahrnuje prevenci, detekci, reakci a obnovu.

3) „Útvarem Komise“ se rozumí generální ředitelství či služba Komise nebo kabinet člena Komise.

4) „Bezpečnostní orgán Komise“ odkazuje na úlohu vymezenou rozhodnutím (EU, Euratom) 2015/444.

5) „Komunikačním a informačním systémem“ se rozumí jakýkoli systém, který umožňuje manipulaci s informacemi v elektronickém formátu, včetně všech aktiv potřebných pro jeho fungování a včetně infrastruktury, organizace, personálu a informačních zdrojů. Definice zahrnuje obchodní aplikace, sdílené služby IT, externě zajišťované systémy a zařízení koncových uživatelů.

6) „Řídící rada“ (CMB) zajišťuje nejvyšší úroveň řídicího dohledu v oblasti operací a administrativy v Komisi.

7) „Vlastníkem údajů“ se rozumí osoba odpovídající za zajišťování ochrany a využívání konkrétního datového souboru zpracovávaného v komunikačním a informačním systému.

8) „Datovým souborem“ se rozumí soubor informací, který slouží konkrétnímu postupu nebo činnosti Komise.

9) „Nouzovým postupem“ se rozumí předem stanovený soubor metod a povinností pro reakce na naléhavé situace za účelem zabránit vážným dopadům pro Komisi.

10) „Politikou bezpečnosti informací“ se rozumí soubor cílů v oblasti bezpečnosti informací, které jsou nebo musí být stanoveny, prováděny a kontrolovány. Patří sem mimo jiné rozhodnutí (EU, Euratom) 2015/444 a (EU, Euratom) 2015/443.

11) „Radou pro řízení informační bezpečnosti“ (ISSB) se rozumí řídicí orgán, který podporuje řídící radu v úkolech souvisejících s bezpečností IT.

12) „Interním poskytovatelem služeb IT“ se rozumí útvar Komise poskytující sdílené služby IT.

13) „Bezpečností IT“ nebo „bezpečností komunikačního a informačního systému“ se rozumí zachování důvěrnosti, integrity a dostupnosti komunikačních a informačních systémů a datových souborů, které zpracovávají.

14) „Pokyny pro bezpečnost IT“ tvoří doporučená, ale dobrovolná opatření, která napomáhají podpoře standardů bezpečnosti IT, případně slouží jako reference v případě, že není žádný použitelný standard zaveden.

15) „Incidentem v oblasti bezpečnosti IT“ se rozumí událost, která by mohla mít nepříznivý vliv na důvěrnost, integritu nebo dostupnost komunikačního a informačního systému.

16) „Opatřením pro bezpečnost IT“ se rozumí technické nebo organizační opatření, jehož cílem je zmírňování bezpečnostních rizik IT.

17) „Potřebou v oblasti bezpečnosti IT“ se rozumí přesná a jednoznačná definice úrovně důvěrnosti, integrity a dostupnosti spojená s údajem nebo systémem IT, jejímž cílem je určit požadovanou úroveň ochrany.

18) „Cílem v oblasti bezpečnosti IT“ se rozumí stanovení záměru s cílem čelit určeným hrozbám či vyhovět určeným organizačním bezpečnostním požadavkům či předpokladům.

19) „Plánem bezpečnosti IT“ se rozumí dokumentace opatření pro bezpečnost IT nutných ke splnění potřeb v oblasti bezpečnosti IT konkrétního komunikačního a informačního systému.

20) „Politikou bezpečnosti IT“ se rozumí soubor cílů bezpečnosti IT, které jsou nebo musí být přijaty, prováděny a kontrolovány. Zahrnuje toto rozhodnutí a jeho prováděcí pravidla.

21) „Požadavkem na bezpečnost IT“ se rozumí potřeba v oblasti bezpečnosti IT formalizovaná předem stanoveným postupem.

22) „Bezpečnostním rizikem IT“ se rozumí důsledek, který by mohl využitím zranitelného místa vyplynout z hrozby pro bezpečnost IT pro komunikační a informační systém. Bezpečnostní riziko IT charakterizují dva faktory: 1) nejistota, tj. pravděpodobnost, že hrozba pro bezpečnost IT způsobí nežádoucí událost, a 2) dopady, tj. důsledky, které takováto nežádoucí událost může mít na komunikační a informační systém.

23) „Standardy bezpečnosti IT“ se rozumí konkrétní povinná opatření pro bezpečnost IT, která pomáhají prosazovat a podporovat politiku bezpečnosti IT.

24) „Strategií pro bezpečnost IT“ se rozumí soubor projektů a činností, které jsou určeny k dosažení cílů Komise a které je nutné zavést, provádět a kontrolovat.

25) „Hrozbou pro bezpečnost IT“ se rozumí faktor, který může potenciálně vést k nežádoucí události, v jejímž důsledku dojde k narušení komunikačního a informačního systému. Takovéto hrozby mohou být neúmyslné či úmyslné a vyznačují se ohrožujícími prvky, potenciálními cíli a metodami útoku.

26) „Úředníkem pro bezpečnost informatiky na místní úrovni“ nebo „LISO“ se rozumí úředník, který za útvar Komise odpovídá za bezpečnostní spolupráci.

27) „Osobní údaje“, „zpracování osobních údajů“, „správce“ a „evidence osobních údajů“ mají stejný význam, jaký uvádí nařízení (ES) č. 45/2001, a zejména jeho článek 2.

28) „Zpracováním údajů“ se rozumí veškeré funkce komunikačního a informačního systému týkající se datových souborů včetně vytvoření, úpravy, zobrazení, uložení, přenosu, smazání a archivace údajů. Zpracování údajů může zajišťovat komunikační a informační systém jako sadu funkcí pro uživatele a jako služby IT pro další komunikační a informační systém.

29) „Profesním tajemstvím“ se rozumí ochrana obchodních údajů, které svým charakterem spadají pod profesní tajemství, zejména informací o podnicích, jejich obchodních vztazích či složkách nákladů, jak stanovuje článek 339 SFEU.

30) „Odpovědným“ se rozumí mající povinnost jednat a přijímat rozhodnutí k dosažení požadovaných výsledků.

31) „Bezpečností v Komisi“ se rozumí bezpečnost osob, majetku a informací v rámci Komise, zejména pak fyzická nedotknutelnost osob a majetku, integrita, důvěrnost a dostupnost informací a komunikačních a informačních systémů a nerušené fungování Komise při plnění jejích úkolů.

32) „Sdílenou službou IT“ se rozumí služba, kterou komunikační a informační systém poskytuje jiným komunikačním a informačním systémům v rámci zpracování údajů.

33) „Vlastník systému“ je osoba odpovědná za celkové obstarání, vývoj, integraci, úpravy, provoz, údržbu a vyřazení komunikačního a informačního systému.

34) „Uživatelem“ se rozumí kdokoli, kdo využívá funkce poskytované komunikačním a informačním systémem, a to uvnitř Komise i mimo ni.

Článek 3

Zásady bezpečnosti IT v Komisi

1. Bezpečnost IT v Komisi vychází ze zásad legality, transparentnosti, proporcionality a odpovědnosti.

2. Problematika bezpečnosti IT se zohledňuje od počátku vývoje a zavádění komunikačních a informačních systémů Komise. Proto se v oblastech, za které odpovídají, zapojují Generální ředitelství pro informatiku a Generální ředitelství pro lidské zdroje a bezpečnost.

3. Účinná bezpečnost IT zajistí odpovídající úroveň:

a) autenticity: záruka, že informace jsou autentické a z důvěryhodných zdrojů;

b) dostupnosti: přístupnost a použitelnost informací na žádost oprávněného subjektu;

c) důvěrnosti: skutečnost, že informace se nezpřístupňují neoprávněným osobám a subjektům nebo pro nedovolené účely;

d) integrity: zajištění správnosti a úplnosti aktiv a informací;

e) nepopiratelnosti: schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny;

f) ochrany osobních údajů: zajištění vhodných ochranných opatření týkajících se osobních údajů zcela vyhovujících nařízení (ES) č. 45/2001;

g) profesního tajemství: ochrana údajů, které svým charakterem spadají pod profesní tajemství, zejména informací o podnicích, jejich obchodních vztazích či složkách nákladů, jak stanovuje článek 339 SFEU.

4. Bezpečnost IT je založena na procesu řízení rizik. Cílem tohoto procesu je určení úrovně bezpečnostních rizik IT a stanovení bezpečnostních opatření ke snížení těchto rizik na odpovídající úroveň za přiměřenou cenu.

5. Všechny komunikační a informační systémy musí být identifikovány, přiřazeny vlastníkovi systému a zaznamenány v evidenci.

6. Bezpečnostní požadavky na všechny komunikační a informační systémy je nutné stanovit na základě příslušných bezpečnostních potřeb a požadavků na bezpečnost údajů, které zpracovávají. Komunikační a informační systémy, které poskytují služby jiným komunikačním a informačním systémům, mohou být konstruovány tak, aby podporovaly stanovené úrovně bezpečnostních potřeb.

7. Plány a opatření pro bezpečnost IT musí být úměrné bezpečnostním potřebám komunikačního a informačního systému.

Postupy související s těmito zásadami a činnostmi se podrobněji stanoví v prováděcích pravidlech.

KAPITOLA 2

ORGANIZACE A ODPOVĚDNOST

Článek 4

Řídící rada

Řídící rada převezme v Komisi celkovou odpovědnost za řízení bezpečnosti IT jako celku.

Článek 5

Rada pro řízení informační bezpečnosti (ISSB)

1. ISSB předsedá náměstek generálního tajemníka odpovědný za řízení bezpečnosti IT v Komisi. Její členové zastupují obchodní, technologické i bezpečnostní zájmy všech útvarů Komise a jsou mezi nimi zástupci Generálního ředitelství pro informatiku, Generálního ředitelství pro lidské zdroje a bezpečnost, Generálního ředitelství pro rozpočet a střídavě po dvou letech zástupci čtyř dalších zúčastněných útvarů Komise, pro jejichž operace je bezpečnost IT důležitou otázkou. Členství je na úrovni vyššího vedení.

2. ISSB podporuje řídící radu v úkolech týkajících se bezpečnosti IT. ISSB převezme v Komisi operační odpovědnost za řízení bezpečnosti IT jako celku.

3. ISSB doporučí politiku bezpečnosti IT Komise k přijetí Komisí.

4. ISSB prověřuje záležitosti řízení a otázky související s bezpečností IT včetně závažných incidentů v oblasti bezpečnosti IT a každé dva roky o tom podává zprávu řídící radě.

5. ISSB sleduje a prověřuje celkové provádění tohoto rozhodnutí a podává o tom zprávu řídící radě.

6. Na návrh Generálního ředitelství pro informatiku ISSB prověřuje, schvaluje a sleduje provádění aktuální strategie pro bezpečnost IT. Podává o tom zprávu řídící radě.

7. ISSB sleduje, vyhodnocuje a kontroluje situaci v Komisi z hlediska řízení rizik spojených s informacemi a má pravomoc v nezbytných případech vznášet formální požadavky na zlepšení.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 6

Generální ředitelství pro lidské zdroje a bezpečnost

V souvislosti s bezpečností IT má Generální ředitelství pro lidské zdroje a bezpečnost následující odpovědnost. Musí:

1) zajišťovat soulad mezi politikou bezpečnosti IT a politikou bezpečnosti informací Komise;

2) vytvořit rámec pro autorizaci používání šifrovacích technologií pro ukládání a komunikaci údajů v komunikačních a informačních systémech;

3) informovat Generální ředitelství pro informatiku o konkrétních hrozbách, které by mohly mít významný dopad na bezpečnost komunikačních a informačních systémů a datových souborů, které zpracovávají;

4) provádět bezpečnostní kontroly IT k vyhodnocení souladu komunikačních a informačních systémů Komise s bezpečnostní politikou a podávat zprávy o výsledcích ISSB;

5) vytvořit rámec pro autorizaci přístupu ke komunikačním a informačním systémům Komise z vnějších sítí a pro související vhodná bezpečnostní pravidla a vypracovat související standardy a pokyny pro bezpečnost IT v úzké spolupráci s Generálním ředitelstvím pro informatiku;

6) navrhnout zásady a pravidla pro externí zajišťování komunikačních a informačních systémů za účelem udržení vhodné kontroly nad bezpečností údajů;

7) vypracovat příslušné standardy a pokyny pro bezpečnost IT v souvislosti s článkem 6 v úzké spolupráci s Generálním ředitelstvím pro informatiku.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 7

Generální ředitelství pro informatiku

V souvislosti s celkovou bezpečností IT Komise má Generální ředitelství pro informatiku následující odpovědnost. Musí:

1) vypracovat standardy a pokyny pro bezpečnost IT, s výjimkou ustanovení článku 6, v úzké spolupráci s Generálním ředitelstvím pro lidské zdroje a bezpečnost, aby byla zajištěna konzistentnost mezi politikou bezpečnosti IT a politikou bezpečnosti informací Komise, a navrhnout je ISSB;

2) vyhodnotit metody, postupy a výsledky řízení rizik pro bezpečnost IT u všech útvarů Komise a podávat o tom pravidelně zprávu ISSB;

3) navrhnout aktuální strategii pro bezpečnost IT k revizi a schválení ISSB a dalšímu přijetí řídící radou a navrhnout program, včetně plánování projektů a činností k provádění strategie pro bezpečnost IT;

4) sledovat plnění strategie Komise pro bezpečnost IT a pravidelně o tom podávat zprávu ISSB;

5) sledovat bezpečnostní rizika IT a opatření pro bezpečnost IT zavedená v komunikačních a informačních systémech a pravidelně o tom podávat zprávu ISSB;

6) pravidelně ISSB podávat zprávu o celkovém provádění a dodržování tohoto rozhodnutí;

7) po konzultaci s Generálním ředitelstvím pro lidské zdroje a bezpečnost požádat vlastníky systémů, aby provedli konkrétní opatření pro bezpečnost IT za účelem zmírnění bezpečnostních rizik IT u komunikačních a informačních systémů Komise;

8) zajistit, aby měli vlastníci systémů a údajů k dispozici odpovídající katalog služeb pro bezpečnost IT Generálního ředitelství pro informatiku, a mohli tak plnit své povinnosti v oblasti bezpečnosti IT a dodržovat politiku a standardy bezpečnosti IT;

9) poskytovat vlastníkům systémů a údajů odpovídající dokumentaci a v případě potřeby s nimi konzultovat opatření pro bezpečnost IT přijatá pro jejich služby IT za účelem usnadnění dodržování politiky bezpečnosti IT a podpory vlastníků systémů v řízení rizik IT;

10) organizovat pravidelná setkání sítě LISO a podporovat LISO při plnění jejich povinností;

11) ve spolupráci s útvary Komise určit potřeby školení a koordinovat školicí programy v oblasti bezpečnosti IT a v úzké spolupráci s Generálním ředitelstvím pro lidské zdroje a bezpečnost vypracovat, provádět a koordinovat informační kampaně o bezpečnosti IT;

12) zajistit, že vlastníci systémů, vlastníci údajů a další zúčastnění odpovídající za bezpečnost IT v útvarech Komise jsou obeznámeni s politikou bezpečnosti IT;

13) informovat Generální ředitelství pro lidské zdroje a bezpečnost o konkrétních hrozbách pro bezpečnost IT, incidentech a výjimkách z politiky bezpečnosti IT Komise, které oznámili vlastníci systémů a které by mohly mít významný dopad na bezpečnost v Komisi;

14) z hlediska jeho role interního poskytovatele služeb IT dodat Komisi katalog sdílených služeb IT, které poskytují stanovenou úroveň bezpečnosti. To se provádí systematickým vyhodnocováním, řízením a sledováním bezpečnostních rizik IT za účelem zavádění bezpečnostních opatření, kterými se dosáhne stanovené úrovně bezpečnosti.

Související postupy a podrobnější informace o odpovědnostech se dále vymezují v prováděcích pravidlech.

Článek 8

Útvary Komise

V souvislosti s bezpečností IT ve svém oddělení každý vedoucí útvaru Komise:

1) formálně jmenuje pro každý komunikační a informační systém vlastníka systému, kterým bude úředník nebo dočasný zaměstnanec a který bude odpovídat za bezpečnost IT daného komunikačního a informačního systému, a formálně jmenuje vlastníka údajů pro každý datový soubor údajů zpracovávaných v komunikačním a informačním systému, který by měl patřit ke stejnému správnímu subjektu, jenž je správcem datových souborů podléhajících nařízení (ES) č. 45/2001;

2) formálně jmenuje úředníka pro bezpečnost informatiky na místní úrovni (LISO), který může vykonávat své úkoly nezávisle na vlastnících systému či údajů. LISO může být jmenován pro více než jeden útvar Komise;

3) zajišťuje vypracování a provádění vhodných vyhodnocení a plánů bezpečnosti IT;

4) zajišťuje pravidelné podávání souhrnných zpráv o bezpečnostních rizicích IT a příslušných opatření Generálnímu ředitelství pro informatiku;

5) zajišťuje, s podporou Generálního ředitelství pro informatiku, že budou zavedeny vhodné procesy, postupy a řešení sloužící k účinnému zjišťování, hlášení a řešení incidentů v oblasti bezpečnosti IT souvisejících s jejich komunikačními a informačními systémy;

6) spouští nouzový postup v případě nouzové situace v oblasti bezpečnosti IT;

7) nese nejvyšší odpovědnost za bezpečnost IT včetně odpovědností vlastníka systému a vlastníka údajů;

8) nese rizika týkající se jejich komunikačních a informačních systémů a datových souborů;

9) řeší případné neshody mezi vlastníky údajů a vlastníky systémů a v případě pokračující neshody předkládá záležitost k řešení ISSB;

10) zajišťuje provádění plánů a opatření pro bezpečnost IT a odpovídající pokrytí rizik.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 9

Vlastníci systémů

1. Vlastník systému odpovídá za bezpečnost IT v komunikačním a informačním systému a je podřízený vedoucímu útvaru Komise.

2. V souvislosti s bezpečností IT vlastník systému:

a) zajišťuje soulad komunikačního a informačního systému s politikou bezpečnosti IT;

b) zajišťuje, že komunikační a informační systém je správně zaznamenán v příslušné evidenci;

c) ve spolupráci s vlastníky údajů a po konzultaci s Generálním ředitelstvím pro informatiku vyhodnocuje bezpečnostní rizika IT a určuje potřeby v oblasti bezpečnosti IT pro každý komunikační a informační systém;

d) připravuje bezpečnostní plán, v nezbytných případech včetně podrobností o vyhodnocených rizicích a případných dalších nutných bezpečnostních opatření;

e) zavádí vhodná opatření pro bezpečnost IT úměrná zjištěným bezpečnostním rizikům IT a postupuje podle doporučení ISSB;

f) identifikuje případnou závislost na jiných komunikačních a informačních systémech nebo sdílených službách IT a zavádí vhodná bezpečnostní opatření podle úrovně bezpečnosti doporučované těmito komunikačními a informačními systémy nebo sdílenými službami IT;

g) řídí a sleduje bezpečnostní rizika IT;

h) pravidelně podává zprávu vedoucímu útvaru Komise o profilu bezpečnostních rizik IT ve svých komunikačních a informačních systémech a podává zprávu Generálnímu ředitelství pro informatiku o souvisejících rizicích, činnostech řízení rizik a přijatých bezpečnostních opatřeních;

i) konzultuje s LISO příslušného útvaru (útvarů) Komise aspekty bezpečnosti IT;

j) vydává pro uživatele pokyny k používání komunikačního a informačního systému a souvisejících údajů a k odpovědnosti uživatelů v souvislosti s těmito systémy;

k) vyžádá si autorizaci od Generálního ředitelství pro lidské zdroje a bezpečnost, které vystupuje ve funkci orgánu pro kryptografickou ochranu, pro každý komunikační a informační systém, který využívá šifrování;

l) s předstihem vede s bezpečnostním orgánem Komise konzultace ohledně všech systémů zpracovávajících utajované informace EU;

m) zajišťuje, že budou zálohy všech šifrovacích klíčů uloženy v účtu třetí strany. Obnovení šifrovaných údajů lze provádět pouze v případě autorizace v souladu s rámcem definovaným Generálním ředitelstvím pro lidské zdroje a bezpečnost;

n) řídí se pokyny od příslušných správců dat ohledně ochrany osobních údajů a uplatnění pravidel ochrany údajů na bezpečnost zpracování;

o) uvědomí Generální ředitelství pro informatiku o případných výjimkách z politiky bezpečnosti IT Komise včetně příslušných odůvodnění;

p) vedoucímu útvaru Komise hlásí veškeré neřešitelné neshody mezi vlastníky údajů a vlastníky systémů, podle potřeby včas hlásí incidenty v oblasti bezpečnosti IT příslušným zúčastněným stranám podle závažnosti, jak vymezuje článek 15;

q) u externě zajišťovaných systémů zajišťuje, že ve smlouvách o externím zajišťování jsou zahrnuta vhodná ustanovení týkající se bezpečnosti IT a že incidenty v oblasti bezpečnosti IT, ke kterým dochází v externě zajišťovaných komunikačních a informačních systémech, jsou hlášeny v souladu s článkem 15;

r) u komunikačního a informačního systému poskytujícího sdílené služby IT zajišťuje, aby byla poskytnuta a jednoznačně dokumentována určená úroveň bezpečnosti a zavedena bezpečnostní opatření pro daný komunikační a informační systém za účelem dosažení určené úrovně bezpečnosti.

3. Vlastníci systémů mohou formálně delegovat některé nebo všechny své úkoly související s bezpečností IT, ale za bezpečnost IT svých komunikačních a informačních systémů zůstávají odpovědní.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 10

Vlastníci údajů

1. Vlastník údajů odpovídá za bezpečnost IT pro konkrétní datový soubor vedoucímu útvaru Komise a ručí za důvěrnost, integritu a dostupnost tohoto datového souboru.

2. V souvislosti s tímto datovým souborem vlastník údajů:

a) zajišťuje, aby veškeré datové soubory, za které odpovídá, byly odpovídajícím způsobem klasifikovány v souladu s rozhodnutími (EU, Euratom) 2015/443 a (EU, Euratom) 2015/444;

b) definuje potřeby v oblasti bezpečnosti informací a informuje o těchto potřebách příslušné vlastníky systémů;

c) podílí se na vyhodnocování rizik pro komunikační a informační systém;

d) hlásí případné neřešitelné neshody mezi vlastníkem údajů a vlastníkem systému vedoucímu útvaru Komise;

e) hlásí incidenty v oblasti bezpečnosti IT, jak stanovuje článek 15.

3. Vlastníci údajů mohou formálně delegovat některé nebo všechny své úkoly související s bezpečností IT, ale odpovědnost podle tohoto článku jim zůstává zachována.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 11

Úředník pro bezpečnost informatiky na místní úrovni (LISO)

V souvislosti s bezpečností IT LISO:

a) aktivně identifikuje vlastníky systémů, vlastníky údajů a další zúčastněné odpovídající za bezpečnost IT v útvarech Komise a informuje je o politice bezpečnosti IT;

b) v otázkách bezpečnosti IT v útvarech Komise spolupracuje s Generálním ředitelstvím pro informatiku v rámci sítě LISO;

c) účastní se pravidelných setkání LISO;

d) udržuje přehled o procesech řízení rizika pro bezpečnost informací a o vývoji a provádění plánů bezpečnosti informačního systému;

e) poskytuje vlastníkům údajů, vlastníkům systémů a vedoucím útvarů Komise poradenství ohledně otázek souvisejících s bezpečností IT;

f) spolupracuje s Generálním ředitelstvím pro informatiku při šíření doporučených postupů pro bezpečnost IT a navrhuje konkrétní školicí a informativní programy;

g) podává zprávy o bezpečnosti IT, hlásí nedostatky a možná zlepšení vedoucím útvarů Komise.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 12

Uživatelé

1. V souvislosti s bezpečností IT uživatel:

a) dodržuje politiku bezpečnosti IT a pokyny vydávané vlastníkem systému k používání každého komunikačního a informačního systému;

b) hlásí incidenty v oblasti bezpečnosti IT, jak stanovuje článek 15.

2. Používání komunikačního a informačního systému Komise v rozporu s politikou bezpečnosti IT nebo pokyny vydanými vlastníkem systému mohou být důvodem zahájení disciplinárního řízení.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

KAPITOLA 3

BEZPEČNOSTNÍ POŽADAVKY A POVINNOSTI

Článek 13

Provádění tohoto rozhodnutí

1. Přijetí prováděcích pravidel k článku 6 a souvisejících standardů a pokynů bude předmětem rozhodnutí Komise o zmocnění člena Komise odpovědného za záležitosti bezpečnosti.

2. Přijetí jiných prováděcích pravidel a souvisejících standardů a pokynů pro bezpečnost IT bude předmětem rozhodnutí Komise o zmocnění člena Komise odpovědného za záležitosti informatiky.

3. ISSB schválí prováděcí pravidla, standardy a pokyny uvedené v odstavcích 1 a 2 před jejich přijetím.

Článek 14

Povinnost dodržovat ustanovení

1. Dodržování ustanovení obsažených v politice bezpečnosti IT a standardů je povinné.

2. Nedodržení politiky a standardů bezpečnosti IT může vést k zahájení disciplinárního řízení v souladu se Smlouvami, služebním řádem a pracovním řádem ostatních zaměstnanců Evropské unie, ke smluvním postihům či k právním krokům podle vnitrostátních právních a správních předpisů.

3. Generální ředitelství pro informatiku je informováno o případných výjimkách z politiky bezpečnosti IT.

4. V případě, že ISSB rozhodne, že hrozí trvalé nepřijatelné riziko pro komunikační a informační systém Komise, navrhne Generální ředitelství pro informatiku ve spolupráci s vlastníkem systému zmírňující opatření a předloží je ISSB ke schválení. Tato opatření mohou mimo jiné zahrnovat intenzivnější sledování a hlášení, omezení služby či odpojení.

5. ISSB v případě potřeby uloží provedení schválených zmírňujících opatření. ISSB může rovněž doporučit generálnímu řediteli Generálního ředitelství pro lidské zdroje a bezpečnost zahájení správního šetření. Generální ředitelství pro informatiku informuje ISSB o každé situaci, kdy jsou zavedena zmírňující opatření.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

Článek 15

Řešení bezpečnostních incidentů v oblasti IT

1. Generální ředitelství pro informatiku odpovídá za poskytování hlavních operačních kapacit pro reakci na incidenty v oblasti bezpečnosti IT v Evropské komisi.

2. Generální ředitelství pro lidské zdroje a bezpečnost jako zúčastněná strana reakce na incident v oblasti IT:

a) má právo na přístup k souhrnným informacím u záznamů všech incidentů a k úplným záznamům na vyžádání;

b) účastní se skupin krizového řízení incidentů v oblasti bezpečnosti IT a nouzových postupů pro bezpečnost IT;

c) má na starosti vztahy s donucovacími orgány a zpravodajskými službami;

d) provádí forenzní analýzu v oblasti kybernetické bezpečnosti v souladu s článkem 11 rozhodnutí (EU, Euratom) 2015/443;

e) rozhoduje o zahájení formálního šetření;

f) informuje Generální ředitelství pro informatiku o veškerých incidentech v oblasti bezpečnosti IT, které mohou představovat riziko pro jiné komunikační a informační systémy.

3. Mezi Generálním ředitelstvím pro informatiku a Generálním ředitelstvím pro lidské zdroje a bezpečnost probíhá pravidelná komunikace za účelem výměny informací a koordinace řešení bezpečnostních incidentů, zejména veškerých incidentů v oblasti IT, které mohou vyžadovat formální šetření.

4. V případě potřeby lze využít služeb pro koordinaci incidentů skupiny pro reakci na počítačové hrozby pro orgány a agentury EU (CERT-EU) k podpoře procesů řešení incidentů a ke sdílení poznatků s dalšími orgány a agenturami EU, kterých se to může rovněž týkat.

5. Vlastníci systémů, kterých se dotkl incident v oblasti IT:

a) neprodleně uvědomí vedoucí útvarů Komise, Generální ředitelství pro informatiku, Generální ředitelství pro lidské zdroje a bezpečnost, LISO a případně také vlastníka údajů o veškerých závažných incidentech v oblasti bezpečnosti IT, zejména pokud se jedná o porušení důvěrnosti údajů;

b) při informování o incidentech, reakcích na ně a jejich nápravě spolupracuje s příslušnými orgány Komise a řídí se jejich pokyny.

6. Uživatelé včas hlásí veškeré skutečné i domnělé incidenty v oblasti bezpečnosti IT na příslušná kontaktní místa.

7. Vlastníci údajů včas hlásí veškeré skutečné i domnělé incidenty v oblasti bezpečnosti IT příslušným týmům IT určeným pro reakci na bezpečnostní incidenty.

8. Generální ředitelství pro informatiku s podporou ostatních přispívajících zúčastněných stran odpovídá za řešení veškerých incidentů v oblasti bezpečnosti IT zjištěných v souvislosti s komunikačními a informačními systémy Komise, které nejsou zajišťovány externě.

9. Generální ředitelství pro informatiku v nezbytně nutném rozsahu informuje o bezpečnostních incidentech v oblasti IT zasažené útvary Komise, příslušné LISO, případně i CERT-EU.

10. Generální ředitelství pro informatiku pravidelně podává zprávy ISSB o incidentech v oblasti bezpečnosti IT, které ovlivňují komunikační a informační systém Komise.

11. Příslušný LISO získá na vyžádání přístup k záznamům o incidentech v oblasti bezpečnosti IT týkajících se komunikačního a informačního systému příslušného útvaru Komise.

12. V případě závažného incidentu v oblasti bezpečnosti IT je Generální ředitelství pro informatiku kontaktním bodem pro řízení krizových situací a koordinuje činnost skupin krizového řízení incidentů v oblasti bezpečnosti IT.

13. V případě nouzových situací může generální ředitel Generálního ředitelství pro informatiku rozhodnout o zahájení nouzového postupu pro bezpečnost IT. Generální ředitelství pro informatiku vypracuje nouzové postupy, které schválí ISSB.

14. Generální ředitelství pro informatiku podává ISSB a vedoucím zasažených útvarů Komise zprávy o provádění nouzových postupů.

Postupy související s těmito odpovědnostmi a činnostmi se podrobněji stanoví v prováděcích pravidlech.

KAPITOLA 4

ZÁVĚREČNÁ USTANOVENÍ

Článek 16

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 17

Vztah k jiným právním předpisům

Ustanovení tohoto rozhodnutí se nedotýkají rozhodnutí (EU, Euratom) 2015/443**,** rozhodnutí (EU, Euratom) 2015/444**,** nařízení (ES) č. 45/2001, nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ([1]), rozhodnutí Komise ES, ESUO, Euratom 2002/47 ([2]), nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ([3]), rozhodnutí 1999/352/ES, ESUO, Euratom.

Článek 18

Zrušení a přechodná opatření

Rozhodnutí C(2006) 3602 ze dne 16. srpna 2006 se zrušuje.

Prováděcí pravidla a standardy bezpečnosti IT přijaté podle článku 10 rozhodnutí C(2006) 3602 zůstávají v platnosti, pokud nejsou v rozporu s tímto rozhodnutím, dokud nebudou nahrazeny prováděcími pravidly a standardy, které je třeba přijmout podle článku 13 tohoto rozhodnutí. Veškeré odkazy na článek 10 rozhodnutí C(2006) 3602 se považují za odkaz na článek 13 tohoto rozhodnutí.

Článek 19

Vstup v platnost

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

V Bruselu dne 10. ledna 2017.

Za Komisi
předseda
Jean-Claude JUNCKER

([1]) Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

([2]) Rozhodnutí Komise 2002/47/ES, ESUO, Euratom ze dne 23. ledna 2002 o doplnění jejího jednacího řádu (Úř. věst. L 21, 24.1.2002, s. 23).

([3]) Nařízení Evropského parlamentu a Rady (EU, Euratom) č. 883/2013 ze dne 11. září 2013 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF) a o zrušení nařízení Evropského parlamentu a Rady (ES) č. 1073/1999 a nařízení Rady (Euratom) č. 1074/1999 (Úř. věst. L 248, 18.9.2013, s. 1).