ROZHODNUTIA

ROZHODNUTIE KOMISIE (EÚ, Euratom) 2017/46

z 10. januára 2017

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,

keďže:

(1) Komunikačné a informačné systémy Komisie sú neoddeliteľnou súčasťou fungovania Komisie a incidenty v oblasti bezpečnosti informačných technológií môžu mať vážny vplyv na činnosti Komisie, ako aj na tretie strany vrátane osôb, podnikov a členských štátov.

(2) Existuje mnoho hrozieb, ktoré môžu poškodiť dôvernosť, integritu alebo dostupnosť komunikačných a informačných systémov Komisie a informácií, ktoré sa v nich spracovávajú. K týmto hrozbám patria nehody, chyby, úmyselné útoky a prírodné javy a treba ich uznať ako prevádzkové riziká.

(3) Komunikačné a informačné systémy sa musia poskytovať s úrovňou ochrany zodpovedajúcou pravdepodobnosti, dosahu a povahe rizík, ktorým sú vystavené.

(4) Bezpečnosťou informačných technológií by sa malo zaistiť, aby sa komunikačnými a informačnými systémami (CIS) Komisie chránili informácie, ktoré sa v nich spracovávajú, a aby fungovali tak, ako potrebujú, kedy potrebujú a pod kontrolou oprávnených používateľov.

(5) Politika Komisie v oblasti bezpečnosti informačných technológií by sa mala vykonávať spôsobom, ktorý je v súlade s politikami týkajúcimi sa bezpečnosti v Komisii.

(6) Riaditeľstvo pre bezpečnosť Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť má všeobecnú zodpovednosť za bezpečnosť v Komisii pod dohľadom a zodpovednosťou člena Komisie, ktorý je zodpovedný za bezpečnosť.

(7) V rámci prístupu Komisie by sa mali zohľadniť politické iniciatívy EÚ a právne predpisy týkajúce sa bezpečnosti sietí a informácií, priemyselné normy a osvedčené postupy, aby bol v súlade so všetkými príslušnými právnymi predpismi a aby sa umožnila interoperabilita a kompatibilita.

(8) Oddelenia Komisie zodpovedné za informačné a komunikačné systémy by mali vypracovať a zaviesť vhodné opatrenia a bezpečnostné opatrenia v oblasti informačných technológií na ochranu komunikačných a informačných systémov by mali byť koordinované v rámci Komisie s cieľom zabezpečiť efektívnosť a účinnosť.

(9) Pravidlá a postupy pre prístup k informáciám v súvislosti s bezpečnosťou informačných technológií vrátane riešenia incidentov v oblasti bezpečnosti informačných technológií by mali byť primerané vzhľadom na hrozbu pre Komisiu alebo jej zamestnancov a v súlade so zásadami stanovenými v nariadení Európskeho parlamentu a Rady (ES) č. 45/2001 ([1]) o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Únie a o voľnom pohybe takýchto údajov a malo by sa pri nich prihliadať na zásadu služobného tajomstva, ako je stanovené v článku 339 ZFEÚ.

([1]) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

(10) Zásady a pravidlá pre komunikačné a informačné systémy, v rámci ktorých sa spracovávajú utajované informácie EÚ (EUCI), citlivé neutajované informácie a neutajované informácie, majú byť v plnom súlade s rozhodnutiami Komisie (EÚ, Euratom) 2015/443 ([1]) a (EÚ, Euratom) 2015/444 ([2]).

(11) Je potrebné, aby Komisia preskúmala a aktualizovala ustanovenia o bezpečnosti komunikačných a informačných systémov používaných v rámci Komisie.

(12) Rozhodnutie Komisie K(2006) 3602 by sa preto malo zrušiť,

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA 1

VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet a rozsah pôsobnosti

1. Toto rozhodnutie sa vzťahuje na všetky komunikačné a informačné systémy (CIS), ktoré sú vo vlastníctve, obstarané, riadené alebo prevádzkované Komisiou alebo v mene Komisie a na každé používanie týchto CIS Komisiou.

2. V tomto rozhodnutí sa stanovujú základné zásady, ciele, organizácia a zodpovednosti týkajúce sa bezpečnosti týchto CIS, a to najmä pre oddelenia Komisie, ktoré vlastnia, obstarávajú, riadia alebo prevádzkujú CIS vrátane CIS, ktoré zabezpečuje interný poskytovateľ IT služieb. V prípade, že CIS zabezpečuje, vlastní, riadi alebo prevádzkuje externá strana na základe dvojstrannej dohody alebo zmluvy s Komisiou, podmienky dohody alebo zmluvy musia byť v súlade s týmto rozhodnutím.

3. Toto rozhodnutie sa vzťahuje na všetky oddelenia Komisie a výkonné agentúry. V prípade, že CIS Komisie používajú iné orgány a inštitúcie na základe dvojstrannej dohody s Komisiou, podmienky dohody musia byť v súlade s týmto rozhodnutím.

4. Bez ohľadu na akékoľvek špecifické údaje o konkrétnych skupinách zamestnancov sa toto rozhodnutie vzťahuje na členov Komisie, pracovníkov Komisie patriacich do rozsahu pôsobnosti služobného poriadku úradníkov Európskej únie (ďalej len „služobný poriadok“) a Podmienok zamestnávania ostatných zamestnancov Únie (ďalej len „PZOZ“) ([3]), na národných expertov vyslaných do Komisie (ďalej len „VNE“) ([4]), na externých poskytovateľov služieb a ich zamestnancov, na stážistov a na každú osobu s prístupom k CIS v rámci rozsahu pôsobnosti tohto rozhodnutia.

5. Toto rozhodnutie sa vzťahuje na Európsky úrad pre boj proti podvodom (OLAF), pokiaľ je to zlučiteľné s právnymi predpismi Únie a rozhodnutím Komisie 1999/352/ES, ESUO, Euratom ([5]). Konkrétne sa opatrenia stanovené v tomto rozhodnutí vrátane pokynov, inšpekcií, prieskumov a podobných opatrení nemôžu vzťahovať na CIS úradu, kde to nie je zlučiteľné s nezávislosťou vyšetrovacej funkcie úradu a/alebo dôvernosťou informácií, ktoré úrad získal pri výkone tejto funkcie.

Článok 2

Vymedzenie pojmov

Na účely tohto rozhodnutia sa uplatňuje toto vymedzenie pojmov:

1. „zodpovedný“ je niekto, kto nesie zodpovednosť za kroky, rozhodnutia a výkon;

([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).
([2]) 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).
([3]) Stanovené v nariadení Rady (EHS, Euratom, ESUO) č. 259/68 z 29. februára 1968, ktorým sa ustanovuje Služobný poriadok a podmienky zamestnávania ostatných zamestnancov Európskych spoločenstiev a osobitné pravidlá, ktoré sa dočasne uplatňujú na úradníkov Komisie (podmienky zamestnávania ostatných zamestnancov) (Ú. v. ES L 56, 4.3.1968, s. 1).
([4]) Rozhodnutie Komisie z 12. novembra 2008 o pravidlách uplatniteľných na vyslaných národných expertov a národných expertov, účastníkov odborných stáží, v útvaroch Komisie [K(2008) 6866 v konečnom znení].
([5]) Rozhodnutie Komisie 1999/352/ES, ESUO, Euratom z z 28. apríla 1999, ktorým sa zriaďuje Európsky úrad pre boj proti podvodom (OLAF) (Ú. v. ES L 136, 31.5.1999, s. 20).

2. „CERT-EU“ je tím reakcie na núdzové počítačové situácie v inštitúciách a agentúrach EÚ. Jeho poslaním je podporovať európske inštitúcie, aby sa chránili pred zámernými a škodlivými útokmi, ktoré by narušili integritu ich IT aktív a poškodzovali záujmy EÚ. Do rozsahu činností CERT-EÚ patrí prevencia, odhaľovanie, reakcia a obnova;

3. „oddelenie Komisie“ je akékoľvek generálne riaditeľstvo či útvar Komisie alebo kabinet člena Komisie;

4. „bezpečnostný orgán Komisie“ sa vzťahuje na úlohu stanovenú v rozhodnutí (EÚ, Euratom) 2015/444;

5. „komunikačný a informačný systém“ alebo „CIS“ je každý systém, ktorý umožňuje manipuláciu s informáciami v elektronickej podobe vrátane všetkých prostriedkov potrebných na jeho prevádzku, ako aj infraštruktúry, organizácie, zamestnancov a informačných zdrojov. Toto vymedzenie pojmu zahŕňa podnikové aplikácie, spoločne využívané IT služieb, externé systémy a zariadenia koncových používateľov;

6. „správna rada organizácie“ (CMB) poskytuje najvyššiu úroveň dohľadu manažmentu organizácie nad prevádzkovými a administratívnymi záležitosťami v Komisii;

7. „vlastník údajov“ je osoba zodpovedná za zabezpečenie ochrany a používania určitého súboru údajov spracovávaného v rámci CIS;

8. „súbor údajov“ je súbor informácií, ktoré slúžia osobitným pracovným postupom alebo činnosť Komisie;

9. „núdzový postup“ je vopred určený súbor metód a zodpovedností v súvislosti s riešením naliehavých situácií s cieľom zabrániť výraznému dosahu na Komisiu;

10. „politika v oblasti informačnej bezpečnosti“ je súbor cieľov v oblasti informačnej bezpečnosti, ktoré sú zavedené, vykonávané a kontrolované alebo ktoré sa musia zaviesť, vykonávať a kontrolovať. Zahŕňa okrem iného rozhodnutia (EÚ, Euratom) 2015/444 a (EÚ, Euratom) 2015/443;

11. „Riadiaci výbor pre informačnú bezpečnosť“ (ISSB) je riadiaci orgán, ktorý podporuje správnu radu organizácie v jej úlohách týkajúcich sa bezpečnosti informačných technológií;

12. „interný poskytovateľ IT služieb“ je oddelenie Komisie poskytujúce spoločne využívané IT služieb;

13. „bezpečnosť informačných technológií“ alebo „bezpečnosť CIS“ je zachovanie dôvernosti, integrity a dostupnosti CIS a súborov údajov, ktoré spracúvajú;

14. „usmernenia v oblasti bezpečnosti informačných technológií“ tvoria odporúčané, ale dobrovoľné opatrenia, ktoré pomáhajú pri podpore noriem v oblasti bezpečnosti informačných technológií alebo slúžia ako referencia, ak nie je zavedená žiadna platná norma;

15. „incident v oblasti bezpečnosti informačných technológií“ je udalosť, ktorá by mohla mať negatívny vplyv na dôvernosť, integritu alebo dostupnosť CIS;

16. „bezpečnostné opatrenie v oblasti informačných technológií“ je technické alebo organizačné opatrenie zamerané na zmiernenie bezpečnostných rizík v oblasti informačných technológií;

17. „potreba v oblasti bezpečnosti informačných technológií“ je presné a jednoznačné vymedzenie úrovní dôvernosti, integrity a dostupnosti spojených s informáciou alebo s informačným systémom s cieľom stanoviť požadovanú úroveň ochrany;

18. „cieľ v oblasti bezpečnosti informačných technológií“ je vyhlásenie o zámere čeliť špecifikovaným hrozbám a/alebo splniť špecifikované organizačné bezpečnostné požiadavky alebo predpoklady;

19. „plán bezpečnosti informačných technológií“ je dokumentácia bezpečnostných opatrení v oblasti informačných technológií, ktorá je potrebná na splnenie potrieb CIS v oblasti bezpečnosti informačných technológií;

20. „politika v oblasti bezpečnosti informačných technológií“ je súbor cieľov v oblasti bezpečnosti informačných technológií, ktoré sú zavedené, vykonávané a kontrolované alebo ktoré sa musia zaviesť, vykonávať a kontrolovať. Obsahuje toto rozhodnutie a jeho vykonávacie predpisy;

21. „požiadavka na bezpečnosť informačných technológií“ je potreba v oblasti bezpečnosti informačných technológií formalizovaná vopred stanoveným postupom;

22. „bezpečnostné riziko v oblasti informačných technológií“ je účinok na CIS, ktorý by pre bezpečnosť informačných technológií mohla predstavovať hrozba zneužitia zraniteľnosti. Bezpečnostné riziko v oblasti informačných technológií ako také charakterizujú dva faktory: 1. neistota, to znamená pravdepodobnosť, že bezpečnostná hrozba v oblasti informačných technológií spôsobí nežiaducu udalosť, a 2. vplyv, to znamená dôsledky, ktoré takáto nežiaduca udalosť môže mať na CIS;

23. „bezpečnostné normy v oblasti informačných technológií“ sú osobitné povinné bezpečnostné opatrenia v oblasti informačných technológií, ktoré pomáhajú pri presadzovaní a podpore politiky v oblasti bezpečnosti informačných technológií;

24. „stratégia v oblasti bezpečnosti informačných technológií“ je súbor projektov a činností, ktoré sú určené na dosiahnutie cieľov Komisie a ktoré sa majú zaviesť, vykonať a skontrolovať;

25. „bezpečnostná hrozba v oblasti informačných technológií“ je faktor, ktorý môže potenciálne viesť k nežiaducej udalosti, ktorá môže mať za následok poškodenie CIS; Takéto hrozby môžu byť náhodné alebo úmyselné a sú charakterizované prvkami hrozby, potenciálnymi cieľmi a metódami útoku;

26. „miestny úradník informačnej bezpečnosti“ je úradník, ktorý je pre určité oddelenie Komisie zodpovedný za spoluprácu v oblasti bezpečnosti informačných technológií;

27. „osobné údaje“, „spracovávanie osobných údajov“, „prevádzkovateľ“ a „systém archivovania osobných údajov“ majú rovnaký význam ako v nariadení (ES) č. 45/2001, a najmä v jeho článku 2;

28. „spracovanie informácií“ sú všetky funkcie CIS s ohľadom na súbory údajov vrátane vytvárania, úpravy, zobrazovania, ukladania, prenosu, vymazávania a archivovania informácií. Spracovanie informácií môže zabezpečiť CIS ako súbor funkcií pre používateľov a ako IT služby pre ostatné CIS;

29. „služobné tajomstvo“ je ochrana informácií o obchodných údajoch, na ktoré sa vzťahuje povinnosť služobného tajomstva, najmä informácií o podnikoch, ich obchodných vzťahoch alebo zložkách nákladov, ako je stanovené v článku 339 ZFEÚ;

30. „zodpovednosť“ je povinnosť konať a prijímať rozhodnutia s cieľom dosiahnuť požadované výsledky;

31. „bezpečnosť v Komisii“ je bezpečnosť osôb, majetku a informácií v Komisii, a najmä fyzická integrita osôb a majetku, integrita, dôvernosť a dostupnosť informácií a komunikačných a informačných systémov, ako aj nerušený chod činností Komisie;

32. „spoločne využívaná IT služba“ je služba, ktorú CIS poskytuje ostatným komunikačným a informačným systémom pri spracovávaní informácií;

33. „vlastník systému“ je osoba zodpovedná za celkové obstaranie, vývoj, integráciu, úpravu, prevádzku, údržbu a vyradenie CIS;

34. „používateľ“ je osoba, ktorá používa funkcie poskytované CIS, či už v Komisii alebo mimo nej.

Článok 3

Zásady pre bezpečnosť informačných technológií v Komisii

1. Pri bezpečnosti informačných technológií v Komisii sa vychádza zo zásad zákonnosti, transparentnosti, proporcionality a zodpovednosti.

2. Otázky bezpečnosti informačných technológií sa musia brať do úvahy od začiatku vývoja a realizácie komunikačných a informačných systémov Komisie. Generálne riaditeľstvo pre informatiku a Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť sa preto podieľajú na svojich príslušných oblastiach zodpovednosti.

3. Účinnou bezpečnosťou informačných technológií sa zabezpečia primerané úrovne:

a) pravosti: záruka, že informácie sú pravé a pochádzajú z dôveryhodných zdrojov;

b) dostupnosti: vlastnosť charakterizovaná prístupnosťou informácií a ich použiteľnosťou na požiadanie oprávneného subjektu;

c) dôvernosti: vlastnosť, ktorá znamená, že informácie sa nesprístupnia neoprávneným osobám, subjektom či procesom;

d) integrity: vlastnosť charakterizovaná zabezpečením presnosti a úplnosti informácií a majetku;

e) nespochybniteľnosti: schopnosť preukázať, že sa činnosť alebo udalosť uskutočnila, takže túto činnosť alebo udalosť nemožno následne poprieť;

f) ochrany osobných údajov: poskytnutie primeraných záruk v súvislosti so spracovaním osobných údajov v úplnom súlade s nariadením (ES) č. 45/2001;

g) služobného tajomstva: ochrana informácií, na ktoré sa vzťahuje povinnosť služobného tajomstva, najmä informácií o podnikoch, ich obchodných vzťahoch alebo zložkách nákladov, ako je stanovené v článku 339 ZFEÚ.

4. Bezpečnosť v oblasti informačných technológií sa zakladá na procese riadenia rizík. Tento proces sa zameriava na určovanie úrovní bezpečnostných rizík v oblasti informačných technológií a na definovanie bezpečnostných opatrení na zníženie rizík na primeranú úroveň a za primerané náklady.

5. Všetky komunikačné a informačné systémy sa identifikujú, priradia majiteľovi systému a zaznamenajú sa v inventári.

6. Požiadavky na bezpečnosť všetkých komunikačných a informačných systémov sa určia na základe ich potrieb týkajúcich sa bezpečnosti a potrieb týkajúcich sa bezpečnosti informácií, ktoré spracovávajú. Komunikačné a informačné systémy, ktoré poskytujú služby pre iné komunikačné a informačné systémy, môžu byť navrhnuté na podporu špecifikovaných úrovní potrieb v oblasti bezpečnosti.

7. Plány bezpečnosti informačných technológií a bezpečnostné opatrenia v oblasti informačných technológií musia byť primerané potrebám týkajúcim sa bezpečnosti CIS.

Procesy súvisiace s týmito zásadami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

KAPITOLA 2

ORGANIZÁCIA A ZODPOVEDNOSTI

Článok 4

Správna rada organizácie

Správna rada organizácie má celkovú zodpovednosť za riadenie bezpečnosti informačných technológií ako celku v rámci Komisie.

Článok 5

Riadiaci výbor pre informačnú bezpečnosť (ISSB)

1. Riadiacemu výboru ISSB predsedá zástupca generálneho tajomníka zodpovedný za riadenie bezpečnosti informačných technológií v Komisii. Jeho členovia zastupujú obchod, technológie a bezpečnostné záujmy v rámci oddelení Komisie a patria k nim zástupcovia Generálneho riaditeľstva pre informatiku, Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť, Generálneho riaditeľstva pre rozpočet a, na dvojročnom rotujúcom základe, zástupcovia ďalších štyroch oddelení Komisie, ktoré sa zapájajú v prípade, že má bezpečnosť informačných technológií pre ich činnosti zásadný význam. Členstvo je na úrovni vrcholového manažmentu.

2. ISSB podporuje správnu radu organizácie v jej úlohách týkajúcich sa bezpečnosti informačných technológií. ISSB má prevádzkovú zodpovednosť za riadenie bezpečnosti informačných technológií ako celku v rámci Komisie.

3. ISSB odporučí Komisii, aby prijala politiku Komisie v oblasti bezpečnosti informačných technológií.

4. ISSB skúma otázky riadenia, ako aj otázky bezpečnosti informačných technológií vrátane závažných incidentov v oblasti bezpečnosti informačných technológií a každé dva roky o tom podáva správu správnej rade organizácie.

5. ISSB monitoruje a skúma celkové vykonávanie tohto rozhodnutia a podáva o ňom správu správnej rade organizácie.

6. ISSB na návrh Generálneho riaditeľstva pre informatiku preskúmava, schvaľuje a monitoruje vykonávanie otvorenej stratégie v oblasti bezpečnosti informačných technológií. ISSB podáva o tom správu správnej rade organizácie.

7. ISSB monitoruje, hodnotí a kontroluje podmienky riešenia rizík v oblasti podnikových informácií a má právomoc vydávať formálne požiadavky na vylepšenia, kedykoľvek to bude potrebné.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 6

Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť

V súvislosti s bezpečnosťou informačných technológií má Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť tieto zodpovednosti. Musí:

1. zaistiť súlad medzi politikou v oblasti bezpečnosti informačných technológií a politikou Komisie v oblasti informačnej bezpečnosti;

2. vytvoriť rámec na povolenie používať šifrovacie technológie na ukladanie a komunikáciu informácií komunikačnými a informačnými systémami;

3. informovať Generálne riaditeľstvo pre informatiku o špecifických hrozbách, ktoré by mohli mať významný vplyv na bezpečnosť komunikačných a informačných systémov a súborov údajov, ktoré spracovávajú,

4. vykonávať kontroly bezpečnosti informačných technológií na posúdenie zhody komunikačných a informačných systémov Komisie s politikou v oblasti bezpečnosti a podávať správu o výsledkoch ISSB;

5. vytvoriť rámec na povolenie prístupu a príslušné bezpečnostné predpisy pre komunikačné a informačné systémy Komisie z externých sietí a vypracovať súvisiace normy a usmernenia v oblasti bezpečnosti informačných technológií v úzkej spolupráci s Generálnym riaditeľstvom pre informatiku;

6. navrhnúť zásady a pravidlá pre externé obstaranie komunikačných a informačných systémov na udržanie primeranej kontroly bezpečnosti informácií;

7. vypracovať súvisiace bezpečnostné normy a usmernenia v oblasti informačných technológií v súvislosti s článkom 6, a to v úzkej spolupráci s Generálnym riaditeľstvom pre informatiku.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 7

Generálne riaditeľstvo pre informatiku

Vo vzťahu k celkovej bezpečnosti informačných technológií Komisie má Generálne riaditeľstvo pre informatiku tieto úlohy. Musí:

1. v úzkej spolupráci s Generálnym riaditeľstvom pre ľudské zdroje a bezpečnosť vypracovať bezpečnostné normy a usmernenia v oblasti informačných technológií, s výnimkou uvedenou v článku 6, s cieľom zabezpečiť súlad medzi politikou v oblasti bezpečnosti informačných technológií a politikou Komisie v oblasti informačnej bezpečnosti a navrhnúť ich výboru ISSB;

2. posudzovať metódy, procesy a výsledky riadenia bezpečnostných rizík v oblasti informačných technológií všetkých oddelení Komisie a pravidelne o tom podávať správu výboru ISSB;

3. navrhnúť otvorenú stratégiu v oblasti bezpečnosti informačných technológií na revíziu a schválenie zo strany výboru ISSB a následné prijatie správnou radou organizácie a navrhnúť program vrátane plánovania projektov a činností, ktorými sa vykonáva stratégia v oblasti bezpečnosti informačných technológií,

4. monitorovať vykonávanie stratégie Komisie v oblasti bezpečnosti informačných technológií a pravidelne o tom podávať správu výboru ISSB;

5. monitorovať bezpečnostné riziká v oblasti informačných technológií a bezpečnostné opatrenia v oblasti informačných technológií, ktoré sa zaviedli v komunikačných a informačných systémoch a pravidelne o tom podávať správu výboru ISSB;

6. pravidelne podávať správu o celkovom vykonávaní a súlade s týmto rozhodnutím výboru ISSB;

7. po porade s Generálnym riaditeľstvom pre ľudské zdroje a bezpečnosť požadovať od vlastníkov systému, aby prijali osobitné bezpečnostné opatrenia v oblasti informačných technológií s cieľom zmierniť bezpečnostné riziká v oblasti informačných technológií pre komunikačné a informačné systémy Komisie;

8. zaistiť, aby bol pre vlastníkov systému a vlastníkov údajov k dispozícii adekvátny katalóg služieb poskytovaných v oblasti bezpečnosti informačných technológií Generálneho riaditeľstva pre informatiku, aby si plnili svoje povinnosti súvisiace s bezpečnosťou informačných technológií a dodržať politiku v oblasti bezpečnosti informačných technológií a bezpečnostné normy v oblasti informačných technológií;

9. poskytnúť vlastníkom systému a vlastníkom údajov adekvátnu dokumentáciu a konzultovať s nimi, ak je to vhodné, o bezpečnostných opatreniach v oblasti informačných technológií, ktoré sa zaviedli pre svoje IT služby s cieľom uľahčiť súlad s politikou v oblasti bezpečnosti informačných technológií a podporiť vlastníkov systému pri riadení rizík v oblasti informačných technológií;

10. organizovať pravidelné stretnutia siete miestnych úradníkov informačnej bezpečnosti a podporovať miestnych úradníkov informačnej bezpečnosti pri vykonávaní ich povinností;

11. určiť potreby odbornej prípravy a koordinovať vzdelávacie programy týkajúce sa bezpečnosti informačných technológií v spolupráci s oddeleniami Komisie a vytvárať, realizovať a koordinovať kampane na zvyšovanie povedomia o bezpečnosti informačných technológií v úzkej spolupráci s Generálnym riaditeľstvom pre ľudské zdroje,

12. zaistiť, aby vlastníci systému, vlastníci údajov a ďalšie pozície so zodpovednosťami týkajúcimi sa bezpečnosti v oblasti informačných technológií v oddeleniach Komisie boli oboznámení s politikou v oblasti bezpečnosti informačných technológií;

13. informovať Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť o osobitných bezpečnostných hrozbách v oblasti informačných technológií, o incidentoch a výnimkách z politiky Komisie v oblasti bezpečnosti informačných technológií, ktoré oznámili vlastníci systémov a ktoré by mohli mať významný vplyv na bezpečnosť v Komisii;

14. v súvislosti s jeho úlohou poskytovateľa IT služieb poskytnúť Komisii katalóg spoločne využívaných IT služieb, ktoré poskytujú stanovené úrovne bezpečnosti. Dosiahne sa to systematickým hodnotením, riadením a monitorovaním bezpečnostných rizík v oblasti informačných technológií na vykonanie bezpečnostných opatrení s cieľom dosiahnuť stanovenú úroveň bezpečnosti.

Súvisiace procesy a podrobnejšie povinnosti sa ďalej určia vo vykonávacích predpisoch.

Článok 8

Oddelenia Komisie

Pokiaľ ide o bezpečnosť informačných technológií v príslušnom oddelení, každý vedúci oddelenia Komisie musí:

1. formálne vymenovať vlastníka systému, ktorý je úradníkom alebo dočasným zamestnancom, pre každý CIS, ktorý bude zodpovedný za bezpečnosť informačných technológií tohto CIS a formálne vymenovať vlastníka údajov pre každý súbor údajov spracovávaný v CIS, ktorý by mal patriť do tej istej administratívnej jednotky, ktorá je prevádzkovateľom pre súbory údajov podľa nariadenia (ES) č. 45/2001;

2. formálne vymenovať miestneho úradníka informačnej bezpečnosti (LISO), ktorý dokáže vykonávať svoje povinnosti nezávisle od vlastníkov systémov a vlastníkov údajov. Miestneho úradníka informačnej bezpečnosti možno vymenovať pre jedno alebo viac oddelení Komisie;

3. uistiť sa, že boli prijaté a zavedené posúdenia bezpečnostných rizík v oblasti informačných technológií a plánov bezpečnosti informačných technológií;

4. zaistiť pravidelné podávanie správy o súhrne bezpečnostných rizík a opatrení v oblasti informačných technológií Generálnemu riaditeľstvu pre informatiku;

5. s podporou Generálneho riaditeľstva pre informatiku zaistiť, aby sa zaviedli príslušné procesy, postupy a riešenia s cieľom zabezpečiť účinné zisťovanie, nahlasovanie a riešenie incidentov v oblasti bezpečnosti informačných technológií, ktoré súvisia s ich komunikačnými a informačnými systémami;

6. začať núdzový postup v prípade núdzových situácií týkajúcich sa bezpečnosti informačných technológií;

7. niesť plnú zodpovednosť za bezpečnosť informačných technológií vrátane zodpovednosti vlastníka systému a vlastníka údajov;

8. vlastniť riziká súvisiace s ich komunikačnými a informačnými systémami a súbormi údajov;

9. vyriešiť všetky spory medzi vlastníkmi údajmi a vlastníkmi systémov a v prípade pretrvávajúceho sporu predložiť výboru ISSB túto otázku na jej vyriešenie;

10. zaistiť zavedenie plánov bezpečnosti informačných technológií a bezpečnostných opatrení v oblasti informačných technológií a primerané krytie rizík.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 9

Vlastníci systémov

1. Vlastník systému je zodpovedný za bezpečnosť CIS v oblasti informačných technológií a podáva správu vedúcemu oddelenia Komisie.

2. V súvislosti s bezpečnosťou informačných technológií musí vlastník systému:

a) zabezpečiť súlad CIS s politikou v oblasti bezpečnosti informačných technológií;

b) zaistiť správne zaznamenanie CIS v príslušnom inventári;

c) vyhodnotiť bezpečnostné riziká v oblasti informačných technológií a určiť potreby v oblasti bezpečnosti informačných technológií každého CIS, a to v spolupráci s príslušnými vlastníkmi údajov a po porade s Generálnym riaditeľstvom pre informatiku;

d) pripraviť bezpečnostný plán vrátane, ak je to vhodné, informácií o posudzovaných rizikách a všetky ďalšie potrebné bezpečnostné opatrenia;

e) zaviesť vhodné bezpečnostné opatrenia v oblasti informačných technológií primerané stanoveným bezpečnostným rizikám v oblasti informačných technológií a dodržiavať odporúčania potvrdené výborom ISSB;

f) identifikovať všetky závislosti od iných komunikačných a informačných systémoch alebo spoločne využívaných IT služieb a zaviesť primerané bezpečnostné opatrenia na základe úrovní bezpečnosti, ktoré sú navrhované v rámci týchto komunikačných a informačných systémov alebo spoločne využívaných IT služieb;

g) riadiť a monitorovať bezpečnostné riziká v oblasti informačných technológií;

h) pravidelne podávať správy vedúcemu oddelenia Komisie o profile bezpečnostných rizík v oblasti informačných technológií ich komunikačných a informačných systémov a podávať správy Generálnemu riaditeľstvu pre informatiku o súvisiacich rizikách, činnostiach riadenia rizík a prijatých bezpečnostných opatreniach;

i) viesť konzultácie s miestnym úradníkom informačnej bezpečnosti príslušného oddelenia (oddelení) Komisie o aspektoch bezpečnosti informačných technológií;

j) vydávať pokyny pre používateľov o používaní CIS a súvisiacich údajov, ako aj o zodpovednostiach používateľov týkajúcich sa CIS;

k) požiadať o povolenie od Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť, ktoré koná ako kryptografický orgán, pre každý CIS, v rámci ktorého sa využíva technológia šifrovania;

l) vopred viesť konzultácie s bezpečnostným orgánom Komisie o akomkoľvek systéme, ktorým sa spracovávajú utajované informácie EÚ;

m) zaistiť, aby sa zálohovania všetkých dešifrovacích kľúčov ukladali na viazanom účte. Obnovenie šifrovaných údajov sa vykoná len v prípade povolenia v súlade s rámcom, ktorý stanovilo Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť;

n) dodržiavať všetky pokyny príslušného prevádzkovateľa(-ov) týkajúce sa ochrany osobných údajov a uplatňovania pravidiel ochrany údajov na bezpečnosť spracovania;

o) informovať Generálne riaditeľstvo pre informatiku o všetkých výnimkách z politiky Komisie v oblasti bezpečnosti informačných technológií vrátane príslušných odôvodnení;

p) vedúcemu oddelenia Komisie nahlasovať každý neriešiteľný spor medzi vlastníkom údajov a vlastníkom systému, oznamovať incidenty v oblasti bezpečnosti informačných technológií príslušným zainteresovaným stranám včas podľa ich závažnosti, ako je stanovené v článku 15;

q) v prípade externých systémov zaistiť, aby do zmlúv o externom obstaraní boli zahrnuté príslušné ustanovenia týkajúce sa bezpečnosti informačných technológií a aby sa incidenty v oblasti bezpečnosti informačných technológií, ktoré sa vyskytli v externom CIS, nahlásili v súlade s článkom 15;

r) v prípade CIS poskytujúcom spoločne využívané IT služby zaistiť, aby sa poskytla a jasne zdokumentovala stanovená úroveň bezpečnosti a aby sa pre tento CIS zaviedli bezpečnostné opatrenia s cieľom dosiahnuť stanovenú úroveň bezpečnosti.

3. Vlastníci systémov môžu formálne delegovať niektoré alebo všetky svoje úlohy týkajúce sa bezpečnosti informačných technológií, zostávajú však zodpovední za bezpečnosť informačných technológií v súvislosti so svojím CIS.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 10

Vlastníci údajov

1. Vlastník údajov sa zodpovedá za bezpečnosť informačných technológií v súvislosti s konkrétnym súborom údajov vedúcemu oddelenia Komisie a je zodpovedný za dôvernosť, integritu a dostupnosť súboru údajov.

2. V súvislosti s týmto súborom údajov musí vlastník:

a) zaistiť, aby boli všetky súbory údajov v rámci jeho zodpovednosti príslušne klasifikované v súlade s rozhodnutím Rady (EÚ, Euratom) 2015/443 a (EÚ, Euratom) 2015/444;

b) určiť potreby informačnej bezpečnosti a informovať príslušných vlastníkov systémov o týchto potrebách,

c) zúčastňovať sa na posudzovaní rizík CIS;

d) podávať správy o všetkých neriešiteľných sporoch medzi vlastníkom údajov a vlastníkom systému vedúcemu oddelenia Komisie;

e) oznamovať incidenty v oblasti bezpečnosti informačných technológií, ako je uvedené v článku 15.

3. Vlastníci údajov môžu formálne delegovať niektoré alebo všetky svoje úlohy týkajúce sa bezpečnosti informačných technológií, svoje zodpovednosti si však zachovávajú, ako je uvedené v tomto článku.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 11

Miestni úradníci informačnej bezpečnosti (LISO)

V súvislosti s bezpečnosťou informačných technológií musí miestny úradník informačnej bezpečnosti:

a) aktívne identifikovať a oznamovať vlastníkom systému, vlastníkom údajov a ďalším pozíciám so zodpovednosťami v oblasti bezpečnosti informačných technológií v oddeleniach Komisie o politike v oblasti bezpečnosti informačných technológií;

b) spolupracovať v otázkach bezpečnosti informačných technológií v oddeleniach Komisie s Generálnym riaditeľstvom pre informatiku ako súčasť siete miestnych úradníkov informačnej bezpečnosti;

c) zúčastňovať sa na pravidelných stretnutiach miestnych úradníkov informačnej bezpečnosti;

d) udržiavať si prehľad o procese riadenia bezpečnostných rizík v oblasti informácií a o vytváraní a zavádzaní plánov bezpečnosti informačných systémov;

e) radiť vlastníkom údajov, vlastníkom systémov a vedúcim oddelení Komisie v otázkach bezpečnosti informačných technológií;

f) spolupracovať s Generálnym riaditeľstvom pre informatiku v šírení osvedčených postupov týkajúcich sa bezpečnosti informačných technológií a navrhovať konkrétne informačné a vzdelávacie programy;

g) podávať správy o bezpečnosti informačných technológií, identifikovať nedostatky a zlepšenia vedúcemu oddelenia (oddelení) Komisie.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 12

Používatelia

1. V súvislosti s bezpečnosťou informačných technológií musia používatelia:

a) dodržiavať politiku v oblasti bezpečnosti informačných technológií a pokyny, ktoré vydal vlastník systému o používaní každého CIS;

b) oznamovať incidenty v oblasti bezpečnosti informačných technológií, ako je uvedené v článku 15.

2. Použitie CIS Komisie v rozpore s jej politikou v oblasti bezpečnosti informačných technológií alebo pokynmi, ktoré vydal vlastník systému, môže viesť k disciplinárnemu konaniu.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

KAPITOLA 3

BEZPEČNOSTNÉ POŽIADAVKY A POVINNOSTI

Článok 13

Vykonávanie tohto rozhodnutia

1. Prijatie vykonávacích predpisov podľa článku 6 a súvisiacich noriem a usmernení bude predmetom splnomocňujúceho rozhodnutia prijatého Komisiou v prospech člena Komisie zodpovedného za záležitosti bezpečnosti.

2. Prijatie všetkých ďalších vykonávacích predpisov v súvislosti s týmto rozhodnutím a súvisiacich bezpečnostných noriem a usmernení v oblasti informačných technológií bude predmetom splnomocňujúceho rozhodnutia, ktoré prijme Komisia v prospech člena Komisie zodpovedného za informatiku.

3. ISSB schváli vykonávacie predpisy, normy a usmernenia vo vyššie uvedených odsekoch 1 a 2 pred ich prijatím.

Článok 14

Povinnosť dodržiavať ustanovenia

1. Súlad s ustanoveniami uvedenými v politike a normách v oblasti bezpečnosti informačných technológií je povinný.

2. Nedodržiavanie politiky v oblasti bezpečnosti informačných technológií a bezpečnostných noriem v oblasti informačných technológií môže viesť k disciplinárnemu konaniu v súlade so zmluvami, služobným poriadkom a PZOZ, k zmluvným sankciám a/alebo súdnemu konaniu podľa vnútroštátnych zákonov a iných právnych predpisov.

3. Generálnemu riaditeľstvu pre informatiku sa oznámia všetky výnimky z politiky v oblasti bezpečnosti informačných technológií.

4. V prípade, že výbor ISSB rozhodne o tom, že pre CIS Komisie pretrváva neprijateľné riziko, Generálne riaditeľstvo pre informatiku v spolupráci s vlastníkom systému navrhne zmierňujúce opatrenia na schválenie ISSB. Tieto opatrenia môžu okrem iného zahŕňať posilnené monitorovanie a podávanie správ, obmedzenia služieb a odpojenie.

5. ISSB nariadi zavedenie schválených zmierňovacích opatrení, kedykoľvek to bude potrebné. ISSB môže tiež odporučiť generálnemu riaditeľovi Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť, aby otvoril administratívne vyšetrovanie. Generálne riaditeľstvo pre informatiku predloží správu výboru ISSB o každej situácii pri nariadení zmierňovacích opatrení.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

Článok 15

Riešenie incidentov v oblasti bezpečnosti informačných technológií

1. Generálne riaditeľstvo pre informatiku je zodpovedné za zabezpečenie základnej operačnej spôsobilosti pre reakcie na incidenty v oblasti bezpečnosti informačných technológií v rámci Európskej komisie.

2. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť ako zainteresovaná strana podieľajúca sa na reakcii na incidenty v oblasti bezpečnosti informačných technológií musí:

a) mať právo na prístup k súhrnným informáciám v prípade záznamov o všetkých incidentoch a k úplným záznamom na požiadanie;

b) sa zapájať do skupín pre krízové riadenie v súvislosti s incidentmi v oblasti bezpečnosti informačných technológií a núdzových postupov pre bezpečnosť informačných technológií;

c) mať na starosti vzťahy s orgánmi presadzovania práva a spravodajskými službami;

d) vykonávať forenznú analýzu týkajúcu sa kybernetickej bezpečnosti v súlade s článkom 11 rozhodnutia (EÚ, Euratom) 2015/443;

e) rozhodovať o potrebe začať formálne vyšetrovanie;

f) informovať Generálne riaditeľstvo pre informatiku o všetkých incidentoch v oblasti bezpečnosti informačných technológií, ktoré môžu predstavovať riziko pre ostatné komunikačné a informačné systémy.

3. Medzi Generálnym riaditeľstvom pre informatiku a Generálnym riaditeľstvom pre ľudské zdroje a bezpečnosť sa uskutočňuje pravidelná komunikácia s cieľom vymieňať si informácie a koordinovať riešenie bezpečnostných incidentov, najmä akýchkoľvek incidentov v oblasti bezpečnosti informačných technológií, ktoré si môžu vyžadovať formálne vyšetrovanie.

4. Útvary koordinácie incidentov v rámci tímu reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach („CERT-EU“) možno využiť na podporu procesu riešenia incidentov, keď je to vhodné, a na spoločné využívanie vedomostí s ostatnými inštitúciami a agentúrami EÚ, ktorých sa to môže dotýkať.

5. Vlastníci systémov zapojení do incidentu v oblasti bezpečnosti informačných technológií musia:

a) bezodkladne oznámiť vedúcemu oddelenia Komisie, Generálnemu riaditeľstvu pre informatiku, Generálnemu riaditeľstvu pre ľudské zdroje, miestnemu úradníkovi informačnej bezpečnosti a v prípade potreby vlastníkovi údajov akýkoľvek významný incident v oblasti bezpečnosti informačných technológií, najmä tie, ktoré sa týkajú porušenia dôvernosti údajov;

b) spolupracovať a postupovať podľa pokynov príslušných orgánov Komisie o oznamovaní, reakcii a náprave incidentov.

6. Používatelia včasne nahlasujú všetky skutočné alebo domnelé incidenty v oblasti bezpečnosti informačných technológií príslušnému asistenčnému pracovisku IT (helpdesku).

7. Vlastníci údajov včasne nahlasujú všetky skutočné alebo domnelé incidenty v oblasti bezpečnosti informačných technológií príslušnému tímu reakcie na incidenty v oblasti bezpečnosti informačných technológií.

8. Generálne riaditeľstvo pre informatiku s podporou zo strany ostatných podieľajúcich sa zainteresovaných strán je zodpovedné za riešenie všetkých incidentov v oblasti bezpečnosti informačných technológií zistených v súvislosti s komunikačnými a informačnými systémami Komisie, ktoré nie sú externé systémy.

9. Generálne riaditeľstvo pre informatiku informuje dotknuté oddelenia Komisie o incidentoch v oblasti bezpečnosti informačných technológií, miestnych úradníkov informačnej bezpečnosti a prípadne CERT-EÚ na základe opodstatnenej potreby.

10. Generálne riaditeľstvo pre informatiku pravidelne podáva správy výboru ISSB o významných incidentoch v oblasti bezpečnosti informačných technológií, ktoré majú dosah na komunikačné a informačné systémy Komisie.

11. Príslušný miestny úradník informačnej bezpečnosti má na požiadanie prístup k záznamom o incidentoch v oblasti bezpečnosti informačných technológií, ktoré sa týkajú CIS oddelenia Komisie.

12. V prípade významného incidentu v oblasti bezpečnosti informačných technológií je Generálne riaditeľstvo pre informatiku kontaktným miestom pre riadenie krízových situácií prostredníctvom koordinovania skupín pre riadenie kríz v súvislosti s incidentmi v oblasti bezpečnosti informačných technológií.

13. V prípade núdzovej situácie môže generálny riaditeľ Generálneho riaditeľstva pre informatiku rozhodnúť o začatí núdzového postupu pre bezpečnosť informačných technológií. Generálne riaditeľstvo pre informatiku vypracuje núdzové postupy, ktoré má schváliť výbor ISSB.

14. Generálne riaditeľstvo pre informatiku predloží správu o vykonaní núdzových postupov výboru ISSB a vedúcim dotknutých oddelení Komisie.

Procesy súvisiace s týmito zodpovednosťami a činnosťami sa podrobnejšie uvedú vo vykonávacích predpisoch.

KAPITOLA 4

ZÁVEREČNÉ USTANOVENIA

Článok 16

Transparentnosť

Na toto rozhodnutie budú upozornení zamestnanci Komisie a všetky osoby, ktorých sa týka a uverejní sa v Úradnom vestníku Európskej únie.

Článok 17

Vzťah k iným aktom

Ustanoveniami tohto rozhodnutia je dotknuté rozhodnutie (EÚ, Euratom) 2015/443, rozhodnutie (EÚ, Euratom) 2015/444, nariadenie (ES) č. 45/2001, nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 ([1]), rozhodnutie Komisie 2002/47/ ES, ESUO, Euratom ([2]), nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 ([3]), rozhodnutie 1999/352/ES, ESUO, Euratom.

Článok 18

Zrušenie a prechodné opatrenia

Rozhodnutie K(2006) 3602 zo 16. augusta 2006 sa zrušuje.

Vykonávacie predpisy a normy v oblasti bezpečnosti informačných technológií prijaté podľa článku 10 rozhodnutia Komisie K(2006) 3602 zostávajú v platnosti, pokiaľ nie sú v rozpore s týmto rozhodnutím, až kým sa nenahradia vykonávacími predpismi a normami, ktoré sa majú prijať na základe článku 13 tohto rozhodnutia. Akýkoľvek odkaz na článok 10 rozhodnutia Komisie K(2006)3602 sa považuje za odkaz na článok 13 tohto rozhodnutia.

Článok 19

Nadobudnutie účinnosti

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

V Bruseli 10. januára 2017

Za Komisiu

predseda

Jean-Claude JUNCKER

([1]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

([2]) Rozhodnutie Komisie 2002/47/ES, ESUO, Euratom z 23. januára 2002, ktorým sa mení a dopĺňa jej rokovací poriadok (Ú. v. ES L 21, 24.1.2002, s. 23).

([3]) Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom (OLAF), ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 1073/1999 a nariadenie Rady (Euratom) č. 1074/1999 (Ú. v. EÚ L 248, 18.9.2013, s. 1).