RADA EVROPSKÉ UNIE

Brusel 12. února 2013 (13.02)
(OR. en)

6342/13

Interinstitucionální spis: 2013/0027 (COD)

TELECOM	**24**
DATAPROTECT	**14**
CYBER	**2**
MI	**104**
CODEC	**313**

NÁVRH

Odesílatel:	Komise
Ze dne:	7. února 2013
Č. dok. Komise:	COM(2013) 48 final
Předmět:	Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

Delegace naleznou v příloze návrh Komise podaný s průvodním dopisem Jordiho AYETA PUIGARNAUA, ředitele, pro Uweho CORSEPIUSE, generálního tajemníka Rady Evropské unie.

Příloha: COM(2013) 48 final

EVROPSKÁ
KOMISE

V Bruselu dne 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

{SWD(2013) 31 final}
{SWD(2013) 32 final}

DŮVODOVÁ ZPRÁVA

Cílem navrhované směrnice je zaručit vysokou společnou úroveň bezpečnosti sítí a informací. To znamená zvýšit bezpečnost Internetu a soukromých sítí a informačních systémů, na nichž je do značné míry postaveno fungování naší společnosti a hospodářství. Za tím účelem bude požadováno od členských států, aby zlepšily svou připravenost a vzájemnou spolupráci, a od provozovatelů klíčových infrastruktur, jako je energetika či doprava, klíčoví poskytovatelé služeb informační společnosti (platforem pro elektronické obchodování, sociálních sítí apod.), jakož i od orgánů veřejné správy, aby podnikli odpovídající kroky v zájmu řízení bezpečnostních rizik a oznamování případů závažných narušení bezpečnosti odpovědným vnitrostátním orgánům.

Návrh se předkládá v souvislosti se společným sdělením Komise a vysoké představitelky Evropské unie pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost. Jejím cílem strategie je zajistit bezpečné a důvěryhodné digitální prostředí a zároveň prosazovat a chránit základní práva a další základní hodnoty EU. Tento návrh představuje hlavní opatření v rámci této strategie. Další opatření strategie v této oblasti se zaměřují na zvyšování povědomí, rozvoj vnitřního trhu s produkty a službami kybernetické bezpečnosti a na podporu investic do výzkumu a vývoje. Tato opatření budou doplněna dalšími, jejichž cílem bude zintenzívnit boj proti kybernetické kriminalitě a vypracovat politiku EU pro mezinárodní kybernetickou bezpečnost.

1.1. Důvody a cíle návrhu

Bezpečnost sítí a informací je pro naši ekonomiku i společnost čím dál důležitější. Je také důležitým předpokladem pro vytvoření spolehlivého prostředí pro celosvětový obchod se službami. Informační systémy a jejich bezpečnost však může narušit například lidská chyba, přírodní událost, technické selhání nebo úmyslný útok. Tato narušení či incidenty jsou stále větší, častější a komplexnější. Z internetové veřejné konzultace na téma „Zvyšování bezpečnosti sítí a informací v EU“[1], kterou provedla Komise, vyplynulo, že 57 % respondentů mělo v uplynulém roce zkušenost s narušením bezpečnosti, které mělo vážný dopad na jejich činnost. Nedostatečná bezpečnost sítí a informací přitom může ohrozit zcela zásadní služby, jež jsou závislé na integritě sítí a informačních systémů. V důsledku pak mohou podniky přestat fungovat, může dojít ke značným finančním ztrátám v ekonomice EU a k nepříznivým dopadům na fungování společnosti.

Digitální informační systémy, zejména internet, jsou navíc jakožto komunikační nástroj bez hranic vzájemně propojené napříč členskými státy a hrají zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Výrazné narušení těchto systémů v jednom členském státě se může dotknout dalších členských států i EU jako celku. Odolnost a stabilita sítí a informačních systémů je proto základním předpokladem pro dokončení jednotného digitálního trhu a pro hladké fungování vnitřního trhu. Pravděpodobnost a četnost výskytu bezpečnostních incidentů a nemožnost zajistit účinnou ochranu rovněž podrývají důvěru veřejnosti v síťové a informační služby: například průzkum Eurobarometr o kybernetické bezpečnosti v roce 2012 zjistil, že 38 % uživatelů internetu v EU se obává, že online platby nejsou bezpečné, a kvůli obavám týkajícím se bezpečnosti změnili své chování: 18 % z nich

[1] Internetová veřejná konzultace s názvem „Zvyšování bezpečnosti sítí a informací v EU“ proběhla od 23. července do 15. října 2012.

uvedlo, že si kvůli tomu pravděpodobně nekoupí žádné zboží online a 15 % spíše nepoužije internetové bankovnictví[2].

Současná situace v EU odráží dosavadní přístup založený na čistě dobrovolné bázi, a tedy nenabízí dostatečnou ochranu před bezpečnostními incidenty a riziky napříč EU, pokud jde o sítě a informace. Stávající kapacity a mechanismy pro zajišťování bezpečnosti sítí a informací jednoduše nedokáží udržet krok s rychle se měnící povahou hrozeb a zaručit společnou vysokou úroveň ochrany ve všech členských státech.

Navzdory podniknutým iniciativám se úroveň kapacit a připravenosti v jednotlivých členských státech velmi liší a v celé EU panuje roztříštěnost různých přístupů. Jelikož jsou sítě a systémy vzájemně propojené, snižují členské státy, jejichž míra zabezpečení je nedostatečná, celkovou bezpečnost sítí a informací v EU. Tato skutečnost také brání vytváření vzájemné důvěry mezi subjekty na stejné úrovni, která je předpokladem pro spolupráci a sdílení informací. V důsledku spolu spolupracuje jen malá část členských států, jejichž kapacity jsou na vysoké úrovni.

V EU tak v současnosti neexistuje účinný mechanismus pro efektivní spolupráci a spolehlivé sdílení informací o rizicích a případech narušení bezpečnosti sítí a informací mezi členskými státy. Výsledkem mohou být nekoordinované regulatorní zásahy, nesourodé strategie a rozdílné standardy vedoucí k nedostatečné ochraně před bezpečnostními incidenty v celé EU. Mohou také vznikat překážky na vnitřním trhu a spolu s nimi náklady související s dodržováním předpisů pro podniky působící ve více než jednom členském státě.

[2] Eurobarometr 390/2012.

Konečně hráči řídící klíčovou infrastrukturu nebo nabízející služby nezbytné pro fungování naší společnosti ani nejsou odpovídajícím způsobem nuceni přijímat opatření v oblasti řízení rizik a vyměňovat si informace s příslušnými úřady. Podnikům se nedostává účinných pobídek k provádění seriózního řízení rizik, a to včetně posouzení rizik a přijímání vhodných opatření k zajištění bezpečnosti sítí a informací. Na druhé straně k odpovědným orgánům se velká část incidentů ani nedostane a přejde bez povšimnutí. Informace o incidentech jsou přitom základním předpokladem pro to, aby orgány veřejné správy mohly jednat, přijmout vhodná protiopatření a stanovit odpovídající strategické priority v oblasti bezpečnosti sítí a informací.

Podle současného právního rámce mají povinnost přijmout opatření v oblasti řízení rizik a oznamovat vážná narušení bezpečnosti sítí a informací pouze telekomunikační společnosti. Na informačních a komunikačních technologiích (ICT) však plně závisí i řada dalších odvětví, a i ta by se proto měla bezpečností sítí a informací zabývat. Mnozí poskytovatelé specifické infrastruktury a služeb jsou kvůli své značné závislosti na správně fungující síti a informačních systémech obzvlášť zranitelní. Tato další odvětví hrají zásadní roli při poskytování klíčových podpůrných služeb pro hospodářství i společnost a bezpečnost jejich systémů je pro fungování vnitřního trhu zvlášť důležitá. K těmto odvětvím patří bankovnictví, burzy cenných papírů, výroba, přenos a distribuce energie, doprava (letecká, železniční, námořní), zdravotnictví, internetové služby a veřejná správa.

Způsob, jakým se v EU přistupuje k bezpečnosti sítí a informací, je proto třeba zásadním způsobem změnit. Je nutné přijmout právní předpisy, které vytvoří rovné podmínky a odstraní současné mezery v legislativě. V zájmu odstranění těchto problémů a zvýšení bezpečnosti sítí a informací v Evropské unii jsou cíle navrhované směrnice následující:

Zaprvé, návrh vyžaduje, aby všechny členské státy zajistily alespoň minimální úroveň vnitrostátních kapacit ustavením orgánů odpovědných za bezpečnost sítí a informací, zřízením skupin pro reakci na počítačové hrozby (CERT) a přijetím národní strategie a plánu spolupráce pro bezpečnost sítí a informací.

Zadruhé, odpovědné vnitrostátní orgány by měly spolupracovat v rámci sítě umožňující bezpečnou a efektivní spolupráci včetně koordinované výměny informací, jakož i odhalování a reakci na úrovni EU. Prostřednictvím této sítě by si členské státy měly vyměňovat informace a spolupracovat na potírání bezpečnostních hrozeb a incidentů na základě evropského plánu spolupráce v oblasti bezpečnosti sítí a informací.

Zatřetí, po vzoru rámcové směrnice o elektronických komunikacích je účelem tohoto návrhu zajistit rozvoj určité kultury řízení rizik a sdílení informací mezi soukromým a veřejným sektorem. Podniky z výše uvedených konkrétních klíčových odvětví a orgány veřejné správy budou mít povinnost posuzovat rizika, jimž čelí, a přijímat odpovídající a přiměřená opatření k zajištění bezpečnosti sítí a informací. Tyto subjekty budou odpovědným orgánům povinně podávat zprávy o všech incidentech vážně ohrožujících jejich sítě a informační systémy a majících významný dopad na kontinuitu klíčových služeb a dodávek zboží.

1.2. Obecné souvislosti

Komise nastínila rostoucí důležitost bezpečnosti sítí a informací již v roce 2001 ve svém sdělení Bezpečnost sítí a informací – návrh evropského politického přístupu[3]. Po něm

[3] KOM(2001) 298.

následovalo v roce 2006 přijetí strategie pro bezpečnou informační společnost[4], jejímž cílem bylo vytvořit v Evropě kulturu bezpečnosti sítí a informací. Její hlavní body byly potvrzeny usnesením Rady[5].

Komise dále dne 30. března 2009 vydala sdělení o ochraně kritické informační infrastruktury (CIIP)[6], v němž se zaměřila na ochranu Evropy před narušením kybernetického prostoru a posílení bezpečnosti. V rámci tohoto sdělení byl vyhlášen akční plán na podporu snah členských států zajistit ochranu a odpovídající reakci, který byl poté zakotven v závěrech předsednictví z ministerské konference o ochraně kritické informační infrastruktury CIIP v Talinu v roce 2009. Dne 18. prosince 2009 pak Rada přijala usnesení o společném evropském přístupu k bezpečnosti sítí a informací[7].

Digitální agenda pro Evropu[8], přijatá v květnu 2010, a související závěry Rady[9] zdůraznily společné přesvědčení, že důvěra a bezpečnost jsou základními podmínkami pro široké rozšíření ICT, a tím i pro dosažení cílů strategie Evropa 2020 a jejího rozměru spočívajícího v „inteligentním růstu“[10]. V kapitole Digitální agendy pro Evropu nazvané „Důvěra a bezpečnost“ se zdůrazňuje, že je třeba, aby všechny zainteresované strany spojily své síly a uceleným způsobem se pomocí prevence, připravenosti a informovanosti snažily zajistit bezpečnost a odolnost infrastruktury ICT a rovněž aby vytvořily účinné a koordinovaně fungující bezpečnostní mechanismy. Zejména pak klíčové opatření č. 6 Digitální agendy pro Evropu vyzývá k opatřením zaměřeným na posílení a zajištění vysoké úrovně politiky bezpečnosti sítí a informací.

Ve svém sdělení o CIIP z března 2011 nazvaném „Dosažené výsledky a další kroky – směrem ke globální kybernetické bezpečnosti“[11] Komise bilancuje, čeho bylo od vyhlášení akčního plánu o CIIP v roce 2009 dosaženo, a dochází k závěru, že realizace plánu ukázala, že řešení otázky bezpečnosti a odolnosti na čistě vnitrostátní úrovni je nedostačující a že Evropa by měla ve svém úsilí vybudovat jednotný a společný celounijní přístup pokračovat. V rámci sdělení o CIIP z roku 2011 byla ohlášena řada opatření a Komise vyzvala členské státy, aby zřídily kapacity pro zajišťování bezpečnosti sítí a informací a přeshraniční spolupráci. Většina z těchto opatření měla být dokončena do roku 2012, dosud však realizována nebyla.

Rada Evropské unie ve svých závěrech o CIIP ze dne 27. května 2011 zdůraznila naléhavou potřebu zajistit bezpečnost ICT systémů a sítí a jejich odolnost proti jakýmkoliv možným narušením, ať už náhodným nebo úmyslným, vybudovat v celé EU kapacity zajišťující připravenost, bezpečnost a odolnost, zdokonalit technickou způsobilost, s níž by se Evropa zhostila úkolu ochrany sítí a informační infrastruktury, a upevnit spolupráci členských států pomocí mechanismů spolupráce členských států v případech narušení bezpečnosti.

1.3. Stávají unijní a mezinárodní úprava v této oblasti

Na základě nařízení (ES) č. 460/2004 Evropské společenství v roce 2004 zřídilo Evropskou agenturu pro bezpečnost sítí a informací (ENISA)[12], která měla přispět k zajištění vysokého

4 KOM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/cs/com/2006/com2006_0251cs01.pdf.
5 2007/068/01.
6 KOM(2009) 149.
7 2009/C 321/01.
8 KOM(2010) 245.
9 KOM(2010) 2020 a závěry Evropské rady ze dne 25.–26. března 2010 (EUCO 7/10).
10 Závěry Rady ze dne 31. května 2010 o Digitální agendě pro Evropu (10130/10).
11 KOM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:CS:HTML.

stupně bezpečnosti a vytvoření kultury bezpečnosti sítí a informací v EU. Dne 30. září 2010 byl přijat návrh na aktualizaci mandátu agentury[13], který v současnosti projednává Rada a Evropský parlament. Revidovaný právní rámec pro elektronické komunikace[14], platný od listopadu 2009, ukládá poskytovatelům služeb elektronické komunikace povinnosti týkající se bezpečnosti[15]. Vnitrostátní právní předpisy měly být uvedeny do souladu s těmito povinnostmi do května 2011.

Všichni hráči vystupující coby správci údajů (například banky nebo nemocnice) jsou podle právního rámce upravujícího ochranu údajů[16] povinni zavést bezpečnostní opatření na ochranu osobních údajů. Podle návrhu obecného nařízení o ochraně údajů[17] předloženého Komisí v roce 2012 by správci také měli oznamovat porušení ochrany osobních údajů vnitrostátním orgánům dozoru. To znamená, že například porušení bezpečnosti sítí a informací, které se dotkne poskytování nějaké služby, avšak nenaruší ochranu osobních údajů (např. výpadek ICT v energetické společnosti, v jehož důsledku dojde k výpadku elektrického proudu), by se oznamovat nemusel.

Podle směrnice 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu zavádí „Evropský program na ochranu kritické infrastruktury (EPCIP)“[18] obecný zastřešující přístup k ochraně klíčových infrastruktur v EU. Cíle programu EPCIP plně odpovídají tomuto návrhu a použitím směrnice by nebyla dotčena směrnice 2008/114/ES. Program EPCIP neukládá provozovatelům povinnost ohlašovat významná porušení bezpečnosti ani nezakládá mechanismy spolupráce členských států a odezvy na případy narušení.

Evropský parlament a Rada v současnosti projednávají návrh směrnice o útocích proti informačním systémům[19] vypracovaný Komisí, jehož účelem je sladit trestněprávní úpravu určitého jednání. Návrh se týká pouze trestněprávní úpravy vymezených činů a nezabývá se ani předcházením rizik a narušení bezpečnosti sítí a informací, ani reakcí na narušení bezpečnosti sítí a informací nebo zmírňováním jejich dopadů. Směrnice, která je předmětem tohoto návrhu, by se měla použít, aniž by byla dotčena směrnice o útocích proti informačním systémům.

Dne 28. března 2012 vydala Komise sdělení o zřízení Evropského centra pro boj proti kyberkriminalitě[20]. Centrum bylo zřízeno 11. ledna 2013 jako součást Evropského policejního úřadu (EUROPOL) a má fungovat jako základna boje proti kyberkriminalitě v EU. Evropské centrum pro boj proti kyberkriminalitě by mělo v rámci Evropy shromažďovat dostupné odborné poznatky o kyberkriminalitě a podporovat tak členské státy při budování kapacit, poskytovat členským státům pomoc při vyšetřování kybernetické trestné činnosti a vyjadřovat, ve spolupráci s Evropskou jednotkou pro soudní spolupráci (Eurojust), společné zájmy evropských vyšetřovatelů kyberkriminality působících v donucovacích a soudních orgánech.

---

13 KOM(2010) 521.

14 Viz http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Články 13a a 13b rámcové směrnice.

16 Směrnice 2002/58/ES ze dne 12. července 2002.

17 COM(2012) 11.

18 KOM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/cs/com/2006/com2006_0786cs01.pdf.

19 KOM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:cs:PDF.

20 COM(2012) 140, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:cs:PDF.

Evropské orgány, agentury a instituce zřídily svou vlastní skupinu pro reakci na počítačové hrozby s názvem CERT-EU.

V mezinárodním měřítku se EU zabývá kybernetickou bezpečností jak na bilaterální, tak multilaterální úrovni. Na summitu EU–USA, který se konal v roce 2010[21], byla ustavena zvláštní pracovní skupina EU a USA pro počítačovou bezpečnost a počítačovou trestnou činnost. Evropská unie se též účastní příslušných mnohostranných fór, jako je Organizace pro hospodářskou spolupráci a rozvoj (OECD), Valné shromáždění Organizace spojených národů, Mezinárodní telekomunikační unie (ITU), Organizace pro bezpečnost a spolupráci v Evropě (OBSE), Světový summit o informační společnosti (WSIS) a Fórum pro správu internetu (IGF).

2. VÝSLEDKY KONZULTACÍ SE ZÚČASTNĚNÝMI STRANAMI A POSOUZENÍ DOPADŮ

2.1. Konzultace se zúčastněnými stranami a využití výsledků odborných konzultací

Internetová veřejná konzultace s názvem „Zvyšování bezpečnosti sítí a informací v EU“ proběhla od 23. července do 15. října 2012. Komise obdržela celkem 160 vyplněných online dotazníků.
Hlavním poznatkem bylo, že zainteresované strany obecně souhlasí s potřebou zvýšit bezpečnost sítí a informací v EU. Například: 82,2 % respondentů bylo toho názoru, že vlády v EU by měly pro zajištění vysokého stupně bezpečnosti sítí a informací dělat více; 82,2 % se domnívalo, že uživatelé informačních systémů si nejsou vědomi existujících bezpečnostních hrozeb a narušení bezpečnosti sítí a informací; 66,3 % by v zásadě souhlasilo se zavedením zákonné povinnosti řízení rizik v oblasti bezpečnosti sítí a informací a 84,8 % uvedlo, že by takové povinnosti měly být stanoveny na úrovni EU. Velká část respondentů se domnívala, že povinnosti týkající se bezpečnosti sítí a informací by měly být zavedeny zejména v těchto odvětvích: bankovnictví a finance (91,1 %), energetika (89,4 %), doprava (81,7 %), zdravotnictví (89,4 %), internetové služby (89,1 %) a veřejná správa (87,5 %). Respondenti se rovněž domnívali, že pokud by byla zavedena povinnost oznamovat porušení bezpečnosti sítí a informací odpovědnému vnitrostátnímu orgánu, měla by být stanovena na úrovni EU (65,1 %), a potvrdili, že by se měla vztahovat i na orgány veřejné správy (93,5 %). Respondenti konečně také uvedli, že povinné zavedení řízení rizik v oblasti bezpečnosti sítí a informací podle nejmodernějších standardů by pro ně nepředstavovalo významné dodatečné náklady (63,4 %) a že významné dodatečné náklady by neznamenala ani povinnost oznamovat případy porušení bezpečnosti (72,3 %).

Konzultace s členskými státy proběhly v několika odpovídajících složeních Rady v rámci Evropského fóra členských států (EFMS), na konferenci o kybernetické bezpečnosti pořádané Komisí a Evropskou službou pro vnější činnost dne 6. července 2012 a na zvláštních dvoustranných jednáních svolaných na žádost jednotlivých členských států.

Rozhovory se soukromým sektorem se konaly také v rámci Evropského partnerství veřejného a soukromého sektoru pro odolnost[22] a formou bilaterálních setkání. Pokud jde o veřejný sektor, jednala Komise s Evropskou agenturou pro bezpečnost sítí a informací (ENISA) a s vládní skupinou pro reakci na počítačové hrozby (CERT) coby zástupce orgánů EU.

---

21 http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

22 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

2.2. Posouzení dopadů

Komise posoudila dopady tří alternativních politik:

Alternativa č. 1: bez opatření (základní scénář): zachování stávajícího přístupu;

Alternativa č. 2: regulatorní přístup spočívající v legislativním návrhu, kterým by se zaváděl společný evropský právní rámec pro bezpečnost sítí a informací ve vztahu ke kapacitám členských států, mechanismy spolupráce na úrovni EU a povinnosti klíčových soukromých subjektů a orgánů veřejné správy;

Alternativa č. 3: kombinovaný přístup založený na kombinaci dobrovolné iniciativy členských států, pokud jde o kapacity pro zajištění bezpečnosti sítí a informací a mechanismy spolupráce na úrovni EU, a zákonných povinností klíčových soukromých subjektů a orgánů veřejné správy.

Komise došla k závěru, že nejvýraznější pozitivní dopad by měla alternativa č. 2, neboť by významně zlepšila ochranu spotřebitelů, podniků i vlád v EU před narušováním bezpečnosti sítí a informací. Zejména by povinnosti uložené členským státům zaručovaly odpovídající připravenost na vnitrostátní úrovni a přispěly by k vytvoření vzájemné důvěry, která je předpokladem efektivní spolupráce na úrovni EU. Nastavení mechanismů spolupráce na úrovni EU prostřednictvím sítě by umožnilo předcházet přeshraničním rizikům a narušení bezpečnosti sítí a informací a reagovat na ně jednotným a koordinovaným způsobem. Zavedení povinného řízení rizik v oblasti bezpečnosti sítí a informací pro orgány veřejné správy a klíčové soukromé subjekty by bylo silným podnětem ke skutečně efektivnímu řízení rizik. Povinnost oznamovat narušení bezpečnosti sítí a informací s významným dopadem by posílila schopnost na taková narušení reagovat a zvýšila transparentnost. Kromě toho tzv. zametení před vlastním prahem by EU umožnilo větší mezinárodní dosah a dodalo na důvěryhodnosti coby partnera pro dvoustrannou i mnohostrannou spolupráci. Evropská unie by tak mohla lépe prosazovat základní práva a hodnoty EU v zahraničí.

Kvantitativní posouzení ukázalo, že alternativa č. 2 by pro členské státy neznamenala neúměrnou zátěž. Náklady pro soukromý sektor by byly rovněž nízké, neboť řada z dotčených subjektů by již měla splňovat stávající bezpečností požadavky (především povinnost správců údajů přijmout technická a organizační opatření k zajištění ochrany osobních údajů, včetně opatření v oblasti bezpečnosti sítí a informací). Rovněž byly vzaty v úvahu současné výdaje na bezpečnost v soukromém sektoru.

Tento návrh ctí zásady přiznávané především Listinou základních práv Evropské unie, zejména právo na respektování soukromého života a komunikace, ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Tato směrnice musí být provedena v souladu s těmito právy a zásadami.

3. PRÁVNÍ STRÁNKA NÁVRHU

3.1. Právní základ

Evropská unie je oprávněná přijímat opatření k vytvoření nebo zajištění fungování vnitřního trhu v souladu s příslušnými ustanoveními Smluv (článek 26 Smlouvy o fungování Evropské unie – SFEU). Podle článku 114 SFEU může EU přijímat „opatření ke *sbližování ustanovení*

právních a správních předpisů členských států, jejichž účelem je vytvoření a fungování vnitřního trhu".

Jak je uvedeno výše, sítě a informační systémy hrají zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Často jsou propojené a internet je ze své podstaty globálním nástrojem. Vzhledem k tomuto přirozenému nadnárodnímu rozměru se může narušení těchto systémů v jednom členském státě dotknout dalších členských států i celé EU. Odolnost a stabilita sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu.

Evropský zákonodárce již uznal, že v zájmu rozvoje vnitřního trhu je nutné sladit předpisy týkající se bezpečnosti sítí a informací, což se týkalo především nařízení (ES) č. 460/2004 o zřízení agentury ENISA[23], které vychází z článku 114 SFEU.

Vlivem nesrovnalostí vyplývajících z nestejných vnitrostátních kapacit pro zajištění bezpečnosti sítí a informací, politik a úrovně ochrany v jednotlivých členských státech vznikly na vnitřním trhu bariéry, a tím i důvod k zásahu ze strany EU.

3.2. Subsidiarita

Odůvodněnost zásahu EU v oblasti bezpečnosti sítí a informací je dána zásadou subsidiarity.

Zaprvé, ve vztahu k přeshraniční povaze bezpečnosti sítí a informací by absence zásahu ze strany EU znamenala, že jednotlivé členské státy budou jednat samostatně a bez ohledu na vzájemnou provázanost evropských sítí a informačních systémů. Odpovídající míra koordinace mezi členskými státy by přitom zajistila, aby rizika týkající se bezpečnosti sítí a informací mohla být efektivně řízena na přeshraniční úrovni, na níž vznikají. Rozdílné předpisy o bezpečnosti sítí a informací představují bariéru pro podniky, které chtějí působit v několika zemích, i pro dosažení globálních úspor z rozsahu.

Zadruhé, k vytvoření rovných podmínek a odstranění mezer v legislativě je třeba zavést právní povinnosti na úrovni EU. Přístup založený čistě na dobrovolnosti vedl k tomu, že spolu spolupracuje jen malá část členských států, které mají kapacity na vysoké úrovni. Aby se mohly zapojit všechny členské státy, musí být zajištěna požadovaná minimální úroveň kapacit každého z nich. Opatření přijatá v oblasti bezpečnosti sítí a informací jednotlivými vládami musí být jednotná a koordinovaná, aby zabraňovala vzniku incidentů týkajících se bezpečnosti sítí a informací a minimalizovala jejich dopady. Spolupráce Komise a odpovědných orgánů založená na výměně osvědčených postupů a zapojení agentury ENISA v rámci sítě usnadní jednotné provádění směrnice napříč EU. Kromě toho společný postup ve věci politiky bezpečnosti sítí a informací může velmi pozitivně ovlivnit ochranu základních práv a především práva na ochranu osobních údajů a soukromí. Společným postupem na úrovni EU by se tak zvýšila účinnost stávajících vnitrostátních politik a usnadnil jejich rozvoj.

Navrhovaná opatření jsou odůvodněná rovněž z hlediska proporcionality. Povinnosti členských států jsou nastavené na nejnižší možné úrovni nezbytné k dosažení odpovídající připravenosti a k zajištění spolupráce založené na důvěře. Kromě toho tak členské státy mohou řádně zohlednit svá vnitrostátní specifika a společné zásady EU jsou uplatňovány přiměřeným způsobem. Díky širokému rozsahu působnosti bude moci každý členský stát provádět směrnici s ohledem na skutečná rizika, jimž čelí a jež uvedl ve své národní strategii

[23] Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací (Úř. věst. L 77 13.3.2004, s. 1).

pro bezpečnost sítí a informací. Povinnost zavést systém řízení rizik se vztahuje pouze na klíčové subjekty a vyžaduje opatření úměrná daným rizikům. Skutečnost, že je důležité u těchto klíčových subjektů zajistit bezpečnost, vyzdvihla veřejná konzultace. Oznamovací povinnost by se týkala pouze incidentů s významným dopadem. Jak je uvedeno výše, daná opatření by nepřinesla nepřiměřené náklady, neboť řadě těchto subjektů coby správcům údajů ukládá povinnost zajistit ochranu osobních údajů již současná legislativa o ochraně dat.

Aby se zabránilo nepřiměřenému zatížení malých provozovatelů a především malých a středních podniků, jsou povinnosti přiměřené rizikům, jež dotčené sítě a informační systémy přinášejí, a neměly by se vztahovat na mikropodniky. Rizika budou identifikována v prvé řadě subjekty, na něž se tyto povinnosti vztahují a jež rozhodnou, jaká opatření ke zmenšení daných rizik budou přijata.

S ohledem na přeshraniční charakter rizik a incidentů v oblasti bezpečnosti sítí a informací lze uvedených cílů snáze dosáhnout na úrovni EU než jednotlivých členských států. Unie proto může přijmout opatření v souladu se zásadou subsidiarity, jak stanoví článek 5 Smlouvy o Evropské unii. Navrhovaná směrnice zároveň v souladu se zásadou proporcionality nepřekračuje rámec toho, co je nezbytné k dosažení stanovených cílů.

K dosažení uvedených cílů je třeba zmocnit Komisi k přijetí aktů v přenesené pravomoci v souladu s článkem 290 SFEU, a to pro účely doplnění nebo pozměnění některých nikoliv podstatných prvků základního právního aktu. Cílem návrhu Komise je také podpořit uplatňování proporcionality při zavádění povinností uložených soukromým a veřejným subjektům

Za účelem zajištění jednotných podmínek k provedení tohoto základního aktu by Komise měla být oprávněna přijmout prováděcí akty podle článku 291 SFEU.

S ohledem především na široký rozsah působnosti navrhované směrnice, na skutečnost, že se dotýká silně regulovaných odvětví, a na právní povinnosti vyplývající z kapitoly IV směrnice by k oznámení o prováděcích opatřeních měly být připojeny informativní dokumenty. Členské státy se v souladu se Společným politickým prohlášením členských států a Komise o informativních dokumentech ze dne 28. září 2011 zavázaly, že v odůvodněných případech doplní oznámení o opatřeních přijatých za účelem provedení směrnice do vnitrostátního práva o jeden či více dokumentů, které objasňují vztah mezi jednotlivými složkami směrnice a příslušnými částmi vnitrostátních prováděcích nástrojů. V případě této směrnice považuje zákonodárce předložení těchto dokumentů za odůvodněné.

4. ROZPOČTOVÉ DŮSLEDKY

Spolupráce a výměna informací mezi členskými státy by se měla opírat o bezpečnou infrastrukturu. Návrh bude mít důsledky pro rozpočet EU, pouze pokud se členské státy rozhodnou přizpůsobit stávající infrastrukturu (např. sTESTA) a pověří Komisi provedením takového opatření v rámci VFR 2014–2020. Jednorázový náklad se odhaduje na 1 250 000 EUR a byl by hrazen z rozpočtu EU, rozpočtové položky 09.03.02 (na podporu propojení a interoperability vnitrostátních veřejných online služeb a přístupu k takovým sítím – kapitola 09.03, nástroj pro propojení Evropy – telekomunikační sítě), za podmínky, že bude v rámci uvedeného nástroje k dispozici dostatek prostředků. Členské státy se také mohou rozhodnout, že buď ponesou společně jednorázové náklady na přizpůsobení stávající infrastruktury, nebo zvolí zřízení nové infrastruktury a ponesou s tím spojené náklady, jejichž výše se odhaduje na přibližně 10 miliónů EUR ročně.

2013/0027 (COD)

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 114 této smlouvy,

s ohledem na návrh Evropské komise,

po postoupení návrhu legislativního aktu vnitrostátním parlamentům,

s ohledem na stanovisko Evropského hospodářského a sociálního výboru[1],

po konzultaci s evropským inspektorem ochrany údajů,

v souladu s řádným legislativním postupem,

vzhledem k těmto důvodům:

(1) Sítě a informační systémy a služby hrají ve společnosti zcela zásadní roli. Jejich spolehlivost a bezpečnost je nezbytná pro hospodářskou činnost a sociální blahobyt a především pro fungování vnitřního trhu.

(2) Rozsah a četnost výskytu úmyslných či náhodných bezpečnostních incidentů roste a představuje velkou hrozbu pro fungování sítí a informačních systémů. Tyto incidenty mohou bránit ve výkonu hospodářské činnosti, způsobovat významné finanční ztráty, narušovat důvěru uživatelů a způsobovat značnou újmu hospodářství Unie.

(3) Jakožto komunikační nástroj bez hranic hrají digitální informační systémy a především internet zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Vzhledem k tomuto nadnárodnímu rozměru se může narušení těchto systémů v jednom členském státě dotknout dalších členských států i celé EU. Odolnost a stabilita sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu.

(4) Na úrovni Unie by měl být zřízen mechanismus spolupráce, který by umožnil výměnu informací a koordinované odhalování a reakci v záležitostech týkajících se bezpečnosti sítí a informací. Aby byl tento mechanismus účinný a všeobecně přístupný, musí mít všechny členské státy alespoň minimální kapacity a strategii, které zajistí vysoký stupeň bezpečnosti sítí a informací na jejich území. Minimální požadavky na bezpečnost by se měly vztahovat rovněž na orgány veřejné správy a provozovatele

[1] Úř. věst. C […], […], s. […].

kritické informační infrastruktury, aby byla podpořena kultura řízení rizik a zaručeno oznamování nejzávažnějších incidentů.

(5) Tato směrnice by se měla vztahovat na všechny sítě a informační systémy, aby byly pokryty všechny relevantní incidenty a rizika. Povinnosti orgánů veřejné správy a hospodářských subjektů by se však neměly vztahovat na podniky poskytující veřejné komunikační sítě nebo veřejně přístupné služby elektronických komunikací ve smyslu směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice)[2], na něž se vztahují zvláštní požadavky na bezpečnost a integritu podle článku 13a uvedené směrnice, ani na poskytovatele důvěryhodných služeb.

(6) Stávající kapacity nejsou pro zajištění vysokého stupně bezpečnosti sítí a informací v Unii dostačující. Míra připravenosti jednotlivých členských států se velmi liší, což vede v rámci Unie k roztříštěnosti přístupů. Důsledkem je různá úroveň ochrany spotřebitelů a podniků a zhoršená celková úroveň bezpečnosti sítí a informací v Unii. Kvůli neexistenci společných minimálních požadavků, jež by byly stanoveny pro veřejnou správu a hospodářské subjekty, je pak nemožné nastavit komplexní a účinný mechanismus spolupráce na úrovni Unie.

(7) Účinná odezva na výzvy, jež přináší bezpečnost sítí a informačních systémů, proto vyžaduje komplexní přístup na úrovni Unie, jenž se vztahuje na společné minimální požadavky, pokud jde o plánování a budování kapacit, výměnu informací a koordinaci opatření, jakož i společné minimální bezpečnostní požadavky, jež se týkají všech dotčených hospodářských subjektů a orgánů veřejné správy.

(8) Ustanoveními této směrnice by neměla být dotčena možnost jednotlivých členských států přijmout nezbytná opatření, aby tak zajistily ochranu svých zásadních bezpečnostních zájmů, ochranu veřejného pořádku a veřejné bezpečnosti a umožnily vyšetřování, odhalování a stíhání trestných činů . Podle článku 346 SFEU není žádný členský stát povinen poskytovat informace, jejichž zpřístupnění považuje za neslučitelné se svými základními bezpečnostními zájmy.

(9) V zájmu dosažení a udržení vysoké společné úrovně bezpečnosti sítí a informačních systémů by každý členský stát měl mít národní strategii pro bezpečnost sítí a informací, která by definovala strategické cíle a konkrétní opatření, jež je třeba v rámci této politiky přijmout. Na vnitrostátní úrovni je třeba vypracovat plány spolupráce v oblasti bezpečnosti sítí a informací, jež budou splňovat základní požadavky a umožní dosáhnout takové úrovně reakce daných kapacit, která zaručí efektivní spolupráci v případě, že dojde k bezpečnostnímu incidentu, a to jak na vnitrostátní úrovni, tak na úrovni Unie.

(10) Za účelem účinného provedení předpisů přijatých na základě této směrnice by měl být v každém členském státě zřízen nebo určen orgán, který bude odpovídat za koordinaci v oblasti bezpečnosti sítí a informací a fungovat jako ústřední bod přeshraniční spolupráce na úrovni EU. Tyto orgány by měly disponovat odpovídajícími technickými, finančními a lidskými zdroji, které zaručí, že budou moci účinně plnit úkoly jim svěřené a naplnit tak cíle této směrnice.

---

[2] Úř. věst. L 108, 24.4.2002, s. 33.

(11) Všechny členské státy by měly být náležitě vybaveny jak technicky, tak organizačně, aby mohly předcházet vzniku incidentů a rizik spojených se sítěmi a informačními systémy, odhalovat je, reagovat na ně a zmírňovat je. Ve všech členských státech by proto měly být zřízeny dobře fungující skupiny pro reakci na počítačové hrozby splňující základní požadavky, aby byly zaručeny efektivní a kompatibilní kapacity pro řešení incidentů a rizik a zajištěna účinná spolupráce na úrovni Unie.

(12) Členské státy a Komise by měly využít značného pokroku, kterého dosáhlo Evropské fórum členských států (EFMS) v podporování diskuzí a výměny informací o osvědčených postupech v této oblasti politiky, včetně vypracování zásad spolupráce v případě evropské počítačové krize, a vytvořit síť na podporu vzájemné spolupráce a stálé komunikace. Tento mechanismus pro bezpečnou a efektivní spolupráci by měl umožnit strukturovanou a koordinovanou výměnu informací a odhalování a reakci na úrovni Unie.

(13) Evropská agentura pro bezpečnost sítí a informací (ENISA) by měla členským státům a Komisi pomoci poskytnutím svých odborných znalostí a doporučení a umožněním vzájemné výměny osvědčených postupů. Především Komise by při uplatňování této směrnice měla agenturu ENISA konzultovat. V zájmu účinného a včasného poskytování informací členským státům a Komisi by v rámci sítě pro spolupráci měla být vydávána včasná varování o vzniku incidentů a rizik. Síť pro spolupráci by rovněž měla sloužit jako nástroj pro vzájemnou výměnu osvědčených postupů, pomáhat svým členům při budování kapacit, řídit organizaci vzájemných hodnocení a plnění úkolů souvisejících s bezpečností sítí a informací, aby se v členských státech vybudovaly kapacity a příslušná znalostní základna.

(14) Měla by být vytvořena infrastruktura pro bezpečné sdílení informací, která umožní výměnu citlivých a důvěrných informací v rámci sítě pro spolupráci. Přístup k důvěrným informacím z jiného členského státu by měl být členskému státu poskytnut, pouze pokud prokáže, že jeho technické, finanční a lidské zdroje a postupy, jakož i komunikační infrastruktura, zaručují jeho účinné a bezpečné zapojení do sítě, aniž by tím byla dotčena jeho povinnost ohlašovat uvnitř sítě pro spolupráci incidenty a rizika unijních rozměrů.

(15) Jelikož většinu sítí a informačních systémů provozují soukromé subjekty, je naprosto nezbytná spolupráce mezi soukromým a veřejným sektorem. Hospodářské subjekty by měly být podněcovány k vytváření svých vlastních neoficiálních mechanismů spolupráce k zajištění bezpečnosti sítí a informací. Měly by rovněž spolupracovat s veřejným sektorem a sdílet informace a osvědčené postupy výměnou za provozní podporu v případě vzniku incidentu.

(16) V zájmu zajištění transparentnosti a řádného informování občanů a hospodářských subjektů v EU by odpovědné orgány měly zřídit společné internetové stránky, na nichž by zveřejňovaly informace o incidentech a rizicích, které nemají důvěrný charakter.

(17) Pokud se v souladu s unijními a vnitrostátními předpisy o obchodním tajemství jedná o důvěrné informace, musí být jejich důvěrnost při provádění činností a plnění cílů stanovených touto směrnicí zachována.

(18) Na základě především vnitrostátních zkušeností s řešením krizí a ve spolupráci s agenturou ENISA by členské státy měly vypracovat evropský plán spolupráce

v oblasti bezpečnosti sítí a informací, který by vymezil mechanismy spolupráce pro potírání rizik a incidentů. Tento plán by měl být řádně zohledněn při práci s včasnými varováními v síti pro spolupráci.

(19) Oznámení o vydání včasného varování v této síti by mělo být vyžadováno pouze v případě, že rozsah a závažnost daného incidentu nebo rizika jsou nebo by se mohly stát natolik významnými, že je nutné informovat nebo koordinovaně zareagovat na úrovni Unie. Včasná varování by se proto měla omezit na skutečné nebo hrozící incidenty či rizika, jež rychle rostou, přesahují národní reakční kapacitu nebo postihují více než jeden členský stát. Pro účely řádného vyhodnocení daného rizika nebo incidentu by měly být všechny informace, které jsou relevantní pro jeho posouzení, sděleny prostřednictvím sítě pro spolupráci.

(20) Jakmile obdrží a vyhodnotí včasné varování, měly by se odpovědné orgány dohodnout na koordinované reakci v souladu s evropským plánem spolupráce v oblasti bezpečnosti sítí a informací. Odpovědné orgány a Komise by měly být informovány o tom, jaká opatření byla na základě koordinované reakce na vnitrostátní úrovni přijata.

(21) Vzhledem ke globální povaze problémů bezpečnosti sítí a informací je nutná užší mezinárodní spolupráce zaměřená na zdokonalení bezpečnostních norem a výměnu informací a prosazování společného a komplexního přístupu k otázkám bezpečnosti sítí a informací.

(22) Odpovědnost za zajištění bezpečnosti sítí a informací leží do značné míry na orgánech veřejné správy a hospodářských subjektech. Stanovením vhodných právních povinností a pomocí dobrovolných postupů uplatňovaných v tomto odvětví by měla být prosazována a vytvářena kultura řízení rizik, včetně posuzování rizik a zavádění bezpečnostních opatření úměrných hrozícím rizikům. Pro účinné fungování sítě pro spolupráci a účinnou spolupráci všech členských států je zásadní rovněž vytvoření rovných podmínek.

(23) Podle směrnice 2002/21/ES mají podniky poskytující veřejné komunikační sítě nebo veřejně přístupné služby elektronických komunikací povinnost přijmout vhodná opatření k zabezpečení vlastní integrity a bezpečnosti. Směrnice také zavádí oznamovací povinnost ve vztahu k porušení bezpečnosti a ztrátě integrity. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)[3] ukládá poskytovateli veřejně přístupné služby elektronických komunikací povinnost přijmout odpovídající technická a organizační opatření k zajištění bezpečnosti svých služeb.

(24) Uvedené povinnosti by měly platit i mimo odvětví elektronických komunikací a vztahovat se na klíčové poskytovatele služeb informační společnosti, jak je stanoveno ve směrnici Evropského Parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti[4], jež podporují následné služby informační společnosti či online aktivity, jako jsou například platformy elektronického obchodu, internetové platební brány, sociální sítě, vyhledavače, služby cloud computingu a obchody s aplikacemi. Narušení těchto služeb vytvářejících informační společnost

[3] Úř. věst. L 201, 31.7.2002, s. 37.
[4] Úř. věst. L 204, 21.7.1998, s. 37.

brání poskytování dalších služeb informační společnosti, které jsou na nich jakožto na klíčových vstupech závislé. Vývojáři softwaru a výrobci hardwaru nejsou poskytovateli služeb informační společnosti, a jsou proto z této povinnosti vyňati. Uvedené povinnosti by se rovněž měly vztahovat na orgány veřejné správy a provozovatele kritických infrastruktur, které jsou silně závislé na informačních a komunikačních technologiích a mají zásadní význam pro zachování životně důležitých ekonomických a společenských funkcí, jako elektřina a plyn, doprava, úvěrové instituce, burzy cenných papírů a zdravotnictví. Narušení těchto sítí a informačních systémů by zasáhlo vnitřní trh.

(25) Technická a organizační opatření, jež by měly přijímat orgány veřejné správy a hospodářské subjekty, by neměla vyžadovat, aby byla konkrétní komerční informační a komunikační technologie navržena, vyvinuta nebo vyrobena určitým konkrétním způsobem.

(26) Orgány veřejné správy a hospodářské subjekty by měly zajistit bezpečnost jimi řízených sítí a informačních systémů. K těm by patřily především soukromé sítě a systémy buď řízené jejich vlastními odděleními IT, nebo takové, jejichž bezpečnost zajišťuje externí dodavatel. Povinnosti týkající se zabezpečení a oznamování by měly platit pro příslušné orgány veřejné správy a hospodářské subjekty bez ohledu na to, zda své sítě a informační systémy spravují interně nebo s pomocí externího dodavatele.

(27) Povinnosti by měly být úměrné rizikům, jež daná síť nebo informační systém představuje, aby na malé provozovatele a uživatele nebyla uvalena nepřiměřená finanční a administrativní zátěž, a to s ohledem na stávající stupeň technického vývoje takových opatření. Tyto povinnosti by se neměly týkat mikropodniků.

(28) Odpovědné orgány by měly věnovat náležitou péči zachování neformálních a důvěryhodných informačních kanálů pro sdílení informací mezi hospodářskými subjekty a mezi soukromým a veřejným sektorem. Zveřejňování incidentů oznámených odpovědným orgánům by mělo být přiměřené zájmu veřejnosti na informacích o hrozbách, jež by mohly poškodit dobrou pověst či obchodní zájmy orgánů veřejné správy a hospodářských subjektů, které incidenty ohlašují. Při zavádění ohlašovací povinnosti by odpovědné orgány měly věnovat pozornost především skutečnosti, že informace o zranitelnosti produktu musí až do zjednání odpovídající nápravy v oblasti bezpečnosti zůstat přísně důvěrné.

(29) Odpovědné orgány by měly mít k dispozici potřebné prostředky k výkonu svých povinností, včetně pravomoci získat od hospodářských subjektů a orgánů veřejné správy dostatek informací, aby mohly posoudit míru bezpečnosti sítí a informačních systémů, jakož i spolehlivých a úplných dat týkajících se skutečných bezpečnostních incidentů, jež měly dopad na provoz sítí a informačních systémů.

(30) Na pozadí mnoha bezpečnostních incidentů je často trestná činnost. Trestněprávní povahu incidentů lze usuzovat, i pokud důkazy o ní nejsou od začátku dostatečně jasné. V tomto kontextu by měla být součástí účinné a komplexní reakce na hrozbu bezpečnostního incidentu odpovídající spolupráce mezi odpovědnými a donucovacími orgány. Prosazování zabezpečeného, bezpečného a odolnějšího prostředí pak vyžaduje především systematické oznamování incidentů, u nichž panuje podezření, že mají povahu závažného trestného činu, donucovacím orgánům. To, zda mají incidenty

povahu závažného trestného činu, by mělo být posuzováno ve světle předpisů EU o kyberkriminalitě.

(31) V důsledku incidentů je v mnoha případech ohrožena ochrana osobních údajů. V tomto ohledu by odpovědné orgány a úřady pro ochranu údajů měly spolupracovat a vyměňovat si informace o všech významných skutečnostech, aby zabránily porušení ochrany osobních údajů, k němuž v důsledku incidentů dochází. Členské státy by měly povinnost oznamovat bezpečnostní incidenty zavádět tak, aby v případě, že je incident zároveň porušením ochrany osobních údajů podle nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů[5], byla administrativní zátěž minimální. Agentura ENISA, ve spolupráci s odpovědnými orgány a úřady pro ochranu údajů, by mohla přispět vytvořením mechanismů a vzorových formulářů pro výměnu informací, aby se pro oznamování nemusely používat dva formuláře. Tento jednotný oznamovací formulář by usnadnil oznamování incidentů, kterými zároveň dochází k porušení ochrany osobních údajů, a zmírnil tak administrativní zátěž pro podniky a orgány veřejné správy.

(32) Standardizace bezpečnostních požadavků vychází z potřeb trhu. V zájmu zajištění jednotného uplatňování bezpečnostních norem by členské státy měly podporovat dodržování či soulad s určitými normami, tak aby byla zaručena vysoká míra bezpečnosti na úrovni Unie. Za tímto účelem může být nutné vypracovat jednotné normy, které by měly být v souladu s nařízením Evropského parlamentu a Rady (EU) č. 1025/2012 ze dne 25. října 2012 o evropské normalizaci, změně směrnic Rady 89/686/EHS a 93/15/EHS a směrnic Evropského parlamentu a Rady 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES a 2009/105/ES, a kterým se ruší rozhodnutí Rady 87/95/EHS a rozhodnutí Evropského parlamentu a Rady č. 1673/2006/ES[6].

(33) Komise by ustanovení této směrnice měla pravidelně přezkoumávat, zejména s ohledem na stanovení nutnosti změn zohledňujících měnící se technologické nebo tržní podmínky.

(34) Aby mohla síť pro spolupráci řádně fungovat, měla by být na Komisi v souladu s článkem 290 Smlouvy o fungování Evropské unie přenesena pravomoc přijímat akty, pokud jde o stanovení kritérií, jež by měly členské státy splňovat, aby byly oprávněny používat bezpečný systém pro sdílení informací, o další upřesnění skutečností, jež mají být spouštěčem včasného varování, a o vymezení okolností, za nichž jsou hospodářské subjekty a orgány veřejné správy povinny oznámit, že došlo k bezpečnostnímu incidentu.

(35) Je obzvláště důležité, aby Komise v rámci přípravné činnosti vedla odpovídající konzultace, a to i na odborné úrovni. Při přípravě a vypracování aktů v přenesené pravomoci by Komise měla zajistit, aby byly příslušné dokumenty předávány současně, včas a vhodným způsobem Evropskému parlamentu a Radě.

(36) Za účelem zajištění jednotných podmínek k provedení této směrnice by měly být Komisi svěřeny prováděcí pravomoci, pokud jde o spolupráci odpovědných orgánů a Komise v rámci sítě pro spolupráci, přístup k bezpečnému systému pro sdílení

[5] SEC(2012) 72 final.

[6] Úř. věst. L 316, 14.11.2012, s. 12.

informací, evropský plán spolupráce v oblasti bezpečnosti sítí a informací, formu a postupy platné pro informování veřejnosti o incidentech a normy a/nebo technické specifikace týkající se bezpečnosti sítí a informací. Tyto pravomoci by měly být vykonávány v souladu s nařízením Evropského parlamentu a Rady (EU) č. 182/2011 ze dne 16. února 2011, kterým se stanoví pravidla a obecné zásady způsobu, jakým členské státy kontrolují Komisi při výkonu prováděcích pravomocí[7].

(37) Při uplatňování této směrnice by Komise měla vhodným způsobem úzce spolupracovat s příslušnými odvětvovými výbory a orgány zřízenými na úrovni EU, zejména v oblasti energetiky, dopravy, bankovnictví a zdravotnictví.

(38) Informace, které odpovědný orgán v souladu s právními předpisy Unie a vnitrostátními právními předpisy o obchodním tajemství považuje za důvěrné, by měly být vyměňovány s Komisí a jinými odpovědnými orgány pouze tehdy, pokud je taková výměna nezbytně nutná pro použití ustanovení této směrnice. Vyměňované informace by se měly omezovat na informace, které jsou relevantní a přiměřené účelu takové výměny.

(39) V rámci výměny informací o rizicích a incidentech prostřednictvím sítě pro spolupráci a dodržování povinnosti oznamovat incidenty odpovědným vnitrostátním orgánům může být potřeba zpracovat osobní údaje. Toto zpracování osobních údajů je nutné k tomu, aby byly splněny cíle obecného zájmu, které sleduje tato směrnice, a je proto v souladu s článkem 7 směrnice 95/46/ES oprávněné. Ve vztahu k těmto oprávněným cílům nepředstavuje nepřiměřený ani nepřípustný zásah do samé podstaty práva na ochranu osobních údajů zaručovaného článkem 8 Listiny základních práv. Při uplatňování této směrnice by se podle potřeby mělo použít nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise[8]. V případech, kdy osobní údaje zpracovávají orgány a instituce Unie, mělo by být takové zpracování pro účely provedení této směrnice v souladu s nařízením Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

(40) Protože cíle této směrnice, totiž zajištění vysoké úrovně bezpečnosti sítí a informací v Unii, nelze uspokojivě dosáhnout na úrovni členských států a z důvodu účinku této směrnice jej lze lépe dosáhnout na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v uvedeném článku nepřekračuje tato směrnice rámec toho, co je nezbytné pro dosažení uvedených cílů.

(41) Tato směrnice respektuje základní práva a ctí zásady přiznávané především Listinou základních práv Evropské unie, zejména právo na ochranu soukromého života a komunikace, ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces. Tato směrnice musí být provedena v souladu s těmito právy a zásadami,

---

[7] Úř. věst. L 55, 28.2.2011, s. 13.

[8] Úř. věst. L 145, 31.5.2001, s. 43.

PŘIJALY TUTO SMĚRNICI:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Předmět a oblast působnosti

1. Tato směrnice stanoví opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.

2. Za tím účelem tato směrnice:

a) stanoví povinnosti všech členských států týkající se prevence a řešení rizik a bezpečnostních incidentů postihujících sítě a informační systémy a reakce na ně;

b) vytváří mechanismus spolupráce mezi členskými státy, který má zajistit jednotné uplatňování této směrnice v Unii a v případě potřeby koordinované a účinné řešení rizik a bezpečnostních incidentů postihujících sítě a informační systémy a reakci na ně;

c) stanoví bezpečnostní požadavky pro hospodářské subjekty a orgány veřejné správy.

3. Bezpečnostní požadavky, které stanovuje článek 14, se nevztahují na podniky poskytující veřejné komunikační sítě nebo veřejně přístupné služby elektronických komunikací ve smyslu směrnice 2002/21/ES, na něž se vztahují zvláštní požadavky na bezpečnost a integritu podle článků 13a a 13b uvedené směrnice, ani na poskytovatele důvěryhodných služeb.

4. Touto směrnicí nejsou dotčeny právní předpisy EU o kyberkriminalitě ani směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu[9].

5. Touto směrnicí rovněž není dotčena směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů[10], směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ani nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů[11].

6. Při sdílení informací v rámci sítě pro spolupráci podle kapitoly III a oznamování bezpečnostních incidentů týkajících se sítí a informací podle článku 14 může být nutné zpracování osobních údajů. Toto zpracování osobních údajů, jež je nutné ke splnění cílů obecného zájmu, které sleduje tato směrnice, musí v souladu s článkem 7

[9] Úř. věst. L 345, 23.12.2008, s. 75.
[10] Úř. věst. L 281, 23.11.1995, s. 31.
[11] SEC(2012) 72 final.

směrnice 95/46/ES a směrnicí 2002/58/ES, jak jsou provedeny do vnitrostátního práva, schválit příslušný členský stát.

Článek 2

Minimální harmonizace

Členské státy mohou přijmout či zachovat v platnosti ustanovení zajišťující vyšší míru bezpečnosti, aniž by tím byly dotčeny jejich povinnosti stanovené právními předpisy Unie.

Článek 3

Definice

Pro účely této směrnice se rozumí:

1) „sítí a informačními systémy“:

   a) síť elektronických komunikací ve smyslu směrnice 2002/21/ES,

   b) jakýkoli přístroj nebo skupina vzájemně propojených nebo přidružených přístrojů, z nichž jeden nebo více provádí na základě programu automatické zpracování počítačových dat, jakož i

   c) počítačová data prvky uvedenými pod písmeny a) a b) uložená, zpracovaná, opětovně vyhledaná nebo přenesená za účelem jejich provozu, použití, ochrany a údržby;

2) „bezpečností“ schopnost sítě a informačního systému odolávat na určitém stupni spolehlivosti náhodným či svévolným zásahům, které narušují dostupnost, pravost, integritu a důvěrnost uložených nebo přenášených dat nebo souvisejících služeb, které tato síť nebo informační systém nabízí nebo které jsou jejich prostřednictvím přístupné;

3) „rizikem“ jakákoliv okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost;

4) „incidentem“ jakákoliv okolnost nebo událost, která má reálný negativní dopad na bezpečnost;

5) „službou informační společnosti“ služba ve smyslu čl. 1 bodu 2 směrnice 98/34/ES;

6) „plánem spolupráce v oblasti bezpečnosti sítí a informací“ plán tvořící rámec pro organizační pravomoci, odpovědnosti a postupy, jejichž cílem je udržení, případně obnovení provozu sítí a informačních systémů v případě, že jim hrozí riziko nebo došlo k bezpečnostními incidentu;

7) „řešením bezpečnostního incidentu“ veškeré postupy, které pomáhají incident, resp. narušení bezpečnosti, analyzovat, zamezit jeho šíření a reagovat na něj;

8) „hospodářským subjektem“:

a) poskytovatel služeb informační společnosti, na nichž závisí poskytování dalších služeb informační společnosti, jejichž demonstrativní výčet je uveden v příloze II;

b) provozovatel kritické infrastruktury, která má zásadní význam pro zachování životně důležitých ekonomických a společenských činností v oblasti energetiky, dopravy, bankovnictví, obchodování s cennými papíry a zdravotnictví, jejichž demonstrativní výčet je uveden v příloze II.

9) „normou“ norma, jak je uvedená v nařízení (EU) č. 1025/2012;

10) „specifikací“ specifikace, jak je uvedená v nařízení (EU) č. 1025/2012;

11) „poskytovatelem důvěryhodné služby“ se rozumí fyzická nebo právnická osoba, která poskytuje jakoukoli elektronickou službu spočívající ve vytváření, ověřování, potvrzování, zpracovávání a uchovávání elektronických podpisů, elektronických značek, elektronických časových razítek, elektronických dokumentů, v elektronickém doručování, ověřování webových stránek a elektronických certifikátů, včetně certifikátů pro elektronické podpisy a pro elektronické značky.

KAPITOLA II

NÁRODNÍ RÁMCE PRO BEZPEČNOST SÍTÍ A INFORMACÍ

Článek 4

Zásada

Členské státy v souladu s touto směrnicí zajistí vysokou míru bezpečnosti sítě a informačních systémů na svých územích.

Článek 5

Národní strategie a národní plán spolupráce pro bezpečnost sítí a informací

1. Každý členský stát přijme národní strategii pro bezpečnost sítí a informací, která vymezí strategické cíle a zákonná opatření k dosažení a udržení vysoké úrovně bezpečnosti sítí a informací. Předmětem národní strategie pro bezpečnost sítí a informací budou především následující cíle a opatření:

a) Stanovení cílů a priorit strategie na základě aktuální analýzy rizik a incidentů;

b) Řídící rámec pro naplnění cílů a priorit strategie, včetně jasně vymezených pravomocí a odpovědnosti vládních orgánů a dalších relevantních subjektů;

c) Stanovení obecných opatření týkajících se připravenosti, reakce a obnovy, včetně mechanismů spolupráce soukromého a veřejného sektoru;

d) Určení vzdělávacích, informačních a školicích programů;

e) Plány výzkumu a vývoje a způsoby, jakými budou tyto plány odrážet stanovené priority.

2. Součástí národní strategie pro bezpečnost sítí a informací bude národní plán spolupráce pro bezpečnost sítí a informací, který bude obsahovat či splňovat alespoň následující požadavky:

a) Plán posouzení rizik pro odhalení rizik a posouzení dopadů možných incidentů;

b) Vymezení pravomocí a odpovědnosti různých stran zapojených do realizace plánu;

c) Vymezení postupů spolupráce a komunikace, které zajistí prevenci, odhalení, reakci, nápravu a obnovu a které budou přizpůsobeny stupni vyhlášené pohotovosti;

d) Harmonogram bezpečnostních cvičení a školení, jejichž cílem bude zdokonalit, prověřit a otestovat tento plán. Získané poznatky budou zdokumentovány a promítnuty do aktualizovaných verzí tohoto plánu.

3. Národní strategie a národní plán spolupráce pro bezpečnost sítí a informací budou sděleny Komisi do jednoho měsíce od přijetí.

Článek 6

Vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů

1. Každý členský stát jmenuje vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů (dále jen „odpovědný orgán“).

2. Odpovědné orgány budou vykonávat dohled nad uplatňováním této směrnice na vnitrostátní úrovni a přispívat k jejímu jednotnému uplatňování na úrovni Unie.

3. Členské státy zajistí, aby tyto orgány měly k dispozici odpovídající technické, finanční a lidské zdroje k účinnému plnění svěřených úkolů a tím k naplnění cílů této směrnice. Členské státy zajistí, aby odpovědné orgány vzájemně účinně a bezpečně spolupracovaly prostřednictvím sítě uvedené v článku 8.

4. Členské státy zajistí, aby odpovědné orgány dostávaly od orgánů veřejné správy a hospodářských subjektů oznámení o incidentech, jak je uvedeno v čl. 14 odst. 2, a aby jim byly uděleny prováděcí a donucovací pravomoci uvedené v článku 15.

5. Odpovědné orgány budou podle potřeby konzultovat příslušné vnitrostátní donucovací orgány a úřady pro ochranu údajů a spolupracovat s nimi.

6. Každý členský stát Komisi neprodleně oznámí jmenování odpovědného orgánu, jeho úkoly a jakékoliv změny s ním související. Každý členský stát zveřejní jmenování příslušného odpovědného orgánu.

Článek 7

Skupina pro reakci na počítačové hrozby

1. Každý členský stát zřídí skupinu pro reakci na počítačové hrozby (dále jen „CERT“), odpovědnou za řešení incidentů a rizik v souladu s řádně vymezeným postupem, jež bude splňovat požadavky stanovené v bodě 1 přílohy I. Skupina CERT může být zřízena v rámci odpovědného orgánu.

2. Členské státy zajistí, aby skupiny CERT měly k dispozici odpovídající technické, finanční a lidské zdroje k účinnému plnění svěřených úkolů, jež jsou uvedeny v bodě 2 přílohy I.

3. Členské státy zajistí, aby se skupiny CERT na vnitrostátní úrovni opíraly o bezpečnou a odolnou komunikační a informační infrastrukturu, která bude kompatibilní a interoperabilní se zabezpečeným systémem pro sdílení informací podle článku 9.

4. Členské státy oznámí Komisi, jakými zdroji a pravomocemi skupiny CERT disponují, jakož i postup, který budou při řešení bezpečnostních incidentů uplatňovat.

5. Skupiny CERT budou podřízené odpovědným orgánům, které budou pravidelně přezkoumávat přiměřenost jejich zdrojů, jejich pravomoci a účinnost postupu pro řešení incidentů.

KAPITOLA III

SPOLUPRÁCE MEZI ODPOVĚDNÝMI ORGÁNY

Článek 8

Síť pro spolupráci

1. Odpovědné orgány a Komise zřídí síť pro spolupráci na ochranu proti rizikům a incidentům narušujícím bezpečnost sítí a informačních systémů (dále jen „síť pro spolupráci“.

2. Sítí pro spolupráci bude vytvořeno stálé komunikační spojení mezí Komisí a odpovědnými orgány. Evropská agentura pro bezpečnost sítí a informací (ENISA) na žádost poskytne síti pro spolupráci své odborné znalosti a doporučení.

3. Odpovědné orgány budou v rámci sítě pro spolupráci:

   a) šířit včasná varování týkající se rizik a incidentů v souladu s článkem 10;

   b) zajišťovat koordinovanou reakci v souladu s článkem 11;

   c) pravidelně zveřejňovat na společných internetových stránkách informace o aktuálních včasných varováních a koordinovaných reakcích, které nemají důvěrný charakter;

   d) v rámci působnosti této směrnice na žádost členského státu nebo Komise společně projednávat a posuzovat jednu či více národních strategií a národních plánů spolupráce pro bezpečnost sítí a informací, jež jsou uvedeny v článku 5;

e) na žádost členského státu nebo Komise společně projednávat a posuzovat účinnost skupin CERT, zejména pokud činnosti týkající se bezpečnosti sítí a informací probíhají na úrovni Unie;

f) spolupracovat s Evropským centrem pro boj proti kyberkriminalitě zřízeným v rámci Europolu a dalšími příslušnými evropskými orgány zejména v oblastech energetiky, dopravy, bankovnictví, obchodování s cennými papíry a zdravotnictví a vzájemně si s nimi vyměňovat informace o všech významných záležitostech;

g) vyměňovat si informace a osvědčené postupy mezi sebou a s Komisí a poskytovat si vzájemnou součinnost při budování kapacit pro bezpečnost sítí a informací;

h) organizovat pravidelná vzájemná hodnocení svých kapacit a připravenosti;

i) pořádat cvičení bezpečnosti sítí a informací na úrovni Unie a účastnit se dle potřeby mezinárodních cvičení bezpečnosti sítí a informací.

4. Komise prostřednictvím prováděcích aktů určí způsoby nezbytné pro usnadnění spolupráce mezi odpovědnými orgány a Komisí uvedené v odstavcích 2 a 3. Tyto prováděcí akty se přijímají konzultačním postupem podle čl. 19 odst. 2.

Článek 9

Bezpečný systém pro sdílení informací

1. Výměna citlivých a důvěrných informací uvnitř sítě pro spolupráci bude probíhat s pomocí bezpečné infrastruktury.

2. Komise je zmocněna přijímat akty v přenesené pravomoci v souladu s článkem 18 týkající se formulace kritérií, jež by měly členské státy splňovat, aby byly oprávněny používat bezpečný systém pro sdílení informací, pokud jde o:

a) dostupnost bezpečné a odolné vnitrostátní komunikační a informační infrastruktury, která bude kompatibilní a interoperabilní s bezpečnou infrastrukturou sítě pro spolupráci podle čl. 7 odst. 3, a

b) existenci odpovídajících technických, finančních a lidských zdrojů a postupů umožňujících odpovědnému orgánu a skupině CERT daného členského státu účinné a bezpečné zapojení do bezpečného systému pro sdílení informací podle čl. 6 odst. 3 a čl. 7 odst. 2 a 3.

3. Komise formou prováděcích aktů a na základě kritérií uvedených v odstavcích 2 a 3 rozhodne o přístupu členských států do této bezpečné infrastruktury. Tyto prováděcí akty se přijímají v souladu s přezkumným postupem podle čl. 19 odst. 3.

Článek 10
Včasná varování

1. Odpovědné orgány, případně Komise, vydají prostřednictvím sítě pro spolupráci včasná varování ohledně rizik a incidentů, jež splňují alespoň jednu z následujících podmínek:

   a) jejich rozsah rychle roste nebo by mohl rychle růst;

   b) překračují nebo by mohly překročit národní reakční kapacitu;

   c) postihují nebo by mohly postihnout více než jeden členský stát.

2. V rámci včasného varování odpovědné orgány, případně Komise, sdělí veškeré relevantní informace, které mají k dispozici a které by mohly být užitečné při posuzování daného rizika či incidentu.

3. Komise může na žádost členského státu nebo z vlastní iniciativy vyzvat členský stát, aby poskytl veškeré relevantní informace o určitém riziku nebo incidentu.

4. Pokud panuje podezření, že riziko nebo incident, který je předmětem včasného varování, má povahu trestného činu, odpovědné orgány, případně Komise, uvědomí Evropské centrum pro boj proti kyberkriminalitě v rámci Europolu.

5. Komise je zmocněna přijímat akty v přenesené pravomoci podle článku 18 týkající se specifikace rizik a incidentů, na jejichž základě se vydává včasné varování podle odstavce 1.

Článek 11
Koordinovaná reakce

1. Po vydání včasného varování podle článku 10 odpovědné orgány posoudí relevantní informace a následně se dohodnou na koordinované reakci v souladu s evropským plánem spolupráce v oblasti bezpečnosti sítí a informací uvedeným v článku 12.

2. Jednotlivá opatření přijatá na vnitrostátní úrovni v rámci koordinované reakce budou oznámena prostřednictvím sítě pro spolupráci.

Článek 12

Unijní plán spolupráce v oblasti bezpečnosti sítí a informací

1. Komise je zmocněna prostřednictvím prováděcích aktů přijmout unijní plán spolupráce v oblasti bezpečnosti sítí a informací. Tyto implementační akty se přijímají přezkumným postupem podle čl. 19 odst. 3.

2. Unijní plán spolupráce v oblasti bezpečnosti sítí a informací stanoví:

   a) pro účely článku 10:

– definici formy a postupů odpovědných orgánů pro sběr a sdílení kompatibilních a srovnatelných informací o rizicích a incidentech,

– definici postupů a kritérií pro posouzení rizik a incidentů v rámci sítě pro spolupráci;

b) postupy pro koordinovanou reakci podle článku 11, včetně určení pravomocí a odpovědnosti a postupů spolupráce;

c) harmonogram bezpečnostních cvičení a školení v oblasti bezpečnosti sítí a informací s cílem zdokonalit, prověřit a otestovat plán;

d) program pro předávání znalostí mezi členskými státy ve vztahu k budování kapacit a vzájemné učení;

e) program zvyšování informovanosti a školení v členských státech.

3. Unijní plán spolupráce v oblasti bezpečnosti sítí a informací bude přijat nejpozději do jednoho roku od data, kdy tato směrnice vstoupí v platnost, a bude pravidelně přezkoumáván.

Článek 13

Mezinárodní spolupráce

Aniž by byla dotčena možnost sítě pro spolupráci provozovat mezinárodní spolupráci na neformální úrovni, může Unie uzavřít mezinárodní dohody o spolupráci se třetími zeměmi nebo s mezinárodními organizacemi, na jejichž základě bude možná a jimiž se bude řídit účast dané třetí země či mezinárodní organizace na určitých činnostech sítě pro spolupráci. Takové dohody budou zohledňovat nutnost zajistit odpovídající ochranu osobních údajů šířených v síti pro spolupráci.

KAPITOLA IV

BEZPEČNOST SÍTÍ A INFORMAČNÍCH SYSTÉMŮ ORGÁNŮ VEŘEJNÉ SPRÁVY A HOSPODÁŘSKÝCH SUBJEKTŮ

Článek 14

Bezpečnostní požadavky a oznamování incidentů

1. Členské státy zajistí, aby jejich orgány veřejné správy a hospodářské subjekty přijaly vhodná technická a organizační opatření k řízení bezpečnostních rizik, jimž čelí jimi kontrolované a používané sítě a informační systémy. S ohledem na současné technické možnosti zaručí tato opatření takovou úroveň bezpečnosti, která odpovídá míře existujícího rizika. Zejména budou přijata taková opatření, která zabrání vzniku bezpečnostních incidentů v jejich sítích a informačních systémech, jež by poškodily jimi poskytované základní služby, případně minimalizují dopad takových incidentů, a zajistí tak kontinuitu služeb podporovaných těmito sítěmi a informačními systémy.

2. Členské státy zajistí, aby orgány veřejné správy a hospodářské subjekty oznamovaly odpovědným orgánům incidenty, které mají významný dopad na bezpečnost jimi poskytovaných základních služeb.

3. Povinnosti uvedené v odstavcích 1a 2 se týkají všech hospodářských subjektů poskytujících služby v Evropské unii.

4. V případě, že odpovědný orgán rozhodne, že je ve veřejném zájmu, aby byl daný incident zveřejněn, je oprávněn o něm informovat veřejnost, případně vyzvat orgány veřejné správy a hospodářské subjekty, aby tak učinily. Jednou ročně předloží odpovědný orgán síti pro spolupráci souhrnnou zprávu o obdržených oznámeních a o opatřeních přijatých v souladu s tímto odstavcem.

5. Komise je zmocněna přijímat akty v přenesené pravomoci v souladu s článkem 18 týkající se určení okolností, za nichž jsou orgány veřejné správy a hospodářské subjekty povinny oznamovat incidenty.

6. Na základě aktu v přenesené pravomoci přijatého v souladu s odstavcem 5 jsou odpovědné orgány oprávněny přijmout obecné zásady a v případě potřeby vydat pokyny týkající se okolností, za nichž jsou orgány veřejné správy a hospodářské subjekty povinny oznamovat incidenty.

7. Komise je zmocněna prostřednictvím prováděcích aktů stanovit formu a postupy platné pro účely odstavce 2. Tyto prováděcí akty se přijímají přezkumným postupem podle čl. 19 odst. 3.

8. Ustanovení odstavců 1 a 2 se nevztahují na mikropodniky, jak jsou definovány v doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků[12].

Článek 15

Provádění a prosazování

1. Členské státy zajistí, aby odpovědné orgány měly všechny nezbytné pravomoci pro vyšetřování případů porušení povinností podle článku 14 ze strany orgánů veřejné správy či hospodářských subjektů a dopadů takového porušení na bezpečnost sítí a informačních systémů.

2. Členské státy zajistí, aby odpovědné orgány byly oprávněny požadovat od orgánů veřejné správy a hospodářských subjektů, aby:

   a) poskytly informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů, včetně dokladů o bezpečnostní politice;

   b) se podrobily bezpečnostnímu auditu, který provede kvalifikovaný nezávislý subjekt nebo vnitrostátní orgán, a jeho výsledky zpřístupnily odpovědnému orgánu.

[12] Úř. věst. L 124, 20.5.2003, s. 36.

3. Členské státy zajistí, aby odpovědné orgány byly oprávněny dávat orgánům veřejné správy a hospodářským subjektům závazné pokyny.

4. Odpovědné orgány oznámí jakýkoliv incident, u nějž panuje podezření, že má povahu závažného trestného činu, donucovacím orgánům.

5. Odpovědné orgány budou při řešení incidentů, v jejichž důsledku došlo k porušení ochrany osobních údajů, úzce spolupracovat s úřady pro ochranu osobních údajů.

6. Členské státy zajistí, aby bylo možné všechny povinnosti uložené na základě této kapitoly orgánům veřejné správy a hospodářským subjektům podrobit soudnímu přezkumu.

Článek 16

Standardizace

1. V zájmu jednotného provádění čl. 14 odst. 1 budou členské státy podporovat používání norem a/nebo specifikací týkajících se bezpečnosti sítí a informací.

2. Komise formou prováděcích aktů vypracuje seznam norem uvedených v odstavci 1. Seznam bude zveřejněn v *Úředním věstníku Evropské unie*.

KAPITOLA V

ZÁVĚREČNÁ USTANOVENÍ

Článek 17

Sankce

1. Členské státy stanoví pravidla pro sankce za porušení vnitrostátních právních předpisů přijatých podle této směrnice a přijmou veškerá nezbytná opatření k zajištění jejich uplatňování. Stanovené sankce musí být účinné, přiměřené a odrazující. Členské státy uvědomí o takových předpisech Komisi nejpozději do data provedení této směrnice a neprodleně ji informují také o jakýchkoliv pozdějších změnách těchto předpisů.

2. Členské státy zajistí, aby v případech, kdy se bezpečnostní incident týká osobních údajů, byly navrhované sankce v souladu se sankcemi stanovenými nařízením Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů[13].

Článek 18

Výkon přenesené pravomoci

[13] SEC(2012) 72 final.

1. Pravomoc přijímat akty v přenesené pravomoci je svěřena Komisi za podmínek stanovených v tomto článku.

2. Komisi se svěřuje pravomoc přijímat akty v přenesené pravomoci uvedené v čl. 9 odst. 2, čl. 10 odst. 5 a čl. 14 odst. 5. Komise vypracuje zprávu o přenesené pravomoci nejpozději devět měsíců před koncem příslušného pětiletého období. Přenesení pravomocí se automaticky prodlužuje o stejně dlouhá období, pokud Evropský parlament nebo Rada nevysloví proti tomuto prodloužení námitku nejpozději tři měsíce před koncem každého z těchto období.

3. Evropský parlament nebo Rada mohou přenesení pravomoci uvedené v čl. 9 odst. 2, v čl. 10 odst. 5 a v čl. 14 odst. 5 kdykoli zrušit. Rozhodnutím o zrušení se ukončuje přenesení pravomocí uvedených v daném rozhodnutí. Rozhodnutí nabývá účinku prvním dnem po zveřejnění v *Úředním věstníku Evropské unie*, nebo k pozdějšímu dni, který je v něm upřesněn. Nedotýká se platnosti již platných aktů v přenesené pravomoci.

4. Přijetí aktu v přenesené pravomoci Komise neprodleně oznámí současně Evropskému parlamentu a Radě.

5. Akt v přenesené pravomoci přijatý podle čl. 9 odst. 2, čl. 10 odst. 5, a čl. 14 odst. 5 vstoupí v platnost, pouze pokud proti němu Evropský parlament nebo Rada nevysloví námitky ve lhůtě dvou měsíců ode dne, kdy jim byl tento akt oznámen, nebo pokud Evropský parlament i Rada před uplynutím této lhůty informují Komisi o tom, že námitky nevysloví. Z podnětu Evropského parlamentu nebo Rady se tato lhůta prodlouží o dva měsíce.

Článek 19

Postup projednávání ve výboru

1. Komisi je nápomocen výbor (Výbor pro bezpečnost sítí a informací). Uvedený výbor je výborem ve smyslu nařízení (EU) č. 182/2011.

2. Odkazuje-li se na tento odstavec, použije se článek 4 nařízení (EU) č. 182/2011.

3. Odkazuje-li se na tento odstavec, použije se článek 5 nařízení (EU) č. 182/2011.

Článek 20

Přezkum

Komise pravidelně přezkoumává uplatňování této směrnice a podává zprávu Evropskému parlamentu a Radě. První zprávu předloží nejpozději do tří let od data provedení podle článku 21. Za tím účelem je Komise oprávněna vyzvat členské státy, aby jí neprodleně poskytly informace.

Článek 21

Provedení

1. Členské státy přijmou a zveřejní právní a správní předpisy nezbytné pro dosažení souladu s touto směrnicí nejpozději do [jednoho a půl roku ode dne přijetí]. Znění těchto ustanovení neprodleně sdělí Komisi.

   Tyto předpisy použijí od [jednoho a půl roku ode dne přijetí].

   Tyto předpisy přijaté členskými státy musí obsahovat odkaz na tuto směrnici nebo musí být takový odkaz učiněn při jejich úředním vyhlášení. Způsob tohoto odkazu si stanoví členské státy.

2. Členské státy sdělí Komisi znění hlavních ustanovení vnitrostátních právních předpisů, které přijmou v oblasti působnosti této směrnice.

Článek 22

Vstup v platnost

Tato směrnice vstupuje v platnost [dvacátým] dnem po vyhlášení v *Úředním věstníku Evropské unie*.

Článek 23

Určení

Tato směrnice je určena členským státům.

V Bruselu dne

Za Evropský parlament	*Za Radu*
předseda	*předseda*

PŘÍLOHA I

Povinnosti a úkoly skupiny pro reakci na počítačové hrozby (CERT)

Povinnosti a úkoly skupiny CERT jasně a odpovídajícím způsobem stanoví a upraví vnitrostátní politika nebo právní předpis. Budou zahrnovat tyto povinnosti a úkoly:

1) Povinnosti skupiny CERT

a) Skupina CERT zajistí, aby v jejích komunikačních službách nebyla žádná kritická místa (tzv. *single points of failure*) a služby tak byly co nejlépe dostupné, a bude mít několik způsobů, jimiž bude kontaktovat ostatní a jimiž bude možné kontaktovat ji. Komunikační kanály budou navíc jasně specifikované a spolupracujícím partnerům a podporovatelům skupiny dobře známé.

b) Skupina CERT zavede a bude spravovat bezpečnostní opatření, aby zajistila důvěrnost, celistvost, dostupnost a pravost informací, jež získává a s nimiž nakládá.

c) Pracoviště skupiny a její podpůrné informační systémy se budou nacházet na bezpečném místě.

d) Bude vytvořen systém řízení jakosti služeb, jehož prostřednictvím bude zajištěna návaznost na výsledky činnosti skupiny a její neustálé zdokonalování. Základem systému budou jasně definovaná měřítka, jako jsou oficiální úrovně služeb a klíčové ukazatele výkonnosti.

e) Kontinuita činnosti:

– Skupina CERT bude vybavená vhodnými systémy řízení a směrování požadavků, které usnadní předávání,

– Skupina CERT bude vhodně personálně obsazena tak, aby byla stále k dispozici,

– Skupina CERT bude spoléhat na infrastrukturu, jejíž kontinuita bude zaručena. Za tím účelem budou pro skupinu zřízeny zálohované systémy a záložní pracoviště, aby byl zajištěn nepřetržitý přístup ke komunikačním prostředkům.

2) Úkoly skupiny CERT

a) Úkoly skupiny CERT budou zahrnovat alespoň:

– monitoring incidentů na vnitrostátní úrovni,

– vydávání včasných varování, vyhlašování pohotovosti, oznamování a šíření informací o rizicích a incidentech důležitých pro zainteresované strany,

– reakce na incidenty,

– poskytování dynamické analýzy rizik a incidentů a přehledu o situaci,

– budování povědomí široké veřejnosti o rizicích spojených s online činnostmi,

– organizace kampaní o bezpečnosti sítí a informací.

b) Skupina CERT naváže spolupráci se soukromým sektorem.

c) V zájmu usnadnění spolupráce bude skupina CERT prosazovat přijetí a používání společných či standardních postupů v oblasti:

– řešení incidentů a rizik,

– klasifikace incidentů, rizik a informací,

– klasifikace a třídění měřítek,

– formy výměny informací o rizicích, incidentech a pravidlech pojmenovávání systémů.

PŘÍLOHA II

Seznam hospodářských subjektů

Pro účely čl. 3 odst. 8 písm. a):

1. platformy pro elektronické obchodování

2. internetové platební brány

3. sociální sítě

4. vyhledávače

5. služby cloud computingu

6. obchody s aplikacemi

Pro účely čl. 3 odst. 8 písm. b):

1. Energetika

- dodavatelé elektřiny a plynu
- provozovatelé distribuční soustavy elektřiny a/nebo plynu a dodavatelé elektřiny a plynu konečnému spotřebiteli
- provozovatelé přenosové soustavy zemního plynu, provozovatelé skladovacích zařízení a LNG zařízení
- provozovatelé přenosové soustavy elektřiny
- ropovody a zařízení pro skladování ropy
- účastníci trhu s elektřinou a zemním plynem
- provozovatelé zařízení na zpracování, rafinaci a úpravu ropy a zemního plynu

2. Doprava

- letečtí přepravci (osobní a nákladní letecká doprava)
- námořní dopravci (podniky námořní a pobřežní osobní dopravy a námořní a pobřežní nákladní dopravy)
- železnice (správci infrastruktury, integrované podniky a provozovatelé železniční dopravy)
- letiště
- přístavy
- provozovatelé kontroly řízení provozu

– pomocné logistické služby (a) skladování, b) manipulace s nákladem a c) další podpůrné činnosti v oblasti dopravy)

3. Bankovnictví: úvěrové instituce podle čl. 4 odst. 1 směrnice 2006/48/ES

4. Infrastruktura finančních trhů: burzy cenných papírů, ústřední protistrany a clearingová centra.

5. Zdravotnictví: zdravotnická zařízení (včetně nemocnic a soukromých klinik) a další subjekty poskytující zdravotní péči

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

1.2. Příslušné oblasti politik podle členění ABM/ABB

1.3. Povaha návrhu/podnětu

1.4. Cíle

1.5. Odůvodnění návrhu/podnětu

1.6. Doba trvání akce a finanční dopad

1.7. Předpokládaný způsob řízení

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

2.2. Systém řízení a kontroly

2.3. Opatření k zamezení podvodů a nesrovnalostí

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

3.2.2. Odhadovaný dopad na operační prostředky

3.2.3. Odhadovaný dopad na prostředky administrativní povahy

3.2.4. Soulad se stávajícím víceletým finančním rámcem

3.2.5. Příspěvky třetích stran

3.3. Odhadovaný dopad na příjmy

LEGISLATIVNÍ FINANČNÍ VÝKAZ

1. RÁMEC NÁVRHU/PODNĚTU

1.1. Název návrhu/podnětu

Návrh směrnice Evropského parlamentu a Rady, kterou se stanoví opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.

1.2. Příslušné oblasti politik podle členění ABM/ABB[37]

- 09 – Komunikační sítě, obsah a technologie

1.3. Povaha návrhu/podnětu

☒ Návrh/podnět se týká **nové akce**

☐ Návrh/podnět se týká **nové akce následující po pilotním projektu / přípravné akci**[38]

☐ Návrh/podnět se týká **prodloužení stávající akce**

☐ Návrh/podnět se týká **akce přesměrované na jinou akci**

1.4. Cíle

1.4.1. Víceleté strategické cíle Komise sledované návrhem/podnětem

Cílem navrhované směrnice je zaručit vysokou společnou úroveň bezpečnosti sítí a informací v Evropské unii.

1.4.2. Konkrétní cíle a příslušné aktivity ABM/ABB

Návrh stanoví opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.

Konkrétní cíle:

1. Nastavení minimální úrovně bezpečnosti sítí a informací v členských státech, a tím i zvýšení celkové míry připravenosti a úrovně reakce.

2. Zlepšení spolupráce v oblasti bezpečnosti sítí a informací na úrovni EU s cílem efektivně zabránit přeshraničním incidentům a hrozbám. Bude vytvořena infrastruktura pro bezpečné sdílení informací, která umožní výměnu citlivých a důvěrných informací mezi odpovědnými orgány.

3. Vznik kultury řízení rizik a lepší sdílení informací mezi soukromým a veřejným sektorem.

Příslušné aktivity ABM/ABB

[37] ABM: řízení podle činností (Activity-Based Management) – ABB: sestavování rozpočtu podle činností (Activity-Based Budgeting).

[38] Uvedené v čl. 49 odst. 6 písm. a) nebo b) finančního nařízení.

Směrnice se týká subjektů (podniků a organizací, včetně některých malých a středních podniků) v řadě odvětví (energetika, doprava, úvěrové instituce a burzy cenných papírů, zdravotnictví a zprostředkovatelé klíčových internetových služeb) a orgánů veřejné správy. Zabývá se souvislostmi s problematikou vymáhání práva, ochrany informací a aspekty bezpečnosti sítí a informací v mezinárodních vztazích.

- 09 – Komunikační sítě, obsah a technologie

- 02 – Podnikáni

- 32 – Energetika

- 06 – Mobilita a doprava

- Hlava 17 – Zdraví a ochrana spotřebitele

- 18 – Vnitřní věci

- 19 – Vnější vztahy

- 33 – Spravedlnost

- 12 – Vnitřní trh

1.4.3. Očekávané výsledky a dopady

Upřesněte účinky, které by návrh/podnět měl mít na příjemce / cílové skupiny.

Značně by se zlepšila ochrana spotřebitele, podniků a vládních institucí v EU před bezpečnostními incidenty, hrozbami a riziky.

Více podrobností lze nalézt v oddíle 8.2 (Dopad alternativy č. 2 – Regulatorní přístup) pracovního dokumentu útvarů Komise o posouzení dopadů, který je připojen k tomuto legislativními návrhu.

1.4.4. Ukazatele výsledků a dopadů

Upřesněte ukazatele, podle kterých je možno uskutečňování návrhu/podnětu sledovat.

Ukazatele pro sledování a hodnocení jsou uvedeny v oddíle 10 zprávy o posouzení dopadů.

1.5. Odůvodnění návrhu/podnětu

1.5.1. Potřeby, které mají být uspokojeny v krátkodobém nebo dlouhodobém horizontu

Každý členský stát by musel mít:

- národní strategii pro bezpečnost sítí a informací ;

- národní plán pro bezpečnost sítí a informací;

- vnitrostátní orgán odpovědný za bezpečnost sítí a informací; a

- skupinu pro reakci na počítačové hrozby (CERT)

Na úrovni EU by spolu členské státy povinně spolupracovaly prostřednictvím sítě.

Orgány veřejné správy a klíčoví hráči by povinně prováděli řízení rizik v oblasti bezpečnosti sítí a informací a oznamovali odpovědným orgánům incidenty značného dopadu v oblasti bezpečnosti sítí a informací.

1.5.2. Přidaná hodnota ze zapojení EU

Vzhledem k přeshraničnímu charakteru bezpečnosti sítí a informací představují rozdíly v příslušné legislativě a politice překážku pro působení podniků ve více zemích a pro dosažení globálních úspor z rozsahu. Pokud by nedošlo k zásahu na úrovni EU, nastala by situace, kdy by každý členský stát jednal samostatně bez ohledu na vzájemnou provázanost a závislost sítí a informačních systémů.

Uvedených cílů lze proto dosáhnout snáze, dojde-li k akci na úrovni EU, než budou-li členské státy postupovat samostatně.

1.5.3. Závěry vyvozené z podobných zkušeností v minulosti

Návrh vychází z výsledků analýzy, podle nichž je třeba pomocí právních povinností vytvořit rovné podmínky a odstranit mezery v legislativě. V této oblasti přístup založený čistě na dobrovolnosti vedl k tomu, že spolu spolupracuje jen malá část členských států, které mají kapacity na vysoké úrovni.

1.5.4. Slučitelnost a možná synergie s dalšími relevantními nástroji

Návrh je zcela v souladu s programem Digitální agenda pro Evropu, a tedy i se strategií EU 2020. Rovněž odpovídá legislativnímu rámci EU o elektronických komunikacích, směrnici EU o evropské kritické infrastruktuře a směrnici EU o ochraně údajů a doplňuje je.

Návrh tvoří nedílnou součást sdělení Komise a vysoké představitelky Evropské unie pro zahraniční věci a bezpečnostní politiku o evropské strategii pro kybernetickou bezpečnost.

1.6. Doba trvání akce a finanční dopad

– ☐ Časově omezený návrh/podnět

– ☐ Návrh/podnět s platností od [DD/MM]RRRR do [DD/MM]RRRR

– ☐ Finanční dopad od RRRR do RRRR

– ☒ Časově neomezený návrh/podnět

– Lhůta pro provedení do vnitrostátního práva začne běžet ihned po přijetí návrhu (očekává se v roce 2015) a bude trvat 18 měsíců. Provádění směrnice však bude zahájeno po jejím přijetí a bude zahrnovat zřízení bezpečné infrastruktury, která umožní lepší spolupráci členských států.

– Následovat bude plné fungování.

1.7. Předpokládané způsoby řízení[39]

– ☒ Přímé centralizované řízení Komisí

– ☒ Nepřímé centralizované řízení, při kterém jsou úkoly plnění rozpočtu svěřeny:

– ☐výkonným agenturám

– ☒ subjektům zřízeným Společenstvími[40]

– ☐ vnitrostátním veřejnoprávním subjektům / subjektům pověřeným výkonem veřejné služby

– ☐ osobám pověřeným prováděním zvláštních opatření podle hlavy V Smlouvy o Evropské unii a označeným v příslušném základním právním aktu ve smyslu článku 49 finančního nařízení

– ☐ Sdílené řízení s členskými státy

– ☐ Decentralizované řízení s třetími zeměmi

– ☐ Společné řízení s mezinárodními organizacemi, včetně Evropské kosmické agentury

Pokud vyberete více způsobů řízení, upřesněte je v části „Poznámky“.

Poznámky:

Decentralizovaná agentura ENISA, zřízená Společenstvími, může členským státům a Komisi poskytnout součinnost při provádění směrnice z titulu svého mandátu a na základě přerozdělení prostředků, s nímž je pro tuto agenturu počítáno ve víceletém finančním rámci na období 2014–2020.

[39] Vysvětlení způsobů řízení spolu s odkazem na finanční nařízení jsou k dispozici na stránkách BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

[40] Uvedené v článku 185 finančního nařízení.

2. SPRÁVNÍ OPATŘENÍ

2.1. Pravidla pro sledování a podávání zpráv

Upřesněte četnost a podmínky.

Komise bude pravidelně přezkoumávat uplatňování této směrnice a podávat zprávy Evropskému parlamentu a Radě.

Komise rovněž posoudí správnost provedení směrnice do vnitrostátního práva členských států.

Návrh nástroje pro propojení Evropy (CEF) rovněž umožňuje provést hodnocení způsobů provádění projektů, jakož i dopady jejich realizace, a to za účelem posouzení, zda bylo dosaženo stanovených cílů, včetně cílů týkajících se ochrany životního prostředí.

2.2. Systém řízení a kontroly

2.2.1. Zjištěná rizika

– zpoždění realizace projektu vzniklé při výstavbě bezpečné infrastruktury

2.2.2. Předpokládané metody kontroly

Dohody a rozhodnutí týkající se provádění opatření v rámci nástroje CEF budou upravovat dohled a finanční kontrolu ze strany Komise, jakož i audity prováděné Účetním dvorem a kontroly na místě prováděné Evropským úřadem pro boj proti podvodům (OLAF).

2.2.3. Náklady na provádění kontrol a jejich přínosy; pravděpodobná míra nesouladu

Díky kontrolám ex-ante a ex-post vycházejícím z rizik a možnosti provádět audity na místě budou náklady na kontroly přiměřené.

2.3. Opatření k zamezení podvodů a nesrovnalostí

Upřesněte stávající či předpokládaná preventivní a ochranná opatření.

Komise přijme vhodná opatření k zajištění toho, aby byly při provádění akcí financovaných podle tohoto rozhodnutí finanční zájmy Unie chráněny, a to tím, že bude předcházeno podvodům, korupci a jinému protiprávnímu jednání, účinnými kontrolami a, jsou-li zjištěny nesrovnalosti, zpětným získáním neoprávněně vyplacených částek a případně účinnými, přiměřenými a odrazujícími sankcemi.

Komise nebo její zástupci a Účetní dvůr mají pravomoc provádět formou kontroly dokumentů a inspekce na místě audit u všech příjemců grantů, zhotovitelů, dodavatelů nebo poskytovatelů a subdodavatelů, kteří v rámci programu obdrželi finanční prostředky Unie.

Evropský úřad pro boj proti podvodům (OLAF) může provádět kontroly a inspekce na místě u hospodářských subjektů, jichž se toto financování přímo nebo nepřímo týká, postupy stanovenými v nařízení (Euratom, ES) č. 2185/96 s cílem zjistit, zda v souvislosti s grantovou dohodou, rozhodnutím o grantu nebo smlouvou o financování Unií nedošlo k podvodu, korupci nebo jinému protiprávnímu jednání ohrožujícímu finanční zájmy Unie.

Aniž jsou dotčena ustanovení výše uvedených odstavců, dohody o spolupráci se třetími zeměmi a mezinárodními organizacemi, grantové dohody, rozhodnutí o grantu a smlouvy vyplývající z provádění tohoto nařízení musí Komisi, Účetní dvůr a OLAF k provádění takových auditů, kontrol a inspekcí na místě výslovně zmocňovat.

S nástrojem CEF je možné, aby smlouvy o poskytnutí grantu a veřejné zakázky vycházely ze standardních vzorů, které budou upravovat obecně používaná opatření proti podvodům.

3. ODHADOVANÝ FINANČNÍ DOPAD NÁVRHU/PODNĚTU

3.1. Okruhy víceletého finančního rámce a dotčené výdajové rozpočtové položky

- Stávající rozpočtové položky

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Počet [Popis……...….]	RP/NRP (41)	ze zemí ESVO[42]	z kandidátských zemí[43]	ze třetích zemí	ve smyslu čl. 18 odst. 1 písm. aa) finančního nařízení
	09 03 02 posilování propojení a interoperability národních veřejných služeb dostupných online i přístupu do těchto sítí	Rozdíl	NE	NE	NE	NE

- Nové rozpočtové položky, jejichž vytvoření se požaduje (nepoužije se)

V pořadí okruhů víceletého finančního rámce a rozpočtových položek.

Okruh víceletého finančního rámce	Rozpočtová položka	Druh výdajů	Příspěvek			
	Počet [Název……...….]	RP/NRP	ze zemí ESVO	z kandidátských zemí	ze třetích zemí	ve smyslu čl. 18 odst. 1 písm. aa) finančního nařízení
	[XX.YY.YY.YY]		ANO/ NE	ANO/NE	ANO/ NE	ANO/NE

41 RP = rozlišené prostředky / NRP = nerozlišené prostředky.

42 ESVO: Evropské sdružení volného obchodu.

43 Kandidátské země a případně potenciální kandidátské země západního Balkánu.

3.2. Odhadovaný dopad na výdaje

3.2.1. Odhadovaný souhrnný dopad na výdaje

v milionech EUR (zaokrouhleno na tři desetinná místa)

Okruh víceletého finančního rámce	1	Inteligentní růst podporující začlenění

GŘ: <…….>			2015* [44]	Rok **2016**	Rok **2017**	Rok **2018**	Následující roky (2019–2021) a další			**CELKEM**
• Operační prostředky										
09 03 02	Závazky	(1)	1,250**	0,000						**1,250**
	Platby	(2)	0,750	0,250	0,250					**1,250**
Prostředky správní povahy financované z rámce na zvláštní programy[45]			**0,000**							**0,000**
Číslo rozpočtové položky		(3)	**0,000**							**0,000**
CELKEM prostředky pro GŘ <….>	Závazky	=1+1a +3	1,250	0,000						**1,250**
	Platby	=2+2a +3	0,750	0,250	0,250					**1,250**

• Operační prostředky CELKEM	Závazky	(4)	1,250	0,000						**1,250**
	Platby	(5)	0,750	0,250	0,250					**1,250**

[44] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět.

[45] Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)	**0,000**							
CELKEM prostředky z OKRUHU 1 víceletého finančního rámce	Závazky	=4+ 6	1,250	0,000						**1,250**
	Platby	=5+ 6	0,750	0,250	0,250					**1,250**

* Přesné načasování bude záviset na datu přijetí návrhu zákonodárným orgánem (tj. bude-li směrnice schválena v průběhu roku 2014, začne se stávající infrastruktura upravovat v roce 2015, v opačném případě pak o rok později).

** Pokud se členské státy rozhodnou využít stávající infrastrukturu a pokrýt jednorázový výdaj na její úpravu z rozpočtu EU, jak je vysvětleno v bodech 1.4.3 a 1.7, odhaduje se cena za úpravu sítě k lepší spolupráci členských států podle kapitoly III směrnice (včasná varování, koordinovaná reakce atd.) na 1 250 000 EUR. Tato částka je mírně vyšší než částka uvedená ve zprávě o posouzení rizik („přibližně 1 milión EUR“), neboť vychází z přesnějšího odhadu stavebních bloků nezbytných pro takovou infrastrukturu. Nezbytné stavební bloky a s nimi související náklady vychází z odhadu SVS, který je založen na zkušenostech střediska s vývojem podobných systémů pro jiné oblasti, např. veřejné zdraví, a zahrnovaly by následující: systém včasného varování a ohlašování pro bezpečnost sítí a informací (275 000 EUR); platformu pro výměnu informací (400 000 EUR); systém včasného varování a reakce (275 000 EUR) a situační středisko (300 000 EUR) v celkové výši 1 250 000 EUR. Podrobnější prováděcí plán by měl být součástí připravované studie proveditelnosti podle zvláštní smlouvy SMART 2012/0010: „Studie proveditelnosti a příprava na zavedení evropského systému včasného varování a reakce na počítačové útoky a narušení“.

Má-li návrh/podnět dopad na více okruhů:

• Operační prostředky CELKEM	Závazky	(4)	0,000	0,000						
	Platby	(5)	0,000	0,000						
• Prostředky správní povahy financované z rámce na zvláštní programy CELKEM		(6)	**0,000**	**0,000**						
CELKEM prostředky z OKRUHU 1 až 4 víceletého finančního rámce (referenční částka)	Závazky	=4+ 6	1,250	0,000						1,250
	Platby	=5+ 6	0,750	0,250	0,250					1,250

Okruh víceletého finančního rámce	**5**	Správní náklady

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2015**	Rok **2016**	Rok **2017**	Rok **2018**	Následující roky (2019–2021) a další			**CELKEM**
GŘ: CNECT									
• Lidské zdroje		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Ostatní správní výdaje		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
GŘ CNECT **CELKEM**	Prostředky	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

CELKEM prostředky pro OKRUH 5 víceletého finančního rámce	(Závazky celkem = platby celkem)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

v milionech EUR (zaokrouhleno na tři desetinná místa)

		Rok **2015**[46]	Rok **2016**	Rok **2017**	Rok **2018**	Následující roky (2019–2021) a další			**CELKEM**
CELKEM prostředky z OKRUHU 1 až 5 víceletého finančního rámce	Závazky	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Platby	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět.

3.2.2. Odhadovaný dopad na operační prostředky

– ☐ Návrh/podnět nevyžaduje využití operačních prostředků

– ☑ Návrh/podnět vyžaduje využití operačních prostředků, jak je vysvětleno dále:

– Prostředky na závazky v milionech EUR (zaokrouhleno na tři desetinná místa)

Uveďte cíle a výstupy ⇩			Rok **2015***		Rok **2016**		Rok **2017**		Rok **2018**		Následující roky (2019–2021) a další						**CELKEM**	
	VÝSTUPY																	
	Druh[47]	Průměrné náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Počet	Náklady	Celkový počet	Náklady celkem
SPECIFICKÝ CÍL Č. 2[48] Zabezpečený systém pro sdílení informací																		
– Výstup	Upravit infrastrukturu																	
Mezisoučet pro specifický cíl č. 2			1	1,250**													1	1,250
NÁKLADY CELKEM				1,250														1,250

47 Výstupy se rozumí produkty a služby, které mají být dodány (např.: počet financovaných studentských výměn, počet vybudovaných kilometrů silnic atd.).

48 Popsaný v části 1.4.2. „Specifické cíle…“

* Přesné načasování bude záviset na datu přijetí návrhu zákonodárným orgánem (tj. bude-li směrnice schválena v průběhu roku 2014, začne se stávající infrastruktura upravovat v roce 2015, v opačném případě pak o rok později).

** Viz bod 3.2.1.

3.2.3. Odhadovaný dopad na prostředky administrativní povahy

3.2.3.1. Shrnutí

– ☐ Návrh/podnět nevyžaduje využití správních prostředků

– ☑ Návrh/podnět vyžaduje využití správních prostředků, jak je vysvětleno dále:

v milionech EUR (zaokrouhleno na tři desetinná místa)

	Rok **2015**[49]	Rok **2016**	Rok **2017**	Rok **2018**	Následující roky (2019–2021) a další			**CELKEM**
OKRUH 5 víceletého finančního rámce								
Lidské zdroje	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Ostatní správní výdaje	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Mezisoučet za OKRUH 5 víceletého finančního rámce	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
Mimo OKRUH 5[50] **víceletého finančního rámce**								
Lidské zdroje	0,000	0,000						**0,000**
Ostatní výdaje správní povahy								
Mezisoučet mimo OKRUH 5 víceletého finančního rámce	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
CELKEM	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ CNECT, které jsou již vyčleněny na řízení opatření a/nebo byly v rámci GŘ přemístěny, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

49 Rokem N se rozumí rok, kdy se návrh/podnět začíná provádět.

50 Technická a/nebo administrativní pomoc a výdaje na podporu provádění programů a/nebo akcí EU (bývalé položky „BA“), nepřímý výzkum, přímý výzkum.

Evropská agentura pro bezpečnost sítí a informací (ENISA) může členským státům a Komisi poskytnout součinnost při provádění směrnice z titulu svého mandátu a na základě přerozdělení prostředků, s nímž počítá víceletý finanční rámec pro tuto agenturu na období 2014–2020, tj. bez přidělení dodatečných rozpočtových prostředků nebo lidských zdrojů.

3.2.3.2. Odhadované potřeby v oblasti lidských zdrojů

– ☐ Návrh/podnět nevyžaduje využití lidských zdrojů

– ☑ Návrh/podnět vyžaduje využití lidských zdrojů Komise, jak je vysvětleno dále:

V zásadě by nebyla nutná žádná dodatečná pracovní síla. Lidské zdroje, které budou třeba, budou velmi omezené a budou pokryté pracovníky GŘ, kteří již byli na řízení akce vyčleněni.

Odhad vyjádřete v celých číslech (nebo zaokrouhlete nejvýše na jedno desetinné místo)

		Rok **2015**	Rok **2016**	Rok 2017	Rok 2018	Následující roky (2019–2021) a další		
• Pracovní místa podle plánu pracovních míst (místa úředníků a dočasných zaměstnanců)								
09 01 01 01 (v ústředí a v zastoupeních Komise)		4	4	4	4	4	4	4
XX 01 01 02 (při delegacích)								
XX 01 05 01 (v nepřímém výzkumu)								
10 01 05 01 (v přímém výzkumu)								
• Externí zaměstnanci (v přepočtu na plné pracovní úvazky: FTE)[51]								
09 01 02 01 (SZ, ZAP, VNO z celkového rámce)		1	1	1	1	1	1	1
XX 01 02 02 (SZ, MZ, VNO, ZAP a MOD při delegacích)								
XX 01 04 **yy**[52]	v ústředí[53]							
	při delegacích							
XX 01 05 02 (SZ, DZ, VNO v nepřímém výzkumu)								
10 01 05 02 (SZ, DZ, VNO v přímém výzkumu)								
Jiné rozpočtové položky (upřesněte)								
CELKEM		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX je oblast politiky nebo dotčená hlava rozpočtu.

Potřeby v oblasti lidských zdrojů budou pokryty ze zdrojů GŘ CNECT, které jsou již vyčleněny na řízení akce a/nebo byly v rámci GŘ přemístěny, a případně doplněny z dodatečného přídělu, který lze řídícímu GŘ poskytnout v rámci ročního přidělování a s ohledem na rozpočtová omezení.

Evropská agentura pro bezpečnost sítí a informací (ENISA) může členským státům a Komisi poskytnout součinnost při provádění směrnice z titulu svého současného

[51] SZ = smluvní zaměstnanec; ZAP = zaměstnanec agentury práce („*intérimaire*“); MOD = mladý odborník při delegaci („*Jeune Expert en Délégation*“); MZ = místní zástupce; VNO = vyslaný národní odborník.

[52] Dílčí strop na externí pracovníky z operačních prostředků (bývalé položky „BA“).

[53] V podstatě na strukturální fondy, Evropský zemědělský fond pro rozvoj venkova (EZFRV) a Evropský rybářský fond.

mandátu a na základě přerozdělení prostředků, s nímž počítá víceletý finanční rámec pro agenturu na období 2014–2020, tj. bez přidělení dodatečných rozpočtových prostředků nebo lidských zdrojů.

Popis úkolů:

Úředníci a dočasní zaměstnanci	– Příprava aktů v přenesené pravomoci podle čl. 14 odst. 3 – Příprava prováděcích aktů podle článku 8, čl. 9 odst. 2, článku 12, čl. 14 odst. 5, článku 16 – Podíl na spolupráci prostřednictvím sítě jak na úrovni politických opatření, tak na provozní úrovni – Zapojení do mezinárodních rozhovorů a případně uzavření mezinárodních dohod
Externí zaměstnanci	Podpora při plnění všech výše uvedených úkolů dle potřeby.

3.2.4. Soulad se stávajícím víceletým finančním rámcem

– ☑ Návrh/podnět je v souladu se stávajícím víceletým finančním rámcem.

– ☐ Návrh/podnět si vyžádá úpravu příslušného okruhu víceletého finančního rámce.

Odhadovaný finanční dopad na provozní výdaje návrhu vznikne v případě, že se členské státy rozhodnou upravit stávající infrastrukturu a pověří Komisi provedením této úpravy v rámci víceletého finančního rámce na období 2014–2020. Související jednorázový výdaj by byl hrazen z programu CEF, za podmínky, že budou k dispozici dostatečné prostředky. Členské státy také mohou jednorázové náklady, ať už na přizpůsobení stávající infrastruktury, nebo na zřízení nové infrastruktury, nést společně.

– ☐ Návrh/podnět vyžaduje použití nástroje flexibility nebo změnu víceletého finančního rámce[54].

Nevztahuje se na tento návrh.

3.2.5. Příspěvky třetích stran

– Návrh/podnět nepočítá se spolufinancováním od třetích stran.

3.3. Odhadovaný dopad na příjmy

– ☑ Návrh/podnět nemá žádný finanční dopad na příjmy.

[54] Viz body 19 a 24 interinstitucionální dohody.