EVROPSKÁ
KOMISE

V Bruselu dne 7.2.2013
SWD(2013) 31 final

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu směrnice Evropského parlamentu a Rady

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

{COM(2013) 48 final}
{SWD(2013) 32 final}

PRACOVNÍ DOKUMENT ÚTVARŮ KOMISE

SOUHRN POSOUZENÍ DOPADŮ

Průvodní dokument k

návrhu směrnice Evropského parlamentu a Rady

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

1. ROZSAH

Toto posouzení dopadů se týká alternativ politických opatření zaměřených na zvýšení bezpečnosti Internetu a dalších sítí a informačních systémů, na nichž je do značné míry postaveno fungování naší společnosti (např. veřejné správy, financí a bankovnictví, energetiky, dopravy, zdravotnictví a určitých internetových služeb zajišťujících klíčové ekonomické a společenské procesy, jako jsou platformy pro elektronické obchodování a sociální sítě). Daná problematika se označuje termínem bezpečnost sítí a informací.

2. POLITICKÉ SOUVISLOSTI

Rostoucí důležitost bezpečnosti sítí a informací pro naše hospodářství a společnost Komise poprvé zmínila v roce 2001. Aby se zajistila vysoká a efektivní úroveň bezpečnosti sítí a informací v EU, rozhodlo se Evropské společenství v roce 2004 zřídit Evropskou agenturu pro bezpečnost sítí a informací (ENISA). Doposud Evropská unie ve věci bezpečnosti sítí a informací zastávala přístup, který spočíval především v přijímání řady akčních plánů a strategií, jež vybízely členské státy ke zvyšování jejich kapacit pro zajišťování bezpečnosti sítí a informací a ke spolupráci při řešení problémů v oblasti bezpečnosti sítí a informací, jež mají přeshraniční rozměr.

Jednotlivé aspekty iniciativy (vymezení problémů a možnosti řešení stávajících nedostatků) byly konzultovány se zainteresovanými subjekty prostřednictvím:

- **Internetové veřejné konzultace** nazvané „Zvyšování bezpečnosti sítí a informací v EU“, která proběhla od 23. července do 15. října 2012. Prostřednictvím tohoto online nástroje obdržela Komise celkem 169 odpovědí a dalších 10 reakcí jí bylo zasláno v tištěné podobě.
- Rozhovorů s **členskými státy** konaných v rámci Evropského fóra členských států (EFMS), na zvláštních dvoustranných jednáních a na konferenci o kybernetické bezpečnosti pořádané Komisí a Evropskou službou pro vnější činnost dne 6. července 2012.
- Rozhovorů se **soukromými podniky** a sdruženími, které se konaly v rámci Evropského partnerství veřejného a soukromého sektoru pro odolnost (EP3R) a dvoustranných setkání.
- Rozhovorů s agenturou **ENISA** a skupinami **CERT-EU**.
- Rozhovorů v rámci **shromáždění k Digitální agendě 2012**.

3. POPIS PROBLÉMU

3.1. Vymezení problému

Daný problém lze popsat jako celkovou ***nedostatečnou úroveň ochrany proti incidentům, rizikům a hrozbám v oblasti bezpečnosti sítí a informací v EU, jež narušují řádné fungování vnitřního trhu***.

Jelikož jsou sítě a informační systémy vzájemně propojené a internet je ze své podstaty globálním nástrojem, mnohé incidenty týkající se bezpečnosti sítí a informací přesahují státní hranice a narušují fungování vnitřního trhu.

V důsledku porušení bezpečnosti mohou být přeshraniční služby nedostupné, pozastavené nebo přerušené, jako tomu bylo v případě útoků na eBay a PayPal. Útoky na nizozemského vydavatele digitálních certifikátů DigiNotar poukázaly na nutnost rychlé reakce a sdílení informací o závažných incidentech. V důsledku proběhlých incidentů začínají členské státy zavádět své vlastní předpisy. Nekoordinované regulatorní zásahy však mohou vést k roztříštěnosti a vzniku překážek na vnitřním trhu a spolu s nimi i k nákladům při dodržování předpisů pro podniky, které působí ve více než jednom členském státě

Tento problém se týká všech částí společnosti a hospodářství (vlád, podniků i spotřebitelů). Zejména několik odvětví hraje v poskytování klíčových služeb pro naše hospodářství a společnost zásadní roli a bezpečnost jejich systémů je pro fungování vnitřního trhu obzvlášť důležitá. K těmto odvětvím patří bankovnictví, burzy cenných papírů, výroba, přenos a distribuce energie, doprava (letecká, železniční, námořní), zdravotnictví, zprostředkovatelé klíčových internetových služeb a veřejná správa. Veřejná konzultace ukázala silnou podporu zainteresovaných subjektů, pokud jde o řešení bezpečnosti sítí a informací v daných odvětvích a přijetí odpovídajících opatření na úrovni EU.

Pokud nebudou přijata další opatření proti rostoucímu počtu bezpečnostních incidentů, mohla by utrpět důvěra spotřebitelů v online služby, což by mohlo ohrozit naplnění cílů Digitální agendy.

3.2. Příčiny problému

Výše vymezený problém je způsoben řadou faktorů.

Zaprvé, **nestejná úroveň kapacit jednotlivých členských států EU** brání vytváření vzájemné důvěry mezi subjekty na stejné úrovni, která je předpokladem pro spolupráci a sdílení informací.

Zadruhé, **sdílení informací o incidentech, rizicích a hrozbách není dostatečné**. Většina bezpečnostních incidentů zůstane neoznámena a bez povšimnutí, zejména proto, že podniky se zdráhají informace sdílet z obavy, že utrpí jejich pověst nebo jim vznikne určitá odpovědnost. V současných platformách či partnerstvích soukromého a veřejného sektoru jako EFMS a EP3R se výměna informací omezuje na osvědčené postupy.

4. ÚČINNOST STÁVAJÍCÍCH OPATŘENÍ

4.1. Mezery v současném právním rámci

Podle současných předpisů mají povinnost přijmout opatření v oblasti řízení rizik a oznamovat narušení bezpečnosti sítí a informací pouze telekomunikační společnosti. Bezpečnostní rizika však hrozí všem subjektům závislým na sítích a informačních systémech. Tato skutečnost vytváří nerovné podmínky, neboť tentýž incident, který by zasáhl například poskytovatele telekomunikačních služeb a společnost poskytující hlasové služby

prostřednictvím protokolu IP (VoIP), by v prvním uvedeném případě musel být oznámen vnitrostátnímu odpovědnému orgánu, zatímco ve druhém případě nikoliv.

Všichni hráči působící coby správci osobních údajů (například banky nebo nemocnice) jsou podle právního rámce upravujícího ochranu údajů povinni zavést bezpečnostní opatření přiměřená hrozícím rizikům. Zároveň jsou však povinni oznamovat pouze taková porušení bezpečnosti, jimiž dochází k porušení ochrany osobních údajů.

Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur se vztahuje pouze k odvětví energetiky a dopravy a k dnešnímu dni určily členské státy jen několik málo takových evropských kritických infrastruktur. Směrnice neukládá provozovatelům povinnost oznamovat vážná porušení bezpečnosti ani nestanoví mechanismy pro spolupráci členských států a reakci na incidenty.

Evropský parlament a Rada v současnosti projednávají návrh směrnice o útocích proti informačním systémům[1]. Návrh se týká pouze trestněprávní úpravy určitých druhů činů a nezabývá se ani předcházením rizik a narušení bezpečnosti sítí a informací ani reakcí na narušení bezpečnosti sítí a informací a zmírňováním jejich dopadů.

4.2. Meze přístupu založeného na dobrovolnosti

Dosavadní přístup založený na dobrovolnosti vedl k nestejné míře připravenosti a k omezené spolupráci.

Jelikož členské státy spolu nesdílejí informace o incidentech, rizicích a hrozbách ani nespolupracují na obraně proti přeshraničním hrozbám, má fórum EFMS jen úzkou působnost. Fórum EFMS není oprávněno požadovat od svých členů, aby si zajistili určité minimální kapacity.

Agentura ENISA nemá žádné operativní pravomoci a nemůže například zasáhnout a aktivně řešit problémy bezpečnosti sítí a informací.

Partnerství EP3R pak nemá žádné formální zakotvení a nemůže od soukromého sektoru požadovat, aby oznamoval incidenty vnitrostátním orgánům. V partnerství EP3R neexistuje žádný rámec pro spolehlivé sdílení a předávání informací o hrozbách, rizicích a případech narušení bezpečnosti sítí a informací.

5. POTŘEBA ZÁSAHU EU, SUBSIDIARITA A PROPORCIONALITA

Zajištění bezpečnosti sítí a informací má zásadní význam pro fungování vnitřního trhu a pro blahobyt společnosti. Vhodný právní základ pro harmonizaci požadavků na bezpečnost sítí a informací a pro zavedení společné minimální úrovně bezpečnosti v celé EU představuje článek 114 SFEU.

Odůvodněnost zásahu EU v oblasti bezpečnosti sítí a informací je vzhledem k přeshraniční povaze problému a zvýšené účinnosti (a tedy přidané hodnotě) stávajících vnitrostátních politik, již by přinesla opatření na úrovni EU, dána zásadou **subsidiarity**.

K zajištění spolupráce všech členských států je nutné ujistit se, že všechny členské státy budou mít k dispozici požadované minimální kapacity. Kromě toho je zřejmé, že společný postup ve věci politiky bezpečnosti sítí a informací může mít výrazně pozitivní dopad na účinnou ochranu základních práv a především práva na ochranu osobních údajů a soukromí.

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

Opatření v rámci upřednostňované alternativy jsou odůvodněná z hlediska **proporcionality**, jelikož povinnosti členských států jsou nastavené na nejnižší možné úrovni nezbytné k dosažení odpovídající připravenosti a k zajištění spolupráce založené na důvěře a jelikož povinnost podniků a orgánů veřejné správy provádět řízení rizik a oznamovat incidenty se vztahuje pouze na klíčové subjekty a týká se opatření přiměřených rizikům a incidentů, jejichž dopad je značný. Opatření v rámci upřednostňované alternativy by navíc nepřinesla nepřiměřené náklady.

6. CÍLE

Obecným cílem je zvýšit úroveň ochrany proti narušením, rizikům a hrozbám v oblasti bezpečnosti sítí a informací v EU. Konkrétní cíle jsou následující:

- **Cíl č. 1** – Nastavení minimální úrovně bezpečnosti sítí a informací v členských státech a tím i zvýšení celkové míry připravenosti a úrovně reakce.
- **Cíl č. 2** – Zlepšení spolupráce v oblasti bezpečnosti sítí a informací na úrovni EU s cílem efektivně zabránit přeshraničním incidentům a hrozbám.
- **Cíl č. 3** – Vznik kultury řízení rizik a lepší sdílení informací mezi soukromým a veřejným sektorem.

7. ALTERNATIVY POLITICKÝCH OPATŘENÍ

Alternativy politických opatření, jež byly v tomto posouzení dopadů zváženy, jsou: zachování stávajícího přístupu bez opatření, regulatorní přístup a kombinovaný přístup. Alternativa spočívající v zastavení veškeré iniciativy EU v oblasti bezpečnosti sítí a informací byla zavržena.

7.1. Alternativa č. 1 – bez opatření („základní scénář“)

Komise by ve spolupráci s agenturou ENISA pokračovala v současném přístupu založeném na dobrovolnosti a vyzvala by členské státy ke zřízení vnitrostátních kapacit pro bezpečnost sítí a informací (např. skupin CERT, národních plánů pro případ kybernetické pohotovosti, národních strategií kybernetické bezpečnosti) a ke spolupráci na úrovni EU (např. prostřednictvím evropské sítě skupin CERT a evropského pohotovostního plánu či plánu spolupráce pro případ kybernetického incidentu).

7.2. Alternativa č. 2 – regulatorní přístup

Komise by členským státům uložila povinnost zajistit si alespoň minimální úroveň vnitrostátních kapacit (skupiny CERT, odpovědné orgány, národní plány pro případ kybernetické pohotovosti, národní strategie kybernetické bezpečnosti).

Podle této alternativy by vnitrostátní odpovědné orgány a skupiny CERT musely být součástí **sítě** pro spolupráci na úrovni EU. V této síti by si odpovědné orgány a skupiny CERT vyměňovaly informace a spolupracovaly by spolu v boji proti bezpečnostním hrozbám a incidentům podle **evropského pohotovostního plánu či plánu spolupráce pro případ kybernetického incidentu**, na němž by se členské státy musely dohodnout.

Podniky (s výjimkou mikropodniků) v určitých klíčových odvětvích, tj. bankovnictví, energetika (elektřina a zemní plyn), doprava, zdravotnictví, zprostředkovatelé internetových služeb a orgány veřejné správy, by musely vyhodnocovat rizika, jež jim hrozí, a přijmout odpovídající opatření přiměřená velikosti skutečného rizika. Tyto subjekty by navíc odpovědným orgánům povinně podávaly zprávy o všech incidentech vážně ohrožujících provoz jejich sítí a informačních systémů a majících významný dopad na kontinuitu služeb a dodávek zboží závislých na sítích a informačních systémech. Toto schéma odpovídá

schématu, které je uvedené v článku 13a a 13b rámcové směrnice o elektronických komunikacích.

7.3. Alternativa č. 3 – kombinovaný přístup

Komise by kombinovala dobrovolné iniciativy založené na dobré vůli členských států a zaměřené na zřízení či posílení kapacit členských států pro bezpečnost sítí a informací a na zavedení mechanismů spolupráce na úrovni EU s právními požadavky pro klíčové soukromé subjekty a orgány veřejné správy.

Dobrovolné iniciativy by se v zásadě podobaly iniciativám uvedeným v alternativě č. 1, zatímco právní požadavky by byly shodné s požadavky stanovenými v alternativě č. 2, a to jak co se týká adresátů, tak podstaty jejich povinností.

Agentura ENISA by Komisi, členským státům i soukromému sektoru poskytovala podporu a technické poznatky, například formou technických pokynů a doporučení.

8. ANALÝZA DOPADŮ

Posouzení se kromě úrovně bezpečnosti zabývá ekonomickými a sociálními dopady uvedených tří alternativ. Rovněž bere v úvahu náklady spojené s alternativami č. 2 a 3.

Žádná ze zvažovaných alternativ neimplikuje žádné dopady na životního prostředí, které by bylo možné s přesností předvídat.

8.1. Alternativa č. 1 – bez opatření („základní scénář“)

Úroveň bezpečnosti: Je nepravděpodobné, že by všechny členské státy dosáhly srovnatelné úrovně vnitrostátních kapacit a připravenosti nezbytné ke zvýšení bezpečnosti a zajištění spolupráce a spolehlivého sdílení informací na úrovni EU. Nepodařilo by se vytvořit rovné podmínky, pokud jde o řízení rizik a transparentnější postupy v souvislosti s incidenty, a i nadále by tak existovaly mezery v legislativě.

Ekonomické dopady: Dopad této varianty by závisel na tom, do jaké míry by se členské státy řídily doporučeními Komise. Nedostatečná úroveň bezpečnosti v méně rozvinutých členských státech by narušila jejich konkurenceschopnost a růst a vystavila by je rizikům a bezpečnostním incidentům. Vzhledem k současným trendům by incidenty v oblasti bezpečnosti sítí a informací byly pro podniky i spotřebitele čím dál patrnější a staly by se překážkou pro dokončení vnitřního trhu.

Sociální dopady: Pokračování a očekávané zhoršování bezpečnostních incidentů, rizik a hrozeb by mělo negativní vliv na důvěru občanů v online služby.

8.2. Alternativa č. 2 – regulatorní přístup

Úroveň bezpečnosti: Povinnosti uložené členským státům by zaručovaly jejich odpovídající vybavenost a přispěly by k vytvoření vzájemné důvěry, která je předpokladem efektivní spolupráce na úrovni EU.

Zavedení povinného řízení rizik v oblasti bezpečnosti sítí a informací pro orgány veřejné správy a klíčové soukromé subjekty by bylo silným podnětem ke skutečně účinnému vytyčení a řízení rizik. Celkové dodatečné náklady na splnění těchto povinností, které by musela nést různá odvětví v EU, by se pohybovaly v rozmezí **1 až 2 miliard EUR**. **Pro malý až střední podnik** by tyto náklady na dodržování předpisů činily **2500 až 5000 EUR**.

Ekonomický dopad: V důsledku vyšší úrovně bezpečnosti by se snížily finanční ztráty spojené s riziky a incidenty v oblasti bezpečnosti sítí a informací. Důvěra podniků a

spotřebitelů v digitální svět by zesílila a přinesla prospěch vnitřnímu trhu. Podpora lepší kultury řízení rizik by také zvýšila poptávku po bezpečných ICT produktech a řešeních.

Sociální dopad: Vyšší úroveň bezpečnosti by zvýšila důvěru v online služby na straně občanů, kteří by tak mohli v plné míře těžit z výhod digitálního světa (např. sociálních médií, e-learningu či elektronického zdravotnictví).

8.3. Alternativa č. 3 – kombinovaný přístup

Úroveň bezpečnosti: Stejně jako u alternativy č. 1 zde neexistuje záruka, že úroveň bezpečnosti založená na vnitrostátních kapacitách pro zajištění bezpečnosti sítí a informací a spolupráce na úrovni EU by se v důsledku dobrovolných iniciativ zlepšila. Zavedení určitých povinností v oblasti bezpečnosti pro orgány veřejné správy a klíčové soukromé subjekty by však bylo silným podnětem ke skutečně efektivnímu vytyčení a řízení rizik. Ovšem v členských státech, které by se neřídily doporučeními Komise ohledně zřízení kapacit pro zajištění bezpečnosti sítí a informací, by tyto mechanismy byly neefektivní.

Ekonomické dopady: Tempo rozvoje v jednotlivých členských státech by se výrazně lišilo. Nedostatečná úroveň bezpečnosti v méně rozvinutých členských státech by narušila jejich konkurenceschopnost a růst a vystavila by je negativním důsledkům rizik a bezpečnostních incidentů.

Sociální dopady: Pokračování a očekávané zhoršování bezpečnostních incidentů, rizik a hrozeb by mělo negativní vliv na důvěru občanů v online služby, zejména v těch členských státech, které nepovařují bezpečnost sítí a informací za prioritu.

9. SROVNÁNÍ ALTERNATIV

Alternativy č. 1 a 3 se pro naplnění cílů této politiky nepovažují za vhodné, a proto se nedoporučují. Jejich účinnost by závisela na tom, zda by přístup založený na dobrovolnosti skutečně přinesl určitou minimální úroveň bezpečnosti sítí a informací, a v případě alternativy č. 3 také na dobré vůli členských států zřídit kapacity a spolupracovat s ostatními členskými státy.

Upřednostňovanou alternativou je alternativa č. 2, neboť její realizací by se ochrana spotřebitelů, podniků a vládních institucí v EU před bezpečnostními incidenty, hrozbami a riziky výrazně zvýšila. Kromě toho tzv. zametení před vlastním prahem by zvýšilo mezinárodní dosah EU a dodalo by jí na důvěryhodnosti coby partnera pro dvoustrannou i mnohostrannou spolupráci. Evropská unie by díky tomu byla v lepším postavení i pokud jde o prosazování základních práv a hodnot EU v zahraničí.

10. SLEDOVÁNÍ A HODNOCENÍ

V kapitole 10 zprávy o posouzení dopadů je předloženo několik klíčových ukazatelů pokroku v dosahování vytyčených cílů, mimo jiné:

- u cíle č. 1 počet členských států, které jmenovaly orgán odpovědný za zajišťování bezpečnosti sítí a informací a skupinu CERT nebo přijaly národní strategii kybernetické bezpečnosti a pohotovostní plán či plán spolupráce pro případ kybernetického incidentu,
- u cíle č. 2 počet odpovědných orgánů a skupin CERT členských států, které se zapojily do sítě, a objem informací o bezpečnostních rizicích a incidentech vyměňovaných prostřednictvím sítě,
- u cíle č. 3 míra investic do bezpečnosti sítí a informací ze strany klíčových soukromých subjektů a orgánů veřejné správy a počet oznámení incidentů značného dopadu v oblasti bezpečnosti sítí a informací.