



KOMISE EVROPSKÝCH SPOLEČENSTVÍ

V Bruselu dne 31.5.2006
KOM(2006) 251 v konečném znění

**SDĚLENÍ KOMISE RADĚ, EVROPSKÉMU PARLAMENTU, EVROPSKÉMU
HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ**

Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“

{SEK(2006) 656}

OBSAH

1.	Úvod.....	3
2.	Zlepšení bezpečnosti informační společnosti: klíčové úkoly.....	4
3.	Dynamický přístup k bezpečné informační společnosti.....	6
3.1.	Dialog.....	7
3.2.	Partnerství	8
3.3.	Posílení účasti.....	9
4.	Závěry	10

SDĚLENÍ KOMISE RADĚ, EVROPSKÉMU PARLAMENTU, EVROPSKÉMU HOSPODÁŘSKÉMU A SOCIÁLNÍMU VÝBORU A VÝBORU REGIONŮ

Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“

1. Úvod

Sdělení „i2010 – evropská informační společnost pro růst a zaměstnanost“¹ zdůraznilo důležitost bezpečnosti sítí a informací pro vytvoření jednotného evropského informačního prostoru. Dostupnost, spolehlivost a bezpečnost sítí a informačních systémů je ve stále větší míře ústřední součástí našich hospodářství i struktury společnosti.

Toto sdělení si klade za cíl oživit strategii Evropské komise uvedenou v roce 2001 ve sdělení „Bezpečnost sítí a informací: návrh evropského politického přístupu“². Přezkoumává současný stav hrozeb, kterým bezpečnost informační společnosti čelí, a určuje, jaké další kroky by měly být uskutečněny ke zlepšení bezpečnosti sítí a informací.

Cílem je na základě zkušeností získaných na úrovni členských států a Evropského společenství pokračovat v Evropě v rozvoji dynamické, globální strategie založené na kultuře bezpečnosti a stojící na **dialogu, partnerství a posílení účasti**.

Pro boj s hrozbami v oblasti bezpečnosti, kterým informační společnost čelí, vypracovalo Evropské společenství přístup, který zahrnuje tři prvky: konkrétní opatření v oblasti bezpečnosti sítí a informací, předpisový rámec pro elektronické komunikace (který zahrnuje otázky soukromí a ochrany dat) a boj proti počítačové trestné činnosti. I když lze tyto tři aspekty do jisté míry rozvíjet samostatně, řada vzájemných závislostí vyžaduje koordinovanou strategii. Toto sdělení takovou strategii stanoví a poskytuje rámec pro další rozvoj a vytříbení soudržného přístupu k bezpečnosti sítí a informací.

Sdělení z roku 2001 definuje bezpečnost sítí a informací jako „*schopnost sítě nebo informačního systému odolávat, s danou úrovní spolehlivosti, náhodným událostem nebo zlovolným akcím, které narušují dostupnost, pravost, integritu a důvěrnost uložených či přenášených dat i souvisejících služeb, které tyto sítě a systémy nabízejí nebo které jsou jejich prostřednictvím přístupné*“. Během posledních let uskutečnilo Evropské společenství řadu akcí na zlepšení bezpečnosti sítí a informací.

Předpisový rámec pro elektronické komunikace, jehož přezkum právě probíhá, obsahuje ustanovení související s bezpečností. Zejména směrnice o soukromí a elektronických komunikacích³ stanoví povinnost poskytovatele veřejně dostupných služeb elektronických komunikací zajistit bezpečnost svých služeb. Stanoví rovněž opatření proti spamu⁴ a spywaru⁵.

¹ KOM(2005) 229 v konečném znění ze dne 1. června 2005.

² KOM(2001) 298 v konečném znění ze dne 6. června 2001.

³ Směrnice 2002/58/ES.

⁴ Rovněž nazývaný „nevyžádaná obchodní sdělení“.

⁵ Spywarem se rozumí sledovací software zavedený bez řádného upozornění uživatele, bez jeho souhlasu nebo mimo jeho kontrolu.

Důvěryhodnost a bezpečnost rovněž hrají důležitou úlohu v programech Evropského společenství věnovaných výzkumu a vývoji. Šestý rámcový program pro výzkum se těmito tématy zabývá v řadě projektů. V sedmém rámcovém programu bude výzkum související s bezpečností posílen díky zřízení Evropského programu pro výzkum v oblasti bezpečnosti (ESRP)⁶. Dále pak program Bezpečnější internet plus podporuje projekty na vytváření sítí a výměnu osvědčených postupů s cílem bojovat proti škodlivému obsahu šířenému v informačních sítích.

V rámci reakce na bezpečnostní hrozby rozhodlo Evropské společenství v roce 2004 o vytvoření Evropské agentury pro bezpečnost sítí a informací (ENISA). ENISA přispívá k rozvoji kultury bezpečnosti sítí a informací ve prospěch občanů, spotřebitelů, podniků i organizací ve veřejném sektoru v celé Evropské unii (EU).

EU rovněž hraje aktivní úlohu na mezinárodních fórech, která se těmito tématy zabývají, například v OECD, Radě Evropy nebo OSN. Na Světové vrcholné schůzce o informační společnosti v Tunisu EU silně podporovala diskuse o dostupnosti, spolehlivosti a bezpečnosti sítí a informací. Tuniská agenda⁷, která spolu s tuniským závazkem stanoví další kroky pro politickou diskusi o celosvětové informační společnosti, jak ji podpořili vedoucí činitelé z celého světa, zdůrazňuje nutnost pokračovat v boji proti počítačové trestné činnosti a spamu, ale zajistit přitom ochranu soukromí a svobodu projevu. Uvádí, že je třeba dosáhnout společného porozumění v otázkách internetové bezpečnosti, jakož i dále spolupracovat na usnadnění shromažďování a šíření informací týkajících se bezpečnosti a výměny osvědčených postupů mezi všemi zúčastněnými stranami, pokud jde o opatření pro boj proti bezpečnostním hrozbám.

2. ZLEPŠENÍ BEZPEČNOSTI INFORMAČNÍ SPOLEČNOSTI: KLÍČOVÉ ÚKOLY

Navzdory úsilí na mezinárodní, evropské i vnitrostátní úrovni nás bezpečnost stále staví před obtížné problémy.

Zaprvé, útoky na informační systémy jsou ve stále větší míře motivovány ziskem oproti touze po narušení jako takovém. Údaje se protizákonně extrahují – ve stále větší míře bez vědomí uživatele, přičemž množství variant (a rychlost vývoje) malwaru⁸ rychle roste. Dobrým příkladem tohoto vývoje je spam: stává se nástrojem pro viry, podvody a trestnou činnost, například spyware, phishing⁹ a jiné podoby malwaru. Pro své šíření ve stále větší míře využívá tzv. „botnets“¹⁰, tj. napadené servery a počítače, které bez vědomí majitelů slouží k jeho předávání.

Rostoucí využívání mobilních zařízení (včetně mobilních telefonů 3G, přenosných videoher atd.) a mobilních síťových služeb spolu s rychlým vývojem služeb založených na protokolu

⁶ Program ESRP se připravuje v rámci přípravné akce pro výzkum v oblasti bezpečnosti v období 2004–2006.

⁷ *Směrem ke globálnímu partnerství v informační společnosti: Navázání na tuniskou fázi Světové vrcholné schůzky o informační společnosti (WSIS)*, KOM(2006) 181 v konečném znění ze dne 27. dubna 2006.

⁸ Malwarem se rozumí „škodlivý software“.

⁹ „Phishing“ je forma internetových podvodů, jejichž cílem je ukrást cenné informace, například čísla platebních karet a bankovních účtů, uživatelská jména a hesla.

¹⁰ „Botnet“ je síť „botů“, což jsou aplikace, které vykonávají činnost podle dálkově předávaných povelů a na počítač oběti se instalují skrytě.

IP přinese nové problémy. Tyto služby a zařízení by se případně mohly ukázat jako běžnější prostředek pro útoky než osobní počítače, které již dosahují značné úrovně zabezpečení. Všechny nové formy komunikačních platforem a informačních systémů vskutku nevyhnutelně poskytují nové příležitosti pro zlovolné útoky.

Dalším významným trendem je nástup „inteligentního prostředí“, v němž se inteligentní zařízení za podpory počítačových a síťových technologií stanou všudypřítomnými (např. prostřednictvím RFID¹¹, IPv6 a senzorových sítí). Úplně propojený a zasíťovaný každodenní život nabízí významné příležitosti. Nicméně s sebou rovněž nese další rizika, pokud jde o bezpečnost a soukromí. I když společné platformy a aplikace kladně přispívají k interoperabilitě a využívání informačních a komunikačních technologií (IKT), mohou rovněž zvyšovat rizika. Například, čím více se využívá „standardní“ software, tím větší dopad má zneužití slabin nebo výskyt chyb. Nástup určitých „monokultur“ v oblasti softwarových platforem a aplikací může značně usnadnit růst a šíření bezpečnostních hrozeb, například malwaru a virů. **Rozmanitost, otevřenost a interoperabilita jsou neoddělitelnými složkami bezpečnosti a je třeba je podporovat.**

Význam odvětví IKT pro evropské hospodářství a evropskou společnost jako celek nelze zpochybňovat. IKT jsou kritickou složkou inovací a jsou zodpovědné za téměř 40 % růstu produktivity. Kromě toho toto vysoce inovační odvětví provádí více než čtvrtinu evropského výzkumu a vývoje a hraje klíčovou úlohu v tvorbě hospodářského růstu a zaměstnanosti v celém hospodářství. Stále více Evropanů žije ve společnosti skutečně založené na informacích, v níž využívání IKT jakožto základní funkce společenského a hospodářského styku lidí rychle roste. Podle Eurostatu používalo v roce 2004 aktivně internet 89 % evropských podniků a přibližně 50 % spotřebitelů použilo internet nedávno¹².

Narušení bezpečnosti sítí a informací může mít dopad přesahující hospodářský rozměr. Skutečně se vyskytují obecně rozšířené obavy, že problémy s bezpečností mohou vést k odrazení uživatelů a nižšímu využívání IKT, přičemž dostupnost, spolehlivost a bezpečnost jsou nutné podmínky pro zaručení základních práv on-line.

Navíc se, vzhledem k rostoucí míře propojení mezi sítěmi, stávají i další kritické infrastruktury (například dopravní, energetická atd.) stále více závislé na integritě příslušných informačních systémů.

Podniky i občané v Evropě stále podceňují rizika. Dělají to z různých důvodů, ale jako nejdůležitější se v případě podniků jeví nedostatečná viditelnost návratnosti investic do bezpečnosti a v případě občanů skutečnost, že si nejsou vědomi své odpovědnosti v globálním bezpečnostním řetězci.

Vzhledem ke všudypřítomnosti IKT a informačních systémů je bezpečnost sítí a informací skutečně úkolem pro všechny:

- **orgány veřejné správy** musí řešit bezpečnost svých systémů nejen za účelem ochrany informací veřejného sektoru, ale také aby byly příkladem osvědčených postupů pro ostatní subjekty;

¹¹ Rádiová identifikace.

¹² Eurostat, *Internet activities in the European Union* (Internet v Evropské unii), 40/2005.

- **podniky** musí chápat bezpečnost sítí a informací spíše jako aktivum a konkurenční výhodu než jako „negativní náklady“;
- **jednotliví uživatelé** musí pochopit, že jejich domácí systémy jsou zásadní pro celý „bezpečnostní řetězec“.

Pro úspěšné řešení uvedených problémů potřebují všechny zúčastněné strany spolehlivé údaje o incidentech a tendencích v oblasti bezpečnosti informací. Spolehlivé a úplné údaje o incidentech se však obtížně získávají, z řady důvodů – od rychlého průběhu bezpečnostních incidentů po neochotu některých organizací veřejně informovat o narušení bezpečnosti. **Prohlubování znalostí o problému** je nicméně jedním ze základních kamenů rozvoje kultury bezpečnosti.

Je důležité, aby programy na zvýšení povědomí, které zdůrazňují bezpečnostní hrozby, nepodřývaly důvěru spotřebitelů a uživatelů tím, že by se zaměřovaly pouze na negativní aspekty bezpečnosti. Proto by **bezpečnost sítí a informací měla být pokud možno prezentována jako přednost a příležitost** než jako povinnost a náklady. Je třeba ji považovat za aktivum pro budování důvěryhodnosti organizace a důvěry spotřebitelů, za konkurenční výhodu podniků provozujících informační systémy, a za otázku kvality služeb u poskytovatelů služeb ve veřejném i soukromém sektoru.

Klíčovým úkolem pro tvůrce politik je dosažení uceleného přístupu. Tento přístup musí zohlednit příslušné úlohy různých zúčastněných stran. Musí zajistit řádnou koordinaci řady právních předpisů a veřejných politik, které mají přímý či nepřímý dopad na bezpečnost sítí a informací. Procesy liberalizace, deregulace a konvergence daly vzniknout velkému počtu subjektů rozdělených do různých skupin zúčastněných stran, což úkol neusnadňuje. Pro dosažení tohoto cíle může být důležitý příspěvek agentury ENISA. ENISA by mohla sloužit jako centrum pro sdílení informací, spolupráci všech zúčastněných stran a výměnu doporučených postupů v rámci Evropy i se zbytkem světa, a přispět tak ke konkurenceschopnosti našich odvětví IKT a k dobrému fungování vnitřního trhu.

3. DYNAMICKÝ PŘÍSTUP K BEZPEČNÉ INFORMAČNÍ SPOLEČNOSTI

Bezpečná informační společnost musí být založena na **rozšířené bezpečnosti sítí a informací** a na široce rozšířené **kultuře bezpečnosti**. Za tímto účelem Komise navrhuje **dynamický a integrovaný přístup**, který zahrnuje všechny zúčastněné strany a je založen na **dialogu, partnerství a posílení účasti**. Vzhledem k doplňujícím se úlohám veřejného a soukromého sektoru, pokud jde o vytváření kultury bezpečnosti, musí být politické iniciativy v této oblasti založeny na **otevřeném dialogu s účastí mnoha zúčastněných stran**.

Tento přístup a související akce doplní a obohatí plán Komise pokračovat v roce 2006 v rozvoji komplexního a dynamického politického rámce prostřednictvím řady iniciativ:

- (1) vydání sdělení, které se bude zabývat vývojem v oblasti spamu a hrozeb, jako jsou spyware a jiné podoby malwaru;
- (2) předložení návrhů na zlepšení spolupráce mezi orgány činnými v trestním řízení a zabývajících se novými podobami trestné činnosti, jež zneužívají internet a narušují činnost kritických infrastruktur. To bude předmětem zvláštního sdělení o počítačové trestné činnosti.

Tyto politické iniciativy rovněž doplňují činnosti plánované k dosažení cílů zelené knihy Komise o Evropském programu na ochranu kritické infrastruktury (EPCIP)¹³, který byl vypracován na základě požadavku zasedání Rady v prosinci 2004. Projednávání zelené knihy pravděpodobně povede k akčnímu plánu, který sloučí celkový „zastřešující“ přístup k ochraně kritických infrastruktur s potřebnými odvětvovými politikami, včetně politiky v odvětví IKT. Konkrétní politika v odvětví IKT by prostřednictvím **vícestranného dialogu zúčastněných stran** prošetřila příslušné hospodářské, obchodní a společenské hybné síly s cílem posílit bezpečnost a odolnost sítí a informačních systémů.

Rovněž i přezkum předpisového rámce pro elektronické komunikace probíhající v roce 2006 vezme v úvahu prvky pro zlepšení bezpečnosti sítí a informací, například technická a organizační opatření, která by měli přijmout poskytovatelé služeb, ustanovení týkající se oznamování bezpečnostních incidentů, jakož i konkrétní nápravné prostředky a sankce v případě nesplnění povinností.

Poskytování řešení, služeb a bezpečnostních produktů koncovým uživatelům je ve značné míře záležitostí pro soukromý sektor. Je proto strategicky důležité, aby **evropský průmysl byl jak náročným uživatelem** bezpečnostních produktů a služeb, **tak konkurenceschopným dodavatelem** produktů a služeb v oblasti bezpečnosti sítí a informací.

Vlády členských států musí být schopny určit a zavést osvědčené postupy tvorby politiky, jakož i demonstrovat odhodlání dosáhnout uvedených politických cílů tím, že své informační systémy budou spravovat bezpečně. Orgány veřejné správy v členských státech i na úrovni EU hrají klíčovou úlohu v řádném informování uživatelů, aby tito uživatelé mohli zlepšit svou vlastní bezpečnost. Prioritami by proto mělo být zvyšování povědomí o otázkách bezpečnosti sítí a informací a poskytování vhodných a včasných informací o hrozbách, rizicích a upozorněních, ale také o osvědčených postupech, prostřednictvím webových portálů věnovaných bezpečnosti elektronických technologií. Proto by významným úkolem agentury ENISA mohlo být ověření uskutečnitelnosti **vytvoření evropského mnohojazyčného systému pro varování a sdílení informací**, který by stavěl na stávajících nebo plánovaných vnitrostátních veřejných i soukromých iniciativách a tyto iniciativy spojoval.

Celosvětový rozměr bezpečnosti sítí a informací vybízí Komisi k intenzivnější **podpoře celosvětové spolupráce v otázkách bezpečnosti sítí a informací** na mezinárodní úrovni a ve spolupráci s členskými státy, zejména prováděním agendy přijaté na Světové vrcholné schůzce o informační společnosti (WSIS) v listopadu 2005.

Konečně, výzkum a vývoj, zejména na úrovni EU, pomůže rozvíjet nová a inovační partnerství k posílení růstu celého evropského odvětví IKT, a zejména evropského odvětví bezpečnosti IKT. Komise bude proto usilovat o přidělení příslušných finančních prostředků pro výzkum v rámci sedmých rámcových programů EU v oblasti bezpečnosti sítí a informací a technologií spolehlivosti.

3.1. Dialog

*3.1.1. Jako první krok k rozšíření dialogu mezi orgány veřejné správy Komise navrhuje zahájení **srovnávací analýzy vnitrostátních politik týkajících se bezpečnosti sítí a informací**, včetně zvláštních politik bezpečnosti ve veřejném sektoru. Tato činnost pomůže určit nejúčinnější postupy, které pak budou moci být zaváděny, kdekoli to*

¹³ KOM(2005) 576 v konečném znění ze dne 17. listopadu 2005.

bude možné, v širším měřítku v celé EU a pomohou orgánům veřejné správy prosazovat osvědčené postupy v oblasti bezpečnosti. Práce na elektronické identifikaci, například v rámci nedávného akčního plánu „eGovernment“, může v tomto ohledu hrát důležitou úlohu.

Pokud budou výsledky srovnávací analýzy vhodně strukturovány, **vyplnou z nich osvědčené postupy pro zvýšení povědomí mezi malými a středními podniky a občany o potřebě** plnit jejich vlastní úkoly a požadavky v oblasti bezpečnosti sítí a informací, jakož i pro zlepšení schopností k tomu potřebných. ENISA by měla být vyzvána k vykonávání aktivní úlohy v tomto dialogu i při sjednocování a výměně osvědčených postupů.

3.1.2. *Je zapotřebí **strukturovaná vícestranná diskuse zúčastněných stran** o nejvhodnějších způsobech, jak využít stávající prostředky a regulační nástroje k dosažení vhodné společenské rovnováhy mezi bezpečností a ochranou základních práv, včetně soukromí. K diskusi přispěje plánovaná konference „i2010 – Cesta ke všudypřítomné evropské informační společnosti“, kterou organizuje nadcházející finské předsednictví, jakož i konzultace o bezpečnosti technologie RFID a jejich důsledcích pro soukromí, jež je součástí širší konzultace, kterou nedávno zahájila Komise. Kromě toho Komise uspořádá:*

- obchodní setkání s cílem podnítit odhodlání průmyslových odvětví přijmout účinné přístupy k zavedení kultury bezpečnosti **v průmyslu**;
- seminář o způsobech, jak zvýšit povědomí o bezpečnosti a posílit důvěru **koncových uživatelů** ve využívání elektronických sítí a informačních systémů.

3.2. Partnerství

3.2.1. *Pro účinnou tvorbu politik je třeba pečlivě znát povahu a rozsah úkolů. K tomu jsou zapotřebí nejen spolehlivé a aktuální statistické a ekonomické údaje o incidentech v oblasti informační bezpečnosti i o úrovni důvěry spotřebitelů a uživatelů, ale také aktuální údaje o rozsahu odvětví bezpečnosti IKT v Evropě a souvisejících tendencích. Komise hodlá požádat agenturu ENISA o navázání **důvěryhodného partnerství s členskými státy a zúčastněnými stranami** za účelem vytvoření **vhodného rámce pro sběr údajů**, včetně postupů a mechanismů pro sběr a analýzu údajů z celé EU o bezpečnostních incidentech a důvěře spotřebitelů.*

Vzhledem ke značné roztržiténosti trhu v EU a jeho zvláštní povaze Komise současně vyzve členské státy, soukromý sektor a výzkumnou komunitu k **vytvoření strategického partnerství** s cílem zajistit dostupnost údajů o odvětví bezpečnosti IKT a o vývoji tržních tendencí v EU, pokud jde o produkty a služby.

3.2.2. *Komise s cílem zlepšit schopnosti EU reagovat na hrozby pro bezpečnost sítí požádá agenturu ENISA o ověření **uskutečnitelnosti evropského systému pro varování a sdílení informací**, který by usnadnil účinnou reakci na stávající i vznikající hrozby, jimž elektronické sítě čelí. Požadavkem takového systému bude **mnohojazyčný portál EU** poskytující přizpůsobené informace o hrozbách, rizicích a varováních.*

3.3. Posílení účasti

Posílení účasti všech skupin zúčastněných stran je nutnou podmínkou pro zvyšování povědomí o potřebách a rizicích v oblasti bezpečnosti s cílem podporovat bezpečnost sítí a informací.

3.3.1. *V tomto směru Komise vyzývá **členské státy**, aby:*

- se aktivně účastnily navržené srovnávací analýzy vnitrostátních politik v oblasti bezpečnosti sítí a informací;
- v těsné spolupráci s agenturou ENISA podporovaly kampaně na zvýšení povědomí o přednostech, výhodách a přínosech uplatňování účinných bezpečnostních technologií, postupů a chování;
- využily zavádění služeb elektronické veřejné správy k propagaci a podpoře dobrých bezpečnostních postupů, které lze poté rozšířit i do jiných odvětví;
- podněcovaly rozvoj programů bezpečnosti sítí a informací jako součást osnov vyššího vzdělávání.

3.3.2. *Komise rovněž vyzývá zúčastněné strany ze **soukromého sektoru**, aby vyvíjely iniciativy na:*

- vypracování vhodné definice odpovědností výrobců softwaru a poskytovatelů internetových služeb, pokud jde o poskytování vhodné a kontrolovatelné úrovně bezpečnosti. Zde je zapotřebí podpora standardizovaných postupů, které by splňovaly společně dohodnuté bezpečnostní normy a pravidla pro osvědčené postupy;
- podporu rozmanitosti, otevřenosti, použitelnosti a hospodářské soutěže jako klíčových hnacích sil v oblasti bezpečnosti, jakož i na podporu zavádění produktů, procesů a služeb zvyšujících bezpečnost s cílem předcházet a bránit krádežím identity a jiným útokům narušujícím soukromí;
- šíření dobrých bezpečnostních postupů, které by sloužily jako základní úroveň bezpečnosti a obchodní kontinuity, mezi provozovateli sítí, poskytovateli služeb a malými a středními podniky;
- podporu programů odborné přípravy v podnikatelské sféře, zejména pro malé a střední podniky, aby pracovníci získali znalosti a dovednosti potřebné k účinnému provádění bezpečnostních postupů;

- práci na cenově dostupných programech osvědčování bezpečnosti pro produkty, procesy a služby, které budou zohledňovat specifické potřeby EU (zejména s ohledem na ochranu soukromí);
- zapojení odvětví pojišťovnictví do vývoje vhodných nástrojů a metod na řízení rizik s cílem řešit rizika související s IKT a podporovat kulturu řízení rizik v organizacích a firmách (zejména v malých a středních podnicích).

4. ZÁVĚRY

Stanovení a plnění úkolů v oblasti bezpečnosti v souvislosti s informačními systémy a sítěmi v EU vyžaduje plné odhodlání všech zúčastněných stran. Politický přístup naznačený v tomto sdělení toho hodlá dosáhnout posílením **vícestranného přístupu zahrnujícího zúčastněné strany**. Tím by se stavělo na vzájemných zájmech, stanovily by se příslušné úlohy a rozvíjel by se dynamický rámec na podporu účinné tvorby veřejné politiky a iniciativ soukromého sektoru.

Komise v polovině roku 2007 podá Radě a Parlamentu zprávu o zahájených činnostech, o počátečních zjištěních a o stavu provádění jednotlivých iniciativ, včetně iniciativ a činností agentury ENISA, členských států a soukromého sektoru. Komise případně předloží návrh doporučení o bezpečnosti sítí a informací.