31992D0242

8.5.1992 ÚŘEDNÍ VĚSTNÍK EVROPSKÝCH SPOLEČENSTVÍ L 123/19

ROZHODNUTÍ RADY ze dne 31. března 1992 o bezpečnosti informačních systémů

(92/242/EHS)

RADA EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského hospodářského společenství, a zejména na článek 235 této smlouvy,

s ohledem na návrh Komise [1],

s ohledem na stanovisko Evropského parlamentu [2],

s ohledem na stanovisko Hospodářského a sociálního výboru [3],

vzhledem k tomu, že úkolem Společenství je zřízením společného trhu a postupným sbližováním hospodářských politik členských států podporovat v celém Společenství harmonický rozvoj hospodářských činností, stálý a vyvážený rozvoj, zvýšenou stabilitu, rychlejší zvyšování životní úrovně a těsnější vztahy mezi členskými státy;

vzhledem k tomu, že informace uložená, zpracovaná a předávaná elektronickými prostředky se stává stále významnější v hospodářské a sociální činnosti;

vzhledem k tomu, že zavádění účinných globálních komunikací a širšího využívání elektronického zpracování informací zdůrazňuje nezbytnost odpovídající ochrany;

vzhledem k tomu, že ve svých rozpravách a usneseních Evropský parlament opakovaně zdůraznil význam bezpečnosti informačních systémů;

vzhledem k tomu, že Hospodářský a sociální výbor zdůraznil potřebu projednat otázky bezpečnosti informačních systémů v rámci akcí Společenství, zejména s ohledem na dopad na vytváření vnitřního trhu;

vzhledem k tomu, že akce na úrovni vnitrostátní, mezinárodní a na úrovni Společenství poskytují dobrou základnu;

vzhledem k tomu, že mezi telekomunikacemi, informačními technologiemi, normalizací, informačním trhem a zásadami výzkumu a technologického vývoje (R & DT) a již vykonanou prací Společenství v těchto oblastech je úzký vztah;

vzhledem k tomu, že je vhodné sjednotit opatření s využitím stávajících poznatků na vnitrostátní a mezinárodní úrovni a s podporou spolupráce mezi hlavními dotčenými stranami; že je tedy výhodné postupovat v rámci jednotného akčního plánu;

vzhledem k tomu, že složitost bezpečnosti informačních systémů vyžaduje vytvoření strategií umožňujících volný pohyb informací uvnitř jednotného trhu a současně zajišťujících bezpečnost používání informačních systémů v celém Společenství;

vzhledem k tomu, že je věcí každého členského státu, aby vzal v úvahu omezení vyplývající z bezpečnosti a veřejného pořádku;

vzhledem k tomu, že odpovědnost členských států v této oblasti předpokládá společný přístup založený na úzké spolupráci s vyššími úředníky členských států;

vzhledem k tomu, že je třeba stanovit akční plán na počáteční období dvaceti čtyř měsíců a zřízení výboru vyšších úředníků s dlouhodobým pověřením, jako poradního orgánu Komise v oblasti bezpečnosti informačních systémů;

vzhledem k tomu, že částka 12 milionů ECU se považuje za nezbytnou pro provádění akce v počátečním období dvaceti čtyř měsíců; že pro rok 1992 s ohledem na současný finanční výhled činí částka považovaná za nezbytnou 2 miliony ECU;

vzhledem k tomu, že částky, které mají být použity pro financování programu na období po rozpočtovém roce 1992 se budou muset zaznamenat do platného finančního rámce Společenství,

ROZHODLA TAKTO:

Článek 1

Tímto rozhodnutím se přijímá akce v oblasti bezpečnosti informačních systémů. Zahrnuje:

— rozvíjení globálních strategií pro zajištění bezpečnosti informačních systémů (akční plán) pro počáteční období dvaceti čtyř měsíců a

— vytvoření skupiny vyšších úředníků s dlouhodobým pověřením (dále jen „výbor“) jako poradního orgánu Komise pro akce v oblasti bezpečnosti informačních systémů.

(1) Úř. věst. C 277, 5.11.1990, s. 18.
(2) Úř. věst. C 94, 13.3.1992.
(3) Úř. věst. C 159, 17.6.1991, s. 38.

Článek 2

1. Komise systematicky konzultuje výbor o otázkách vztahujících se na bezpečnost informačních systémů pro různé činnosti Společenství, zejména o definici strategií a programů práce.

2. Akční plán, jak je uvedeno v příloze, zahrnuje přípravné práce na tato témata:

I. vývoj strategického rámce pro bezpečnost informačních systémů;

II. zjištění potřeb uživatelů a poskytovatelů služeb v oblasti bezpečnosti informačních systémů;

III. vypracování řešení pro některé krátkodobé a střednědobé potřeby uživatelů, dodavatelů a poskytovatelů služeb;

IV. vypracování specifikací, normalizace, hodnocení a osvědčování ve vztahu k bezpečnosti informačních systémů;

V. technologický a funkční vývoj v oblasti bezpečnosti informačních systémů;

VI. zavedení bezpečnosti informačních systémů.

Článek 3

1. Výše finančních prostředků Společenství považovaná za nezbytnou pro provedení akce pro počáteční období je 12 milionů ECU včetně 2 milionů ECU pro rok 1992 v rámci finančního výhledu na roky 1988–1992.

Pro následující období plnění programu bude třeba zaznamenat částku do platného finančního rámce Společenství.

2. Rozpočtový orgán určí volné prostředky pro každý finanční rok, s přihlédnutím k zásadám řádné správy uvedeným v článku 2 finančního nařízení, které se vztahuje na souhrnný rozpočet Evropských společenství.

Článek 4

Skupina nezávislých odborníků provede pro Komisi zhodnocení pokroku dosaženého během počátečního období. Zpráva této skupiny, doplněná případnými poznámkami Komise, je předložena Evropskému parlamentu a Radě.

Článek 5

1. Komise odpovídá za provedení akce. Bude jí nápomocen poradní výbor složený ze zástupců členských států za předsednictví zástupce Komise.

2. Akční plán je prováděn v souladu s cíli vymezenými v článku 2 a podle potřeby je aktualizován. Obsahuje podrobné cíle a typy akcí, které je třeba uskutečnit, jakož i související finanční opatření. Komise vyzve k předložení návrhů na základě akčního plánu.

3. Akční plán musí být prováděn v úzké spolupráci s hlavními činiteli odvětví. Musí respektovat, podporovat a doplňovat probíhající normalizační činnosti na evropské a mezinárodní úrovni v této oblasti.

Článek 6

1. Postup stanovený v článku 7 se vztahuje na

— opatření související s politikou Společenství v oblasti bezpečnosti informačních systémů.

2. Postup stanovený v článku 8 se vztahuje na:

— vypracování a aktualizaci akčního plánu uvedeného v článku 5,

— obsah výzvy k předkládání návrhů, zhodnocení návrhů a předpokládanou částku příspěvku Společenství na opatření, pokud přesahuje 200 000 ECU,

— spolupráci organizací mimo Společenství na jakékoli činnosti, kterou upravuje toto rozhodnutí;

— na způsoby šíření, ochrany a zhodnocení výsledků opatření;

— opatření, která mají být přijata pro vyhodnocení akce.

3. Je-li výše příspěvku Společenství na opatření menší nebo rovná 200 000 ECU, konzultuje Komise výbor o opatřeních, která mají být přijata, a informuje ho o výsledku svého odhadu.

Článek 7

Zástupce Komise předloží výboru návrh opatření, která mají být přijata. Výbor zaujme své stanovisko k tomuto návrhu ve lhůtě, kterou může předseda stanovit podle naléhavosti dané věci, případně hlasováním.

Stanovisko je uvedeno do zápisu; kromě toho má každý členský stát právo požádat, aby byl v tomto zápisu uveden jeho postoj.

Komise přihlíží co nejvíce ke stanovisku podanému výborem. Sdělí výboru způsob, jakým vzala toto stanovisko v úvahu.

Článek 8

Zástupce Komise předloží výboru návrh opatření, která mají být přijata. Výbor zaujme své stanovisko k tomuto návrhu ve lhůtě, kterou může předseda stanovit podle naléhavosti dané věci. Stanovisko se přijímá většinou podle čl. 148 odst. 2 Smlouvy pro přijímání rozhodnutí, která má Rada přijímat na návrh Komise,

přičemž hlasům členských států je přidělena váha podle čl. 148 odst. 2 Smlouvy. Předseda nehlasuje.

Komise přijme zamýšlená opatření, jsou-li v souladu se stanoviskem výboru.

Pokud zamýšlená opatření nejsou v souladu se stanoviskem výboru nebo pokud výbor žádné stanovisko nezaujme, předloží Komise neprodleně Radě návrh opatření, která mají být přijata. Rada se usnese kvalifikovanou většinou.

Pokud se Rada neusnese ve lhůtě tří měsíců od předložení věci Radě, přijme navrhovaná opatření Komise s výjimkou případů, kdy se Rada proti zmíněným opatřením vysloví prostou většinou.

V Bruselu dne 31. března 1992.

Za Radu

předseda

Vitor MARTINS

PŘÍLOHA

Přehled směrů akce

HLAVNÍ SMĚRY AKČNÍHO PLÁNU V OBLASTI BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

ÚVOD

Cílem akčního plánu je rozvoj globálních strategií zaměřených na to, aby uživatelům a tvůrcům elektronicky uchovávaných, zpracovávaných nebo předávaných informací byla poskytována odpovídající ochrana informačních systémů proti náhodným nebo úmyslným ohrožením.

Akční plán bere v úvahu a doplňuje současnou normalizační činnost na světové úrovni.

Zahrnuje tyto směry akce:

— vývoj strategického rámce pro bezpečnost informačních systémů,

— zjištění potřeb uživatelů a poskytovatelů služeb v oblasti bezpečnosti informačních systémů,

— vypracování řešení pro některé krátkodobé a střednědobé potřeby uživatelů, dodavatelů a poskytovatelů služeb,

— vypracování specifikací, normalizace, hodnocení a osvědčování ve vztahu k bezpečnosti informačních systémů,

— technologický a operační vývoj v oblasti bezpečnosti informačních systémů,

— zavedení bezpečnosti informačních systémů.

Akční plán provádí Komise v úzké spolupráci se souvisejícími akcemi členských států a ve spojení s akcemi Společenství v oblasti výzkumu a technologického vývoje v této oblasti.

1. **Směr akce I: vývoj strategického rámce pro bezpečnost informačních systémů**

1.1 *Předmět*

Bezpečnost informačních systémů se považuje za kvalitu, která je nezbytná všude v moderní společnosti. Elektronické informační služby vyžadují bezpečné telekomunikační infrastruktury, zabezpečený software a hardware, jakož i bezpečné podmínky užívání a správy. Je třeba vytvořit globální strategii, která vezme v úvahu všechna hlediska bezpečnosti informačních systémů a vyloučí veškeré dílčí přístupy. Všechny strategie bezpečnosti elektronicky zpracovávaných informací musí brát v úvahu přání všech společností pracovat účinně a přitom se chránit v rychle se měnícím světě.

1.2 *Cíl*

Musí být vytvořen strategický rámec tak, aby byly sloučeny sociální, hospodářské a politické cíle s technickými, provozními a právními možnostmi Společenství v mezinárodních souvislostech. Osoby činné v daném odvětví, které pracují společně na vývoji společného postoje a smluveného strategického rámce, musí nalézt citlivou rovnováhu mezi různými zájmy, cíli a omezeními. Jedná se o předpoklad pro sladění zájmů a potřeb jak v oblasti politiky, tak průmyslového rozvoje.

1.3 *Situace a tendence*

Situace se vyznačuje rostoucím vědomím potřeby jednat. Pokud se však neobjeví podnět pro koordinaci opatření, je velmi pravděpodobné, že rozptýlené snahy v různých odvětvích vytvoří situaci, která bude ve skutečnosti protikladná, a bude postupně vytvářet stále více právních, sociálních a hospodářských obtíží.

1.4 *Potřeby, možnosti a priority*

Takový rámec musí zpracovat a prozkoumat analýzu a zvládnutí rizik souvisejících se zranitelností informačních systémů a souvisejících služeb, harmonizaci právních předpisů týkajících se zneužívání a nesprávného užívání výpočetní techniky a telekomunikací, administrativní infrastruktury včetně bezpečnostních politik, a jak mohou být tyto politiky účinně využity v různých průmyslových odvětvích nebo oblastech, sociální zájmy a zájmy na ochranu soukromí (například použití systémů identifikace, ověřování pravosti, dokazatelnosti a případně oprávnění v demokratickém prostředí).

Musí být vytvořeny jasné směry, aby byly vypracovány fyzické a logické struktury pro bezpečné rozložení informačních služeb, normy, hlavní směry a definice pro produkty a služby se zajištěnou bezpečností, pilotní projekty a prototypy, aby byla zajištěna životnost různých administrativních struktur, jakož i struktur a norem týkajících se potřeb zvláštních odvětví.

Je třeba posílit vědomí o obtížích spojených s bezpečností, aby došlo ke zvýšení zájmu uživatelů o bezpečnost v oblasti informačních technologií (IT).

2. **Směr akce II: zjištění potřeb uživatelů a poskytovatelů služeb v oblasti bezpečnosti informačních systémů**

2.1 *Předmět*

Bezpečnost informačních systémů je podstatnou podmínkou bezúhonnosti a věrohodnosti obchodního využití, duševního vlastnictví a důvěrnosti. To vytváří otázku citlivé rovnováhy – a někdy výběru – mezi podporou volného obchodu na jedné straně a ochranou soukromí a duševního vlastnictví na straně druhé. K výběru a kompromisu musí dojít na základě globálního zhodnocení potřeb a dopadu rozhodnutí přijatých v oblasti bezpečnosti informačních systémů pro uspokojení těchto potřeb.

Uživatelé potřebují, aby informační systémy bezpečně fungovaly z technologických, provozních a normotvorných hledisek. Je tedy nezbytné provést systematický průzkum potřeb bezpečnosti informačních systémů, aby došlo k vypracování odpovídajících a účinných opatření.

2.2 *Cíl*

Je vhodné zjistit povahu a vlastnosti potřeb uživatelů a poskytovatelů služeb a jejich vztah k opatřením v oblasti bezpečnosti informačních systémů.

2.3 *Situace a tendence*

Až dosud nebylo vyvinuto žádné jednotné úsilí ke zjištění rychle se vyvíjejících potřeb hlavních činitelů v oblasti bezpečnosti informačních systémů. Některé členské státy Společenství zjistily potřeby harmonizace vnitrostátních činností (zejména „hodnotící kritéria bezpečnosti informačních technologií"). Jednotná hodnotící kritéria a pravidla pro vzájemné uznávání osvědčení o hodnocení mají stále větší význam.

2.4 *Potřeby, možnosti a priority*

Z důvodu, aby byly oprávněné potřeby činitelů odvětví zpracovávány spojitě a průhledně, se jeví jako nezbytné vytvořit schválenou klasifikaci potřeb uživatelů a jejich vztahu k zavádění bezpečnosti informačních systémů.

Je rovněž důležité zjistit potřeby v oblasti právních předpisů a pravidel chování v souvislosti s hodnocením tendencí, pokud jde o charakteristiku a technologii služeb, vymezit další strategie umožňující dosažení cílů prostřednictvím správních, služebních, provozních a technických opatření a zhodnotit účinnost, vhodnost a náklady náhradních voleb a strategií v oblasti bezpečnosti informačních systémů pro uživatele, poskytovatele služeb a operátory.

3. **Směr akce III: vypracování řešení pro některé krátkodobé a střednědobé potřeby uživatelů, dodavatelů a poskytovatelů služeb**

3.1 *Předmět*

V současnosti je možné účinně zamezit neoprávněnému přístupu do počítačů s využitím „izolování", to znamená tradičních organizačních a fyzikálních opatření. Je tomu tak rovněž u elektronické komunikace uvnitř uzavřené skupiny uživatelů, kteří pracují na vymezené síti. Situace je velmi rozdílná, pokud jsou informace sdíleny mezi různými skupinami uživatelů nebo vyměňovány prostřednictvím veřejně nebo obecně přístupné sítě. Technologie, terminály a služby, na jedné straně a normy a související postupy, na straně druhé nejsou obecně v těchto případech schopny zajistit bezpečnost informačních systémů na srovnatelné úrovni.

3.2 *Cíl*

Cílem musí být v krátké lhůtě poskytnutí řešení, která mohou vyhovět okamžitým potřebám uživatelů, poskytovatelů služeb a výrobců. To zahrnuje používání společných hodnotících kritérií bezpečnosti informačních technologií. Tato kritéria mají být sestavena způsobem otevřeným budoucím potřebám a řešením.

3.3 *Situace a tendence*

Některé skupiny uživatelů vytvořily pro svou vlastní potřebu techniky a postupy odpovídající zejména potřebám ověřování pravosti, jednotnosti a dokazatelnosti. Obecně se používají magnetické nebo čipové karty. Některé užívají více méně komplikované techniky šifrování. Často to předpokládá vymezení zvláštního „orgánu" pro skupiny uživatelů. Je však obtížné zobecnit tyto techniky a metody, aby se vyhovělo potřebám v otevřeném prostředí.

ISO pracuje na bezpečnosti informačních systémů OSI (ISO DIS 7498-2) a CCITT v kontextu X 400. Je rovněž možné zahrnout segmenty bezpečnosti do zpráv. Ověřování pravosti, jednotnost a dokazatelnost jsou zpracovávány jako součást zpráv (EDI-FACT) a součást X 400 MHS.

Právní rámec systému Electronic Data Interchange (EDI) je v současnosti stále ve stavu příprav. Mezinárodní obchodní komora zveřejnila jednotná pravidla chování pro výměnu obchodních dat po telekomunikačních sítích.

Několik zemí (například Německo, Francie, Spojené království a Spojené státy americké) vytvořily nebo připravují kritéria pro hodnocení věrohodnosti produktů a systémů informačních technologií a odpovídající postupy pro hodnocení. Tato kritéria byla koordinována s vnitrostátními výrobci a povedou ke vzniku většího počtu spolehlivých výrobků a systémů počínaje jednoduchými produkty. Vytvoření vnitrostátních organizací pověřených prováděním hodnocení a vydáváním osvědčení bude tuto tendenci podporovat.

Většina uživatelů považuje ustanovení v oblasti důvěrnosti za méně důležitá. Je však pravděpodobné, že v budoucnosti se tato situace změní v důsledku velkého rozšíření vyspělých komunikačních služeb a zejména mobilních služeb.

3.4 *Potřeby, možnosti a priority*

Je podstatné vyvinout co nejdříve postupy, normy, produkty a nástroje vhodné pro zajištění bezpečnosti informačních systémů jako takových (počítače, periferní zařízení) a veřejných komunikačních sítí. Prioritu musí mít ověřování pravosti, jednotnost a dokazatelnost. Měly by být uskutečněny pilotní projekty, aby určily správnost navrhovaných řešení. Řešení určitých prioritních potřeb v oblasti EDI se hledají v rámci programu *Tedis* a koordinují v širším rámci tohoto akčního plánu.

4. Směr akce IV: vypracování specifikací, normalizace, hodnocení a osvědčování ve vztahu k bezpečnosti informačních systémů

4.1 *Předmět*

Požadavky v oblasti bezpečnosti informačních systémů se objevují všude, a proto je rozhodující vytvoření společných norem a specifikací. Nevytvoření norem a specifikací sjednaných pro bezpečnost informačních technologií může vytvořit hlavní překážku vývoje postupů a služeb založených na informacích v celém hospodářství a ve společnosti. Je rovněž nezbytné přijmout opatření k urychlení vypracování a užívání technologie a norem v několika oblastech souvisejících s komunikacemi a počítačovými sítěmi, které mají základní význam pro uživatele, průmysl a správu.

4.2 *Cíl*

Na podporu a provádění zvláštních bezpečnostních funkcí v obecných oblastech OSI, ONP, ISDN/IBC a správy sítí je třeba přijmout opatření. Techniky a přístupy v oblasti ověřování, včetně osvědčování, které vede k vzájemnému uznávání, jsou vnitřně spojeny s normalizací a specifikací. Kdykoli je to možné, je vhodné podporovat řešení přijatá na mezinárodní úrovni. Rovněž by mělo být podporováno vytváření a užívání informačních systémů s bezpečnostními funkcemi.

4.3 *Situace a tendence*

Pro řešení otázky bezpečnosti informačních systémů daly významný podnět zejména Spojené státy americké. V Evropě je toto téma projednáváno v souvislosti s normalizací informačních technologií a telekomunikací v rámci ETSI a CEN/Cenelec při přípravě činnosti CCIT a ISO v této oblasti.

Z důvodu rostoucích obav se práce ve Spojených státech amerických rychle zintenzivňuje a prodejci i poskytovatelé služeb stupňují své úsilí v této oblasti. V Evropě samostatně zahájily obdobné činnosti Francie, Německo a Spojené království, ale společné úsilí jako ve Spojených státech amerických se rozvíjí pouze pomalu.

4.4 *Potřeby, možnosti a priority*

V oblasti bezpečnosti informačních systémů jsou normotvorná, provozní administrativní a technická hlediska velice úzce spojena. Normy musí odrážet právní úpravu a musí být možné prokázat, že ustanovení v oblasti bezpečnosti informačních systémů jsou v souladu s normami a právní úpravou. Z více hledisek musí právní úprava obsahovat specifikace, které jsou mimo obvyklý rámec normalizace, to znamená které zahrnují pravidla chování. Požadavky v oblasti norem a pravidel chování se vyskytují ve všech odvětvích bezpečnosti informačních systémů a je třeba rozlišovat požadavky na ochranu odpovídající cílům v oblasti bezpečnosti a některé z technických požadavků, které mohou být svěřeny příslušným evropským subjektům pro normalizaci (CEN/Cenelec/ETSI).

Specifikace a normy musí pokrývat oblasti služeb pro bezpečnost informačních systémů (ověřování osob a podniků, protokoly o dokazatelnosti, právně závazný elektronický důkaz, kontrola autorizace), jejich komunikační služby (ochrana soukromí při přenosu obrazu, hlasu a údajů, ochrana databází a obrazových databází, bezpečnost integrovaných služeb), jejich správu komunikace a bezpečnosti (systém veřejných/soukromých klíčů pro fungování otevřených sítí, pro ochranu správy sítě, ochrana poskytovatelů služeb) a jejich osvědčování (kritéria a úroveň zajištění, postupy zajištění bezpečnosti informačních systémů).

5. Směr akce V: technologický a operační vývoj v oblasti bezpečnosti informačních systémů

5.1 *Předmět*

Výzkum a systematický technologický vývoj, který umožňuje nalézt řešení hospodářsky přijatelná a provozně vyhovující pro soubor stávajících a budoucích potřeb v oblasti bezpečnosti informačních systémů, je nezbytnou podmínkou rozvoje trhu služeb a soutěživosti evropského hospodářství jako celku.

Veškerý technologický vývoj v oblasti bezpečnosti informačních systémů se bude muset vztahovat jak na bezpečnost počítačů, tak na bezpečnost komunikací, neboť většina stávajících systémů jsou systémy rozptýlené, ke kterým se přistupuje přes komunikační služby.

5.2 *Cíl*

Výzkum a systematický technologický vývoj, který umožňuje nalézt řešení hospodářsky přijatelná a provozně vyhovující pro soubor stávajících a budoucích potřeb v oblasti bezpečnosti informačních systémů.

5.3 *Potřeby, možnosti a priority*

Práce v oblasti bezpečnosti informačních systémů by se měla týkat strategií rozvoje a provádění, technologií, jakož i integrace a ověřování.

Strategická práce ve výzkumu a technologickém vývoji by měla zahrnovat studii koncepčních modelů bezpečných systémů (bezpečných s ohledem na nepovolené změny a na zákaz služby), modelů funkčních požadavků, modelů rizik a struktury pro bezpečnost.

Výzkum a technologický vývoj by měl zahrnovat ověřování uživatele a ověřování sdělení (například pomocí hlasové analýzy nebo elektronických podpisů), technická rozhraní a protokoly pro kódování, mechanismy kontroly přístupu a metod provádění pro vytvoření systémů se zaručenou bezpečností.

Ověřování a potvrzování platnosti bezpečnosti technických systémů a její použitelnost by měla být zkoumána prostřednictvím projektů sjednocování a ověřování.

Vedle konsolidace a rozvoje technologie bezpečnosti je nezbytný určitý počet doplňujících opatření v oblasti vytváření, aktualizování a jednotného uplatňování norem, jakož i v oblasti potvrzování platnosti a osvědčování produktů informačních technologií a telekomunikací, pokud jde o jejich vlastnosti v oblasti bezpečnosti včetně potvrzování platnosti a osvědčování metod vytváření a provádění systémů.

Třetí rámcový program Společenství o výzkumu a technologickém vývoji by mohl být použit na podporu projektů spolupráce na úrovni předcházející soutěži a právní úpravě.

6. **Směr akce VI: zavedení bezpečnosti informačních systémů**

6.1 *Předmět*

Podle přesné povahy prvků bezpečnosti informačních systémů bude třeba požadované funkce zahrnout v různých částech informačního systému včetně terminálů, služeb, správy sítě šifrovacích zařízení, čipových karet, veřejných a soukromých klíčů atd. Některé z těchto funkcí budou pravděpodobně zahrnuty v hardwaru nebo softwaru dodávaném prodejcem, zatímco jiné mohou být součástí rozptýlené soustavy (například správa sítě), ve vlastnictví jednotlivých uživatelů (například čipové karty) nebo dodány zvláštním subjektem (například veřejné a soukromé klíče).

Většina bezpečnostních produktů a služeb bude pravděpodobně dodána prodejcem, poskytovatelem služeb a operátorem. Pro určité zvláštní funkce, například dodání veřejných a soukromých klíčů a oprávnění ke kontrole, bude zřejmě nezbytné určit a pověřit vhodné subjekty.

Totéž se vztahuje na osvědčování, hodnocení a ověřování kvality služeb, což jsou funkce, které musí být svěřeny subjektům nezávislým na zájmech prodejců, poskytovatelů služeb nebo operátorů. Tyto subjekty by mohly být soukromé, veřejné nebo zmocněné státem k výkonu těchto funkcí.

6.2 *Cíl*

Pro usnadnění harmonického zavádění bezpečnosti informačních systémů ve Společenství s ohledem na ochranu veřejnosti a obchodních zájmů, bude nezbytné přijmout jednotný přístup pro zavádění bezpečnosti informačních systémů. Pokud budou zmocněny nezávislé subjekty, musí být jejich funkce a podmínky fungování vymezeny a přijaty a – je-li to nezbytné – právně upraveny. Cílem by bylo dospět předběžně, než dojde k vzájemnému uznávání, k jasně vymezenému a dohodnutému rozdělení odpovědnosti mezi různými činiteli na úrovni Společenství.

6.3 *Situace a tendence*

V současnosti je zavádění bezpečnosti informačních systémů řádně organizováno pouze pro zvláštní oblasti a odpovídá pouze jejich zvláštním potřebám. Organizace na evropské úrovni je nejčastěji neformální a ke vzájemnému uznávání ověřování a osvědčování mimo některé uzavřené skupiny nedochází. S rostoucím významem bezpečnosti informačních systémů se stává naléhavou potřeba vymezit jednotný přístup v této oblasti v Evropě a na mezinárodní úrovni.

6.4 *Potřeby, možnosti a priority*

Vzhledem k velkému počtu dotčených činitelů a k úzkým vztahům k otázkám právní úpravy je zvlášť důležité se shodnout na zásadách, které by měly řídit zavádění bezpečnosti informačních systémů.

Při vymezování jednotného přístupu k této otázce bude třeba určit hlediska identifikace a specifikace funkcí vyžadujících, ze své podstaty, zásah nezávislých subjektů (nebo subjektů, které spolupracují). To by mohlo zahrnout takové funkce, jako je správa systému veřejných/soukromých klíčů.

Mimo jiné je nezbytné urychleně určit a upřesnit funkce, které musí být ve veřejném zájmu svěřeny nezávislým subjektům (nebo subjektům, které spolupracují). Tyto funkce by mohly například zahrnovat kontrolu, záruku kvality, ověřování, osvědčování a obdobné funkce.