31992D0242

8.5.1992 ÚRADNÝ VESTNÍK EURÓPSKYCH SPOLOČENSTIEV L 123/19

ROZHODNUTIE RADY
z 31. marca 1992
o bezpečnosti informačných systémov

(92/242/EHS)

RADA EURÓPSKYCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho hospodárskeho spoločenstva, najmä na jej článok 235,

so zreteľom na návrh Komisie [1],

so zreteľom na stanovisko Európskeho parlamentu [2],

so zreteľom na stanovisko Hospodárskeho a sociálneho výboru [3],

keďže úlohou spoločenstva je zriadením spoločného trhu a postupným zbližovaním hospodárskych politík členských štátov podporovať v celom spoločenstve harmonický rozvoj hospodárskych činností, stály a vyvážený rozvoj, zvýšenú stabilitu, rýchlejšie zvyšovanie životnej úrovne a užšie vzťahy medzi členskými štátmi;

keďže informácie uložené, spracované a odovzdávané elektronickými prostriedkami sa stávajú čoraz významnejšími v hospodárskej a sociálnej činnosti;

keďže zavádzanie účinných globálnych komunikácií a širšieho využívania elektronického spracovania informácií zdôrazňuje nevyhnutnosť zodpovedajúcej ochrany;

keďže Európsky parlament vo svojich rozpravách a uzneseniach opakovane zdôraznil význam bezpečnosti informačných systémov;

keďže Hospodársky a sociálny výbor zdôraznil potrebu prerokovať otázky bezpečnosti informačných systémov v rámci akcií spoločenstva, najmä s ohľadom na dopad na vytvorenie vnútorného trhu;

keďže akcie na vnútroštátnej, medzinárodnej úrovni a na úrovni spoločenstva poskytujú dobrú základňu;

keďže medzi telekomunikáciami, informačnými technológiami, normalizáciou, informačným trhom a zásadami výskumu a technického rozvoja (RDT) a už vykonanou prácou spoločenstva v týchto oblastiach existuje úzky vzťah;

keďže je vhodné zabezpečiť zosúladenie snáh pri využívaní existujúcich výsledkov národných a medzinárodných prác a pri presadzovaní spolupráce medzi hlavnými dotknutými stranami; keďže je teda výhodné postupovať v rámci jednotného akčného plánu;

keďže zložitosť bezpečnosti informačných systémov vyžaduje vypracovanie stratégií umožňujúcich voľný pohyb informácií vo vnútri jednotného trhu a súčasne zaisťujúcich bezpečnosť používania informačných systémov v celom spoločenstve;

keďže je povinnosťou každého členského štátu, aby bral do úvahy obmedzenia vyplývajúce z bezpečnosti a verejného poriadku;

keďže zodpovednosť členských štátov v tejto oblasti predpokladá spoločný prístup založený na úzkej spolupráci s vyššími úradníkmi členských štátov;

keďže je potrebné stanoviť akčný plán na začiatočné obdobie dvadsiatich štyroch mesiacov a zriadiť výbor vyšších úradníkov s dlhodobým mandátom ako poradného orgánu Komisie v oblasti bezpečnosti informačných systémov;

keďže suma 12 miliónov ECU sa považuje za nevyhnutnú na vykonávanie akcie pre začiatočné obdobie dvadsiatich štyroch mesiacov; keďže na rok 1992 v súvislosti so súčasným finančným výhľadom predstavuje suma považovaná za nevyhnutnú 2 milióny ECU;

keďže sumy, ktoré majú byť použité na financovanie programu na obdobie po rozpočtovom roku 1992, budú tvoriť súčasť jestvujúceho finančného rámca spoločenstva,

ROZHODLA TAKTO:

Článok 1

Týmto rozhodnutím sa prijíma akcia v oblasti bezpečnosti informačných systémov. Zahŕňa:

— vypracovanie globálnych stratégií na zaistenie bezpečnosti informačných systémov (akčného plánu) na začiatočné obdobie dvadsiatich štyroch mesiacov, a

— vytvorenie skupiny vyšších úradníkov s dlhodobým mandátom (ďalej len „výbor“) ako poradného orgánu Komisie pre akcie podnikané v oblasti bezpečnosti informačných systémov.

[1] Ú. v. ES C 277, 5.11.1990, s. 18.
[2] Ú. v. ES C 94, 13.3.1992.
[3] Ú. v. ES C 159, 17.6.1991, s. 38.

Článok 2

1. Komisia sa systematicky radí s výborom o otázkach týkajúce sa bezpečnosti informačných systémov pre rôzne činnosti vykonávané spoločenstvom, najmä definície pracovných stratégií a programov.

2. Akčný plán, ako sa uvádza v prílohe, zahŕňa prípravné práce v rámci týchto tém:

I. vypracovanie strategického rámca pre bezpečnosť informačných systémov;

II. zistenie potrieb užívateľov a poskytovateľov služieb v oblasti bezpečnosti informačných systémov;

III. vypracovanie riešení pre niektoré krátkodobé a strednodobé potreby užívateľov, dodávateľov a poskytovateľov služieb;

IV. vypracovanie špecifikácií, normalizácie, hodnotenia a osvedčovania vo vzťahu k bezpečnosti informačných systémov;

V. technologický a funkčný vývoj v oblasti bezpečnosti informačných systémov;

VI. zaistenie bezpečnosti informačných systémov.

Článok 3

1. Výška finančných prostriedkov spoločenstva považovaná za nevyhnutnú na uskutočnenie akcie na začiatočné obdobie je 12 miliónov ECU vrátane 2 miliónov ECU na rok 1992 v rámci finančného výhľadu na roky 1988-1992.

Pre nasledujúce obdobie vykonávania programu bude potrebné zahrnúť sumu do platného finančného rámca spoločenstva.

2. Rozpočtový orgán určí voľné prostriedky na každý finančný rok s prihliadnutím na zásady správneho riadenia uvedené v článku 2 finančného nariadenia, ktoré sa vzťahuje na všeobecný rozpočet Európskych spoločenstiev.

Článok 4

Skupina nezávislých odborníkov vykoná pre Komisiu vyhodnotenie pokroku dosiahnutého v priebehu začiatočného obdobia. Správa tejto skupiny, doplnená prípadnými pripomienkami Komisie, sa predloží Európskemu parlamentu a Rade.

Článok 5

1. Komisia zodpovedá za uskutočnenie akcie. Bude jej pomáhať poradný výbor pozostávajúci zo zástupcov členských štátov za predsedníctva zástupcu Komisie.

2. Akčný plán sa uskutoční v súlade s cieľmi vymedzenými v článku 2 a podľa potreby sa aktualizuje. Vytýči podrobné ciele a typy akcií, ktoré sa majú uskutočniť, ako aj súvisiace finančné opatrenia. Komisia vyzve na predloženie návrhov na základe akčného plánu.

3. Akčný plán sa musí uskutočňovať v úzkej spolupráci s činiteľmi odvetvia. Musí zohľadňovať, podporovať a doplňovať prebiehajúce normalizačné činnosti na európskej a medzinárodnej úrovni v tejto oblasti.

Článok 6

1. Postup stanovený v článku 7 sa vzťahuje na

— opatrenia súvisiace s politikou spoločenstva v oblasti bezpečnosti informačných systémov.

2. Postup stanovený v článku 8 sa vzťahuje na:

— vypracovanie a aktualizáciu akčného plánu uvedeného v článku 5;

— obsah výzvy na predkladanie návrhov, vyhodnotenie návrhov a odhadovanú výšku príspevku spoločenstva na opatrenia, pokiaľ presahuje 200 000 ECU;

— spoluprácu organizácií z krajín nepatriacich do spoločenstva na akejkoľvek činnosti, ktorú upravuje toto rozhodnutie;

— na spôsoby šírenia, ochrany a vyhodnocovania výsledkov opatrení;

— opatrenia, ktoré majú byť prijaté na vyhodnotenie akcie.

3. Ak výška príspevku spoločenstva na opatrenia nepresahuje 200 000 ECU, Komisia sa poradí s výborom o opatreniach, ktoré majú byť prijaté, a informuje ho o výsledku svojho hodnotenia.

Článok 7

Zástupca Komisie predloží výboru návrh opatrení, ktorá majú byť prijaté. Výbor zaujme svoje stanovisko k tomuto návrhu v lehote, ktorú môže predseda stanoviť podľa naliehavosti danej otázky, prípadne hlasovaním.

Stanovisko sa zaznamená do zápisu; okrem toho má každý členský štát právo požiadať, aby bol v tomto zápisu uvedený jeho postoj.

Komisia v maximálnej miere prihliada k stanovisku predloženému výborom. Informuje výbor o spôsobe, akým toto stanovisko zohľadnila.

Článok 8

Zástupca Komisie predloží výboru návrh opatrení, ktoré majú byť prijaté. Výbor zaujme svoje stanovisko k tomuto návrhu v lehote, ktorú môže predseda stanoviť podľa naliehavosti danej otázky. Stanovisko sa prijíma väčšinou podľa článku 148 ods. 2 zmluvy

v prípade rozhodnutí, ktorá má Rada prijímať na návrh Komisie, pričom hlasom členských štátov sa prideľuje váha podľa článku 148 ods. 2 zmluvy. Predseda nehlasuje.

Komisia prijme zamýšľané opatrenia, ak sú v súlade so stanoviskom výboru.

Pokiaľ zamýšľané opatrenia nie sú v súlade so stanoviskom výboru, alebo pokiaľ výbor nijaké stanovisko nezaujme, Komisia neodkladne predloží Rade návrh opatrení, ktoré majú byť prijaté. Rada sa uznesie kvalifikovanou väčšinou.

Pokiaľ sa Rada neuznesie v lehote troch mesiacov od predloženia veci Rade, prijme navrhované opatrenia Komisia s výnimkou prípadov, keď sa Rada proti uvedeným opatreniam vysloví jednoduchou väčšinou.

V Bruseli 31. marca 1992

Za Radu

predseda

Vitor MARTINS

PRÍLOHA

Prehľad smerov akcie

HLAVNÉ SMERY AKČNÉHO PLÁNU V OBLASTI BEZPEČNOSTI INFORMAČNÝCH SYSTÉMOV

ÚVOD

Cieľom akčného plánu je rozvoj globálnych stratégií zameraných na to, aby užívateľom a tvorcom elektronicky uchovávaných, spracovávaných alebo odovzdávaných informácií bola poskytovaná zodpovedajúca ochrana informačných systémov proti náhodným nebo úmyselným ohrozeniam.

Akčný plán zohľadňuje a doplňuje súčasnú normalizačnú činnosť na svetovej úrovni.

Zahŕňa tieto smery akcie:

— vypracovanie strategického rámca pre bezpečnosť informačných systémov,

— zisťovanie potrieb užívateľov a poskytovateľov služieb v oblasti bezpečnosti informačných systémov,

— vypracovanie riešení pre niektoré krátkodobé a strednodobé potreby užívateľov, dodávateľov a poskytovateľov služieb,

— vypracovanie špecifikácií, normalizácie, hodnotenia a osvedčovania vo vzťahu k bezpečnosti informačných systémov,

— technologický a operačný rozvoj v oblasti bezpečnosti informačných systémov,

— zabezpečenie bezpečnosti informačných systémov.

Akčný plán uskutočňuje Komisia v úzkej spolupráci so súvisiacimi akciami členských štátov a v spojení s akciami spoločenstva v oblasti výskumu a technologického rozvoja v tejto oblasti.

1. **Smer akcie I: Vypracovanie strategického rámca pre bezpečnosť informačných systémov**

1.1. *Predmet*

Bezpečnosť informačných systémov sa považuje za kvalitu, ktorá je nevyhnutná všade v modernej spoločnosti. Elektronické informačné služby vyžadujú bezpečné telekomunikačné infraštruktúry, bezpečný software a hardware, ako aj bezpečné podmienky používania a spravovania. Je potrebné vytvoriť globálnu stratégiu, ktorá zohľadní všetky hľadiská bezpečnosti informačných systémov a vylúči všetky dielčie prístupy. Všetky stratégie bezpečnosti elektronicky spracovávaných informácií musia odzrkadľovať želanie všetkých spoločností pracovať efektívne a pritom sa chrániť v rýchlo sa meniacom svete.

1.2. *Cieľ*

Musí byť vytvorený strategicky orientovaný rámec tak, aby boli zladené sociálne, hospodárske a politické ciele s technickými, prevádzkovými a právnymi možnosťami spoločenstva v medzinárodných súvislostiach. Osoby činné v danom odvetví, ktoré pracujú spoločne na vypracovaní spoločného postoja a dohodnutého strategického rámca, musia nájsť citlivú rovnováhu medzi rôznymi záujmami, cieľmi a obmedzeniami. Sú to o predpoklady pre zladenie záujmov a potrieb tak v oblasti politiky, ako aj v oblasti priemyselného rozvoja.

1.3. *Situácia a trendy*

Situácia sa vyznačuje rastúcim uvedomením si potreby konať. Pokiaľ sa však neobjaví podnet pre koordináciu opatrení, je veľmi pravdepodobné, že rozptýlené snahy v rôznych odvetviach vytvoria situáciu, ktorá bude v skutočnosti protikladná, a bude postupne vytvárať čoraz viac právnych, sociálnych a hospodárskych problémov.

1.4. *Požiadavky, možnosti a priority*

Taký zdieľaný rámec musí spracovať a preskúmať analýzu a zvládnutie rizík súvisiacich so zraniteľnosťou informačných systémov a súvisiacich služieb, harmonizáciu právnych predpisov týkajúcich sa zneužívania a nesprávneho používania výpočtovej techniky a telekomunikácií, administratívne infraštruktúry vrátane bezpečnostných politík, a ako môžu byť tieto politiky účinne implementované v rôznych priemyselných odvetviach alebo oblastiach, sociálne záujmy a záujmy ochrany súkromia (napríklad používanie systémov identifikácie, overovania pravosti, dokázateľnosti a, prípadne, oprávnenia v demokratickom prostredí).

Musia byť vytvorené jasné pokyny na vypracovanie fyzikálnych a logických štruktúr pre bezpečné rozloženie informačných služieb, noriem, pokynov a definícií pre produkty a služby so zaistenou bezpečnosťou, pilotných projektov a prototypov, aby bola zaistená životnosť rôznych administratívnych štruktúr, ako aj štruktúr a noriem týkajúcich sa potrieb špecifických odvetví.

Je potrebné vytvoriť vedomie bezpečnosti, aby sa ovplyvnil postoj užívateľov smerom k zvýšenému záujmu o bezpečnosť v oblasti informačných technológií (IT).

2. Smer akcie II: zisťovanie potrieb užívateľov a poskytovateľov služieb v oblasti bezpečnosti informačných systémov

2.1. *Predmet*

Bezpečnosť informačných systémov je neodmysliteľným predpokladom bezúhonnosti a vierohodnosti obchodného uplatňovania, duševného vlastníctva a utajenia. To neodvratne vytvára otázku citlivej rovnováhy a niekedy výberu medzi podporou voľného obchodu na jednej strane a ochranou súkromia a duševného vlastníctva na strane druhej. Tieto výbery a kompromisy sa musia zakladať na úplnom zhodnotení požiadaviek a dopadu možných rozhodnutí prijatých v oblasti bezpečnosti informačných systémov na splnenie týchto požiadaviek.

Užívatelia požadujú, aby informačné systémy fungovali bezpečne z technologických, prevádzkových a normotvorných aspektov. Je teda nevyhnutné vykonať systematický prieskum požiadaviek na bezpečnosť informačných systémov, aby došlo k vypracovaniu zodpovedajúcich a účinných opatrení.

2.2. *Cieľ*

Zistiť povahu a charakteristiky požiadaviek užívateľov a poskytovateľov služieb a ich vzťah k opatreniam v oblasti bezpečnosti informačných systémov.

2.3. *Situácia a trendy*

Až doteraz nebolo vynaložené nijaké jednotné úsilie na zistenie rýchlo sa vyvíjajúcich a meniacich požiadaviek hlavných činiteľov v oblasti bezpečnosti informačných systémov. Niektoré členské štáty spoločenstva zistili požiadavky na harmonizáciu vnútroštátnych činností (najmä „hodnotiace kritériá bezpečnosti informačných technológií“). Jednotné hodnotiace kritériá a pravidlá pre vzájomné uznávanie osvedčení o hodnotení majú čoraz väčší význam.

2.4. *Požiadavky, možnosti a priority*

Z dôvodu, aby boli oprávnené požiadavky činiteľov odvetvia spracovávané dôsledne a transparentne, zdá sa nevyhnutné vytvoriť dohodnutú klasifikáciu požiadaviek užívateľov a ich vzťahu k zaisťovaniu bezpečnosti informačných systémov.

Rovnako sa považuje za dôležité zistiť požiadavky v oblasti legislatívy, právnych predpisov a pravidiel správania sa v súvislosti s hodnotením tendencií, pokiaľ ide o charakteristiku a technológiu služieb, vymedziť alternatívne stratégie umožňujúce dosiahnutie cieľov prostredníctvom administratívnych, služobných, prevádzkových a technických opatrení a ohodnotiť efektívnosť, užívateľskú optimálnosť a náklady alternatívnych možností voľby a stratégií v oblasti informačných systémov pre užívateľov, poskytovateľov služieb a operátorov.

3. Smer akcie III: vypracovanie riešení pre niektoré krátkodobé a strednodobé potreby užívateľov, dodávateľov a poskytovateľov služieb

3.1. *Predmet*

V súčasnosti je možné účinne zabrániť neoprávnenému prístupu do počítačov z vonkajšieho sveta využitím „izolovania“, to znamená tradičných organizačných a fyzikálnych opatrení. To isté platí aj pre elektronické komunikácie vnútri uzatvorenej skupiny užívateľov, ktorí pracujú na vymedzenej sieti. Situácia je veľmi rozdielna, ak sú informácie zdieľané medzi rôznymi skupinami užívateľov alebo sa vymieňajú prostredníctvom verejnej alebo všeobecne prístupnej siete. Technológie, terminály a služby, na jednej strane, ani normy a súvisiace postupy, na strane druhej, nie sú všeobecne v týchto prípadoch schopné zaistiť bezpečnosť informačných systémov na porovnateľnej úrovni.

3.2. *Cieľ*

Cieľom musí byť poskytnutie riešení v krátkej lehote, ktoré môžu uspokojiť najnaliehavejšie potreby užívateľov, poskytovateľov služieb a výrobcov. To zahŕňa využívanie spoločných hodnotiacich kritérií bezpečnosti informačných technológií. Tieto kritériá majú byť zostavené spôsobom otvoreným pre budúce požiadavky a riešenia.

3.3. *Situácia a trendy*

Niektoré skupiny užívateľov vytvorili pre svoju osobitnú potrebu metódy a postupy zodpovedajúce najmä potrebám overovania pravosti, jednotnosti a dokázateľnosti. Všeobecne sa používajú magnetické karty alebo čipové karty. Niektorí používajú viac-menej komplikované metódy šifrovania. Často to predpokladá vymedzenie osobitného „orgánu“ pre skupiny užívateľov. Je však ťažké zovšeobecniť tieto postupy a metódy, aby boli uspokojené potreby v otvorenom prostredí.

ISO pracuje na bezpečnosti informačných systémov OSI (ISO DIS 7498-2) a CCITT v kontexte X 400. Je taktiež možné zahrnúť segmenty bezpečnosti do správ. Overovanie pravosti, jednotnosť a dokázateľnosť sú riešené ako súčasť správ (EDIFACT) a súčasť X 400 MHS.

Právny rámec systému Electronic Data Interchange (EDI) je v súčasnosti stále v štádiu koncipovania. Medzinárodná obchodná komora uverejnila jednotné pravidlá správania sa pre výmenu obchodných údajov cez telekomunikačné siete.

Niektoré krajiny (napríklad Nemecko, Francúzsko, Spojené kráľovstvo a Spojené štáty americké) vypracovali alebo vypracúvajú kritériá pre hodnotenie vierohodnosti produktov a systémov informačných technológií a zodpovedajúce postupy pre hodnotenia. Tieto kritériá boli koordinované s vnútroštátnymi výrobcami a povedú k vzniku väčšieho počtu spoľahlivých produktov a systémov, počnúc jednoduchými produktmi. Vytvorenie vnútroštátnych organizácií poverených vykonávaním hodnotení a vydávaním osvedčení bude tento trend podporovať.

Väčšina užívateľov považuje ustanovenia v oblasti utajenia za bezprostredne menej dôležité. Je však pravdepodobné, že v budúcnosti sa táto situácia zmení v dôsledku veľkého rozšírenia vyspelých komunikačných služieb, a najmä mobilných služieb.

3.4. *Požiadavky, možnosti a priority*

Je veľmi dôležité vypracovať čo najskôr postupy, normy, produkty a nástroje vhodné na zaistenie bezpečnosti informačných systémov ako takých (počítače, periférne zariadenia) a verejných komunikačných sietí. Prioritu musí dostať overovanie pravosti, jednotnosť a dokázateľnosť. Mali by sa uskutočniť pilotné projekty, aby určila správnosť navrhovaných riešení. Riešenia určitých prioritných potrieb v oblasti EDI sa hľadajú v programe TEDIS v rámci všeobecnejšieho obsahu tohto akčného plánu.

4. Smer akcie IV: vypracovanie špecifikácií, normalizácie, hodnotenia a osvedčovania vo vzťahu k bezpečnosti informačných systémov

4.1. *Predmet*

Požiadavky v oblasti bezpečnosti informačných systémov sa objavujú všade, a preto je rozhodujúce vytvoriť spoločné špecifikácie a normy. Absencia noriem a špecifikácií dohodnutých pre bezpečnosť informačných technológií môže vytvoriť hlavnú prekážku pre vývoj postupov a služieb založených na informáciách v celom hospodárstve a v spoločnosti. Je tiež nezbytné prijať opatrenia na urýchlenie vypracovania a používania technológie a noriem vo viacerých oblastiach súvisiacich s komunikáciami a počítačovými sieťami, ktoré majú základný význam pre užívateľov, priemysel a administratívu.

4.2. *Cieľ*

Je potrebné vynaložiť úsilie na podporu a vykonávanie osobitných bezpečnostných funkcií vo všeobecných oblastiach OSI, ONP, ISDN/IBC a spravovania sietí. Metódy a prístupy v oblasti overovania, vrátane osvedčovania, ktoré vedú k vzájomnému uznávanie, sú vnútorne spojené s normalizáciou a špecifikáciou. Kedykoľvek je to možné, treba podporovať riešenia dohodnuté na medzinárodnej úrovni. Taktiež by sa malo podporovať vytváranie a používanie informačných systémov s bezpečnostnými funkciami.

4.3. *Situácia a trendy*

K riešeniu otázky bezpečnosti informačných systémov dali významný podnet najmä Spojené štáty americké. V Európe sa táto téma posudzuje v súvislosti s normalizáciou informačných technológií a telekomunikácií v rámci ETSI a CEN/CENELEC pri príprave činnosti CCITT a ISO v tejto oblasti.

Vzhľadom na rastúce obavy sa práca v Spojených štátoch amerických rýchlo zintenzívňuje a tak predajcovia, ako aj poskytovatelia služieb stupňujú svoje úsilie v tejto oblasti. V Európe Francúzsko, Nemecko a Spojené kráľovstvo samostatne odštartovali podobné činnosti, ale spoločné úsilie ako v Spojených štátoch amerických sa rozvíja len pomaly.

4.4. *Požiadavky, možnosti a priority*

V oblasti bezpečnosti informačných systémov sú normotvorné, prevádzkové, administratívne a technické aspekty vnútorne veľmi úzko spojené. Normy musia odzrkadľovať právne predpisy a musí byť možné preukázať, že ustanovenia v oblasti bezpečnosti informačných systémov sú v súlade s normami a právnymi predpismi. Z viacerých aspektov musia právne predpisy obsahovať špecifikácie, ktoré sú mimo obvyklého rámca normalizácie, to znamená, ktoré zahŕňajú pravidlá správania sa. Požiadavky v oblasti noriem a pravidiel správania sa sú prítomné vo všetkých oblastiach bezpečnosti informačných systémov a treba rozlišovať medzi požiadavkami na ochranu, ktoré zodpovedajú cieľom v oblasti bezpečnosti, a niektorými technickými požiadavkami, ktoré môžu byť zverené príslušným európskym orgánom pre normalizáciu (CEN/CENELEC/ETSI).

Špecifikácie a normy musia pokrývať subjekty služieb pre bezpečnosť informačných systémov (overovanie osôb a podnikov, protokoly o dokázateľnosti, právne akceptovateľný elektronický dôkaz, kontrola autorizácie), ich komunikačné služby (ochrana súkromia pri prenose obrazu, hlasu a údajov, ochrana údajov a obrazových databáz, bezpečnosť integrovaných služieb), ich spravovanie komunikácie a bezpečnosti (systém verejných/súkromných kľúčov pre fungovanie otvorených sietí, na ochranu spravovania siete, ochrana poskytovateľov služieb) a ich osvedčovanie (kritériá a úrovne zaistenia, postupy zaistenia bezpečnosti informačných systémov).

5. Smer akcie V: technologický a operačný vývoj v oblasti bezpečnosti informačných systémov

5.1. *Predmet*

Systematický výskum a vývoj technológie, ktorý umožní nájsť hospodársky prijateľné a prevádzkovo vyhovujúce riešenia pre široké spektrum súčasných a budúcich požiadaviek v oblasti bezpečnosti informačných systémov, je nevyhnutným predpokladom rozvoja trhu služieb a súťaživosti európskeho hospodárstva ako celku.

Všetok technologický vývoj v oblasti bezpečnosti informačných systémov sa bude musieť vzťahovať tak na bezpečnosť počítačov, ako aj na bezpečnosť komunikácií, pretože väčšina súčasných systémov sú rozptýlené systémy, ku ktorým sa pristupuje cez komunikačné služby.

5.2. *Cieľ*

Systematický výskum a vývoj technológie, ktorý umožní nájsť hospodársky prijateľné a prevádzkovo vyhovujúce riešenia pre široké spektrum súčasných a budúcich požiadaviek v oblasti bezpečnosti informačných systémov.

5.3. *Požiadavky, možnosti a priority*

Práca v oblasti bezpečnosti informačných systémov by sa mala týkať stratégií vypracúvania a implementácie, technológií, ako aj integrácie a overovania.

Strategická práca vo výskume a technologickom vývoji by mala zahŕňať koncepčné modely bezpečných systémov (bezpečných proti ohrozeniu, nepovoleným úpravám a odmietnutiu služby), modely funkčných požiadaviek, modely rizík a štruktúry pre bezpečnosť.

Technologicky zameraný výskum a vývoj by mal zahŕňať overovanie užívateľov a overovanie správ (napríklad pomocou hlasovej analýzy alebo elektronických podpisov), technické rozhrania a protokoly pre šifrovanie, mechanizmy kontroly prístupu a implementačné metódy na vytváranie systémov so zaručenou bezpečnosťou.

Overovanie a potvrdzovanie platnosti bezpečnosti technických systémov a jej použiteľnosť by sa mala skúmať prostredníctvom projektov zjednocovania a overovania.

Okrem konsolidácie a rozvíjania technológie bezpečnosti je nevyhnutný určitý počet sprievodných opatrení v oblasti vytvárania, zachovávania a dôsledného uplatňovania noriem, ako aj v oblasti potvrdzovania platnosti a osvedčovania produktov informačných technológií a telekomunikácií, pokiaľ ide o ich vlastnosti v oblasti bezpečnosti, vrátane potvrdzovania platnosti a osvedčovania metód vytvárania a implementovania systémov.

Tretí rámcový program spoločenstva v oblasti výskumu a technologického vývoja by sa mohol použiť na podporu projektov spolupráce na úrovni predchádzajúcej súťaži a právnej úprave.

6. Smer akcie VI: zabezpečenie bezpečnosti informačných systémov

6.1. *Predmet*

V závislosti od presného charakteru prvkov bezpečnosti informačných systémov bude potrebné požadované funkcie zahrnúť do rôznych častí informačného systému, vrátane terminálov/počítačov, služieb, spravovania sietí šifrovacích zariadení, čipových kariet, verejných a súkromných kľúčov atď. Niektoré z týchto funkcií budú pravdepodobne zahrnuté do hardwaru alebo softwaru dodávanému predajcami, zatiaľ čo iné môžu byť súčasťou rozptýlených systémov (napríklad spravovanie siete), vo vlastníctve jednotlivých užívateľov (napríklad čipové karty) alebo poskytované špecializovanou organizáciou (napríklad verejné a súkromné kľúče).

Väčšinu bezpečnostných produktov a služieb budú pravdepodobne dodávať predajcovia, poskytovatelia služieb alebo operátori. Pre určité osobné funkcie, napríklad dodanie verejných a súkromných kľúčov a oprávnenie na kontrolu, bude zrejme potrebné určiť a poveriť vhodné organizácie.

To isté sa vzťahuje na osvedčovanie, hodnotenie a overovanie kvality služieb, čo sú funkcie, ktoré musia byť zverené organizáciám nezávislým od záujmov predajcov, poskytovateľov služieb alebo operátorov. Tieto organizácie by mohli byť súkromné, verejné alebo splnomocnené vládou na vykonávanie týchto funkcií.

6.2. *Cieľ*

Na uľahčenie harmonického vývoja pri zavádzaní bezpečnosti informačných systémov v spoločenstve s ohľadom na ochranu verejnosti a obchodných záujmov bude nevyhnutné vypracovať jednotný prístup pre zavádzanie bezpečnosti informačných systémov. Ak tým budú splnomocnené nezávislé organizácie, musia byť ich funkcie a podmienky fungovania vymedzené a prijaté a, ak je to nevyhnutné, právne upravené. Cieľom by bolo dospieť k jasne vymedzenému a dohodnutému rozdelenie zodpovednosti medzi rôznymi činiteľmi na úrovni spoločenstva ako nevyhnutnému predpokladu vzájomného uznávania.

6.3. *Situácia a trendy*

V súčasnosti je zavádzanie bezpečnosti informačných systémov riadne organizované iba pre osobitné oblasti a obmedzené len na uspokojenie ich osobitných potrieb. Organizácia na európskej úrovni je najčastejšie neformálna a vzájomné uznávanie overovania a osvedčovania mimo niektorých uzavretých skupín sa ešte nerealizuje. S rastúcim významom bezpečnosti informačných systémov sa stáva naliehavou potreba vymedziť jednotný prístup k zavádzaniu bezpečnosti informačných systémov v Európe a na medzinárodnej úrovni.

6.4. *Požiadavky, možnosti a priority*

Vzhľadom na veľký počet dotknutých činiteľov a úzke vzťahy s otázkami právnej úpravy a legislatívy je obzvlášť dôležité vopred sa zhodnúť na zásadách, ktorými by sa malo riadiť zavádzanie bezpečnosti informačných systémov.

Pri vypracúvaní jednotného prístupu k tejto otázke bude potrebné určiť aspekty identifikácie a špecifikácie funkcií vyžadujúcich, zo svojej podstaty, existenciu niektorých nezávislých organizácií (alebo spolupracujúcich organizácií). To by mohlo zahŕňať také funkcie, ako je spravovanie systému verejných/súkromných kľúčov.

Okrem toho je nevyhnutné v ranom štádiu určiť a upresniť funkcie, ktoré musia byť vo verejnom záujme zverené nezávislým organizáciám (alebo spolupracujúcim organizáciám). Tieto funkcie by mohli napríklad zahŕňať kontrolu, zistenie kvality, overovanie, osvedčovanie a podobné funkcie.