31992D0242

1992.5.8. *AZ EURÓPAI KÖZÖSSÉGEK HIVATALOS LAPJA* L 123/19

A TANÁCS HATÁROZATA
(1992. március 31.)
az információs rendszerek biztonságának tárgykörében

(92/242/EGK)

AZ EURÓPAI KÖZÖSSÉGEK TANÁCSA,

tekintettel az Európai Gazdasági Közösséget létrehozó szerződésre és különösen annak 235. cikkére,

tekintettel a Bizottság javaslatára [1],

tekintettel az Európai Parlament véleményére [2],

tekintettel a Gazdasági és Szociális Bizottság véleményére [3],

mivel a Közösségnek feladata, hogy a közös piac létrehozásával és a tagállamok gazdaságpolitikai elképzeléseinek fokozatos közelítésével a Közösség egész területén elősegítse a gazdasági tevékenységek összehangolt fejlődését, folyamatos és kiegyensúlyozott terjedését, a stabilitás növelését, az életszínvonal gyors emelkedését és a tagállamok közötti kapcsolatok szorosabbá tételét;

mivel az elektronikus formában tárolt, feldolgozott és továbbított adatok egyre fontosabb szerepet játszanak a gazdasági és szociális tevékenységekben;

mivel a hatékony globális kommunikáció elérkezte és az adatok elektronikus kezelésének elterjedt felhasználása hangsúlyozottan igényli a megfelelő védelmet;

mivel az Európai Parlament vitáiban és állásfoglalásaiban több alkalommal hangsúlyozta az információs rendszerek biztonságának fontosságát;

mivel a Gazdasági és Szociális Bizottság hangsúlyozta, hogy a közösségi fellépési formákban feltétlenül foglalkozni kell az információs rendszerek biztonságával, különös tekintettel a belső piac megvalósulásának hatására;

mivel a nemzeti, nemzetközi és közösségi szintű fellépési formák erre jó alapot nyújtanak;

mivel szoros kapcsolat van a távközlési, informatikai, szabványosítási, információs piaci és a kutatási, fejlesztési és technológiai politikák, valamint a Közösség által ezeken a területeken már elvállalt munka között;

mivel helyénvaló az eddigi nemzeti és nemzetközi munkára építve és a főbb érintett szereplők közötti együttműködés szorgalmazásával biztosítani, hogy az erőfeszítések összehangoltak legyenek; mivel ezért helyénvaló egy koherens cselekvési program keretében folytatni tovább a munkát;

mivel az információs rendszerek biztonságának összetettsége szükségessé teszi olyan stratégiák kifejlesztését, amelyek lehetővé teszik az egységes piacon az információ szabad áramlását, miközben a Közösség egészében szavatolják az információs rendszerek alkalmazásának biztonságát;

mivel az egyes tagállamok saját felelőssége a biztonság és a közrend miatt szükséges korlátozások figyelembevétele;

mivel az e téren a tagállamokra nehezedő felelősség feltétlenül indokolttá teszi a tagállamok vezető tisztviselőivel való szoros együttműködésére alapozott egységes megközelítést;

mivel rendelkezni kell a huszonnégy hónapos kezdeti időszakra vonatkozó cselekvési programról, valamint a vezető tisztviselőkből álló olyan bizottság felállításáról, amelynek hosszú távú megbízása arra szól, hogy tanácsokkal segítse a Bizottságot az információs rendszerek biztonsága terén szükséges cselekvési formákkal kapcsolatban;

mivel 12 millió ECU-s összeget tartanak szükségesnek a huszonnégy havi kezdeti időszak cselekvéseinek végrehajtására; mivel 1992-re a szükséges becsült összeg a jelenlegi pénzügyi terv ismeretében 2 millió ECU;

mivel az 1992-es költségvetési évet követően a program finanszírozására szánt összegek a Közösség meglevő pénzügyi keretének részét fogják képezni,

A KÖVETKEZŐKÉPPEN HATÁROZOTT:

1. cikk

Ezennel sor kerül az információs rendszerek biztonsága terén szükséges cselekvés elfogadására. Ez a következőkből áll:

– az információs rendszerek biztonságára vonatkozó, a kezdeti 24 havi időszakra vonatkozó átfogó stratégiák (cselekvési terv) fejlesztése, valamint

– vezető tisztviselőkből álló olyan csoport felállítása, amelynek hosszú távú megbízatása arra szól, hogy tanácsokkal segítse a Bizottságot az információs rendszerek biztonsága terén vállalt cselekvések megtételében (a továbbiakban: bizottság).

[1] HL C 277., 1990.11.5., 18. o.
[2] HL C 94., 1992.3.13.
[3] HL C 159., 1991.6.17., 38. o.

2. cikk

(1) A Bizottság rendszeresen konzultál a bizottsággal a Közösség által végzett és az információs rendszerek biztonságára vonatkozó kérdésekről, különös tekintettel a stratégiák és programok meghatározására.

(2) A cselekvési terv a mellékletben feltüntetettek szerint tartalmazza az előkészítő munkát a következő témák alapján:

I. az információs rendszerek biztonságára vonatkozó stratégiai keret fejlesztése;

II. a felhasználó és a szolgáltató által az információs rendszerek biztonsága tekintetében támasztott elvárások feltérképezése;

III. a felhasználók, szállítók és szolgáltatók azonnali és átmeneti igényeire vonatkozó megoldások;

IV. az előírások fejlesztése, az információs rendszerek biztonságára vonatkozó szabványosítás, értékelés és tanúsítás;

V. technológiai és működési fejlesztések az információs rendszerek biztonsága terén;

VI. az információs rendszerek biztonságának megteremtése.

3. cikk

(1) A cselekvés végrehajtásához szükséges becsült közösségi alapok összege az 1988. és 1992. közötti pénzügyi kilátások ismeretében a kezdeti időszakban becslések szerint 12 millió ECU, beleértve az 1992. évre vonatkozó 2 millió ECU-t.

A program alkalmazásának következő időszakában az összegnek szerepelnie kell a Közösség hatályos pénzügyi keretében.

(2) A költségvetési hatóság meghatározza a minden egyes pénzügyi évre vonatkozó előirányzatokat, ennek során figyelembe veszi a hatékony és eredményes gazdálkodásnak az Európai Közösség általános költségvetéséről szóló költségvetési rendelet 2. cikkében említett elveit.

4. cikk

Független szakértők egy csoportja elkészíti a Bizottság számára a kezdeti időszakban elért eredmények értékelését. Ennek a csoportnak a jelentését a Bizottság megjegyzéseivel együtt az Európai Parlamenthez és a Tanácshoz kell benyújtani.

5. cikk

(1) A Bizottság felel a cselekvés végrehajtásáért. A Bizottságot a tagállamok képviselőiből álló és a Bizottság képviselőjének elnökletével működő bizottság segíti.

(2) A cselekvési tervet a 2. cikkben megfogalmazott célokkal összhangban kell végrehajtani és szükség szerint frissíteni. A terv tartalmazza a részletes célkitűzéseket és a megvalósítandó cselekvések jellegét, valamint az ezekhez szükséges pénzügyi megoldásokat. A Bizottság a cselekvési terv alapján teszi közzé javaslati felhívásait.

(3) A cselekvési tervet az ágazati szereplőkkel szorosan együttműködve kell végrehajtani. A terv figyelembe veszi, elősegíti és kiegészíti az ezen a területen folyamatban levő európai és nemzetközi egységesítési tevékenységeket.

6. cikk

(1) A 7. cikkben megállapított eljárást a következőkre kell alkalmazni:

– az információs rendszerek biztonsága területén megvalósítandó közösségi politikára vonatkozó intézkedések.

(2) A 8. cikkben megállapított eljárást a következőkre kell alkalmazni:

– az 5. cikkben említett cselekvési terv elkészítése és frissítése,

– a javaslati felhívások tartalma, a javaslatok értékelése és az intézkedésekhez a Közösség hozzájárulásának becsült összege, amennyiben ez az összeg meghaladja a 200 000 ECU-t,

– a Közösségen kívüli szervezetek részvétele e határozat szerinti bármely tevékenységben,

– az intézkedések eredményeinek terjesztésére, védelmére és kihasználására vonatkozó rendelkezések,

– a cselekvés értékeléséhez szükséges intézkedések.

(3) Amennyiben a Közösség hozzájárulása az intézkedésekhez legfeljebb 200 000 ECU, a Bizottság egyeztet a bizottsággal az intézkedésekről és tájékoztatja a bizottságot az értékelés eredményéről.

7. cikk

A Bizottság képviselője benyújtja a bizottságnak a szükséges intézkedések tervezetét. A bizottság az elnök által az ügy sürgősségének figyelembevételével meghatározott határidőn belül, szükség esetén szavazással véleményt nyilvánít.

A véleményt jegyzőkönyvben rögzítik; mindegyik tagállam jogosult arra, hogy kérje véleményének rögzítését a jegyzőkönyvben.

A Bizottság a lehető legteljesebb mértékben figyelembe veszi a bizottság véleményét. A bizottságot tájékoztatják arról, hogy véleményét milyen módon vették figyelembe.

8. cikk

A Bizottság képviselője benyújtja a bizottságnak a szükséges intézkedések tervezetét. A bizottság az elnök által az ügy sürgősségének figyelembevételével meghatározott határidőn belül véleményt nyilvánít. A Tanács által a Bizottság javaslata alapján

elfogadandó javaslatok esetében a bizottság a Szerződés 148. cikke (2) bekezdésében meghatározott többséggel nyilvánít véleményt. A bizottságban a tagállamok képviselőinek szavazatait az említett cikkben leírtaknak megfelelően kell súlyozni. Az elnök nem szavazhat.

A Bizottság elfogadja az előirányzott intézkedéseket, amennyiben ezek összhangban állnak a bizottság véleményével.

Amennyiben az előirányzott intézkedések nem állnak összhangban a bizottság véleményével, vagy amennyiben az nem nyilvánít véleményt, a Bizottság késedelem nélkül javaslatot nyújt be a Tanácsnak a megvalósítandó intézkedésekről. A Tanács minősített többséggel határoz.

Amennyiben a Tanács a hozzá való fordulást követő három hónap elteltével nem jár el, a Bizottság elfogadja a javasolt intézkedéseket, kivéve, ha a Tanács egyszerű többséggel határozott az említett intézkedések elutasításáról.

Kelt Brüsszelben, 1992. március 31-én.

a Tanács részéről

az elnök

Vitor MARTINS

MELLÉKLET

A cselekvés főbb irányvonalainak összefoglalása

IRÁNYMUTATÁS AZ INFORMÁCIÓS RENDSZEREK BIZTONSÁGÁVAL KAPCSOLATOS CSELEKVÉSI TERVHEZ

BEVEZETŐ

A cselekvési terv célja olyan átfogó stratégiák kidolgozása, amelyek célja a felhasználók és a gyártók ellátása elektronikus eszközökkel tárolt, kezelt vagy továbbított adatokkal úgy, hogy eközben biztosított az információs rendszerek megfelelő védelme a véletlenül vagy szándékosan okozott veszélyekkel szemben.

A cselekvési tervnek figyelembe kell vennie és ki kell egészítenie az ezen a területen folyamatban levő világméretű szabványosítási tevékenységeket.

A terv a következő cselekvési irányokat tartalmazza:

– az információs rendszerek biztonságára vonatkozó stratégiai keret fejlesztése,

– a felhasználó és a szolgáltató által az információs rendszerek biztonsága tekintetében támasztott elvárások feltérképezése,

– a felhasználók, szállítók és szolgáltatók azonnali és átmeneti igényeire vonatkozó megoldások,

– az előírások fejlesztése, az információs rendszerek biztonságára vonatkozó szabványosítás, értékelés és tanúsítás,

– technológiai és működési fejlesztések az információs rendszerek biztonsága terén,

– az információs rendszerek biztonságának megteremtése.

A cselekvési tervet a Bizottság hajtja végre, szoros összhangban a tagállamok kapcsolódó cselekvéseivel és egyeztetve a Közösség vonatkozó kutatási és fejlesztési fellépéseivel.

1. **I. cselekvési irányvonal – Az információs rendszerek biztonságára vonatkozó stratégiai keret fejlesztése**

1.1. *A kérdés*

Az információs rendszerek biztonsága a modern társadalomban egy mindent átható, meghatározó minőségi követelmény. Az elektronikus adatszolgáltatáshoz biztonságos távközlési infrastruktúrára, biztonságos hardver- és szoftver-eszközökre, valamint biztonságos felhasználására és igazgatásra van szükség. Átfogó, az információs rendszerek biztonságának összes szempontját figyelembe vevő stratégiát kell létrehozni, amelynek segítségével a szórványos megközelítés elkerülhető. Az elektronikus formában kezelt adatok biztonságára vonatkozó stratégiának tükröznie kell a társadalom törekvését a hatékony működésre és egyúttal érdekeinek védelmére egy gyorsan változó világban.

1.2. *Célkitűzés*

Létre kell hozni egy olyan stratégiai irányultságú keretet, amely nemzetközi környezetben összehangolja a szociális, gazdasági és politikai célkitűzéseket a műszaki, működési és jogi megoldási lehetőségekkel. Az ágazati szereplőknek egy közös elképzelés és egyeztetett stratégiai keret kifejlesztésében kell együttműködniük, hogy megtalálják az érzékeny egyensúlyt a különböző aggályok, célkitűzések és korlátozások között. Ezek az előfeltételei annak, hogy a politikai döntésekben és az ipari fejlesztésekben is sikerüljön összehangolni a különböző érdekeket és igényeket.

1.3. *Állapot és tendenciák*

A helyzet jellemzője, hogy egyre inkább tudatosodik a cselekvés szükségessége. Az erőfeszítések összehangolását szolgáló kezdeményezés hiányában azonban nagy a valószínűsége annak, hogy a különböző ágazatokban a szórványosan megvalósuló erőfeszítések olyan helyzetet teremtenek, amely de facto ellentmondásos lesz és fokozatosan egyre súlyosabb jogi, szociális és gazdasági problémákat teremthet.

1.4. *Követelmények, lehetőségek és prioritások*

E megosztott keretnek foglalkoznia kell az információ és a hozzá kapcsolódó szolgáltatások sebezhetőségére vonatkozó kockázatelemzési és kockázatkezelési problémák megoldásával, a számítógépes/távközlési szabálytalanságokkal és visszaélésekkel kapcsolatos törvények és rendeletek összhangjának megteremtésével, a biztonsági politikát megvalósító közigazgatási infrastruktúrák létrehozásával, valamint annak megállapításával, hogyan lehet kellő hatékonysággal végrehajtani mindezt a különböző iparágakban/tudományágakban úgy, hogy eközben megfelelő módon kezeljék a szociális és személyiségi jogi aggályokat (pl. az azonosítás, hitelesítés, nem megtagadás és esetleg engedélyezés rendszereinek alkalmazása egy demokratikus környezetben).

Világos iránymutatást kell adni a biztonságos megosztott információs szolgáltatások, szabványok, útmutatások és a biztonsági termékekre és szolgáltatásokra, kísérletekre és prototípusokra vonatkozó meghatározások fizikai és logikai felépítésének fejlesztéséhez, hogy meg lehessen határozni az egyes ágazatok igényeihez kapcsolódó különböző közigazgatási szerkezetek, felépítések és szabványok megvalósíthatóságát.

Ahhoz, hogy befolyásolni lehessen a felhasználók hozzáállását az informatika (IT) biztonságával kapcsolatos aggodalmak növekedése tekintetében, meg kell teremteni a biztonsági problémákkal kapcsolatos tudatosságot.

2. **II. cselekvési irányvonal – A felhasználó és a szolgáltató által az információs rendszerek biztonsága tekintetében támasztott elvárások feltérképezése**

2.1. *A kérdés*

Az információs rendszerek biztonsága elengedhetetlen előfeltétele az üzleti alkalmazások integritásának és megbízhatóságának, a szellemi tulajdonnak és a titoktartás elvének. Ez elkerülhetetlenül kényes egyensúlyhoz vezet és esetenként választási helyzetet eredményez a szabad kereskedelem iránti elkötelezettség, valamint a magánélet tiszteletben tartásához való jog és a szellemi tulajdon védelme iránti elkötelezettség között. Ezeknek a választásoknak és kompromisszumoknak a követelmények és az ezekre válaszul adható, információs rendszerek biztonságára vonatkozó különböző megoldások hatásainak teljes körű értékelésére kell alapozni.

A felhasználói igények azt jelzik, hogy az információs rendszerek biztonsági funkciói összefüggnek a technológiai, működési és szabályozási vonatkozásokkal. Ezért az információs rendszerekre vonatkozó biztonsági követelmények rendszeres vizsgálata lényeges része a megfelelő és hatékony intézkedések fejlesztésének.

2.2. *Célkitűzés*

A felhasználók és szolgáltatók által támasztott követelmények jellegének és jellemzőinek meghatározása, illetve ezek kapcsolódása az információs rendszerek biztonsági intézkedéseihez.

2.3. *Állapot és tendenciák*

Eddig nem történt semmilyen összehangolt erőfeszítés a főbb szereplők által az információs rendszerek biztonságára vonatkozó, gyorsan változó és átalakuló igények feltérképezésére. A Közösség tagállamai felmérték a nemzeti keretek között végzett tevékenységek összehangolására vonatkozó követelményeket (különösen az „IT biztonság-értékelésének kritériumai”-ra vonatkozóan). Rendkívül fontos az egységes értékelési kritériumok és az értékelési tanúsítványok kölcsönös elfogadása.

2.4. *Követelmények, lehetőségek és prioritások*

Az ágazati szereplők indokolt igényeinek következetes és áttekinthető kezeléséhez el kell készíteni a felhasználói igények egyeztetett osztályozását és ennek kapcsolatát az információs rendszerek biztonságának megteremtésével.

Fontos továbbá, hogy a tendenciák, szolgáltatási tulajdonságok és technológia fényében meghatározzák a jogalkotással, rendeletekkel és cselekvési kódexekkel szembeni követelményeket, azonosítsák a célkitűzések közigazgatási, szolgáltatói, működési és műszaki rendelkezésekkel történő megvalósítására vonatkozó alternatív stratégiákat, valamint felmérjék az alternatív biztonsági megoldások és stratégiák hatékonyságát, felhasználóbarát mivoltát és költségét a felhasználók, szolgáltatók és üzemeltetők számára.

3. **III. cselekvési irányvonal – A felhasználók, szállítók és szolgáltatók azonnali és átmeneti igényeire vonatkozó megoldások**

3.1. *A kérdés*

Napjainkban „elszigeteléssel”, azaz hagyományos szervezési és fizikai intézkedésekkel lehet megóvni a számítógépeket a külvilág felől érkező jogosulatlan hozzáférésektől. Ugyanez vonatkozik az elektronikus kommunikációra zárt felhasználói csoporton belül az e célra kifejlesztett hálózatoknál is. Egészen más a helyzet akkor, ha az információ megosztott a felhasználói csoportok között, illetve nyilvános vagy általánosan hozzáférhető hálózaton keresztül cserél gazdát. Sem a technológia, a berendezések és szolgáltatások, sem a kapcsolódó szabványok és eljárások nem állnak általánosan rendelkezésre ahhoz, hogy ilyen esetekben biztosítani lehessen az információs rendszereknek az előbbihez mérhető biztonságát.

3.2. *Célkitűzés*

A cél, hogy rövid időn belül megszülessenek a felhasználók, szolgáltatók és gyártók legsürgetőbb igényeinek megfelelő megoldások. Ebbe beletartozik az egységes IT biztonsági értékelő kritériumok alkalmazása. Ennek a rendszernek a jövő követelményei és megoldásai szempontjából nyitottnak kell lennie.

3.3. *Állapot és tendenciák*

Egyes felhasználói csoportok kifejlesztették a saját konkrét igényeinek, többek között a hitelesítés, integritás és a nem megtagadás igényeinek megfelelő technikákat és eljárásokat. Általában mágneskártyákat vagy intelligens kártyákat alkalmaznak. Egyesek többékevésbé fejlett kriptográfiai technikákat alkalmaznak. Ez gyakorta együtt jár a felhasználói csoport konkrét „hatóságának” kijelölésével. Nehéz azonban úgy általánosítani ezeket a technikákat és módszereket, hogy azok megfeleljenek egy nyitott környezet követelményeinek.

Az ISO dolgozik az OSI Information System Security (ISO DIS 7498-2) és a CCITT kifejlesztésén X400-as környezetben. Lehetséges továbbá biztonsági szegmensek beépítése az egyes üzenetekbe. A hitelesítés, az integritás és a nem megtagadás az üzenetek részeként (EDIFACT) és az X400 MHS részeként is kezelhető.

Napjainkban az elektronikus adatcsere (EDI) jogi keret még a koncepció megfogalmazásának szakaszában van. A Nemzetközi Kereskedelmi Kamara megjelentette a kereskedelmi adatok távközlési hálózatokon keresztül történő kicserélésének egységes magatartási szabályait.

Számos ország (többek között Németország, Franciaország és az Egyesült Királyság) kifejlesztette vagy napjainkban fejleszti az IT, valamint a távközlési termékek és rendszerek megbízhatóságának értékelésére vonatkozó kritériumokat és a megfelelő értékelések elvégzésére alkalmas eljárásokat. Ezeket a kritériumokat egyeztették a nemzeti gyártókkal, ennek eredménye lesz az egyre több megbízható termék és rendszer, kezdetben egyszerű termékek megjelenése. Az értékeléseket végző és igazolásokat kiállító nemzeti szervezetek létrehozása segíteni fogja ennek a tendenciának a kibontakozását.

Az információ bizalmas kezelésére vonatkozó rendelkezés a felhasználók többsége szerint egyelőre kevésbé lényeges. Az egyre korszerűbb hírközlési szolgáltatások, különösen a mobil szolgáltatások elterjedésével azonban ez a helyzet a jövőben valószínűleg megváltozik.

3.4. *Követelmények, lehetőségek és prioritások*

Alapvető fontosságú, hogy a lehető legrövidebb időn belül jöjjenek létre az információs rendszerekben (számítógépekben, perifériákban) és a nyilvános hírközlési hálózatokban a kellő biztonságot szavatoló eljárások, szabványok, termékek és eszközök. Elsődleges fontosságot élvez a hitelesítés, az integritás és a nem megtagadás. Kísérleti projektekkel kell meggyőződni a javasolt megoldások életképességéről. A TEDIS programban, a program e cselekvési tervnél általánosabb tartalma szabta kereteken belül igyekeznek megfogalmazni az EDI-rendszerre vonatkozó, elsődleges fontosságot élvező igényeket.

4. IV. cselekvési irányvonal – Az előírások fejlesztése, az információs rendszerek biztonságára vonatkozó szabványosítás, értékelés és tanúsítás

4.1. *A kérdés*

Az információs rendszerek biztonságára vonatkozó követelmények mindenre kiterjednek, ezért fontos az egységes előírások és szabványok elfogadása. Az IT biztonságra vonatkozó egyeztetett szabványok és előírások hiánya a gazdaságban és a társadalomban jelentős akadálya lehet az információkon alapuló folyamatok és szolgáltatások fejlesztésének. Fel kell gyorsítani a technológia és szabványok fejlesztését és alkalmazását a távközléshez és a számítógépes hálózatokhoz kapcsolódó területeken, amelyek különösen fontosak a felhasználók, az ipar és a közigazgatás számára.

4.2. *Célkitűzés*

További erőfeszítésekre van szükség ahhoz, hogy az OSI, ONP, ISDN/IBC és a hálózat-működtetés általános területein kifejleszthetők legyenek a konkrét biztonsági funkciók ellátásának támogatásához szükséges módszerek. A hitelesítéshez, többek között a kölcsönös elfogadás előfeltételeként szolgáló azonosításhoz szükséges technikák és megközelítések elengedhetetlenül kapcsolódnak az előírások és szabványok kimunkálásához. Mindenütt, ahol ez lehetséges, a nemzetközileg egyeztetett megoldásokat kell támogatni. Ugyancsak ösztönözni kell a biztonsági funkciókkal rendelkező számítógépes rendszerek fejlesztését és alkalmazását.

4.3. *Állapot és tendenciák*

Különösen az Egyesült Államok jelentős és fontos kezdeményezéseket tett az információs rendszerek biztonságával kapcsolatos problémák megoldására. Európában ezzel a kérdéssel az IT és távközlési szabványok keretében, az ETSI és a CEN/CENELEC tevékenységgel összefüggésben, a CCITT és az ISO előkészítésével kapcsolatban foglalkoznak.

Tekintettel az egyre fokozódó aggályokra, az Egyesült Államokban ez a munka egyre intenzívebbé válik, és a kereskedők és a szolgáltatók egyaránt egyre nagyobb erőfeszítéseket tesznek ezeknek a problémáknak a kezelésére. Európában Franciaországban, Németországban és az Egyesült Királyságban egymástól függetlenül indultak el hasonló fejlesztések, de az Egyesült Államok gyakorlatának megfelelő közös erőfeszítések csak nagyon lassan bontakoznak ki.

4.4. *Követelmények, lehetőségek és prioritások*

Az információs rendszerek biztonságánál elengedhetetlenül rendkívül szoros az összefüggés a szabályzó, működési, közigazgatási és műszaki vonatkozások között. A rendeletek különböző rendelkezéseinek meg kell jelenniük a szabványokban, és az információs rendszerek biztonságára vonatkozó rendelkezéseknek ellenőrizhető módon igazodniuk kell a szabványokhoz és rendeletekhez. A rendeletekben bizonyos vonatkozásokban olyan előírásokra is szükség van, amelyek túlmutatnak a szabványosítás hagyományos hatókörén, azaz tartalmaznak bizonyos gyakorlati szabályokat. A szabványokra és gyakorlati kódexekre vonatkozó követelmények az információs rendszerek biztonságának minden területén jelen vannak, és különbséget kell tenni a biztonsági célkitűzéseknek megfelelő védelmi követelmények és az illetékes európai szabványügyi testületekre (CEN/CENELEC/ETSI) átruházható műszaki követelmények között.

Az előírásoknak és szabványoknak ki kell terjedniük az információs rendszerek biztonsági szolgáltatásainak tárgyára (személyi és vállalati azonosítás, nem megtagadási protokollok, jogi értelemben elfogadható elektronikus bizonyíték, engedélyezés ellenőrzése), kommunikációs szolgáltatásaira (a képi kommunikáció védelme, a mobil távközlés hang- és adatátviteli védelme, adatok és képi információk adatbázisvédelme, integrált szolgáltatások biztonsága), az ezek közötti kommunikáció és a biztonság kérdéseinek kezelésére (nyilvános/zárt kulcsrendszer a nyitott hálózati tevékenységhez, hálózatkezelés védelme, szolgáltató védelme) és a rendszerek hitelesítésére (biztosítási kritériumok és szintek, az információs rendszerek biztonságával összefüggő, biztonságot szavatoló eljárások).

5. V. cselekvési irányvonal – Technológiai és működési fejlesztések az információs rendszerek biztonságának területén

5.1. *A kérdés*

Az információs rendszerek biztonságával összefüggő jelenlegi és a jövőben várható követelményekre vonatkozó, gazdasági értelemben életképes és működési vonatkozásban megfelelő technológiák rendszerbe foglalt vizsgálata és fejlesztése a szolgáltató piac fejlődésének és az egész európai gazdaság versenyképességének előfeltétele.

Az információs rendszerek biztonsága terén elindított bármely fejlesztésnek ki kell terjednie a számítógépek biztonságára és a hírközlés biztonságára, hiszen a legkorszerűbb rendszerek általában megosztott rendszerek, és az ilyen rendszerekhez a kommunikációs hálózatokon keresztül lehet hozzáférni.

5.2. *Célkitűzés*

Az információs rendszerek biztonságával összefüggő jelenlegi és a jövőben várható követelményekre vonatkozó, gazdasági értelemben életképes és működési vonatkozásban megfelelő megoldásokat lehetővé tevő technológiák rendszerezett vizsgálata és fejlesztése.

5.3. *Követelmények, lehetőségek és prioritások*

Az információs rendszerek biztonságával összefüggő munka során foglalkozni kell fejlesztési és megvalósítási stratégiákkal, technológiákkal, valamint integrációval és hitelesítéssel.

A stratégiai K&F munkának ki kell terjednie a rendszerek biztonságának elméleti modelljeire (a veszélyeztetés, engedély nélküli módosítás és szolgáltatás megtagadása elleni védekezés), a modellek funkcionális követelményeire, a kockázati modellekre és a biztonsági felépítésekre.

A technológiai jellegű K&F munkának ki kell terjednie a felhasználó és az üzenet hitelesítésének elméleti modelljére (pl. hangelemzés és elektronikus aláírások eszközeivel), a kódoláshoz szükséges műszaki interfészekre és protokollokra, a hozzáférést vezérlő mechanizmusokra és a bevált biztonsági rendszerek bevezetésének mechanizmusaira.

A műszaki rendszer biztonságának és alkalmazhatóságának hitelesítését és engedélyezését integrációs és hitelesítési projekteken keresztül kell vizsgálni.

A biztonsági technológia konszolidációján és fejlesztésén túl számos kísérő intézkedésre van szükség, többek között a jelenlegi szabványok alkalmazásának elkészítése, karbantartása és következetes alkalmazása, az IT és távközlési termékek biztonsági tulajdonságainak ellenőrzése és hitelesítése, beleértve a rendszerek tervezésére és bevezetésére vonatkozó hitelesítési és minősítési módszerek terén.

A harmadik RDT közösségi keretprogram is felhasználható az együttműködési projektek megvalósítására prekompetitív és prenormatív szinten.

6. VI. cselekvési irányvonal – Az információs rendszerek biztonságának megteremtése

6.1. *A kérdés*

Az információs rendszerek biztonsági tulajdonságainak pontos jellegétől függően a szükséges funkciókat az információs rendszer különböző részeibe kell beépíteni, beleértve a végberendezéseket/számítógépeket, szolgáltatásokat, hálózatkezelést, kriptográfiai eszközöket, intelligens kártyákat, nyilvános és zárt jellegű kulcsokat stb. Ezeknek az elemeknek egy bizonyos része beépülhet a kereskedők által forgalmazott hardver és szoftver eszközökbe, mások a megosztott rendszerek részeiként működhetnek (pl. hálózatkezelés), lehetnek az egyes felhasználók birtokában (pl. intelligens kártyák), vagy egy szakosított szervezet termékválasztékában szerepelhetnek (nyilvános/zárt kulcsok).

Várhatóan a kereskedők, szolgáltatók vagy üzemeltetők gondoskodnak a biztonsági termékek és szolgáltatások nagyobb részéről. Meghatározott funkciók esetében, pl. nyilvános/zárt kulcsok biztosításánál, az engedélyezés felülvizsgálatánál szükség lehet megfelelő szervezetek kiválasztására és megbízására.

Ugyanez vonatkozik a szolgáltatás minőségének hitelesítésére, értékelésére és ellenőrzésére; ezeket a funkciókat a kereskedők, szolgáltatók vagy üzemeltetők érdekeitől független szervezeteknek kell ellátniuk. Ezek a szervezetek lehetnek magánvállalkozások, állami vagy állam által engedélyezett és a funkciók ellátásával megbízott szervezetek.

6.2. *Célkitűzés*

A Közösség területén az állami és közérdek védelmében az információs rendszerek biztonságossá tételéhez szükséges összehangolt megközelítés kifejlesztése érdekében ki kell alakítani egy egységes és következetes módszert a biztonság szavatolására. Ott, ahol független szervezeteket kell megbízni ennek a feladatnak az ellátásával, szükség van a funkciók és feltételek előzetes meghatározására és egyeztetésére, illetve ezek beágyazására a szabályozó keretbe. A kölcsönös elismerés feltételeként a cél a kötelezettségek világosan meghatározott és egyeztetett közösségi szintű elosztása a különböző szereplők között.

6.3. *Állapot és tendenciák*

Napjainkban az információs rendszerek biztonságának szavatolása csak meghatározott területeken, ezek jól szervezett és konkrét igényeinek kielégítésére korlátozódik. A szervezés európai szinten alapvetően informális és a hitelesítés és minősítés kölcsönös elfogadása zárt csoportokon kívül nem megoldott. Az információs rendszerek biztonságának egyre fontosabbá válásával mind sürgősebbé válik, hogy Európában és a nemzetközi piacokon is szülessenek meg a megfelelő következetes megközelítések az információs rendszerek biztonságának megteremtéséről.

6.4. *Követelmények, lehetőségek és prioritások*

A különböző érintett szereplők száma és a szabályozó és törvényhozó kérdésekhez való szoros kapcsolódás miatt különösen fontos, hogy az érdekeltek előzetesen egyeztessenek egymással az információs rendszerek biztonságára vonatkozó irányadó elvekről.

A kérdés egységes megközelítésének kialakítása során foglalkozni szükséges a funkciók azonosításának és meghatározásának különböző vonatkozásaival, melyek jellegüknél fogva szükségessé teszik bizonyos független szervezetek (vagy egymással együtt dolgozó szervezetek) rendelkezésre állását. Beletartozhatnak ebbe többek között olyan funkciók, mint egy nyilvános/zárt kulcsrendszer működtetése.

Az elmondottakon túl egy korai szakaszban meg kell határozni azokat a funkciókat, amelyeket közérdekből független szervezetekre (vagy egymással együtt dolgozó szervezetekre) kell bízni. Ebbe beletartozhat többek között az ellenőrzés, a minőségbiztosítás, a hitelesítés, a minősítés és egyéb hasonló funkciók ellátása.