

31992D0242

8.5.1992

DZIENNIK URZĘDOWY WSPÓLNOT EUROPEJSKICH

L 123/19

**DECYZJA RADY
z dnia 31 marca 1992 r.
w dziedzinie bezpieczeństwa systemów informatycznych**

(92/242/EWG)

RADA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Gospodarczą, w szczególności jego art. 235,

uwzględniając wniosek Komisji ⁽¹⁾,

uwzględniając opinię Parlamentu Europejskiego ⁽²⁾,

uwzględniając opinię Komitetu Ekonomiczno-Społecznego ⁽³⁾,

a także mając na uwadze, co następuje:

Wspólnota, mając za cel, poprzez ustanowienie wspólnego rynku i stopniowe zbliżanie polityki gospodarczej Państw Członkowskich, wspieranie we Wspólnocie harmonijnego rozwoju działalności gospodarczej, ciągłą i zrównoważoną ekspansję, zwiększenie stabilności, przyspieszenie podnoszenia poziomu życia i zacieśnienie związków między Państwami Członkowskimi;

informacje przechowywane, przetwarzane i przekazywane drogą elektroniczną odgrywają coraz większą rolę w działalności gospodarczej i społecznej;

pojawienie się skutecznej komunikacji ogólnoswiatowej i powszechnego korzystania z elektronicznego przetwarzania oraz przekazywania informacji uwydatnia potrzebę jej właściwej ochrony;

Parlament Europejski na swych posiedzeniach i w przyjmowanych rezolucjach wielokrotnie podkreślał znaczenie bezpieczeństwa systemów informatycznych;

Komitet Ekonomiczno-Społeczny zwrócił uwagę na potrzebę zajęcia się zagadnieniami dotyczącymi bezpieczeństwa systemów informatycznych w formach działania Wspólnoty, zwłaszcza w związku z wpływem tego bezpieczeństwa na wprowadzenie rynku wewnętrznego;

formy działania na poziomie krajowym, międzynarodowym i wspólnotowym dostarczają dobrych ku temu podstaw;

istnieje ścisły związek między telekomunikacją, technologią informatyczną, normalizacją, rynkiem informatycznym a rynkiem informacji politykami w dziedzinie badań, rozwoju i technologii, a także wszelkimi pracami już podjętymi w tych obszarach przez Wspólnotę;

właściwe jest zapewnienie, aby wysiłki i starania zostały połączone poprzez wykorzystanie istniejących opracowań krajowych i międzynarodowych oraz promowanie współpracy między głównymi zainteresowanymi stronami; właściwe jest zatem postępowanie w ramach spójnego planu działania;

złożoność problematyki bezpieczeństwa systemów informatycznych wymaga opracowania strategii umożliwiającej swobodny przepływ informacji w obrębie jednolitego rynku przy jednoczesnym zapewnieniu bezpieczeństwa korzystania z systemów informatycznych w całej Wspólnocie;

każde Państwo Członkowskie odpowiedzialne jest za uwzględnienie ograniczeń nakładanych przez zasady bezpieczeństwa ogólnego i porządku publicznego;

odpowiedzialność Państw Członkowskich w tym zakresie implikuje konieczność opracowania uzgodnionego podejścia do tej problematyki, opartego na bliskiej współpracy z wyższymi urzędnikami Państw Członkowskich;

należy przyjąć przepis dotyczący planu działania na okres pierwszych dwudziestu czterech miesięcy i powołania Komitetu Wyższych Urzędników o długoterminowej kadencji, który będzie ciałem doradczym Komisji odnośnie do form działania w obszarze bezpieczeństwa systemów informatycznych;

uznano, że na realizację działań w okresie pierwszych 24 miesięcy niezbędna jest kwota 12 milionów ECU;

w kontekście obecnej perspektywy finansowej niezbędne potrzeby w zakresie środków na 1992 r. ocenia się na 2 miliony ECU;

kwoty, jakie mają być przeznaczone na finansowanie programu w okresie po roku budżetowym 1992, będą stanowić część obowiązujących ram finansowych Wspólnoty,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Niniejszym przyjmuje się działania w dziedzinie bezpieczeństwa systemów informatycznych. Obejmują one:

- opracowanie ogólnej strategii bezpieczeństwa systemów informatycznych (plan działań) na wstępny okres 24 miesięcy, i
- ustanowienie Zespołu Wyższych Urzędników o długoterminowej kadencji, który będzie ciałem doradczym Komisji w sprawach działań, jakie będą podejmowane w dziedzinie bezpieczeństwa systemów informatycznych, zwanego dalej „Komitetem”.

⁽¹⁾ Dz.U. C 268 z 5.11.1990, str. 18.

⁽²⁾ Dz.U. C 94 z 13.3.1992.

⁽³⁾ Dz.U. C 159 z 17.6.1991, str. 38.

Artykuł 2

1. Komisja regularnie zasięga opinii Komitetu w sprawach dotyczących bezpieczeństwa systemów informatycznych w obszarach różnych działań podejmowanych przez Wspólnotę, zwłaszcza w zakresie określania strategii prac i programów.

2. Plan działań, jak podano w Załączniku, obejmuje prace przygotowawcze w zakresie następującej tematyki:

- I. opracowanie strategicznych ram dla bezpieczeństwa systemów informatycznych;
- II. określenie wymagań użytkownika i usługodawcy w celu zapewnienia bezpieczeństwa systemów informatycznych;
- III. zaspokajanie bieżących i tymczasowych potrzeb użytkowników, dostawców oraz usługodawców;
- IV. opracowanie specyfikacji, normalizacji, oceny i certyfikacji w odniesieniu do bezpieczeństwa systemów informatycznych;
- V. opracowania dotyczące technologii i eksploatacji w dziedzinie bezpieczeństwa systemów informatycznych;
- VI. zapewnienie bezpieczeństwa systemów informatycznych.

Artykuł 3

1. Fundusze Wspólnoty, ocenione jako niezbędne do realizacji działań w okresie początkowym, wynoszą 12 milionów ECU, w tym 2 miliony ECU na 1992 r. w ramach perspektywy finansowej na lata 1988-1992.

Kwota niezbędna w dalszym okresie do realizacji programu powinna zostać ujęta w obowiązujących ramach finansowych Wspólnoty.

2. Władza budżetowa określa środki przyznawane na każdy rok finansowy przy uwzględnieniu zasad należytego zarządzania, określonego w art. 2 rozporządzenia finansowego, stosowanego dla ogólnego budżetu Wspólnot Europejskich.

Artykuł 4

Grupa niezależnych ekspertów dokona na potrzeby Komisji oceny postępów osiągniętych w początkowej fazie działań. Sprawozdanie tej grupy ekspertów, wraz z ewentualnymi komentarzami Komisji, przedstawione zostaje Parlamentowi Europejskiemu i Radzie.

Artykuł 5

1. Za realizację działań odpowiedzialna jest Komisja. Komisja wspomagana jest przez komitet doradczy, składający się z przedstawicieli Państw Członkowskich, któremu przewodniczyć będzie przedstawiciel Komisji.

2. Plan działań realizowany jest zgodnie z celami określonymi w art. 2, a w miarę potrzeb uaktualniany. Plan określa szczegółowo cele i rodzaje działań, jakie mają być podejmowane,

a także ustalenia w sprawach finansowych z nim związanych. Opierając się na tym planie, Komisja wystosowuje zaproszenie do składania odpowiednich wniosków.

3. Plan działań realizowany jest przy ściślejszej współpracy z reprezentantami branży. Uwzględnia, wspiera i uzupełnia europejską i międzynarodową działalność normalizacyjną w zakresie prowadzonych w tej dziedzinie prac.

Artykuł 6

1. Procedura ustanowiona w art. 7 stosuje się do:

— środków dotyczących polityki Wspólnoty w dziedzinie bezpieczeństwa systemów informatycznych.

2. Procedura ustanowiona w art. 8 stosuje się do:

- przygotowania i uaktualniania planu działania, określonego w art. 5;
- treści zaproszeń do składania wniosków, oceny tych wniosków i szacowania kwoty udziału Wspólnoty w środkach w przypadku, kiedy kwota ta przekracza 20 000 tysięcy ECU;
- współpracy wszystkich organizacji pozawspólnotowych we wszelkich rodzajach działalności podejmowanej na mocy niniejszej decyzji;
- ustaleń dotyczących upowszechniania, ochrony i wykorzystywania wyników podejmowanych środków;
- środków, jakie mają być podejmowane w celu oceny działań.

3. W przypadku gdy kwota udziału Wspólnoty w środkach nie przekracza dwustu tysięcy ECU, Komisja zasięga opinii Komitetu w sprawie środków, jakie mają być podjęte, i poinformuje Komitet o wynikach tej oceny.

Artykuł 7

Przedstawiciel Komisji przedstawia Komitetowi projekt środków, które należy podjąć. Komitet wydaje na temat tego projektu swą opinię w czasie, wyznaczonym przez przewodniczącego Komitetu w zależności od pilności sprawy; w miarę potrzeb w drodze głosowania.

Opinia zostaje sporządzona w formie Protokołu. Ponadto Państwo Członkowskie ma prawo zażądać odnotowania swojego stanowiska w Protokole.

Komisja bierze pod uwagę opinię Komitetu w jak największym zakresie. Informuje ona również Komitet o zakresie, w jakim opinia ta została uwzględniona.

Artykuł 8

Przedstawiciel Komisji przedstawia Komitetowi projekt środków, które należy podjąć. Komitet wydaje na temat tego projektu swą opinię w czasie, wyznaczonym przez przewodniczącego Komitetu w zależności od pilności sprawy. Opinia ta jest przyjmowana większością określoną w art. 148 ust. 2 Traktatu,

w przypadku decyzji, które Rada jest zobowiązana podjąć na wniosek Komisji. Głosy oddane przez Państwa Członkowskie reprezentowane w Komitecie są ważone w sposób ustalony w tym artykule. Przewodniczący Komitetu nie bierze udziału w głosowaniu.

Komisja przyjmuje przewidziane środki, jeżeli są one zgodne z opinią Komitetu.

Jeżeli przewidziane środki nie są zgodne z opinią Komitetu albo jeżeli nie przedstawiono żadnej opinii, Komisja bezzwłocznie przedstawia Radzie propozycje dotyczące środków, jakie mają zostać podjęte. Rada podejmuje decyzję kwalifikowaną większością.

Jeżeli przed upływem trzech miesięcy od daty zwrócenia się do Rady, Rada nie podjęła żadnych czynności, proponowane środki są przyjmowane przez Komisję, z wyjątkiem przypadku, kiedy Rada podjęła decyzję negatywną co do wspomnianych środków zwykłą większością.

Sporządzono w Brukseli, dnia 31 marca 1992 r.

W imieniu Rady

Vitor MARTINS

Przewodniczący

ZAŁĄCZNIK

Kierunki działań w skrócie

KIERUNKI PLANU DZIAŁAŃ W DZIEDZINIE BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH

WPROWADZENIE

Celem planu działań jest opracowanie ogólnej strategii, zmierzającej do zapewnienia użytkownikom i autorom informacji przechowywanych w postaci elektronicznej, przetwarzanych lub przesyłanych odpowiedniego zabezpieczenia systemów informatycznych przed przypadkowymi lub umyślnymi zagrożeniami.

Plan działań uwzględnia i uzupełnia ogólnościowe prace normalizacyjne w tej dziedzinie.

Plan ten obejmuje następujące kierunki działania:

- opracowanie strategicznych ram dla bezpieczeństwa systemów informatycznych;
- określenie wymagań użytkownika i usługodawcy związanych z zapewnieniem bezpieczeństwa systemów informatycznych;
- zaspokajanie bieżących i tymczasowych potrzeb użytkowników, dostawców oraz usługodawców;
- opracowanie specyfikacji, normalizacji, oceny i certyfikacji w odniesieniu do bezpieczeństwa systemów informatycznych;
- opracowania dotyczące technologii i eksploatacji w dziedzinie bezpieczeństwa systemów informatycznych;
- zapewnienie bezpieczeństwa systemów informatycznych.

Plan działań wykonywany jest przez Komisję, w ścisłym związku z odpowiednimi działaniami Państw Członkowskich i w połączeniu ze stosownymi pracami badawczo-rozwojowymi we Wspólnocie.

1. Kierunek działań I — opracowanie strategicznych ram dla bezpieczeństwa systemów informatycznych

1.1. Zagadnienia

Bezpieczeństwo systemów informatycznych jest uważane za coraz bardziej powszechną jakość, niezbędną w nowoczesnym społeczeństwie. Usługi dotyczące informacji w postaci elektronicznej wymagają bezpiecznej infrastruktury telekomunikacyjnej, bezpiecznego sprzętu i oprogramowania, a także bezpiecznego wykorzystywania tych informacji i zarządzania nimi. Istnieje potrzeba ustanowienia ogólnej strategii, uwzględniającej wszelkie aspekty bezpieczeństwa systemów informatycznych, unikając rozwiązań cząstkowych. Każda strategia bezpieczeństwa informacji przetwarzanych drogą elektroniczną musi odzwierciedlać wolę funkcjonowania społeczeństwa w sposób efektywny, niemniej jednak przy posiadaniu odpowiednich zabezpieczeń w szybko zmieniającym się świecie.

1.2. Cele

Aby pogodzić cele społeczne, ekonomiczne i polityczne z celami i wyborami technicznymi, funkcjonalnością i kwestiami prawnymi Wspólnoty w aspekcie międzynarodowym, należy ustanowić ramy o charakterze strategicznym. Podmioty tego sektora, pracujące razem nad stworzeniem wspólnego sposobu widzenia tego zagadnienia, muszą określić ten delikatny stan równowagi między różnymi kwestiami, celami i ograniczeniami oraz uzgodnić

strategiczne ramy. Są to warunki wstępne pogodzenia interesów i potrzeb zarówno w tworzeniu polityki postępowania, jak i opracowań przemysłowych.

1.3. Stan obecny i kierunki rozwoju

Stan obecny charakteryzuje się narastającą świadomością potrzeby działań. Jednakże w sytuacji braku inicjatyw dotyczących koordynacji wysiłków i zamierzeń wydaje się, że rozproszenie wysiłków w różnych sektorach doprowadzi do sytuacji, która w istocie będzie sprzeczna ze stanem, jaki zamierza się osiągnąć oraz generować będzie narastające i coraz poważniejsze problemy prawne, społeczne i ekonomiczne.

1.4. Wymagania, opcje i priorytety

Takie wspólne ramy działania wymagają ujęcia i odniesienia się do analizy ryzyka i zarządzania ryzykiem dotyczących wrażliwości informacji i związanych z nią usług, dostosowania przepisów ustawowych i wykonawczych związanych z nadużywaniem i niewłaściwym wykorzystaniem techniki komputerowej i telekomunikacyjnej, infrastruktury administracyjnej, łącznie z polityką bezpieczeństwa i sposobami jej wprowadzania w życie w sposób efektywny przez różne gałęzie przemysłu i branże, a także spraw społecznych i kwestii prywatności (np. stosowania identyfikacji, uwierzytelnienia, uznawania i być może systemów autoryzacji w społeczeństwie demokratycznym).

Muszą być podane jasne wytyczne co do opracowania fizycznej i logicznej architektury służącej bezpiecznemu rozpowszechnianiu informacji, ustalaniu norm, wskazówek i definicji produktów oraz usług zabezpieczających, opracowaniom pilotażowym i prototypowym w celu określenia efektywności różnych struktur administracyjnych, konstrukcji i norm związanych z potrzebami określonych działów gospodarki.

Należy wytwarzać świadomość potrzeby bezpieczeństwa, aby w ten sposób wpływać na stosunek użytkowników do narastających obaw związanych z bezpieczeństwem technologii informatycznych.

2. Kierunek działań II — określenie wymagań użytkownika i usługodawcy związanych z zapewnieniem bezpieczeństwa systemów informatycznych

2.1. Zagadnienia

Bezpieczeństwo systemów informatycznych jest nieodłącznym warunkiem wstępnym integralności i wiarygodności dla zastosowań gospodarczych, własności intelektualnej i poufności. Prowadzi to w sposób nieuchronny do trudności w utrzymaniu równowagi, a czasami wyborów, między zobowiązaniem do wolnego handlu a zobowiązaniem do zapewnienia prywatności i zabezpieczenia własności intelektualnej. Wybory takie, aby mogły spełniać swoje cele w tym zakresie i uwzględniać kompromisy, muszą być oparte na pełnym uznaniu i zrozumieniu wymagań oraz wpływu możliwych opcji na bezpieczeństwo systemów informatycznych.

Z wymagań użytkownika wynika bezpieczeństwo funkcjonowania systemów informatycznych współzależne od uwarunkowań technologicznych, eksploatacyjnych i prawnych. Dlatego też systematyczne badanie wymagań bezpieczeństwa systemów informatycznych stanowi podstawowy element opracowania właściwych i skutecznych środków.

2.2. Cele

Ustalenie charakteru i właściwości wymagań użytkowników oraz usługodawców, a także ich stosunku do środków bezpieczeństwa systemów informatycznych

2.3. Stan obecny i kierunki rozwoju

Dotychczas nie podejmowano wspólnych wysiłków w celu określenia szybko rozwijających się i zmieniających wymagań głównych podmiotów zainteresowanych bezpieczeństwem systemów informatycznych. Państwa Członkowskie Wspólnoty określiły wymagania dotyczące harmonizacji działań państwowych (zwłaszcza w zakresie kryteriów oceny bezpieczeństwa IT). Jednolite kryteria oceny i zasady wzajemnego uznawania certyfikatów oceny mają tu znaczenie podstawowe.

2.4. Wymagania, opcje i priorytety

Za podstawę spójnego i przejrzystego traktowania uzasadnionych potrzeb uczestników tych działań uznano potrzebę opracowania

uzgodnionej klasyfikacji wymagań użytkownika i ich stosunku do zapewnienia bezpieczeństwa systemów informatycznych.

Za ważne uznano również zdefiniowanie wymagań co do legislacji, przepisów i kodeksów postępowania w świetle oceny trendów w charakterystyce usług i technologii, rozpoznanie alternatywnych strategii umożliwiających spełnienie celów poprzez przepisy o charakterze administracyjnym, usługowym, eksploatacyjnym i technicznym, a także ocenę skuteczności, wygody użytkownika w posługiwaniu się systemem oraz kosztów alternatywnych opcji i strategii bezpieczeństwa dotyczących użytkownika, usługodawców i operatorów.

3. Kierunek działań III — rozwiązania zaspokajające bieżące i tymczasowe potrzeby użytkowników, dostawców i usługodawców

3.1. Zagadnienie

Obecnie możliwe jest skuteczne zabezpieczenie komputerów przed nieuprawnionym dostępem ze świata zewnętrznego poprzez tzw. odizolowanie, tzn. użycie konwencjonalnych środków organizacyjnych i fizycznych. Stosuje się to również do komunikacji elektronicznej w obrębie zamkniętej grupy użytkowników korzystających z sieci dedykowanej. Sytuacja staje się zupełnie odmienna, gdy informacje są wymieniane między grupami użytkowników lub dostarczane poprzez sieć publiczną bądź ogólnie dostępną. Zarówno technologia, terminale, czy usługi, jak i normy oraz procedury, które zapewniałyby porównywalne bezpieczeństwo systemów informatycznych, generalnie są w tym przypadku nieosiągalne.

3.2. Cele

Celem musi być dostarczenie, w formie krótkiego opisu, rozwiązań, które mogą zaspokajać najpilniejsze potrzeby użytkowników, usługodawców i producentów. Obejmuje to stosowanie wspólnych kryteriów oceny bezpieczeństwa technologii informacji, które należy traktować jako sprawę otwartą w przyszłych wymaganiach i rozwiązaniach.

3.3. Stan obecny i kierunki rozwoju

Niektóre grupy użytkowników opracowały techniki i procedury przeznaczone do swoich własnych, specjalnych celów, odpowiadające w szczególności potrzebom uwierzytelniania, integralności i uznawania. Generalnie stosowane są karty magnetyczne lub karty procesorowe. Niektórzy stosują mniej lub bardziej wymyślne techniki kryptograficzne. Często wymagało to zdefiniowania specyficznych „władz” grupy użytkowników. Trudno jest jednak tak uogólnić te techniki i metody, aby spełniały one wymagania otwartego środowiska.

Międzynarodowa Organizacja Normalizacyjna ISO pracuje nad Bezpieczeństwem Systemów Informatycznych w modelu OSI (Otwartym Połączeniu Systemów) (ISO DIS 7498-2) oraz w związku ze standardem X400 wraz z Międzynarodowym Komitetem Doradczym ds. telefonii i telegrafii (CCITT). Istnieje również możliwość umieszczenia segmentów zabezpieczających w wiadomościach. Uwierzytelnianie, integralność i uznawanie są traktowane jako część wiadomości (EDIFACT) a także jako część usługi przekazywania komunikatu (MHS) w standardzie X400.

Obecnie prawne ramy elektronicznej wymiany danych (EDI) są ciągle na etapie prac koncepcyjnych. Międzynarodowa Izba Handlu opublikowała jednolite zasady postępowania przy wymianie danych handlowych przez telekomunikacyjne sieci.

Kilka państw (np. Niemcy, Francja, Wielka Brytania i Stany Zjednoczone) opracowało lub jest w trakcie opracowywania kryteriów oceny wiarygodności produktów i systemów informatycznych oraz telekomunikacyjnych, a także i odpowiadających temu procedur umożliwiających dokonywanie takich ocen. Kryteria te zostały uzgodnione z producentami krajowymi i będą prowadzić do wzrostu liczby wiarygodnych produktów i systemów, poczynając od prostych produktów. Ustanowienie narodowych organizacji, które będą dokonywały tych ocen i oferowały certyfikację, wesprze ten kierunek rozwoju.

Zapewnienie poufności uważane jest przez większość użytkowników za rzecz mniej ważną i pilną. W przyszłości jednakże sytuacja ta prawdopodobnie się zmieni, ponieważ zaawansowane usługi telekomunikacyjne, a w szczególności usługi mobilne staną się wszechobecne.

3.4. Wymagania, opcje i priorytety

Jest rzeczą bardzo ważną, aby jak najszybciej opracować procedury, normy, produkty i narzędzia odpowiednie do zapewnienia bezpieczeństwa zarówno w systemach informatycznych jako takich (komputery, urządzenia peryferyjne), jak i w publicznych sieciach komunikacyjnych. Wysoki priorytet powinien zostać nadany uwierzytelnianiu, integralności i uznawania. Powinny zostać przeprowadzone projekty pilotażowe w celu ustalenia stosowności proponowanych rozwiązań. Do rozwiązania potrzeb priorytetowych dotyczących EDI można wykorzystać program TEDIS w zakresie bardziej ogólnej treści tego planu działań.

4. Kierunek działań IV — opracowanie specyfikacji, normalizacji, oceny i certyfikacji w odniesieniu do bezpieczeństwa systemów informatycznych

4.1. Zagadnienie

Wymagania bezpieczeństwa systemów informatycznych są bardzo szerokie i powszechne, dlatego kluczową sprawą staje się wspólna specyfikacja i normalizacja. Brak uzgodnionych norm i specyfikacji dotyczących bezpieczeństwa technologii informatycznej może stanowić główną barierę dla rozwoju gospodarczego i społecznego procesów opartych na wykorzystywaniu informacji i usług z tym związanych. Wymagane jest również podjęcie działań mających na celu przyspieszenie rozwoju oraz wykorzystanie technologii i norm w kilku obszarach związanych z sieciami komunikacyjnymi i komputerowymi, które to obszary mają ogromne znaczenie dla użytkowników, przemysłu i administracji.

4.2. Cele

Należy podjąć wysiłki w celu zapewnienia środków wspierających i realizujących określone funkcje zabezpieczające w ogólnych obszarach OSI, ONP, ISDN/IBC oraz zarządzania siecią. Z natury rzeczy z normalizacją i specyfikacją związane są techniki i metody wymagane przy weryfikacji, włączając w to certyfikację zapewniającą wzajemne uznanie. Tam, gdzie to możliwe należy wspierać rozwiązania uzgodnione na szczeblu międzynarodowym. Należy również zachęcać do rozwoju i wykorzystywania systemów komputerowych posiadających funkcje zabezpieczające.

4.3. Stan obecny i kierunki rozwoju

Poważne inicjatywy w kierunku zapewnienia bezpieczeństwa systemów informatycznych podjęły w szczególności Stany Zjednoczone. W Europie temat ten rozpatrywany jest w ramach zagadnień normalizacji technologii informatycznych i telekomunikacyjnych w kontekście Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI) i Europejskiego Komitetu Normalizacyjnego (CEN)/Europejskiego Komitetu Normalizacyjnego Elektrotechniki (CENELEC) podczas prac przygotowawczych Międzynarodowego Komitetu Doradczego ds. telefonii i telegrafii (CCITT) oraz Międzynarodowej Organizacji Normalizacyjnej (ISO) w tym obszarze.

Zważywszy na coraz większe znaczenie tych zagadnień, Stany Zjednoczone gwałtownie intensyfikują prace, a zarówno producenci, jak i usługodawcy zwiększają swoje wysiłki. W Europie podobne działania rozpoczęły niezależnie Francja, Niemcy i Wielka Brytania, ale łączenie wysiłków w tym kierunku następuje bardzo powoli, w porównaniu do Stanów Zjednoczonych.

4.4. Wymagania, opcje i priorytety

W dziedzinie bezpieczeństwa systemów informatycznych z natury rzeczy istnieje bardzo ścisły związek między aspektami prawnymi, eksploatacyjnymi, administracyjnymi i technicznymi. Uregulowania prawne powinny znaleźć odzwierciedlenie w normach, a przepisy dotyczące bezpieczeństwa systemów informatycznych powinny spełniać normy i uregulowania w sposób możliwy do sprawdzenia. W kilku aspektach uregulowania wymagają specyfikacji, która wykracza poza konwencjonalny zakres normalizacji, tj. obejmuje kodeks postępowania. Wymagania dotyczące norm i kodeksów postępowania istnieją we wszystkich obszarach bezpieczeństwa systemów informatycznych i dlatego powinno zostać wprowadzone rozróżnienie między wymaganiami ochronnymi, które służą celom bezpieczeństwa, a pewnymi wymaganiami technicznymi, które mogą być powierzonym właściwym europejskim instytucjom normalizacyjnym (CEN/CENELEC/ETSI).

Specyfikacje i normy muszą obejmować usługi zapewniające bezpieczeństwo systemów informatycznych (uwierzytelnienie osób i instytucji/firm, protokoły uznawania, prawnie akceptowalne dowody elektroniczne, kontrola upoważnień), usługi komunikowania się tych systemów (zapewnienie prywatności przesyłania obrazu, prywatności bezprzewodowej transmisji głosu i danych i, zabezpieczenia baz danych i obrazów, bezpieczeństwo usług zintegrowanych), zarządzanie komunikacją systemów i jej bezpieczeństwem (system kodów publicznych/prywatnych do pracy w sieciach otwartych, ochrona zarządzania siecią, ochrona usługodawcy) oraz ich certyfikację (kryteria i poziomy pewności, procedury zapewnienia bezpieczeństwa systemów informatycznych).

5. Kierunek działań V — opracowania dotyczące technologii i eksploatacji w dziedzinie bezpieczeństwa systemów informatycznych

5.1. Zagadnienie

Systematyczne badania i rozwój technologii, umożliwiające stosowanie rozwiązań efektywnych gospodarczo i zadowalających z punktu widzenia ich funkcjonalności w odniesieniu do wielu obecnych i przyszłych wymagań bezpieczeństwa systemów informatycznych, jest warunkiem wstępnym rozwoju rynku usług i konkurencyjności gospodarki europejskiej jako całości.

Wszelkie opracowania dotyczące bezpieczeństwa systemów informatycznych będą musiały mieścić w sobie zarówno aspekty bezpieczeństwa sprzętu komputerowego, jak i bezpieczeństwa komunikacji, ponieważ większość dzisiejszych systemów stanowią systemy dystrybucji, a dostęp do nich odbywa się poprzez usługi komunikacyjne.

5.2. Cele

Systematyczne badania i rozwój technologii, umożliwiające stosowanie rozwiązań efektywnych gospodarczo i zadowalających z punktu widzenia ich funkcjonalności i w odniesieniu do wielu obecnych i przyszłych wymagań bezpieczeństwa systemów informatycznych

5.3. Wymagania, opcje i priorytety

Prace nad bezpieczeństwem systemów informatycznych będą wymagały zajęcia się strategiami rozwoju i wdrażania, technologiami oraz integracją i weryfikacją.

Strategiczne prace badawczo-rozwojowe będą musiały objąć modele koncepcyjne systemów bezpiecznych (chroniących przed zagrożeniami, nieuprawnionymi modyfikacjami i odmową usługi), modele funkcjonalne, modele ryzyka i architekturę zapewniającą bezpieczeństwo.

Prace badawczo-rozwojowe zorientowane na technologię będą musiały objąć uwierzytelnianie użytkowników i wiadomości (np. poprzez analizę głosu i podpis elektroniczny), interfejsy techniczne i protokoły kodowania, mechanizmy kontroli dostępu oraz metody wdrażania bezpiecznych systemów z możliwością ich kontrolowania.

Weryfikacja i zatwierdzenie bezpieczeństwa systemu technicznego oraz możliwość jego zastosowania byłyby sprawdzane poprzez plany integracji i weryfikacji.

W uzupełnieniu do konsolidacji i opracowywania technologii zabezpieczeń wymagane będą pewne środki towarzyszące, związane ze stworzeniem, utrzymywaniem i spójnym stosowaniem norm, a także z zatwierdzaniem oraz certyfikacją produktów informatycznych i telekomunikacyjnych w odniesieniu do właściwości ich bezpieczeństwa, z zatwierdzaniem i certyfikacją metod projektowania oraz wdrażania systemów włącznie.

Do wspierania projektów współpracy, w fazie przedkonkurencyjnej i przednormatywnej, mógłby zostać wykorzystany trzeci wspólnotowy ramowy program badawczo-rozwojowy.

6. Kierunek działań VI — zapewnienie bezpieczeństwa systemów informatycznych

6.1. Zagadnienia

W zależności od właściwego charakteru cech zabezpieczenia systemów informatycznych wymagane funkcje będą musiały zostać uwzględnione w różnych częściach systemu informatycznego, począwszy od terminali i komputerów, usług, zarządzania siecią do urządzeń kodujących, kart procesorowych, kluczy publicznych i prywatnych. Można oczekiwać, że niektóre z nich będą wbudowane w urządzenia komputerowe lub oprogramowanie dostarczane przez producentów, inne natomiast mogą stanowić część systemów dystrybucyjnych (np. zarządzania siecią), pozostawać w posiadaniu indywidualnych użytkowników (np. karty procesorowe) lub być dostarczane przez specjalistyczne organizacje (np. klucze publiczne/prywatne).

Większość produktów zabezpieczających i usług będzie prawdopodobnie dostarczana przez producentów, usługodawców lub operatorów. W przypadku funkcji specjalnych, np. dostarczania klucza publicznego/prywatnego, upoważnień do przeprowadzania audytu, może zachodzić potrzeba wyznaczenia i upoważnienia odpowiednich organizacji.

To samo stosuje się do certyfikacji, oceny i weryfikacji jakości usług, które winny być świadczone przez organizacje niezależne od producentów, usługodawców czy operatorów. Mogą to być organizacje prywatne, rządowe lub upoważnione przez rząd do wykonywania swoich zadań.

6.2. Cele

W celu ułatwienia harmonijnego rozwoju zabezpieczania, w obrębie Wspólnoty, systemów informatycznych, dla ochrony interesów publicznych i gospodarczych, zachodzić będzie potrzeba opracowania spójnej metody zapewnienia tych środków bezpieczeństwa. W przypadku gdy konieczne będzie upoważnienie niezależnych organizacji, należy określić i uzgodnić ich funkcje oraz warunki, a gdzie to niezbędne, włączyć je do ram regulacyjnych. Cele te będą musiały zawierać jasno zdefiniowany i uzgodniony podział odpowiedzialności między różnymi podmiotami na poziomie Wspólnoty jako warunek wstępny do wzajemnego uznawania.

6.3. Stan obecny i kierunki rozwoju

Zapewnienie bezpieczeństwa systemów informatycznych jest obecnie dobrze zorganizowane wyłącznie w określonych obszarach i ogranicza się do określonych potrzeb. Organizacja na poziomie europejskim jest przeważnie nieformalna, a wzajemne uznawanie weryfikacji i certyfikacji poza zamkniętymi grupami nie zostało jeszcze ustanowione. Wraz ze wzrostem znaczenia bezpieczeństwa systemów informatycznych sprawą pilną staje się potrzeba określenia spójnego podejścia do sprawy wyposażania systemów informatycznych w zabezpieczenia w Europie i w skali międzynarodowej.

6.4. Wymagania, opcje i priorytety

Z uwagi na dużą liczbę różnych podmiotów zainteresowanych zagadnieniami bezpieczeństwa systemów informatycznych i ścisłym związkiem tych spraw z kwestiami natury prawnej i legislacyjnej jest rzeczą szczególnie ważną, aby dokonać wstępnych uzgodnień co do zasad, które będą rządzić wyposażaniem systemów informatycznych w zabezpieczenia.

Podczas opracowywania spójnych sposobów podejścia do tej kwestii pojawi się potrzeba zwrócenia uwagi na aspekty określenia i specyfikacji funkcji wymagających, z natury rzeczy, istnienia pewnych niezależnych organizacji (lub organizacji współdziałających). Mogłoby to objąć takie funkcje, jak administrowanie systemem kluczy publicznych/prywatnych.

Poza tym na etapie wstępnym wymaga się określenia i podania funkcji, jakie w interesie publicznym powinny być powierzone organizacjom niezależnym (lub organizacjom współdziałającym). Mogą one obejmować np. audyt, zapewnienie jakości, weryfikację, certyfikację i podobne funkcje.