POLITICA EUROPEANĂ ÎN DOMENIUL SECURITĂŢII INFORMATICE

Internetul interesează în mod esenţial atât marile cât şi micile companii. Practic, nu există firmă într-o ţară cu o dezvoltare cel puţin medie care să nu aibă create pagini Web, pe care se găsesc informaţii despre serviciile şi produsele oferite. De asemenea, consumatorii şi producătorii pot comunica instantaneu prin Net, ceea ce le conferă posibilitatea unei informări reciproce şi a unor comunicaţii foarte ieftine. Şi totuşi, aceştia nu s-au „aruncat" încă să facă afaceri sau administrare la scară mare prin Internet. De ce oare această reţinere? Motivele invocate cel mai adesea sunt legate de *securitatea tranzacţiilor on-line*. Preocupările pentru securitatea reţelelor şi a sistemelor informatice au crescut proporţional cu creşterea numărului de utilizatori ai reţelelor şi cu valoarea tranzacţiilor. Securitatea a atins un punct critic, reprezentând o cerinţă esenţială pentru afacerile electronice şi pentru funcţionarea întregii economii. Combinarea câtorva factori a făcut ca securitatea informaţiilor şi a comunicaţiilor să constituie unul dintre punctele principale pe agenda politicii Uniunii Europene:

- Guvernele şi-au dat seama de dependenţa economiilor lor şi a cetăţenilor faţă de buna funcţionare a reţelelor de comunicaţie şi au început să-şi revizuiască aranjamentele de securitate.
- Internetul a creat o legătură globală, conectând milioane de reţele, mari si mici, milioane de calculatoare personale şi alte dispozitive, precum telefoanele mobile. Acest lucru a redus în mod semnificativ costurile accesării informaţiilor economice vitale în cazul unor atacuri de la distanţă.
- Sunt raportaţi numeroşi viruşi, care cauzează pierderi mari prin distrugerea informaţiilor şi prin neacordarea dreptului de acces la reţele. Aceste probleme de securitate nu constituie chestiuni specifice unei ţări anume, ci un fenomen ce s-a răspândit rapid printre ţările membre ale UE.
- Consiliile Uniunii Europene (de la Lisabona şi Feira, de exemplu) au recunoscut Internetul ca un factor cheie al productivităţii economiilor uniunii, atunci când au lansat Planurile de Acţiune eEurope 2002 si eEurope 2005.

În concordanţă cu aceste lucruri, consiliul de la Stockholm a concluzionat *„Consiliul împreună cu Comisia vor dezvolta o strategie comprehensivă asupra securităţii reţelelor, inclusiv acţiuni de implementare în practică".*

În timp ce securitatea a devenit o problemă esenţială pentru cei ce alcătuiesc politici, găsirea unui răspuns adecvat a devenit o sarcină complexă. Cu numai câţiva ani în urmă, securitatea reţelelor era o problemă monopol de stat, care oferea servicii specializate bazate pe reţele publice, în particular pentru reţelele telefonice. Securitatea sistemelor informatice era specifică organizaţiilor mari şi era axată pe controlul accesului la resurse. Aceste lucruri s-au schimbat considerabil datorită unor dezvoltări în contextul unei pieţe lărgite, printre care amintim *liberalizarea, convergenţa şi globalizarea*:

- *Reţelele sunt acum în principal în proprietate privată şi sunt administrate de companii private.* Serviciile de comunicare sunt oferite pe bază de competitivitate, securitatea reprezentând o parte a ofertei pieţei. Totuşi, mulţi clienţi rămân ignoranţi în privinţa riscurilor securităţii atunci când se conectează la o reţea şi iau decizii bazându-se pe informaţii incomplete.
- *Reţelele şi sistemele informatice converg.* Ele devin interconectate, oferind aceleaşi tipuri de servicii şi, mai mult, împart aceeaşi infrastructură. Terminalele (calculatoarele, telefoanele mobile etc.) au devenit un element activ în arhitectura reţelelor şi pot fi conectate la diferite reţele.

- *Reţelele sunt internaţionale.* O parte importantă a comunicaţiilor din ziua de azi se realizează transfrontarier, tranzitând terţe ţări (câteodată chiar fără ca utilizatorul să realizeze acest lucru). Ca urmare, orice soluţie în faţa riscurilor de securitate trebuie să aibă în vedere acest lucru. Multe reţele sunt construite din produse comerciale, de la comercianţi internaţionali. Produsele de securitate trebuie să fie compatibile cu standardele internaţionale.

1. Necesitatea unei politici publice

Protejarea reţelelor de calculatoare este din ce în ce mai mult considerată drept o prioritate pentru politicieni, în special datorită nevoii de protejare a datelor, de asigurare a unei economii funcţionale, din motive de asigurare a securităţii naţionale şi de promovare a comerţului electronic. Aceasta a condus la un ansamblu substanţial de precauţii legale în cadrul Directivelor UE în ce priveşte protecţia datelor şi a Cadrului UE pentru telecomunicaţii. Aceste măsuri însă trebuie aplicate într-un mediu rapid schimbător de noi tehnologii, pieţe concurenţiale, convergenţă a reţelelor şi globalizare. Aceste provocări se corelează de asemenea şi cu tendinţa pieţei de a nu investi suficient în securitate, din motive ce vor fi analizate. Securitatea reţelelor şi a informaţiei reprezintă o marfă cumpărată şi vândută pe piaţă şi o parte a înţelegerilor contractuale între părţi. Piaţa produselor de securitate a crescut substanţial în ultimii ani. În conformitate cu unele studii, piaţa software-ului de securizare pentru Internet valora aproximativ 4,4 miliarde de dolari la sfârşitul anului 1999 şi va creşte cu un procent de 23% pe an pentru a atinge 8,3 miliarde în 2004. În Europa, piaţa pentru securitatea comunicaţiilor electronice se prognozează a creşte de la 465 de milioane de dolari în 2000 la 5,3 miliarde la sfârşitul lui 2006, paralel cu o creştere a pieţei pentru tehnologii de securitate a informaţiei de la 490 de milioane de dolari în 1999 la 2,74 miliarde în 2006. Presupunerea implicită care se face de obicei este că mecanismul preţului va balansa costul ofertei de securitate cu nevoile specifice de securitate. Unii utilizatori vor solicita un nivel înalt de securitate, în vreme ce alţii vor fi satisfăcuţi de un nivel de securitate mai scăzut – deşi statul ar putea să asigure un nivel minim de securitate. Această diferenţă se va reflecta în preţurile pe care vor fi dispuşi să le plătească pentru produsele de securitate. Cu toate acestea, multe riscuri rămân nerezolvate sau soluţiile se impun lent pe piaţă datorită anumitor imperfecţiuni ale acesteia:

Costurile şi beneficiile sociale: Investiţiile într-o mai bună securitate a reţelelor generează costuri şi beneficii sociale care nu se reflectă în mod adecvat în preţurile de pe piaţă. *De partea costurilor,* actorii pieţei nu sunt responsabili pentru vulnerabilităţile legate de comportamentul lor în domeniul securităţii. Utilizatorii şi furnizorii cu niveluri de securitate reduse nu sunt nevoiţi să plătească daune unor terţi. Este ca şi cum un şofer de taxi neatent n-ar fi tras la răspundere pentru costul blocajului de trafic ce rezultă în urma accidentului provocat de el. În mod similar, pe Internet un număr de atacuri au fost „montate" prin intermediul unor maşini slab protejate sau au trecut de nişte utilizatori relativ neglijenţi. *Beneficiile rezultate din securitate, de asemenea, nu sunt complet reflectate în preţurile de pe piaţă.* Când operatorii, furnizorii sau furnizorii de servicii îmbunătăţesc gradul de securitate al produselor lor, o mare parte din beneficiile acestei investiţii ajung nu numai la clienţii lor, dar şi la toţi cei afectaţi direct sau indirect de comunicarea electronică – în esenţă, toată economia.

Asimetria informaţiei: Reţelele devin din ce în ce mai complexe şi ating o piaţă mai largă, care include mulţi utilizatori cu prea puţină înţelegere a tehnologiei şi a potenţialelor ei pericole. Asta înseamnă că utilizatorii nu vor fi complet conştienţi de riscurile de securitate şi mulţi operatori, vânzători sau furnizori de servicii au dificultăţi, dată fiind existenţa şi gradul de întindere al vulnerabilităţilor. Multe noi servicii, aplicaţii şi software oferă posibilităţi atractive, dar adesea acestea sunt surse de noi vulnerabilităţi (de exemplu, marele succes al Internetului este în parte datorat multitudinii de aplicaţii multimedia care pot fi descărcate simplu, dar aceste plug-inuri reprezintă şi puncte de intrare pentru atacuri). În vreme ce beneficiile sunt vizibile, riscurile nu sunt şi este mai atractiv pentru furnizori să ofere facilităţi noi decât o mai bună securitate.

Problema acţiunii publice: Operatorii adoptă într-un ritm crescător standardele Internet sau îşi leagă într-un fel sau altul reţelele proprii la Internet. Cu toate acestea, Internetul nu a fost proiectat cu măsuri de securitate, ci din contră, a fost dezvoltat astfel încât să ofere

acces la informaţii şi să faciliteze schimbul de informaţii. Aceasta a reprezentat baza succesului său. Internetul a devenit o reţea globală de reţele de o neegalată bogăţie şi diversitate. Investiţiile în securitate adesea sunt eficiente doar dacă mulţi oameni procedează în acelaşi mod. De aceea, *cooperarea* pentru a crea soluţii de securitate este necesară. Dar cooperarea funcţionează numai dacă participă o masă critică de jucători, ceea ce e dificil de obţinut. Interoperabilitatea între produse şi servicii va permite concurenţa între soluţiile de securitate. Sunt însă costuri substanţiale de coordonare implicate pe măsură ce se vor generaliza soluţiile globale, iar unii jucători sunt tentaţi să impună o soluţie aflată în posesia lor pe piaţă. Cum o mulţime de produse şi servicii încă folosesc soluţii proprii, nu este nici un avantaj în a folosi standarde sigure, care nu oferă securitate suplimentară, decât dacă toţi ceilalţi le oferă.

Ca rezultat al acestor imperfecţiuni, cadrul european pentru protecţia telecomunicaţiilor şi a datelor impune deja obligaţii legale pentru operatori şi furnizorii de servicii, în scopul de a asigura un anume nivel de securitate în sisteme de comunicaţii şi informatice. Recomandarea pentru o politică europeana în domeniul reţelelor şi securităţii informaţiei poate fi descrisă după cum urmează.

- În primul rând, prevederile legale la nivelul UE trebuie aplicate efectiv, aceasta cerând *o înţelegere comună a problemelor de securitate şi a măsurilor specifice ce se impun*. Cadrul legal va trebui să evolueze în viitor, de exemplu, în legătură cu criminalitatea cibernetică, semnătura electronică etc.
- În al doilea rând, anumite imperfecţiuni ale pieţei au condus la concluzia că forţele de pe piaţă nu „pompează" suficiente investiţii în tehnologiile sau practicile de securitate. *Măsurile politice pot revigora piaţa şi, în acelaşi timp, pot îmbunătăţi funcţionalitatea cadrului legal***.**
- În sfârşit, serviciile din domeniul comunicaţiilor şi informaţiei sunt oferite fără a se ţine cont de graniţe. Aşadar, o politică europeană este necesară în scopul de *a asigura piaţa internă pentru asemenea servicii, de a beneficia de pe urma soluţiilor comune şi de a face posibilă o acţiune eficientă la nivel global.* Măsurile politice propuse cu privire la securitatea reţelelor şi a informaţiilor trebuie privite nu numai în contextul legislaţiei deja existente pentru telecomunicaţii şi protecţia datelor, ci şi în legătură cu politica mai recentă, legată de infracţiuni cibernetice. O politică în privinţa securităţii reţelelor şi informaţiei va constitui veriga lipsă în acest cadru politic.

2. Conştientizarea pericolelor

Mulţi utilizatori (privaţi/publici) încă nu sunt conştienţi de posibilele ameninţări pe care le întâlnesc folosind reţelele de comunicaţii sau de soluţiile care deja există pentru a le face faţă. Problemele de securitate sunt complexe, iar riscurile sunt adesea dificil, chiar şi pentru experţi, de întrevăzut. Lipsa de informare este una dintre imperfecţiunile pieţei, pe care politicile de securitate ar trebui să o aibă în vedere. Există riscul ca unii utilizatori, alarmaţi de multele rapoarte şi ameninţări la adresa securităţii, să evite pur şi simplu folosirea comerţului electronic. Alţii, care fie sunt neinformaţi, fie subestimează riscul, pot fi prea neglijenţi. Unele companii pot avea interesul de a prezenta ca minim riscul pentru a nu pierde clienţi. Paradoxal, există o cantitate impresionantă de informaţie în domeniul securităţii reţelelor şi al informaţiei disponibilă pe Internet, iar revistele despre calculatoare acoperă subiectul destul de bine. Problema utilizatorilor este aceea de a găsi informaţiile potrivite, pe care le pot înţelege, care sunt la zi şi răspund propriilor lor nevoi. În sfârşit, furnizorii de servicii ai unui serviciu public de telecomunicaţii disponibil sunt obligaţi prin legile UE să-i informeze pe abonaţii lor cu privire la riscurile cauzate de o breşă a securităţii reţelei şi despre posibilele remedii, inclusiv costul implicat (cf. art. 4 al Directivei 97/66 al CE). Scopul iniţiativei pentru creşterea conştientizării cetăţenilor, administraţiilor şi mediului de afaceri este deci acela de a furniza informaţii accesibile, independente şi pe care te poţi baza despre securitatea reţelelor şi a informaţiei. O discuţie deschisă despre securitate este necesară. Odată ce conştientizarea a fost asigurată, oamenii devin liberi să facă alegeri proprii asupra nivelului de protecţie pe care şi-l doresc şi permit.

Acţiuni propuse:

- Statele membre ar trebui să lanseze o campanie publică de educare şi informare, iar măsurile care se iau trebuie permanent actualizate. Aceasta ar trebui să includă o campanie mass-media şi acţiuni ce vizează un public larg. O campanie de informare bine plănuită şi eficientă nu este ieftină. Un conţinut al acesteia care să descrie riscurile fără a alarma oamenii şi fără a încuraja potenţialii hackeri, necesită o planificare atentă. Comisia Europeană va facilita un schimb de experienţă în ceea ce priveşte cele mai bune practici şi va asigura un nivel de coordonare a diferitelor campanii naţionale de informare la nivel UE, în particular în ceea ce priveşte corpul de informaţie care trebuie difuzat. Un element al acestei campanii ar fi un portal pentru pagini web, atât la nivel naţional cât şi European. Legarea acestor portaluri cu site-uri web de încredere ale partenerilor internaţionali ar trebui, de asemenea, luată în considerare.
- Statele membre ar trebui să promoveze utilizarea celor mai bune practici în securitate, bazate pe măsuri deja existente, cum ar fi ISO/IEC 17799 (cod de practici pentru managementul securităţii informaţiei www.iso.ch). Companiile de mărimi mici şi medii ar trebui avute în vedere în primul rând. Comisia va susţine statele membre în eforturile lor.
- Sistemele de educaţie din statele membre ar trebui să dea mai multă atenţie cursurilor dedicate securităţii informatice. Dezvoltarea de programe educaţionale la toate nivelurile, de exemplu, cursuri despre riscurile de securitate ale reţelelor deschise şi soluţii eficiente ar trebui încurajate să devină parte a educaţiei despre calculatoare şi informatică din şcoli. Comisia Europeana sprijină dezvoltarea de noi module pentru programa şcolară în cadrul programului său de cercetare.

3. Un sistem european de avertizare şi informare în domeniul securităţii informatice

Chiar şi în cazul în care utilizatorii sunt conştienţi de riscurile de securitate, ei tot trebuie anunţaţi cu privire la noi ameninţări. Atacatorii răuvoitori, în mod aproape inevitabil, vor găsi noi vulnerabilităţi care să ocolească protecţia cea mai sigură. Se dezvoltă în permanenţă aplicaţii şi servicii software noi, oferind o mai buna calitate a serviciilor, făcând Internetul mai atractiv; dar în cursul procesului, neintenţionat, se deschide calea unor noi vulnerabilităţi şi riscuri. Chiar şi inginerii de reţea experimentaţi şi experţi în securitate sunt adesea surprinşi de noutatea adusă de unele atacuri. Aşadar este nevoie de un sistem de alarmare rapid, care să poată alerta toţi utilizatorii, alături de o sursă de informaţii şi sfaturi rapide şi demne de încredere asupra modului în care se poate acţiona împotriva atacurilor. Mediul de afaceri, de asemenea, are nevoie de un mecanism confidenţial de raportare a atacurilor, fără a risca pierderea încrederii publicului. Acesta trebuie să fie complementat de o mai extinsă şi anticipativă analiză de securitate, strângând dovezi şi comparând riscurile cu beneficiile unor soluţii şi costurile aferente. Multă muncă în acest domeniu este făcută de *Computer Emergency Response Teams (CERTs)* sau de entităţi similare. De exemplu, Belgia a organizat un sistem de alertă la viruşi care permite cetăţenilor belgieni informarea în legătură cu alertele cauzate de viruşi în două ore. Totuşi CERT-urile operează în mod diferit în fiecare stat membru, făcând cooperarea complexă, dacă nu chiar dificilă. CERT-urile deja existente nu sunt întotdeauna bine echipate, iar sarcinile lor adesea nu sunt clar definite. Cooperarea la nivel mondial se realizează prin CERT/CC, care este în parte finanţat de guvernul SUA, iar CERT-urile din Europa depind de politica de publicare a informaţiilor de către CERT/CC. Ca rezultat al acestei complexităţi, coordonarea europeană a fost până în prezent limitată. Cooperarea este esenţială în asigurarea avertizării din timp pe cuprinsul UE prin schimbul instantaneu de informaţii la primul semn de atac într-o singură ţară. Aşadar, cooperarea cu sistemul CERT din interiorul UE ar trebui întărită în regim de urgenţă. O primă acţiune vizând întărirea cooperării public/private prin dependenţa de infrastructura de informare (inclusiv dezvoltarea sistemelor de avertizare de urgenţă) şi îmbunătăţirea colaborării între CERT-uri a fost stabilită în cadrul planului de acţiune eEurope.

Acţiuni propuse:

- Statele membre ar trebui să-şi reorganizeze propriile sisteme CERT, având în vedere îmbunătăţirea echipamentului şi a competenţei CERT-urilor existente. În sprijinul

eforturilor naţionale, Comisia Europeana va dezvolta o propunere concretă de întărire a cooperării în cadrul UE. Aceasta va include proiecte de propuneri în cadrul programului TEN Telecom pentru asigurarea navigării eficiente pe reţea şi stabilirea de măsuri companion în cadrul programului IST pentru facilitarea schimbului de informaţii.

- Odată cu stabilirea reţelei CERT la nivel UE, aceasta ar trebui conectată cu instituţii similare din toata lumea, de exemplu, sistemul de raportare a incidentelor propus de G8.
- Comisia propune colaborarea cu statele membre pentru a se organiza cât mai bine colectarea de date la nivel european, analiza şi proiectarea răspunsurilor anticipative la riscuri existente şi posibile.

4. Dezvoltarea suportului tehnologic

Investiţiile în securitatea reţelelor şi a informaţiei sunt actualmente sub optim. Acesta este cazul atât în ceea ce priveşte suportul tehnologic, cât şi cercetarea pentru descoperirea de noi soluţii. În contextul în care noile tehnologii în mod inevitabil aduc cu ele şi riscuri noi, cercetarea continuă este vitală. Securitatea în domeniul reţelelor şi al informaţiei este deja inclusă în Information Technologies (IST) Programme of the EU's 6th Framework Research Programme, reprezentând o investiţie de 3,6 miliarde de euro de-a lungul a patru ani. Cercetarea la nivel tehnic în criptografie este într-un stadiu avansat la nivel european. Algoritmul Belgian numit Rijndael a câştigat concursul Advanced Encryption Standard, organizat de institutul de standardizare al SUA (NIST). Proiectul NESSIE (Noi metode europene pentru Semnătură, Integritate şi Criptare) al IST a lansat o competiţie la nivel extins în domeniul algoritmilor de criptare îndeplinind cerinţele noilor aplicaţii multimedia, comerţului mobil şi smartcard-urilor.

Acţiuni propuse:

- Comisia propune includerea securităţii în al şaselea program cadru. Pentru ca această adăugire să fie optimă, ar trebui legată de o mai largă strategie pentru îmbunătăţirea securităţii reţelelor şi a informaţiei. Cercetarea din cadrul acestui program ar trebui să aibă în vedere provocările cheie de securitate şi va focaliza pe mecanisme de securitate de bază şi pe interoperabilitatea acestora, procese de securitate dinamice, criptografie avansată, tehnologii de îmbunătăţire a facilităţilor de confidenţialitate, tehnologii de operare cu obiecte digitale, tehnologii de încredere pentru suportul afacerilor şi funcţii organizaţionale în sistemele dinamice şi de telefonie mobilă.
- Statele membre ar trebui să promoveze activ folosirea produselor criptografice puternice şi plug-able. Soluţii de securitate bazate pe criptarea plug-in trebuie să fie disponibile ca o alternativă la acelea „fixate" în sistemele de operare.

5. Standardizarea şi certificarea

Pentru ca îmbunătăţirea soluţiilor de securitate să aibă succes, ele trebuie implementate în comun de actori importanţi ai pieţei şi de preferinţă bazate pe standarde internaţionale deschise. Una dintre principalele piedici în adoptarea multor soluţii de securitate, de exemplu semnătura electronică, a fost lipsa interoperabilităţii între diferite implementări. Dacă doi utilizatori doresc să comunice în mod sigur între diferite platforme, trebuie asigurată interoperabilitatea. Folosirea protocoalelor şi interfeţelor standardizate ar trebui încurajată, inclusiv testarea de conformitate. Standarde deschise, de preferat bazate pe software cu sursa liberă, ar putea contribui la înlăturarea mai rapidă a erorilor ca şi la o mai mare transparenţă. De asemenea, evaluarea securităţii contribuie la creşterea încrederii utilizatorilor. Folosirea de criterii comune de evaluare în multe ţări facilitează recunoaşterea mutuală; aceste ţări au intrat de asemenea într-un aranjament cu Canada şi SUA pentru recunoaştere mutuală a certificatelor de securitate IT (Recomandarea Consiliului 95/144/EC referitoare la criteriile de evaluare a securităţii tehnologiei informaţiei, implementată în majoritatea statelor membre). Certificarea proceselor care se desfăşoară în afaceri şi managementul sistemelor de securitate a informaţiei este susţinută de cooperarea

europeană pentru acreditare (EA). Acreditarea organismelor naţionale de certificare măreşte încrederea în competenţa şi imparţialitatea acestora, promovând astfel acceptarea certificatelor în toată UE. În plus faţă de certificare, ar trebui de asemenea efectuate teste de interoperabilitate. Un exemplu al acestei abordări este Iniţiativa Europeană de Standardizare a Semnăturii Electronice (EESSI), care dezvoltă soluţii de consens în sprijinul directivei UE asupra semnăturii electronice. Alte exemple sunt iniţiativele privind smart-card-urile în eEurope şi iniţiativele de implementare a Infrastructurii de Chei Publice (PKI) lansate în interiorul programului Schimb de Date între Administraţii (IDA). Nu lipsesc eforturile de standardizare, dar un mare număr de standarde aflate în competiţie duce la fragmentarea pieţei şi la prezenţa de soluţii non-interoperabile. Aşadar, activităţile de standardizare şi certificare curente au nevoie de o mai bună coordonare şi de asemenea au nevoie să ţină pasul cu introducerea de noi soluţii de securitate. Armonizarea specificaţiilor va conduce la o interoperabilitate crescută, făcând posibilă în acelaşi timp implementarea de către actorii pieţei.

Acţiuni propuse:

- Organizaţiile de standardizare europene sunt invitate să accelereze lucrul la produse şi servicii interoperabile de securitate. Unde va fi necesar, ar trebui urmate forme noi de „deliverabile" şi proceduri pentru a accelera lucrul şi a întări cooperarea cu reprezentanţii consumatorilor şi angajamentul actorilor pieţei. „Pluggable" înseamnă că un produs software de criptare poate fi cu uşurinţă instalat şi făcut complet operaţional în cadrul sistemelor de operare.
- Comisia va continua să sprijine, mai ales prin programele IST şi IDA folosirea semnăturii electronice, implementarea de solutii PKI interoperabile şi prietenoase pentru utilizator şi dezvoltarea pe mai departe a IPv6 şi IPSec (ca în Planul de Acţiune eEurope).
- Statele membre sunt invitate să promoveze folosirea procedurilor de certificare şi acreditare pe baza standardelor europene şi internaţionale general acceptate, favorizând recunoaşterea mutuală de certificate. Comisia va evalua nevoia unei iniţiative legale asupra recunoaşterii mutuale de certificate.
- Actorii de pe piaţa europeană sunt încurajaţi să participe mai activ în activităţi de standardizare europene (CEN, Cenelec, ETSI) şi internaţionale (Internet Engineering Task Force (IETF) , World Wide Web Consortium (W3C)).
- Statele membre ar trebui să-şi revadă toate standardele de securitate relevante. Ar putea fi organizate competiţii împreună cu Comisia pentru metode europene de criptare şi soluţii de securitate, cu scopul de a stimula standarde acceptate pe plan internaţional.

6. Cadrul juridic

Există mai multe texte legale care influenţează securitatea reţelelor de comunicaţii şi a sistemelor informatice. Datorită convergenţei reţelelor, problemele de securitate aduc laolaltă reguli şi tradiţii legale din sectoare variate. Acestea includ *telecomunicaţiile* (încorporând toate reţelele de comunicaţie), *industria calculatoarelor, Internetul* care a funcţionat mai ales în baza unei abordări „hands off" (de neintervenţie) şi comerţul electronic care este din ce în ce mai mult subiectul unei legislaţii specifice. În legătură cu securitatea, prevederile privind daunele terţilor, infracţionalitatea cibernetică, semnătura electronică, regulile privind protejarea şi exportul datelor sunt relevante.

Protejarea intimităţii este un obiectiv politic cheie în Uniunea Europeană. A fost recunoscut ca drept de bază prin articolul 8 al Convenţiei Europene asupra drepturilor omului. Articolele 7 şi 8 ale Cartei Drepturilor Fundamentale ale UE de asemenea stipulează dreptul la respect pentru viaţa de familie şi privată, cămin, comunicaţie şi date personale. Articolul 5 al Directivei de Protejare a Datelor în Telecomunicaţii obligă statele membre să asigure confidenţialitatea în reţelele publice de telecomunicaţii. În plus, la articolul 4 al aceleiaşi Directive se cere furnizorilor de servicii publice şi reţele să ia măsuri tehnice şi organizatorice pentru a asigura securitatea serviciilor oferite. Aceste prevederi au implicaţii asupra necesităţilor de securitate ale reţelelor şi sistemelor informatice folosite de acele

persoane sau organizaţii, de exemplu furnizorii de comerţ electronic. Natura pan-Europeană a acestor servicii şi mai marea competiţie transfrontalieră duc la o creştere tot mai mare de specificaţii asupra mijloacelor de folosit pentru a fi în acord cu aceste prevederi.

Programul cadru pentru servicii în telecomunicaţii al UE conţine mai multe prevederi cu privire la securitatea operaţiilor pe reţea (însemnând disponibilitatea reţelelor în caz de urgenţă) şi integritatea reţelelor (însemnând asigurarea operaţiilor normale în reţelele interconectate). Comisia a propus un nou cadru de reguli pentru serviciile de comunicaţii electronice în iulie 2000. Propunerile Comisiei reafirmau în esenţă – deşi cu modificări – prevederile existente în ce priveşte securitatea şi integritatea reţelelor.

Infracţiunile informatice au declanşat o largă discuţie în UE despre cum să se reacţioneze la activităţile infracţionale care folosesc computerele şi reţelele de calculatoare. Legile penale ale statelor membre trebuie să prevadă şi accesul neautorizat în reţelele de calculatoare, inclusiv securitatea datelor personale. Sunt probleme în investigarea acestor ilegalităţi şi se constată o insuficientă inhibare a hackerilor. Legi penale împotriva intruziunii în reţelele de calculatoare sunt, de asemenea, importante pentru a uşura cooperarea judiciară între statele membre. Îngrijorările legitime faţă de infracţionalitatea electronică necesită investigaţii legale eficiente.

Acţiuni propuse:

- înţelegerea comună a implicaţiilor legislative ale securităţii în comunicarea electronică este necesară. Pentru acest scop, Comisia va crea un inventar de măsuri naţionale care au fost deja luate şi sunt în concordanţă cu legi comunitare relevante.
- Statele membre şi Comisia ar trebui să sprijine în continuare libera circulaţie a produselor şi serviciilor criptografice, prin o mai mare armonizare al procedurilor administrative de export şi o mai mare relaxare a controalelor la exporturi.
- Comisia va propune o măsură legislativă în cadrul Titlului VI al tratatului UE pentru echivalarea legilor penale legate de atacuri împotriva sistemelor de calculatoare, incluzând hacking-ul şi atacurile de refuz al serviciilor.

7. Securitatea în aplicațiile guvernamentale

Planul de acţiune eEurope îşi propune să încurajeze o mai eficientă interacţiune între cetăţeni şi administraţia publică. Cum mare parte din informaţia schimbată între cetăţeni şi administraţie are un caracter confidenţial (medical, financiar, legal etc.), securitatea este vitală pentru asigurarea implementării cu succes a planului. Mai mult, dezvoltarea guvernării electronice face ca administraţia publică să devină atât *exemplu de demonstrare a eficienţei soluţiilor de securitate* cât şi actor al pieţei cu *posibilitatea de a influenţa dezvoltarea în domeniu prin deciziile de achiziţie pe care le face***.** Problema pentru administraţia publică nu este numai aceea de a achiziţiona sisteme informatice şi de comunicaţii cu cerinţe de securitate, ci şi dezvoltarea unei culturi de securitate a organizaţiei. Acest obiectiv poate fi dus la îndeplinire prin stabilirea de *politici organizaţionale de securitate* adaptate la nevoile instituţiei.

Acţiuni propuse:

- Statele membre ar trebui să încorporeze soluţii de securitate informatică eficiente şi interoperabile, ca o cerinţă de bază în activităţile lor de e-guvernare şi e-procurement.
- Statele membre ar trebui să introducă semnătura electronică la oferirea serviciilor publice on-line.
- În cadrul e-Comisiei, Comisia va lua o serie de măsuri pentru a întări cererea de securitate în sistemele sale informatice şi de comunicaţie.

8. Cooperarea internațională

Aşa cum comunicaţiile prin reţele trec cu uşurinţă graniţele în fracţiuni de secundă, la fel se întâmplă şi cu problemele de securitate informatică asociate. Reţeaua este atât de sigură ca şi cea mai slabă verigă a ei, iar Europa nu se poate izola de restul reţelei globale. În

consecinţă, problemele de securitate precizate mai sus cer cooperare internaţională. Comisia Europeană deja contribuie la munca forurilor internaţionale, cum ar fi G8, OECD, Naţiunile Unite. Sectorul privat tratează problemele de securitate în organizaţii cum ar fi Global Business Dialogue (www.GBDe.org) sau Global Internet Project (www.GIP.org). Un dialog continuu între aceste organizaţii va fi esenţial pentru securitatea globală. Comisia va întări dialogul cu organizaţiile internaţionale şi cu partenerii săi în ceea ce priveşte securitatea reţelelor şi, în particular, în ceea ce priveşte interdependenţa crescândă a reţelelor de calculatoare.

9. Securitatea informatică în planul eEurope 2005

Deoarece Societatea Informatizată devine tot mai importantă atât pentru business cât şi pentru societate, asigurarea securităţii, atât pentru infrastructura însăşi, cât şi pentru informaţiile care circulă pe ea, reprezintă un punct critic. Pentru ca Internetul să fie un mediu de încredere al Societăţii Informatizate, trebuie să devină disponibil, informaţia transmisă sau memorată să fie păstrată confidenţial, trebuie să ne putem asigura cine este autorul unei informaţii şi că aceasta nu a fost alterată. Problemele de securitate reduc încrederea noastră în reţele şi în sistemele informatice şi, odată cu aceasta, reduc nivelul de utilizare a Internetului, cu toate avantajele sale.

Ca urmare, securitatea este elementul cheie al proiecţiilor Comisiei UE privind Noua Generaţie de Internet şi reprezintă una dintre cele 6 priorităţi politice ale Planului eEurope 2005.

Asigurarea securităţii informatice nu este numai o provocare pur tehnologică, ci este, în acelaşi timp, o chestiune dependentă de comportamentul uman şi de cunoştinţele cu privire la ameninţări şi remedii. UE a dezvoltat deja reguli pentru comunicaţii electronice sigure, aşa cum sunt de fapt Directiva asupra semnăturii electronice sau legislaţia cu privire la protecţia datelor pentru comunicaţii electronice.

Alte provocări stau de asemenea între obiectivele Planului eEurope 2005:

- *Securitatea reţelelor şi a informaţiilor* împotriva unor atacuri accidentale sau cu caracter criminal;
- *Criminalitatea cibernetică*, pentru armonizarea legislaţiei ţărilor membre;
- *Comunicaţii sigure pentru e-guvernare*, pentru dezvoltarea unei reţele trans-europene sigure, prin care să se poată vehicula informaţii secrete sau confidenţiale (Proiectul IDA- Interchange of Data between Administrations).

Implementarea acestor obiective presupune o serie de activităţi concrete, dintre care amintim:

- Crearea la începutul lui 2004 a *European Network and Information Security Agency (ENISA*) – o agenţie europeană care va acţiona ca un centru privind securitatea informatică al ţărilor membre şi al instituţiilor UE, contribuind la creşterea cooperării şi a schimbului de informaţii în domeniu, precum şi la stabilirea cadrului juridic şi de reglementare. Va contribui la dezvoltarea unui sistem european de alertă şi informare reciprocă în caz de incidente informatice;
- *Planul de Acţiune pentru un Internet mai Sigur*, destinat contracarării unor acţiuni ilegale în domeniul P2P, sisteme mobile, chat-uri, jocuri on-line etc.;
- *Sprijinirea unor cercetări privind securitatea informatică,* prin Programul Cadru nr. 6, în domenii ca e-autentificarea (smart-carduri, biometrice), metode criptografice noi, metode de semnatură electronică, criptare plug-in etc.;
- *Dezvoltarea unor noi standarde*, prin *Network and Information Security (NIS) Focus Group,* care să le completeze pe cele actuale şi să umple eventualele goluri existente.
- *Dezvoltarea unei culturi a securităţii,* în proiectarea, implementarea şi utilizarea sistemelor informatice şi de comunicaţii. Sectorul privat trebuie să dezvolte practici adecvate şi standarde în acest scop.