EUROPAPARLAMENTET

1999 *2004*

Plenarhandling

SLUTLIG VERSION
A5-0311/2002

17 september 2002

BETÄNKANDE

om meddelandet från kommissionen till Europaparlamentet, rådet, Ekonomiska och sociala kommittén och Regionkommittén ”Nät- och informationssäkerhet: förslag till en europeisk strategi”
(KOM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

Föredragande: Elena Ornella Paciotti

INNEHÅLL

Sida

PROTOKOLLSIDA

Med en skrivelse av den 7 juni 2001 förelade kommissionen parlamentet kommissionens meddelande till Europaparlamentet, rådet, Ekonomiska och sociala kommittén och Regionkommittén ”Nät- och informationssäkerhet: förslag till en europeisk strategi” (KOM(2001) 298 – 2001/2280(COS)).

Vid plenarsammanträdet den 13 december 2001 tillkännagav talmannen att detta meddelande hänvisats till utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor, som utsetts till ansvarigt utskott, och till utskottet för rättsliga frågor och den inre marknaden, utskottet för industrifrågor, utrikeshandel, forskning och energi och utskottet för kultur, ungdomsfrågor, utbildning, medier och idrott, som utsetts till rådgivande utskott (C5-0657/2001).

Vid utskottssammanträdet den 10 oktober 2001 hade utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor utsett Elena Ornella Paciotti till föredragande.

Vid utskottssammanträdena den 23 maj, 17 juni, 8 juli och 12 september 2002 behandlade utskottet kommissionens meddelande och förslaget till betänkande.

Vid det sistnämnda sammanträdet godkände utskottet förslaget till resolution med 27 röster för, 1 röst mot och 2 nedlagda röster.

Följande var närvarande vid omröstningen: Jorge Salvador Hernández Mollar (ordförande), Robert J.E. Evans och Giacomo Santini (vice ordförande), Elena Ornella Paciotti (föredragande), Niall Andrews, Roberta Angelilli, Alima Boumediene-Thiery, Marco Cappato (suppleant för Mario Borghezio), Michael Cashman, Charlotte Cederschiöld, Ozan Ceyhun, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Adeline Hazan, Anna Karamanou (suppleant för Martin Schulz), Timothy Kirkhope, Eva Klamt, Alain Krivine (suppleant för Ole Krarup), Bill Newton Dunn, José Ribeiro e Castro, Martine Roure, Miet Smet (suppleant för Hubert Pirker), Patsy Sörensen, The Earl of Stockton (suppleant för The Lord Bethell), Joke Swiebel, Fodé Sylla, Anna Terrón i Cusí, Maurizio Turco, Christian Ulrik von Boetticher och Olga Zrihen Zaari (suppleant för Walter Veltroni).

Yttrandet från utskottet för industrifrågor, utrikeshandel, forskning och energi bifogas detta betänkande. Utskottet för rättsliga frågor och den inre marknaden beslutade den 27 november 2001 att inte avge något yttrande och utskottet för kultur, ungdomsfrågor, utbildning, medier och idrott beslutade den 21 november 2001 att inte avge något yttrande.

Betänkandet ingavs den 17 september 2002.

FÖRSLAG TILL RESOLUTION

Europaparlamentets resolution om meddelandet från kommissionen till Europaparlamentet, rådet, Ekonomiska och sociala kommittén och Regionkommittén ”Nät- och informationssäkerhet: förslag till en europeisk strategi” (COM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Europaparlamentet utfärdar denna resolution

– med beaktande av kommissionens meddelande (KOM(2001) 298 – C5-0657/2001[1]),

– med beaktande av rekommendationen den 6 september 2001 om strategin för att upprätta ett säkrare informationssamhälle genom ökad säkerhet i informationsinfrastrukturen och bekämpning av datorrelaterad brottslighet av den 6 september 2001, samt av Europarådets konvention om datorrelaterad brottslighet som undertecknades i Budapest den 26 november 2001[2],

– med beaktande av förslaget till rådets rambeslut om angrepp mot informationssystemen av den 19 april 2002, vilket genomför motsvarande delar av Europarådets ovannämnda konvention (KOM(2002) 173),

– med beaktande av slutsatserna från Europeiska rådets möten i Stockholm i mars 2001 och i Sevilla den 21-22 juni 2002 samt av meddelandet från kommissionen ”eEurope: Ett informationssamhälle för alla”, i vilka det trängande behovet av att garantera nätverkssäkerhet upprepas,

– med beaktande av övriga relevanta resolutioner på området, bland annat Europaparlamentets resolution av den 5 september 2001 om förekomsten av ett globalt övervakningssystem för kommunikation från privatpersoner och företag (övervakningssystemet Echelon), och de senaste initiativen på internationell nivå (G8, OECD, FN)[3],

– med beaktande av artikel 47.1 i arbetsordningen,

– med beaktande av betänkandet från utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor och yttrandet från utskottet för industrifrågor, utrikeshandel, forskning och energi (A5-0311/2002).

Betydelsen av säkra nätverk inom ramen för informationssamhället

A. Elektroniska kommunikationsnät konvergerar i rask takt, och dessa nät får allt större betydelse för ekonomin och samhället.

[1] EGT C 43, 16.2.2002, s. 2.
[2] Antagna texter (P5_TAPROV(2001) 284).
[3] Antagna texter (P5_TAPROV(2001) 264).

B. Till följd av denna konvergens behöver det skapas lämpliga politiska och rättsliga ramar i Europeiska unionen, vilka garanterar nät- och informationssäkerheten som utgör en avgörande förutsättning för informationssamhället.

C. En adekvat nätverkssäkerhet utgör en nyckelfaktor för att nätverkstjänsterna och den elektroniska handeln skall kunna utvecklas och för att den inre marknaden skall fungera väl.

D. För att de säkerhetshöjande åtgärderna skall bli effektiva måste alla berörda parter (offentliga myndigheter, konsumenter, forskare vid universiteten, företag), däribland medborgarna, bli medvetna om säkerhetsriskerna och det egna ansvaret i fråga om de säkerhetsåtgärder som bör vidtas.

E. För att de säkerhetshöjande åtgärderna skall bli effektiva måste de få en utbredd tillämpning bland samtliga berörda marknadsaktörer och grundas på öppna internationella standarder.

F. Grupper för stöd vid datorhaveri (Computer Emergency Response Teams, CERT) fungerar olika i de olika medlemsstaterna, vilket försvårar samarbetet.

1. Europaparlamentet påpekar att säkerheten i dag är otillfredsställande, eftersom 60 procent av de europeiska företagen redan har stött på allvarliga problem under de senaste två åren, endast 14 procent av dem har en policy för nätverkssäkerhet och för 62 procent av de små och medelstora företagen samt för 81 procent av de stora företagen utgör bristen på säkerhet det främsta hindret för användningen av Internet[1].

2. Europaparlamentet påpekar även att användarna ofta inte förefaller kunna försvara sig mot hot mot nätverkssäkerheten, vilka omfattar uppsåtliga anfall och oförutsedda händelser som

   - avlyssning av trådbunden och trådlös kommunikation genom de elektroniska övervakningssystemen SOTA, *routrar, nätportar och nätservrar*, icke auktoriserad tillgång genom dechiffrering av *lösenord* eller vilseledande framställning av data,
   - nätstörningar till följd av attacker mot *servrar*, *routing*-attacker, ”översvämning” eller blockeringsattacker, attacker mot dataintegritet, genom körning av program gjorda i ont uppsåt, exempelvis virus, som ändrar eller förstör data,
   - miljöolyckor och olyckshändelser (som naturkatastrofer),
   - brottsliga attacker som i vissa fall även kan hänföras till terroristverksamhet.

3. Europaparlamentet noterar att viktig infrastruktur som rör transporter, kommunikationer, energi- och vattenförsörjning samt finans- och banktjänster kan bli föremål för attacker mot nätverk, och följaktligen utgör nätverkens sårbarhet en allvarlig risk som äventyrar möjligheterna för unionens ekonomi att fungera korrekt och en risk för medborgarnas vardagsliv.

[1] ESTO ”Future Bottlenecks in the information society”, rapport till Europaparlamentet, ITRE-utskottet, s. 143, samt Eurostat.

4. Europaparlamentet anser, i ljuset av dessa svagheter, att det är otillräckligt att bemöta problemet med endast frivilliga åtgärder från de berörda aktörernas sida, eftersom dessa handlar på mycket olika sätt, eftersom det saknas gemensamma standarder och eftersom tekniken utvecklas snabbt. Parlamentet betonar samtidigt lämpligheten i att producenterna utvecklar säkra produkter och deltar i utvecklingen på området för produktsäkerhet.

5. Europaparlamentet betonar att man så snart som möjligt måste se till att alla medborgare, företag och myndigheter får tillgång till samtliga EU-organs offentliga elektroniska tjänster genom ett säkert, individanpassat och verifierat system för tillträde. Sådant tillträde måste garanteras genom användning av digitala signaturer och fastställande av europeiska normer som genast skall gälla för EU-institutionerna.

6. Europaparlamentet betonar vikten av att de berörda sektorerna deltar i utarbetandet av strategier avseende nätens säkerhet och integritet samt informationssäkerheten i IP-miljöer.

7. Europaparlamentet noterar ökningen av antalet offentliga och privata initiativ på internationell nivå för att garantera nätverkens tillförlitlighet, exempelvis White House Office of Cyberspace Security i Förenta staterna, nätverket för utbyte om information om säkerhet som upprättats inom ramen för G8 samt Europols och Interpols nätverk.

8. Europaparlamentet håller med Europeiska rådet, rådet och kommissionen om nödvändigheten av ett gemensamt europeiskt tillvägagångssätt för att garantera att den inre marknaden för kommunikationstjänster skall kunna dra nytta av gemensamma lösningar och agera effektivt i internationella sammanhang.

9. Europaparlamentet erinrar om att de ansvariga för tillhandahållandet av nätverkstjänster redan är skyldiga att vidta åtgärder för att garantera ett lämpligt skydd för personuppgifter på grundval av artikel 17 i det allmänna direktivet om dataskydd (95/46/EG), vilket bekräftats i senare bestämmelser om nätens säkerhet och integritet[1].

10. Europaparlamentet betonar att gemensamma definitioner för nätsäkerhet, upprätthållande av nätens integritet och informationssäkerhet måste utvecklas så snabbt som möjligt.

11. Europaparlamentet uppmanar kommissionen att utarbeta en handlingsplan för att främja användningen av digitala signaturer, exempelvis genom att anta gemenskapsbestämmelser som genast skall gälla för EU-institutionerna.

Institutionella aspekter

12. Europaparlamentet uppmanar kommissionen att ge parlamentet och rådet information om problem som uppkommit i samband med tillämpningen av befintliga direktiv i fråga om uppgiftsskydd, i synnerhet i fråga om artiklar som avser nätverkssäkerhet.

[1] Direktiv 97/66/EG om behandling av personuppgifter och skydd för privatliv inom telekommunikationsområdet, direktiv 97/33/EG om samtrafik, direktiv 98/10/EG om taltelefoni, direktiv 99/93/EG om elektroniska signaturer samt direktiv 2000/31/EG om elektronisk handel.

13. Europaparlamentet anser att det inte går att uppskjuta utarbetandet av en europeisk strategi som, samtidigt som den är neutral i förhållande till den teknik som används, skall

    a) definiera eller uppdatera standarder i fråga om säkerhet för telekommunikationsnätverk och garantera kompatibilitet,

    b) gynna utvecklingen av krypterings- och certifieringssystem på gemenskapsnivå och förstärka bestämmelser om uppgiftsskydd,

    c) garantera förebyggande och effektiv bekämpning av brottslighet inom lagens råmärken,

    d) göra medborgarna, offentliga och privata användare och operatörer medvetna genom informationskampanjer på nationell nivå och gemenskapsnivå för att på så sätt gynna spridningen av bästa säkerhetspraxis,

    e) förstärka den vetenskapliga forskningen inom de sektorer som företer störst brister, exempelvis i fråga om bedömning av informationsteknikens säkerhet, deras integration i system, skydd för slutanvändaren och teknik för förbättring av skyddet för privatlivet.

14. Europaparlamentet är ense med kommissionen om att det är nödvändigt att så snart som möjligt upprätta en arbetsgrupp om nätverkssäkerhet, vilken skall ha följande mål:

    - Att identifiera de nationella myndigheter som ansvarar för förvaltningen av nätverken.
    - Att identifiera de nationella myndigheter som ansvarar för samordningen och att fastställa beslutsgången vid EU:s hantering av e-infrastrukturkriser.
    - Att samordna dessa myndigheters verksamhet och utbytet av bästa säkerhetspraxis.
    - Att skapa ett centrum med särskild kompetens med ansvar för förebyggande verksamhet och utbyte av information.
    - Att insamla och analysera uppgifter om problem knutna till nätverkssäkerhet.
    - Att analysera aktuella och framtida säkerhetsrisker.
    - Att organisera diskussionsfora på gemenskapsnivå bland aktörerna på säkerhetsområdet (offentliga myndigheter, konsumenter, forskare vid universitet, företag).

15. Europaparlamentet uppmanar kommissionen att se till att denna arbetsgrupp i sitt arbete tar i beaktande vad som redan sagts i Cybercrime Forum samt involverar detta forum i det framtida arbetet.

16. Europaparlamentet uppmanar kommissionen att efter omfattande samråd med medlemsstaterna och den privata sektorn formulera tydligare målsättningar, uppgifter och ansvarsområden för den särskilda arbetsgrupp som skall inrättas, och att se till att denna grupp får tillräckliga personella och finansiella resurser.

17. Europaparlamentet uppmanar kommissionen att med prioritet granska behoven i fråga om säkerhet och att genomföra studier om e-infrastrukturella system för tidig varning för de nätverk som ansvarar för

a) viktig infrastruktur, väsentliga allmänna tjänster och tjänster som berör folkhälsan,

b) olika system för tidig varning och deras driftskompatibilitet, och

c) utvecklingen av e-government och e-business.

18. Europaparlamentet anser att en första lagstiftningsinsats som EU bör vidta på detta område bör grundas på de befogenheter som unionen erkänns i fråga om transeuropeiska nät (avdelning XV i EG-fördraget) och, för de delar som kräver en harmonisering, i fråga om den inre marknaden (artikel 95 i EG-fördraget). Inrättandet av en arbetsgrupp bör föreskrivas enligt samma lagstiftning som fastslår de mål som skall uppnås på gemenskapsnivå.

19. Europaparlamentet uppmanar kommissionen att så snart som möjligt lägga fram en uppskattning av de finansiella konsekvenserna av unionens ingripande inom denna sektor och ge jämförbara uppgifter om liknande initiativ från medlemsstaterna eller tredje land (exempelvis Förenta staterna).

20. Europaparlamentet håller med Europeiska rådet, rådet och kommissionen om att det behövs en europeisk strategi för en ny lagstiftning eller en uppdatering av gällande lagstiftning om utredningsbefogenheter, åtal och straff för kriminell verksamhet eller terrorverksamhet som är riktade mot viktig infrastruktur.

21. Europaparlamentet uppmanar kommissionen och rådet att i så hög grad som möjligt inordna denna diskussion inom ramen för Eurojusts uppgifter för att utveckla en harmoniserad rättslig ram för upptäckt av och åtal mot datorrelaterad brottslighet.

22. Europaparlamentet uppdrar åt talmannen att översända denna resolution till rådet, kommissionen, medlemsstaternas regeringar och parlament, samt till Europarådet.

MOTIVERING

Inledning

Vid mötet i Stockholm den 23-24 mars 2001 efterlyste Europeiska rådet en övergripande strategi för säkerheten när det gäller elektroniska nätverk. För ett år sedan presenterade därför kommissionen en sådan strategi i sitt meddelande om nät- och informationssäkerhet. Meddelandet bygger på kommissionens tidigare meddelande av den 8 oktober 1997 om säkerhet och pålitlighet vid elektronisk kommunikation (KOM(97) 503).

Den föreslagna strategin, som kompletterar rammeddelandet av den 22 januari 2001 om datorrelaterad brottslighet, övertogs och utökades av rådet (telekommunikation) den 6 december 2001, i det att man antog en detaljerad resolution i frågan. Strategin fick sedan ytterligare kött på benen genom kommissionens förslag av den 19 april 2002 om ett rambeslut om angrepp mot informationssystem.

Vid mötet i Barcelona i mars 2002 uppmanade Europeiska rådet kommissionen att ta fram en ny handlingsplan, eEurope 2005, som bland annat skulle ta upp frågan om nät- och informationssäkerhet ur ett pelarövergripande perspektiv. Kommissionen översände denna handlingsplan till Europeiska rådets möte i Sevilla den 21-22 juni 2002, där den antogs.

Den nuvarande gemenskapslagstiftningen och framtidsutsikterna

När det gäller nätsäkerhet finns det redan gemenskapslagstiftning på tre viktiga områden:

a) dataskydd: särskilt **direktiv 95/46/EG** om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (artikel 17) och Europaparlamentets och rådets **direktiv 97/66/EG** av den 15 december 1997 om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet (artiklarna 4-5), som kommer att ersättas av det direktiv som antogs av rådet den 25 juni 2002 (betänkandet av Cappato - A5-0130/2002),

b) telekommunikationspolitiken: att förbättra nätsäkerheten är även ett av de främsta målen med Europaparlamentets och rådets **direktiv 99/93/EG** av den 13 december 1999 om ett gemenskapsramverk för elektroniska signaturer och **direktiv 2000/31/EG** om elektronisk handel; när det gäller nätsäkerheten är det även angeläget att garantera skydd mot naturkatastrofer och omfattande skador (**direktiv 97/33/EG** om samtrafik, artikel 10, och **direktiv 98/10/EG** om taltelefoni, artikel 13),

c) bekämpning av datorrelaterad brottslighet: en aspekt som specifikt rör nätsäkerheten är bekämpningen av datorrelaterad brottslighet; på detta område är de viktigaste referensdokumenten följande: **kommissionens meddelande** om datorrelaterad brottslighet (KOM(2000) 890), **rådets rekommendation** av den 25 juni 2001 om kontaktpunkter som är tillgängliga dygnet runt inom ramen för bekämpningen av högteknologisk brottslighet samt **förslaget till rådets rambeslut** om angrepp mot informationssystem (KOM(2002) 173).

Syftet med meddelandet är att förena de tre ovannämnda aspekterna i en helhetsstrategi. Denna skall innehålla en bred uppsättning åtgärder som skall ha som mål att

- höja medvetenheten hos allmänheten, så att den lär sig hur man skyddar sig.

Meddelandet innehåller även mer specifika initiativ såsom

- inrättande av ett europeiskt system för rapportering och analys av problem,
- stöd till forskningsverksamhet på säkerhetsområdet,
- standardisering och certifiering,
- fri rörlighet för krypteringsprodukter,
- säkerheten i myndigheternas system,
- internationellt samarbete.

Varför behövs en strategi på gemenskapsnivå?

I Förenta staterna har den privata sektorn valt att agera i förebyggande syfte genom att tillämpa olika självregleringssystem, till exempel uppförandekoder och säkerhetsprogram. Det ligger nämligen i den privata sektorns intresse att förbättra nätets tillförlitlighet och att hålla antalet regleringar på lägsta möjliga nivå.

Frivillighet är dock inte alltid tillräckligt för att trygga säkerheten, och de system som utvecklats av privata aktörer är i högre grad inriktade på att uppfylla marknadens krav än att skydda medborgarnas grundläggande rättigheter. Dessutom skall sägas att privata aktörer, till exempel återförsäljare av mjukvara, inte är ansvariga för de skador som uppstår på grund av deras eget säkerhetsbeteende. Detta bekräftas i kommissionens meddelande: *”Användare och leverantörer med låg säkerhetsnivå har inget skadeståndsansvar gentemot tredje man”*. Europeiska unionen har av denna anledning antagit en lagstiftningsstrategi. Syftet är att utveckla en säkerhetskultur och att främja utbyte av säker information genom att använda de instrument som redan finns på marknaden men som inte är tillräckligt kända eller inbördes kompatibla.

Gemenskapens strategi kan även motiveras med att kommunikations- och informationstjänsterna, på samma sätt som säkerhetshoten, är gränsöverskridande. Det är nödvändigt att vidta strategiska åtgärder på gemenskapsnivå för att främja utvecklingen av e-handeln och för att skapa en äkta inre marknad för telekommunikations- och informationstjänster. Det är även angeläget att denna marknad kan använda sig av gemensamma lösningar och fungera effektivt på den globala arenan. Man kan till exempel hävda att skapandet av unionens Internetdomännamn (.eu) inte enbart var ett sätt att markera den europeiska närvaron i cyberrymden. Denna åtgärd innebar nämligen också – vilket var betydligt viktigare – att cyberrymden fick del av det förtroende som EU har byggt upp tack vare den inre marknaden.

Åtgärder som föreslås av kommissionen

Europaparlamentet stöder kommissionen i dess målsättning att bilda en arbetsgrupp för nätsäkerhet, som skall kunna inleda sitt arbete senast sommaren 2003. Parlamentet anser dock

att kommissionen bör beakta att den rättsliga grunden för ett lagstiftningsinitiativ på detta område bör vara avdelning XV i EG-fördraget om de transeuropeiska näten och artikel 95 i EG-fördraget när det gäller de aspekter som kräver harmonisering inom ramen för den inre marknaden.

Europaparlamentet skulle på detta vis delta fullt ut i beslutsprocessen när det gäller detta ämne som är så angeläget för de medborgare som parlamentet företräder.

Ordlista

Server: det fjärrprogram som ger användaren information. Programmet ägnar sig enbart åt att lagra, hämta och vidarebefordra data till den användare som sökt dem. När användaren söker ett dokument som finns på ett visst ställe på nätet, skickar han/hon en sökning till servern via Internet. När *servern* har mottagit sökningen letar den efter de data som önskas och skickar dem till användarens dator.

Nätport (gateway): förbinder alla datorer i nätverket (till exempel ett företagsnät) till Internet genom att använda alla olika former av förbindelser.

Router: en anordning eller ett program i datorn som bestämmer den närmaste väg på nätet dit användaren vänder sig för att inhämta information. *Routern* är förbunden med minst två nät och bestämmer på vilket nät som informationen skall skickas, baserat på en värdering av situationen för de nät den är ansluten till. *Routern* återfinns i alla nätportar.

29 maj 2002

YTTRANDE FRÅN UTSKOTTET FÖR INDUSTRIFRÅGOR, UTRIKESHANDEL, FORSKNING OCH ENERGI

till utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor

över meddelande från kommissionen till Europaparlamentet, rådet, Ekonomiska och sociala kommittén och Regionkommittén ”Nät- och informationssäkerhet: förslag till en europeisk strategi”
(KOM(2001) 298 – C5-0657/2001 – 2001/2280(COS))

Föredragande: W.G. van Velzen

ÄRENDETS GÅNG

Vid utskottssammanträdet den 22 november 2001 utsåg utskottet för industrifrågor, utrikeshandel, forskning och energi W.G. van Velzen till föredragande.

Vid utskottssammanträdena den 16 april och 22 maj 2002 behandlade utskottet förslaget till yttrande.

Vid det sistnämnda sammanträdet godkände utskottet enhälligt nedanstående slutsatser.

Följande ledamöter var närvarande vid omröstningen: Carlos Westendorp y Cabeza (ordförande), Peter Michael Mombaur och Yves Piétrasanta (vice ordförande), W.G. van Velzen (föredragande), Nuala Ahern, Sir Robert Atkins, María del Pilar Ayuso González (suppleant för Jaime Valdivielso de Cué), Guido Bodrato, David Robert Bowe (suppleant för Norbert Glante), Marco Cappato, Massimo Carraro, Gérard Caudron, Giles Bryan Chichester, Willy C.E.H. De Clercq, Concepció Ferrer, Francesco Fiori (suppleant för Umberto Scapagnini), Christos Folias (suppleant för Christian Foldberg Rovsing), Michel Hansenne, Hans Karlsson, Bashir Khanbhai, Bernd Lange (suppleant för Rolf Linkohr), Werner Langen, Caroline Lucas, Marjo Matikainen-Kallström, Eryl Margaret McNally, William Francis Newton Dunn (suppleant för Nicholas Clegg), Angelika Niebler, Reino Paasilinna, Paolo Pastorelli, Elly Plooij-van Gorsel, Samuli Pohjamo(suppleant för Colette Flesch), Godelieve Quisthoudt-Rowohl, Paul Rübig, Konrad K. Schwaiger, Alejo Vidal-Quadras Roca, Dominique Vlasto, Anders Wijkman (suppleant för John Purvis), Myrsini Zorba och Olga Zrihen Zaari.

KORTFATTAD MOTIVERING

Säkerhet har betydelse i alla aspekter av det dagliga livet. Av medborgare och företag förväntas att de i första hand känner och tar sitt ansvar i fråga om sin egen säkerhet och säkerheten i sin (direkta) omgivning. Detta gäller alltså även när det handlar om elektroniska kommunikationsnät. Angrepp som orsakar kaos på Internet hör numera till vardagen. Virus som sprider sig snabbt via e-postkommunikation har på kort tid gjort många användare medvetna om denna risk och om sårbarheten hos deras datorsystem. Samtidigt konvergerar de elektroniska kommunikationsnäten i rask takt. Därför är det viktigt att kännedomen om både nätverkskonvergens och möjliga säkerhetsrisker ökar.

Förutom datavirus finns det många andra säkerhetsrisker för de elektroniska kommunikationsnäten. Det handlar inte bara om virus som sprids via e-post, utan även avlyssning av kommunikation, identitetsförfalskning eller obehörigt tillträde till ett nät är faktiska risker som användare bör bli medvetna om. Även sådana risker som inte beror på något ont uppsåt, såsom den mänskliga faktorn eller naturkatastrofer, bör beaktas i detta sammanhang.

Till detta kommer att tillgången till elektroniska kommunikationsnät är av mycket stor vikt för andra infrastrukturer, såsom dricksvatten- och energiförsörjningen. Den ständigt ökande nätverkskonvergensen ökar alltså även beroendet och sårbarheten i (informations)samhället.

Eftersom det är bättre att stämma i bäcken än i ån är det av avgörande betydelse att man ökar medvetenheten på detta område. Det är myndigheternas uppgift att i första hand göra det möjligt för medborgare och företag att gardera sig mot vissa säkerhetsrisker. Här har myndigheterna en viktig informationsuppgift som bl. a. bör bestå i att utveckla lämpliga gemensamma definitioner för nätsäkerhet, upprätthålla nätens integritet och garantera informationssäkerheten.

Ett larmsystem för datorer kan vara till hjälp för att få ett redan pågående angrepp eller annat hot under kontroll så snabbt som möjligt. De nuvarande CERT[1]-initiativen (från myndigheter och stora företag) är ett exempel på ett sådant system. Dessa initiativ bör emellertid bli tillgängliga för alla, alltså även för privatpersoner och små (mindre) företag. Här väntar också en viktig uppgift för myndigheterna. Redan befintliga CERT-grupper bör utökas och fungera väl på medlemsstatsnivå innan initiativ tas till att upprätta en europeisk CERT-grupp.

Lösningar och åtgärder som vidtas för att öka säkerheten är endast effektiva om alla kan dra nytta av dem. Med andra ord, initiativ som skall öka säkerheten är inte lika effektiva om de berörda aktörerna väljer olika lösningar som inte är kompatibla. På detta område är det av avgörande betydelse att lösningarna följer en öppen internationell standard. Det finns alltså gott om standardiseringsansatser, men tyvärr konkurrerar flera standarder och specifikationer, vilket gör att marknaden fragmenteras och lösningarna inte är kompatibla. Lösningar baserade på programvara som bygger på en öppen källkod kan bidra till snabbare felrättning och större insyn, vilket främjar säkerheten. Lösningar som syftar till att öka nätsäkerheten skall därför skapas i samråd med alla berörda sektorer. Förutom utveckling av åtgärder är det av vikt att man kontinuerligt och på internationell nivå undersöker hur hög säkerhetsnivån är och hur

[1] Computer Emergency Response Team.

effektiva vissa åtgärder är. Riktmärkning kan vara ett användbart instrument för en kontinuerlig kontroll. På grund av att de elektroniska kommunikationsnäten är internationella, och därigenom även säkerhetsriskerna, är det nödvändigt att föra en dialog med andra länder och institutioner i världen för att exempelvis snabbt bli medveten om existerande risker eller utbyta erfarenheter i fråga om ingripanden och genomförande av politiska åtgärder.

Med tanke på att hoten mot nätsäkerheten (naturligtvis med undantag för tidigare nämnda naturkatastrofer eller mänskliga faktorn) ofta är av kriminell natur bör politiska åtgärder som avser nätsäkerhet i så hög grad som möjligt inordnas inom ramen för Eurojusts uppgifter för att därigenom utveckla en harmoniserad rättslig ram för upptäckt av och åtal mot datorrelaterad brottslighet.

SLUTSATSER

Utskottet för industrifrågor, utrikeshandel, forskning och energi uppmanar utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor att som ansvarigt utskott infoga följande i sitt resolutionsförslag:

A. Elektroniska kommunikationsnät konvergerar i rask takt, och dessa nät får allt större betydelse för ekonomin och samhället.

B. Till följd av denna konvergens behöver det skapas lämpliga politiska och rättsliga ramar i Europeiska unionen, vilka lämnar garantier för att nät- och informationssäkerheten betraktas som en avgörande förutsättning för informationssamhället.

C. Säkerhetshöjande åtgärder blir bara effektiva om alla berörda parter, medborgarna inbegripna, är medvetna om säkerhetsriskerna och det egna ansvaret i fråga om de säkerhetsåtgärder som bör vidtas.

D. Säkerhetshöjande åtgärder blir bara effektiva om de får en utbredd tillämpning bland berörda marknadsaktörer och grundas på öppna internationella standarder.

E. Grupper för stöd vid datorhaveri (Computer Emergency Response Teams, CERT) fungerar olika i olika länder, vilket försvårar samarbetet.

1. Europaparlamentet betonar att gemensamma definitioner för nätsäkerhet, upprätthållande av nätens integritet och informationssäkerhet måste utvecklas så snabbt som möjligt.

2. Europaparlamentet välkomnar kommissionens avsikt att inrätta en särskild arbetsgrupp för datorrelaterad säkerhet och uppmanar rådet att snarast möjligt förverkliga dessa planer och inrätta denna särskilda arbetsgrupp före slutet av 2002.

3. Europaparlamentet uppmanar kommissionen att efter omfattande samråd med medlemsstaterna och den privata sektorn formulera tydligare målsättningar, uppgifter och ansvarsområden för den särskilda arbetsgrupp som skall inrättas, och att se till att denna grupp får tillräckliga personella och finansiella resurser.

4. Europaparlamentet uppmanar kommissionen att under alla omständigheter tilldela den särskilda arbetsgruppen funktionen som oberoende kompetenscentrum i gemenskapen på området för nät- och informationssäkerhet, varigenom gruppen bland annat kommer att kunna fungera som bollplank för medlemsstaterna när det gäller att utforma nationell politik och som oberoende rådgivare åt medlemsstaterna och den privata sektorn, och så att gruppen skall kunna genomföra oberoende undersökningar på området för nät- och informationssäkerhet.

5. Europaparlamentet betonar att man så snart som möjligt måste se till att alla medborgare, företag och myndigheter får tillgång till samtliga EU-organs offentliga elektroniska tjänster genom ett säkert, individanpassat och verifierat system för tillträde. Sådant tillträde måste garanteras genom användning av digitala signaturer och fastställande av europeiska normer som genast skall gälla för EU-institutionerna.

6. Europaparlamentet uppmanar kommissionen att ta initiativ till att öka medborgarnas, företagens och den offentliga sektorns medvetenhet om säkerhetsriskerna i de elektroniska kommunikationsnäten, och att bidra till samordning och innehållsmässig anpassning vid informationskampanjer i medlemsstaterna om säkerhetsaspekter och risker avseende elektroniska kommunikationsnät. Parlamentet uppmanar kommissionen att i första hand anförtro denna uppgift åt den särskilda arbetsgrupp för datorrelaterad säkerhet som skall inrättas inom kort.

7. Europaparlamentet uppmanar kommissionen att utarbeta en handlingsplan för att främja användningen av digitala signaturer, exempelvis genom att anta gemenskapsbestämmelser som genast skall gälla för EU-institutionerna.

8. Europaparlamentet betonar vikten av att de berörda sektorerna deltar i utarbetandet av strategier avseende nätens säkerhet och integritet samt informationssäkerheten i IP-miljöer.

9. Europaparlamentet välkomnar kommissionens avsikt att tillsammans med medlemsstaterna undersöka vilket som är det bästa sättet att organisera insamlingen av uppgifter samt analysen och planeringen av förebyggande åtgärder mot de nuvarande och de nya säkerhetsriskerna.

10. Europaparlamentet uppmanar kommissionen och rådet att i så hög grad som möjligt inordna denna diskussion inom ramen för Eurojusts uppgifter för att utveckla en harmoniserad rättslig ram för upptäckt av och åtal mot datorrelaterad brottslighet.