KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 6.6.2001
KOM(2001)298 endelig

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET, EUROPA-PARLAMENTET, DET ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

Net- og informationssikkerhed: Forslag til en europæisk strategi

MEDDELELSE FRA KOMMISSIONEN TIL RÅDET, EUROPA-PARLAMENTET, DET ØKONOMISKE OG SOCIALE UDVALG OG REGIONSUDVALGET

Net- og informationssikkerhed: Forslag til en europæisk strategi

RESUMÉ

I.

Sikkerhed er ved at blive et hovedanliggende, fordi kommunikation og information er blevet en nøglefaktor i den økonomiske og samfundsmæssige udvikling. Net og informationssystemer er nu blevet medier for tjenester og dataoverførsel i en grad, man ikke kunne forestille sig for få år siden. Anden infrastruktur som vand- og elforsyningssystemer er blevet kritisk afhængig af dem. Da alle - erhvervslivet, private borgere og offentlige forvaltninger - gerne vil udnytte kommunikationsnettenes muligheder, bliver disse systemers sikkerhed en forudsætning for videre fremskridt.

På denne baggrund konkluderede Det Europæiske Råd på Stockholm-mødet den 23.-24. marts 2001, at *"Rådet sammen med Kommissionen vil udarbejde en samlet sikkerhedsstrategi for elektroniske netværk, herunder praktiske gennemførelsesforanstaltninger. Dette bør forelægges inden Det Europæiske Råd i Göteborg."* Denne meddelelse er Europa-Kommissionens reaktion på denne opfordring.

II.

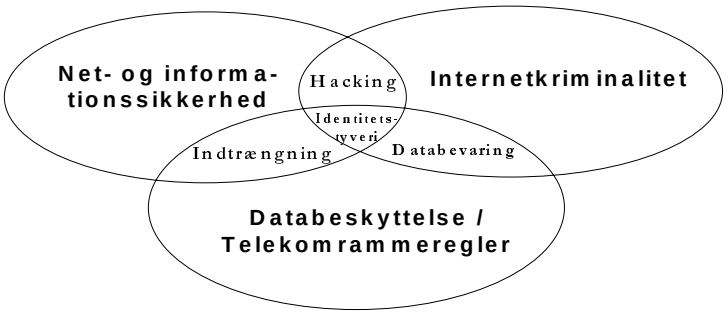
Sikkerhed er blevet en central udfordring for politikerne, men det bliver samtidig en mere og mere kompleks opgave at finde frem til en adækvat politisk løsning. Kommunikationstjenester udbydes ikke længere af statsejede teleoperatører, men af mange private operatører og tjenesteudbydere i indbyrdes konkurrence og i stigende omfang i europæisk og global skala. Nettene konvergerer: de kan formidle de samme tjenester, de er i stigende omfang koblet sammen, og de bruger til en vis grad samme infrastruktur.

For at sikre et minimum af sikkerhed har både medlemsstaterne og EU vedtaget et omfattende sæt af love og regler som led i lovgivningen om telekommunikation og databeskyttelse. Disse lovregler skal anvendes effektivt i et miljø under hastig forandring. Desuden må de videreudvikles, som det fremgår af forslaget om nye lovrammer for telekommunikation og de kommende forslag i forbindelse med debatten om internetkriminalitet. Politikerne må derfor forstå de underliggende sikkerhedsproblemer og have en klar opfattelse af, hvilken rolle de har at spille for forbedring af sikkerheden.

Sikkerhed er blevet en vare, der købes og sælges på markedet og indgår som led i forretningsaftaler. Normalt antages det stiltiende, at prismekanismen vil sørge for, at omkostningerne ved at yde sikkerhed afbalanceres over for det konkrete sikkerhedsbehov. Mange sikkerhedsproblemer er imidlertid stadig uløste, og for andre er løsningerne længe om at slå igennem på markedet på grund af visse ufuldkommenheder på markedet. **Skræddersyede politiske indgreb over for disse ufuldkommenheder på markedet kan styrke markedsprocessen og bidrage til, at lovrammerne kommer til at fungere bedre.** Sådanne indgreb må nødvendigvis indgå i en europæisk strategi - dels af hensyn til det indre marked, dels for at udnytte fordelene ved fælles løsninger og endelig for at give mulighed for en effektiv international indsats.

De foreslåede politiske tiltag på området net- og informationssikkerhed skal ses i sammenhæng med de eksisterende strategier for telekommunikation, databeskyttelse og

internetkriminalitet. En net- og informationssikkerhedspolitik vil udfylde hullet i denne politiske ramme. Følgende diagram viser de tre politikområder og illustrerer med nogle eksempler, hvordan de er forbundet med hinanden:



III.

Net- og informationssikkerhed kan forstås som et nets eller et informationssystems evne til på et givet tillidsniveau at modstå uheld og ondsindede handlinger. Uheld og hærværk kan gøre lagrede og transmitterede data utilgængelige, skade deres autenticitet og integritet og krænke deres fortrolighed og kan tilsvarende skade tjenester, der udbydes over sådanne net og systemer. Sådanne sikkerhedshændelser kan grupperes på følgende måde:

- Elektronisk kommunikation kan opfanges og data blive kopieret eller ændret. Dette kan både anrette skade ved krænkelse af enkeltpersoners privatliv og ved udnyttelse af opfangne data.
- Uautoriseret indtrængen i computere og computernet sker oftest i ond hensigt for at kopiere, ændre eller ødelægge data.
- Driftsforstyrrende angreb på Internettet er blevet ret almindelige og i fremtiden kan telefonnettet også blive mere sårbart.
- Hærværkssoftware som virus kan få computere til at bryde sammen, og slette eller ændre data. Nogle af den senere tids virusangreb har været særdeles destruktive og dyre at rydde op efter.
- Forfalskning af personers eller enheders identitet kan anrette stor skade; f.eks. risikerer kunder at downloade hærværkssoftware fra et websted, der giver sig ud for at være en pålidelig kilde, kontrakter kan blive opsagt eller fortrolige oplysninger sendt til uvedkommende.
- Mange sikkerhedsproblemer skyldes uforudsete og utilsigtede hændelser; det kan være naturkatastrofer (oversvømmelser, storme, jordskælv), svigtende hardware eller software eller menneskelige fejl.

IV.

De foreslåede tiltag:

- **Oplysning:** Der bør lanceres en kampagne for oplysning og fremme af bedste praksis.
- **Et europæisk varslings- og informationssystem** Medlemsstaterne bør styrke deres Computer Emergency Response Teams (CERT) og forbedre samordningen mellem dem. Kommissionen vil sammen med medlemsstaterne undersøge, hvordan man bedst kan

organisere dataindsamling, analyse og planlægning af fremsynede reaktioner på eksisterende og opdukkende sikkerhedstrusler på europæisk niveau.

- **Teknologistøtte:** Støtte til forskning og udvikling inden for sikkerhed bør være et nøgleelement i det sjette rammeprogram og knyttes til en bredere strategi for bedre net- og informationssikkerhed.
- **Støtte til markedsorienteret standardisering og certificering:** Europæiske standardiseringsorganisationer opfordres til at fremskynde arbejdet med interoperabilitet; Kommissionen vil fortsat støtte arbejdet med elektronisk signatur og den videre udvikling af IPv6 og IPSec; Kommissionen vil vurdere behovet for et lovinitiativ vedrørende gensidig anerkendelse af certifikater; medlemsstaterne bør gennemgå alle relevante sikkerhedsstandarder.
- **Retsgrundlag:** Kommissionen vil opstille en oversigt over de nationale foranstaltninger, der er truffet i overensstemmelse med relevante EF-bestemmelser. Medlemsstaterne bør støtte fri omsætning af krypteringsprodukter. Kommissionen vil foreslå lovgivning om internetkriminalitet.
- **Sikkerhed i offentlige instanser:** Medlemsstaterne bør sørge for, at effektive og driftskompatible sikkerhedsløsninger indgår i deres aktiviteter vedrørende e-forvaltning og e-udbud. Medlemsstaterne bør indføre elektroniske signaturer, når der tilbydes offentlige tjenester. Kommissionen vil skærpe sikkerhedskravene til dens egne informations- og kommunikationssystemer.
- **Internationalt samarbejde:** Kommissionen vil styrke dialogen med internationale organisationer og partnere om net- og informationssikkerhed.

V.

I næste fase skal rammen og forslagene drøftes af medlemsstaterne og Europa-Parlamentet. Det Europæiske Råd kan på mødet i Göteborg den 15.-16. juni udstikke retningslinjer for vejen frem.

Kommissionen foreslår, at der iværksættes en grundig drøftelse med industrien og brugerne om den nærmere praktiske gennemførelse af forslagene. Kommentarer kan sendes til eeurope@cec.eu.int frem til udgangen af august 2001. Denne meddelelse er således en opfordring til interesserede parter om at indsende kommentarer med henblik på den endelige fastlæggelse af konkrete tiltag. Det kunne ske ved udarbejdelse af en køreplan hen mod slutningen af 2001.

***

Net- og informationssikkerhed:
Forslag til en europæisk strategi

Indhold

1. Indledning

Bekymringerne for sikkerheden i elektroniske net og informationssystemer er vokset i takt med den hastige stigning i antallet af netbrugere og i værdien af deres transaktioner. Sikkerhed har nu nået et kritisk punkt, hvor den udgør en forudsætning for vækst i elektroniske virksomheder og for, at økonomien som helhed kan fungere. En række faktorer i forening har skubbet informations- og kommunikationssikkerhed op i toppen af den politiske dagsorden i EU:

- Regeringerne har indset, i hvor høj grad deres økonomier og borgerne er afhængige af, at kommunikationsnettene fungerer effektivt, og de er begyndt at tage deres sikkerhedsordninger op til fornyet overvejelse.

- Internettet har skabt et globalt system, der forbinder millioner af net, store og små, og flere hundrede millioner individuelle pc'er samt i stigende grad andet udstyr, herunder mobiltelefoner. Dette har medført et betydeligt fald i omkostningerne ved uretmæssigt at skaffe sig adgang til værdifulde økonomiske oplysninger på afstand.

- Der har været en række meget omtalte tilfælde af virusangreb på Internettet, der har forårsaget omfattende skade ved at ødelægge data og blokere for adgang til nettet. Sådanne sikkerhedsproblemer er ikke begrænset til enkelte lande, men spreder sig hurtigt på tværs af grænserne.

- På topmøderne i Lissabon og Feira anerkendte Det Europæiske Råd i forbindelse med lanceringen af handlingsplanen *e*Europe 2002, at Internettet er en af hoveddrivkræfterne i EU-økonomiernes produktivitet.

På denne baggrund konkluderede Det Europæiske Råd på mødet i Stockholm den 23. - 24. marts 2001, at *"Rådet sammen med Kommissionen [vil] udarbejde en samlet sikkerhedsstrategi for elektroniske netværk, herunder praktiske gennemførelsesforanstaltninger. Dette bør forelægges inden Det Europæiske Råd i Gøteborg"*. Nærværende meddelelse er Europa-Kommissionens reaktion på denne opfordring.

<u>Et miljø i hastig forandring</u>

Sikkerhed er således blevet en central udfordring for beslutningstagerne, men samtidig bliver det en stadig mere kompleks opgave at finde en fyldestgørende politisk løsning. Blot nogle få år tilbage var netsikkerhed hovedsagelig et problem for statslige monopolselskaber, der tilbød specialiserede tjenester via offentlige net, særlig telefonnettet. Sikkerhed i edb-systemer var begrænset til store organisationer og koncentreret om adgangskontrol. Formulering af en sikkerhedspolitik var en forholdsvis enkel opgave. Denne situation har nu ændret sig betydeligt som følge af en række forskellige tendenser i den bredere markedssammenhæng, blandt andet liberalisering, heterogenitet og globalisering:

Nettene ejes og drives nu hovedsagelig privat. Kommunikationstjenester tilbydes på konkurrencevilkår, hvor sikkerhed udgør en del af tilbuddet. Mange kunder er imidlertid

uvidende om, hvor stor en sikkerhedsrisiko de løber, når de kobler sig på et net, og træffer derfor deres beslutninger på et ufuldstændigt grundlag.

Net og informationssystemer konvergerer. De bliver i stigende grad koblet sammen, tilbyder samme slags sømløse og skræddersyede tjenester og deler til en vis grad samme infrastruktur. Slutbrugerterminaler (pc'er, mobiltelefoner o.lign.) er blevet et aktivt element i netarkitekturen og kan tilsluttes forskellige net.

Nettene er internationale. En betydelig del af nutidens kommunikation er grænseoverskridende eller passerer gennem tredjelande (somme tider uden at slutbrugeren er klar over det), og dette må der tages højde for i sikkerhedsløsningerne. De fleste net er bygget op af kommercielle produkter fra internationale leverandører. Sikkerhedsprodukterne skal være i overensstemmelse med internationale standarder.

Behovet for en offentlig strategi

Disse faktorer begrænser regeringernes mulighed for at påvirke sikkerhedsniveauet for elektronisk kommunikation blandt borgere og virksomheder. Det betyder dog ikke, at den offentlige sektor ikke længere spiller nogen rolle.

For det første er der indført **en række retlige bestemmelser på EU-plan, der specifikt vedrører net- og informationssikkerhed**. Navnlig indeholder EU-lovrammerne for telekommunikation og databeskyttelse bestemmelser om, at operatører og tjenesteudbydere skal tilvejebringe et sikkerhedsniveau, der er passende set i forhold til risikoen.

For det andet er der stigende bekymring over **den nationale sikkerhed**, efterhånden som informationssystemer og kommunikationsnet er blevet en kritisk faktor for andre infrastrukturer (f.eks. vand- og elektricitetsforsyning) og andre markeder (f.eks. det globale finansmarked).

Endelig er der behov for, at staten skrider ind for at rette op på **ufuldkommenheder på markedet**. Markedspriserne afspejler ikke altid akkurat de omkostninger og fordele, der er forbundet med investeringer i forbedret netsikkerhed, og hverken udbyderne eller brugerne bærer altid alle følgerne af deres adfærd. Kontrollen over nettet er spredt, og svagheder i ét system kan udnyttes til at angribe andre. Nettenes kompleksitet gør det vanskeligt for brugerne at bedømme de mulige farer.

Det er derfor hensigten med denne meddelelse at fastslå, hvor der er brug for yderligere eller styrkede offentlige tiltag på europæisk eller nationalt plan.

Kapitel 2 definerer begrebet net- og informationssikkerhed, beskriver de vigtigste sikkerhedstrusler og vurderer de nuværende løsninger. Målet er at give den indsigt i emnet net- og informationssikkerhed, der er nødvendig for at forstå de tiltag, der foreslås. Det er ikke hensigten at give en udtømmende teknisk oversigt over sikkerhedsspørgsmålene.

I **kapitel 3** foreslås en europæisk strategi til forbedring af net- og informationssikkerheden. Strategien bygger på en analyse af behovet for at supplere markedets løsninger med politiske tiltag. Den omfatter en række konkrete politiske tiltag, således som Det Europæiske Råd udbad sig på mødet i Stockholm. Den foreslåede strategi bør ses som et integrerende element i

de eksisterende lovrammer for elektroniske kommunikationstjenester og databeskyttelse samt strategien mod internetkriminalitet.

2. Analyse af spørgsmålene omkring net- og informationssikkerhed

2.1. Hvad er net- og informationssikkerhed?

Net er systemer, hvor data lagres og behandles, og gennem hvilke de cirkulerer. De består af transmissionskomponenter (kabler, trådløse forbindelser, satellitter, routere, gateways, omkoblere osv.), og støttetjenester (domænenavnssystemet, herunder rodservere, opkaldsidentifikationstjeneste, autentificeringstjenester osv.). Til nettene er der knyttet et stadig bredere udvalg af applikationer (e-mail-leveringssystemer, browsere osv.) og terminaludstyr (telefonapparater, værtscomputere, pc'er, mobiltelefoner, elektroniske kalendere, husholdningsapparater, industrimaskiner osv.).

De generelle sikkerhedskrav i forbindelse med net og informationssystemer kan betragtes som bestående af følgende indbyrdes forbundne egenskaber:

i) **Disponibilitet**: Data skal være tilgængelige og tjenester funktionsdygtige på trods af mulige forstyrrende hændelser såsom strømafbrydelser, naturkatastrofer, uheld og angreb. Dette er særlig vigtigt i sammenhænge, hvor fejl i kommunikationsnettene kan medføre sammenbrud i kritiske net som f.eks. flytrafik og strømforsyning.

ii) **Autentificering**: Bekræftelse af en enheds eller brugers påståede identitet. Der kræves behørige autentificeringsmetoder til mange applikationer og tjenester, såsom indgåelse af en kontrakt via nettet, kontrol af adgang til visse data og tjenester (f.eks. for distancearbejdere) og autentificering af websteder (f.eks. for internetbanker). Autentificering må også omfatte muligheden for **anonymitet**, da mange tjenester ikke behøver at kende brugerens identitet, men blot skal have en pålidelig bekræftelse af visse kriterier (såkaldte anonyme kreditiver) såsom betalingsevne.

iii) **Integritet**: Bekræftelse af, at de data, der sendes, modtages eller gemmes, er komplette og uændrede. Dette er især vigtigt i forbindelse med autentificering ved indgåelse af kontrakter og i tilfælde, hvor datanøjagtigheden er kritisk (medicinske data, industrielt design osv.)

iv) **Fortrolighed**: Beskyttelse mod, at kommunikation eller lagrede data opfanges og læses af uautoriserede personer. Fortrolighed er især vigtigt ved transmission af følsomme data og er en af forudsætningerne for at tackle netbrugernes bekymringer om brud på privatlivets fred.

Der må tages højde for alle hændelser, der udgør en trussel mod sikkerheden - ikke kun dem, der sker i ond hensigt. Set ud fra brugerens synspunkt er trusler som naturkatastrofer og menneskelige fejl, der forstyrrer nettets drift, potentielt lige så bekostelige som angreb i ond hensigt. **Net- og informationssikkerhed kan således forstås som et nets eller et informationssystems evne til, på et givet tillidsniveau, at modstå uheld og ondsindede handlinger, der er til skade for disponibiliteten, autenticiteten, integriteten og fortroligheden i forbindelse med lagrede og transmitterede data og de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via dette net eller system.**

2.2. Oversigt over sikkerhedstruslerne

Selskaber, der anvender nettet til deres salgsaktiviteter eller til at organisere levering af forsyninger, kan blive lammet af et angreb, der overbelaster systemet og sætter det ud af drift

("denial of service"). Personlige og finansielle oplysninger kan opfanges og misbruges. Den nationale sikkerhed kan være truet. Disse eksempler giver en ide om de trusler, som en utilstrækkelig sikkerhed fører med sig. Formålet med de følgende afsnit er at beskrive de forskellige typer sikkerhedsrisici som grundlag for fastlæggelsen af en overordnet strategi for forbedring af sikkerheden i kapitel 3. Der skelnes mellem bevidste angreb (afsnit 2.2.1 - 2.2.5) og utilsigtede hændelser (afsnit 2.2.6).

2.2.1. Opfangning af kommunikation

Elektronisk kommunikation kan opfanges, og data kan kopieres eller ændres. Indgrebene kan ske på mange forskellige måder, bl.a. ved fysisk adgang til netlinjer, dvs. tapning, og aflytning af radiokommunikation. De mest kritiske punkter i forbindelse med opfangning af kommunikationstrafik er netstyrings- og -koncentrationspunkter, f.eks. routere, gateways, omkoblere og netdriftsservere.

Der må skelnes mellem opfangning af kommunikation, der sker ulovligt eller i ond hensigt, og lovlige indgreb. Opfangning af kommunikation af hensyn til den offentlige sikkerhed er tilladt i bestemte tilfælde og til begrænsede formål i alle EU-lande. Der er lovrammer, der tillader de retshåndhævende myndigheder at indhente retskendelse, eller hvis sagen vedrører to medlemsstater, en tilladelse udstedt personligt af en ledende minister, om opfangning af kommunikation.

Mulig skade - Ulovlig opfangning kan anrette skade, både i form af indgreb i privatlivets fred og i form af udnyttelse af de opfangne data, f.eks. adgangskoder og kreditkortoplysninger, med henblik på kommerciel gevinst eller sabotage. Denne trussel opfattes som en de vigtigste hæmmende faktorer for udbredelsen af e-handel i Europa.

Mulige løsninger – Der kan sættes ind mod ulovlig opfangning dels ved at **operatørerne** sikrer deres net, således som påkrævet bl.a. ifølge direktiv 97/66 EF[1], og dels ved at **brugerne** krypterer de data, de sender via nettene.

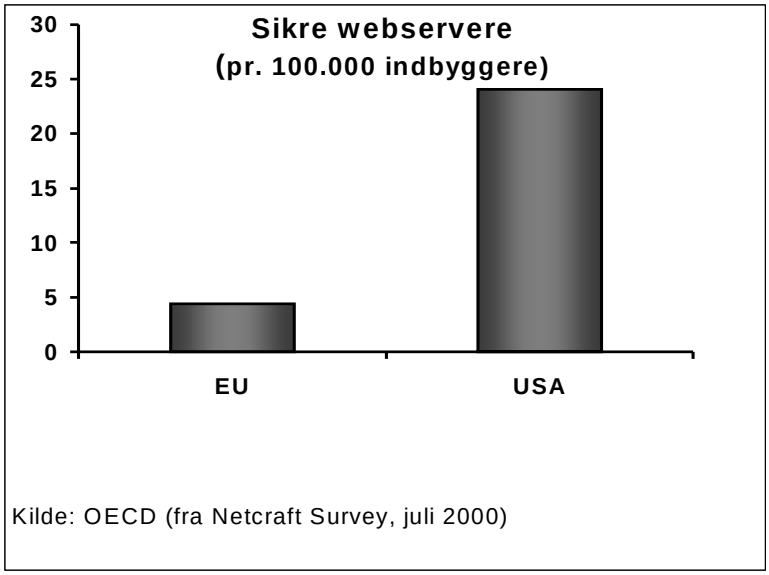
For **operatørerne** er beskyttelse af nettet mod opfangning en kompleks og bekostelig opgave. Traditionelt har telekommunikationsselskaberne sikret nettene gennem fysisk adgangskontrol ved deres anlæg og retningslinjer for de ansatte. Kun lejlighedsvis har de krypteret trafikken. Ved trådløs kommunikation er operatørerne forpligtet til at sikre, at trafikken er tilstrækkeligt krypteret. Mobilkommunikationsoperatører krypterer trafikken mellem mobiltelefonen og basisstationen. Krypteringsstyrken i de fleste EU-lande er lavere end det, der teknisk er muligt, på grund af kravet om at muliggøre lovlig opfangning. Af samme grund kan krypteringen slås til og fra ved basisstationen, uden at brugeren er klar over, at det sker.

Brugerne kan selv beslutte at kryptere data og tale uafhængigt af sikkerhedsforanstaltningerne på nettet. Ordentligt krypterede data er uforståelige for alle undtagen den autoriserede modtager. Der er et bredt udbud af krypteringssoftware og -hardware til praktisk talt alle typer kommunikation[2]. Særlige produkter kan kryptere en telefonsamtale eller en fax-transmission. E-mails kan krypteres ved hjælp af særskilt software eller software, der er integreret i et tekstbehandlingsprogram eller klientsiden af en e-mail-applikation. Problemet for brugere, der krypterer e-mail eller tale, er at modtagerne skal kunne forstå indholdet. Udstyr eller software skal være kompatibelt. Modtagerne skal også

1 Direktivet om databeskyttelse inden for telesektoren (EFT L 24 af 30.1.1998).

2 Se Kommissionens meddelelse om "Sikkerhed og tillid i elektronisk kommunikation", 8. oktober 1997, KOM (1997) 503 endelig udg.

kende dekrypteringsnøglen, hvilket betyder, at der bør være en mekanisme til at modtage nøglen, der omfatter en behørig autentificering af nøglen. Omkostningerne ved kryptering, både penge- og arbejdsmæssigt, er store, og brugerne mangler ofte information om sikkerhedsrisici og -fordele, så det er vanskeligt for dem at træffe de rette beslutninger.



Kilde: OECD (fra Netcraft Survey, juli 2000)

En almindeligt anvendt sikkerhedssystem på Internet er SSL: Secure Socket Layer. SSL krypterer kommunikation mellem en webserver og brugerens webnavigationsprogram (browser). Tidligere hæmmedes udbredelsen af denne teknologi, især den kraftigste udgave (128 bit), af USA's restriktive eksport-kontrol. Den amerikanske eksportkontrol er imidlertid for nylig blevet revideret, efter at der er vedtaget en mere liberal fællesskabsordning for kontrol med udførslen af produkter og teknologier med dobbelt anvendelse[3]. Ifølge statistiske oplysninger halter Europa langt bag USA, når det gælder antallet af sikre webservere (se figuren).

Operatører, brugere og producenter står over for problemet med konkurrerende og ikke-kompatible standarder. For eksempel er der på området sikker e-mail to standarder[4], der konkurrerer om at blive førende. Europas indflydelse på dette punkt har været begrænset. Resultatet er et væld af ikke-europæiske produkter, der gennemfører disse standarder, og hvor de europæiske brugeres adgang til produkterne afhænger af USA's eksportkontrolpolitik. Der er bekymring over sikkerhedsniveauet i mange af disse produkter (jf. Echelon[5]), og nogle regeringer i EU overvejer at bruge åben software for at øge tilliden til krypteringsprodukterne. Disse tiltag befinder sig imidlertid i pilotforsøgsfasen[6], der er endnu ingen koordinering, og markedskræfterne er måske simpelthen stærkere end isolerede offentlige bestræbelser. Problemet kan gribes an ved at gennemføre en omfattende evaluering af både kommerciel og åben software.

2.2.2. Uautoriseret adgang til computere og computernet

Uautoriseret adgang til computere eller net sker normalt i ond hensigt med det formål at kopiere, ændre eller ødelægge data. Teknisk taler man om indtrængen, og denne kan ske på

---

3 Rådets forordning (EF) nr. 1334/2000 om en fællesskabsordning for kontrol med udførslen af produkter og teknologier med dobbelt anvendelse (EFT L 159 af 30.6.2000).

4 S-MIME (secure multiple Internet mail extensions) og OpenPGP (Pretty Good Privacy) er begge standarder fra IETF (Internet Engineering Task Force).

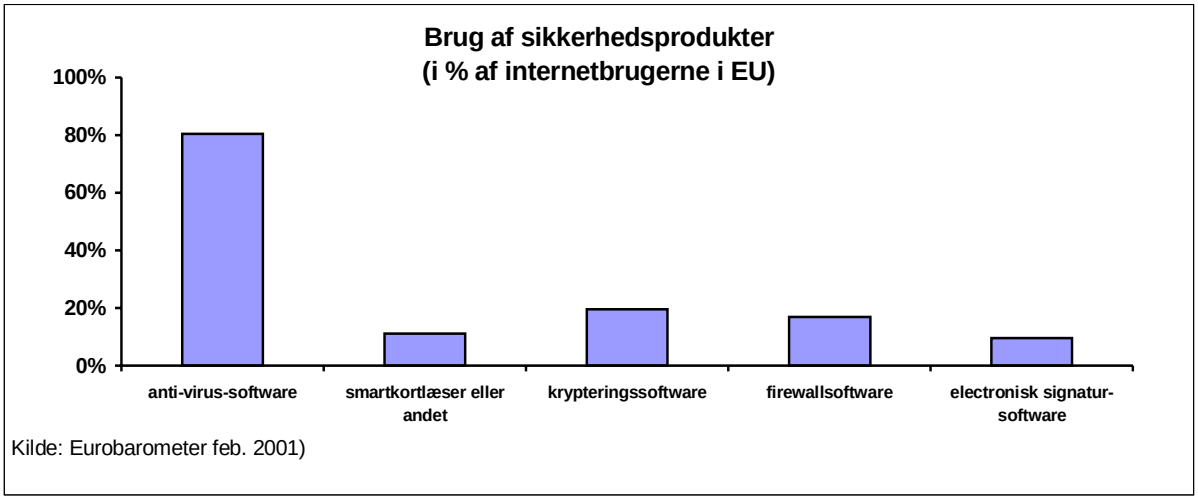
5 ECHELON-systemet bruges efter sigende til at opfange almindelig e-mail-, fax-, telex- og telefontrafik, der formidles via telenettene verden over. Se også aktiviteterne under Europa-Parlamentets Midlertidige Udvalg om Echelon: http://www.europarl.eu.int/committees/echelon_home.htm

6 Den tyske regering finansierer et projekt med betegnelsen GNUPG, der er baseret op den åbne standard OpenPGP (se http://www.gnupg.org).

mange måder, bl.a. ved at udnytte intern information, ved 'ordbogsangreb' (dictionary attacks), direkte indtrængningsangreb ('brute force attacks'), hvor man udnytter folks tendens til at vælge forudsigelige adgangskoder, og social manipulation ('social engineering'), hvor man udnytter folks tendens til at afsløre information over for tilsyneladende pålidelige mennesker, samt ved at opfange adgangskoder. Sådanne angreb udføres ofte af personer inden for den ramte organisation ('insider-angreb').

Mulig skade - I visse tilfælde er motivet bag uautoriseret indtrængen intellektuel udfordring snarere end økonomisk gevinst. Men hvad der begyndte som en irriterende aktivitet (ofte omtalt som 'hacking') har fremhævet informationsnettenes svagheder og ansporet personer med kriminelle og onde hensigter til at udnytte disse svagheder. Beskyttelse mod uautoriseret adgang til personoplysninger, herunder finansielle oplysninger, bankkontti og helbreds-oplysninger, er en ret for det enkelte individ. For den offentlige sektor og erhvervslivet strækker truslen sig fra økonomisk spionage til mulig modificering af interne eller offentlige data, herunder ødelæggelse af websteder.

Mulige løsninger – De mest almindelige beskyttelsesmetoder mod uautoriseret adgang er brug af adgangskoder og installation af 'firewalls'. Dette giver imidlertid kun begrænset beskyttelse og må suppleres med andre sikkerhedsforanstaltninger, såsom angrebsgenkendelse, opdagelse af indtrængningsforsøg og kontrolforanstaltninger på applikationsniveau (bl.a. ved hjælp af smartkort). Disse kontrolforanstaltningers effektivitet afhænger af, om deres funktionalitet er indrettet efter de risici, der er i et bestemt miljø. Der skal opnås en balance mellem beskyttelse af nettet og fordelene ved fri adgang. På grund af den hastige udvikling og deraf følgende nye trusler mod nettene er der behov for en løbende uafhængig revurdering af netsikkerhedskontrollen. Så længe brugere og udbydere ikke er



fuldt opmærksomme på deres nets sårbarhed, vil en række mulige løsninger fortsat ligge uudforskede hen. Ovenstående figur viser en oversigt over brugne af sikkerhedsprodukter i EU (de statistiske oplysninger er baseret på en undersøgelse, der blev gennemført i februar 2001 som led i benchmarkingaktiviteterne under *e*Europe 2002).

2.2.3. Netdriftsforstyrrelser

Nettene er i dag overvejende digitale og edb-styrede. En almindelig årsag til netdrifts-forstyrrelser var før i tiden svigt i det computersystem, der styrer nettet, og angreb på nettene var i de fleste tilfælde rettet mod disse computere. I dag er tendensen, at de fleste angreb udnytter svagheder i netkomponenterne (operativsystemer, routere, omkoblere, navneservere osv.).

Mens forstyrrende angreb på telefonnettet ikke har været noget større problem, er angreb på Internettet ret almindelige. Årsagen er, at styresignalerne i telefonnettet er adskilt fra selve trafikken og kan beskyttes, mens det på Internettet er muligt for brugerne at nå de centrale computere, der styrer trafikken. Men telefonnettet kan blive mere sårbart fremover, efterhånden som der integreres centrale elementer fra Internettet, og styreniveauet i telefonnettet bliver tilgængelige for andre.

Angrebene kan antage forskellige former:

- **Angreb på navneservere**: Internettet er afhængigt af domænenavnssystemet (DNS), der oversætter brugervenlige navne (f.eks. www.europa.eu.int) til abstrakte netadresser (f.eks. IP nr. 147.67.36.16) og omvendt. Hvis en del af domænenavnssystemet svigter, er der nogle websteder, der ikke kan lokaliseres, og e-mail-leveringen holder måske op med at fungere. Hvis der opstår fejl i domænenavnssystemets rodservere eller andre navneservere på højt niveau, kan det medføre omfattende forstyrrelser i netdriften. Tidligere i år opdagede man en række svage punkter i det software, der styrer de fleste navneservere[7].

- **Angreb på routere**: Dirigering af trafikken (routing) på Internettet er stærkt decentraliseret. Hver router informerer med jævne mellemrum naborouterne om, hvilke net den kender, og hvordan de nås. Svagheden er, at disse oplysninger ikke kan verificeres, fordi systemet er udformet således, at hver routers viden om nettopologien er minimal. Derfor kan enhver router præsentere sig som den bedste vej til et hvilket som helst mål, og på denne måde opfange, blokere for eller ændre trafik til dette mål.

- **Overbelastnings- og "denial of service"-angreb**: Denne form for angreb består i at forstyrre netdriften ved at overbelaste nettet med uægte meddelelser og således blokere for eller begrænse den legitime brug af nettet. Det svarer til, at en faxmaskine blokeres af lange meddelelser, der sendes igen og igen. Ved overbelastningsangreb forsøger man at overbelaste webservere eller internetudbydernes behandlingskapacitet med automatisk genererede meddelelser.

Mulig skade - Afbrydelser i driften har anrettet store skader for visse højtprofilerede websteder. Undersøgelser har vist, at skaderne som følge af et angreb for nylig løb op i flere hundrede millioner euro, ud over den uhåndgribelige skade på omdømmet. Virksomhederne bruger i stigende grad deres websteder til forretningsformål, og de selskaber, der er afhængige af deres websted som kanal for 'just-in-time'-levering, er særligt sårbare.

Mulige løsninger - Angreb på DNS-servere er i princippet nemme at forebygge ved at udvide DNS-protokollerne, f.eks. ved at anvende sikre DNS-tillægsfunktioner baseret på kryptering med offentlig nøgle. Dette kræver imidlertid, at der installeres ny software på klientmaskinerne, og denne løsning har ikke stor udbredelse. Desuden må den administrative proces, der er nødvendig for at øge tilliden mellem DNS-domænerne, effektiviseres.

Angreb på rutningssystemet er meget sværere at forebygge. Internettet blev udformet med det formål at skabe størst mulig fleksibilitet i dirigeringen af trafikken, da man derved mindsker risikoen for, at forbindelsen svigter, hvis en del af infrastrukturen bryder sammen. Der findes ingen effektive midler til at sikre rutningsprotokollerne, navnlig ikke på backbonerouterne.

---

[7] Kilde: CERT/CC, se: http://www.cert.org/advisories/CA-2001-02.html

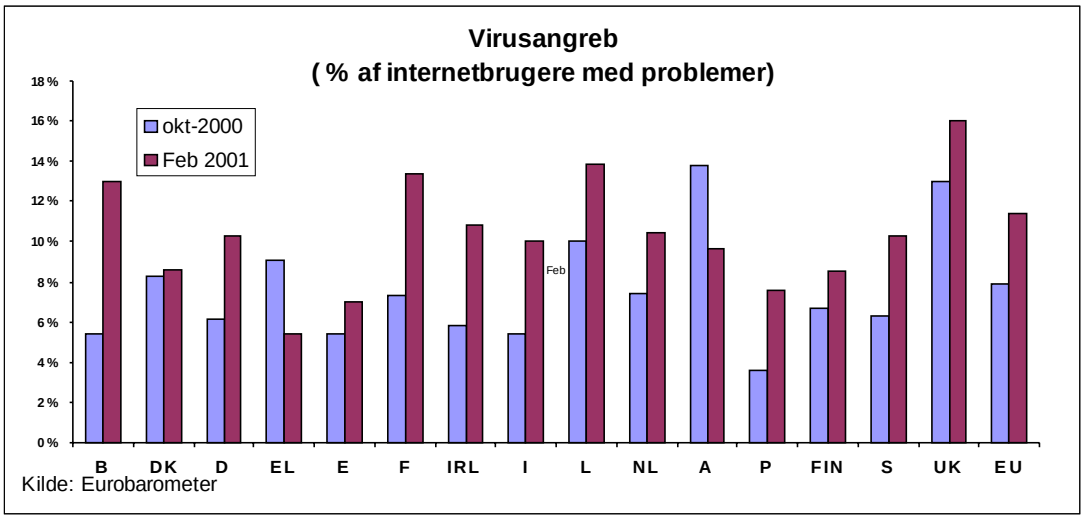
Mængden af data, der sendes, gør det umuligt at gennemføre en detaljeret filtrering, da en sådan kontrol ville sætte trafikken helt i stå. Derfor gennemføres der kun grundlæggende filtrerings- og adgangskontrolfunktioner på nettene, mens de mere specifikke sikkerhedsfunktioner (f.eks. autentificering, integritetskontrol, kryptering) er placeret ved nettenes grænser, dvs. på de terminaler og netservere, der fungerer som endepunkter.

2.2.4. Hærværkssoftware, der ændrer eller ødelægger data

Computere fungerer ved hjælp af software. Uheldigvis kan software også bruges til at sætte en computer ud af drift og til at slette eller ændre data. Som ovenstående beskrivelse viser, kan det have vidtrækkende følger, hvis der opstår fejl i en computer, der er en del af netstyringssystemet. Et eksempel på hærværkssoftware er et virusprogram. Det er et program, der reproducerer sin egen programkode ved at knytte sig til andre programmer på en sådan måde, at virusprogrammet gennemføres, når det inficerede program gennemføres.

Der er forskellige andre typer hærværkssoftware: Nogle skader kun den computer, som softwaren kopieres over på, andre spreder sig til andre computere på nettet. En ofte anvendt type er programmer (kaldet 'logiske bomber'), der ligger i dvale, indtil de sættes i gang af en bestemt hændelse eller på en bestemt dag, f.eks. fredag den 13. Andre programmer lader til at være godartede, men når de åbnes, lancerer de et hærværksangreb (derfor kaldes de 'trojanske heste'). Atter andre programmer (kaldet 'orme') inficerer ikke andre programmer sådan som en virus, men laver i stedet kopier af sig selv, der igen laver kopier af sig selv, så systemet til sidst oversvømmes.

Mulig skade - Virus kan være meget ødelæggende, som det illustreres af de høje omkostninger i forbindelse med en række angreb i den senere tid (f.eks. 'I Love you', 'Melissa og 'Kournikova'). Nedenstående figur viser en oversigt over stigningen i virusangreb, som internetbrugerne i EU har været udsat for fra oktober 2000 til februar 2001 (pr. medlemsstat). I gennemsnit har ca. 11% af internetbrugerne i Europa oplevet en



virusinfektion på deres hjemme-pc.

Mulige løsninger - Det vigtigste forsvar er anti-virus-software, der findes i forskellige former. Der er f.eks. virus-scannere og desinficeringsprogrammer, der finder frem til og sletter kendte virus. Deres største svaghed er, at de - selv når de opdateres jævnligt - ikke altid opdager nye virus. Et andet eksempel på et forsvar mod virus er et integritetskontrolprogram.

For at inficere en computer må en virus ændre noget i systemet. Ved integritetskontrollen skulle disse ændringer kunne opdages, også selv om de er forårsaget af en ukendt virus.

På trods af de forholdsvis veludviklede forsvarsprodukter er problemerne med hærværkssoftware vokset. Det er der to hovedårsager til. For det første gør Internettets åbenhed det muligt for hackere at lære af hinanden og udvikle metoder til at omgå beskyttelsesmekanismerne. For det andet vokser Internettet og når ud til stadig flere brugere, og mange af disse er ikke opmærksomme på, at det er nødvendigt at træffe sikkerhedsforanstaltninger. Sikkerheden afhænger af, hvor udbredt brugen af forsvarssoftware er.

2.2.5. Identitetsforfalskning

Når en bruger etablerer en netforbindelse eller modtager data, gør han sig antagelse om kommunikationspartnerens identitet på basis af kommunikationssammenhængen. Nettet giver visse indikationer, men den største risiko for angreb stammer fra folk, der kender sammenhængen, dvs. insidere. Når brugerne drejer et nummer eller indtaster en internetadresse på computeren, kan de normalt gå ud fra, at de når det forventede mål. Dette er tilstrækkeligt for mange applikationer, men ikke for vigtige forretnings- og finanstransaktioner og medicinske og officielle formål, hvor der kræves et højere niveau af autentificering, integritet og fortrolighed.

Mulig skade - Forfalskning af personers eller enheders identitet kan forårsage skade på forskellig vis. Kunder risikerer at downloade hærværkssoftware fra et websted, der giver sig ud for en pålidelig kilde. Eller de overdrager måske fortrolige oplysninger til den forkerte person. Identitetsforfalskning kan også betyde, at kontrakter og lignende ikke anerkendes. Måske er det største problem, at manglen på autentificering hæmmer forretningsaktiviteterne via nettet. Mange undersøgelser fremhæver sikkerhedsbekymringer som hovedårsagen til ikke at gøre forretninger via Internet. Hvis brugerne kunne være sikre på, at deres kommunikationspartner er den, han giver sig ud for at være, ville tilliden til transaktioner via Internettet vokse.

Mulige løsninger - Forsøg på at indføre autentificering i nettene i forbindelse med indførelsen af SSL har allerede vist, at dette er en nyttig metode til at sikre en vis grad af fortrolighed. Virtuelle privatnet (VPN) bruger SSL og IPsec til at muliggøre kommunikation via ubeskyttede internetforbindelser og åbne kanaler, idet der opretholdes et givet sikkerhedsniveau. Disse løsninger har dog begrænset nytte, da de er baseret på elektroniske certifikater, og der er ingen garanti for, at disse ikke er forfalskede. En tredjepart, der ofte omtales som 'certificeringsmyndighed' eller i direktivet om elektroniske signaturer[8] 'certificeringstjenesteudbyder', kan tilbyde en sådan garanti. Hindringerne for udbredelsen af denne løsning er de samme som i forbindelse med kryptering: behovet for interoperabilitet og forvaltning af nøgler. I et VPN er dette ikke et problem, da der kan udvikles leverandørspecifikke løsninger, men i offentlige net er det en væsentlig hindring.

Direktivet om elektroniske signaturer styrker retsgrundlaget for at lette brugen af elektronisk autentifikation i EU. Direktivet fastlægger rammer, inden for hvilke markedet kan udvikle sig frit, men som også skaber et incitament til at udvikle mere sikre signaturer med henblik på retlig anerkendelse. Medlemsstaterne er i gang med at omsætte direktivet i national ret.

---

[8] Direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer (EFT L 13 af 19.1.2000, s. 12).

2.2.6. Naturkatastrofer og utilsigtede hændelser

Mange sikkerhedsproblemer skyldes uforudsete og utilsigtede hændelser forårsaget af:

- naturkatastrofer (f.eks. storme, oversvømmelser, brande, jordskælv)
- tredjeparter uden noget kontraktligt forhold til operatøren eller brugeren (f.eks. driftsafbrydelser pga. bygge- og anlægsarbejde)
- tredjeparter med et kontraktligt forhold til operatøren eller brugeren (f.eks. hardware- eller softwarefejl i leverede komponenter eller programmer)
- menneskelige fejl eller mangelfuld indsats fra operatørens/tjenesteudbyderens eller brugerens side (f.eks. netstyringsproblemer, ukorrekt installation af software).

Mulig skade: Naturkatastrofer medfører forstyrrelser i netdriften. Uheldigvis er det under sådanne omstændigheder, at der er allermest brug for fungerende kommunikationslinjer. Hardwarefejl og dårligt softwaredesign kan skabe svagheder, der enten umiddelbart medfører netdriftsforstyrrelser eller udnyttes af angribere. Dårlig forvaltning af netkapaciteten kan føre til trafikpropper, med heraf følgende forsinkelser og forstyrrelser i kommunikationskanalerne.

Et centralt spørgsmål i den forbindelse er, hvordan erstatningsansvaret fordeles mellem parterne. I de fleste tilfælde er brugerne uden ansvar for skaden, men har muligvis kun ringe eller slet ingen mulighed for at rejse erstatningskrav.

Mulige løsninger: Risikoen for utilsigtede hændelser er velkendte for telenetoperatørerne, og de har indbygget overskudskapacitet og infrastrukturbeskyttelsesforanstaltninger i deres net. Den øgede konkurrence har muligvis både en negativ og en positiv effekt på operatørernes adfærd. På den ene side kan prishensyn drive operatørerne til at reducere deres overskudskapacitet. På den anden side betyder den omstændighed, at der er flere operatører på markedet som følge af liberaliseringen, at brugerne kan skifte til en anden operatørs net, hvis deres "egen" operatørs net er ude af drift (på samme måde som flypassagerer overflyttes til et andet luftfartsselskab, når en flyafgang aflyses). Ifølge gældende EU-lovgivning er medlemsstaterne forpligtet til at sikre, at de offentlige net er disponible i tilfælde af katastrofale netsammenbrud eller naturkatastrofer (jf. samtrafikdirektivet, 97/33/EF[9], og taletelefonidirektivet, 98/10/EF[10]). Generelt er der for lidt kendskab til, hvordan det stigende antal indbyrdes forbundne net påvirker sikkerhedsniveauet.

Konkurrencen blandt hardware- og softwareleverandører burde presse leverandørerne til at forbedre sikkerheden i deres produkter. Men konkurrencen er ikke stærk nok til at drive sikkerhedsinvesteringerne op, og sikkerhed er ikke altid det centrale element i køberens beslutning. Svagheder i sikkerheden opdages ofte for sent - når skaden allerede er sket. Det er vigtigt at opretholde en fair konkurrence på markederne for informationsteknologi for at skabe bedre sikkerhedsvilkår.

Risikoen for menneskelige fejl og betjeningsfejl kan reduceres gennem bedre uddannelse og øget oplysning. Ved at udforme en hensigtsmæssig sikkerhedspolitik på virksomhedsplan kan man også nedbringe risikoen.

---

9 EFT L 199 af 26.7.1997.

10 EFT L 101 af 1.4.1998.

2.3 Nye udfordringer

Net- og informationssikkerhed bliver sandsynligvis en nøglefaktor i udviklingen af informationssamfundet, efterhånden som brugen af net kommer til at spille en større og større rolle i det økonomiske og sociale liv. Der er to hovedaspekter at drøfte: Den stigende risiko for skader og udviklingen af ny teknologi.

i. Net- og informationssystemer indeholder flere og flere **følsomme data og økonomisk værdifulde oplysninger,** og dette øger incitamentet til angreb. Forstyrrelserne kan være af mindre grad og ubetydelige på nationalt plan, f.eks. når et personligt websted bliver ødelagt eller en harddisk bliver reformateret af en virus. Men der kan også ske forstyrrelser på en langt mere kritisk skala, f.eks. indgreb i stærkt følsom kommunikation, alvorlige strømafbrydelser eller større forretningstab som følge af overbelastningsangreb eller brud på fortroligheden.

   Det er svært at bedømme, nøjagtig hvor stort omfanget af de faktiske og potentielle skader som følge af brud på netsikkerheden er. Det er ikke noget system til systematisk rapportering af skader, og mange selskaber foretrækker at fortie de angreb, de udsættes for, af frygt for negativ omtale. Derfor er den eksisterende dokumentation hovedsagelig af anekdotisk karakter. Omkostningerne som følge af et angreb omfatter ikke blot de direkte omkostninger (indtægtstab, tab af værdifulde oplysninger, omkostninger til genoprettelse af nettet), men også mange uhåndgribelige omkostninger - særlig i form af tab af omdømme - der er vanskelige at sætte tal på.

ii. **Net- og informationssikkerhed er et dynamisk spørgsmål**. Tempoet i den teknologiske udvikling betyder, at der hele tiden opstår nye udfordringer - tidligere problemer forsvinder, og de eksisterende løsninger bliver meningsløse. Markedet byder næsten dagligt på nye applikationer, tjenesteydelser og produkter. Der er dog visse tendenser i udviklingen, der klart udgør en betydelig udfordring for sikkerhedsstrategien i både den private og den offentlige sektor:

   - Der vil blive sendt forskellige digitale objekter via nettene såsom multimedieobjekter, software til downloading og mobile agenter med indbyggede sikkerhedsstrategier. Begrebet disponibilitet, der i dag forstås som mulighed for at bruge nettene, vil udvikle sig hen i retning af mulighed for autoriseret brug, f.eks. ret til at benytte et videospil i en vis periode, ret til at tage en enkelt kopi af et softwareprogram osv.

   - I fremtiden vil IP-netoperatørerne måske vælge at øge sikkerheden ved løbende at kontrollere nettrafikken og kun tillade autoriseret trafik. Sådanne tiltag skal imidlertid overholde de gældende databeskyttelsesregler.

   - Brugerne vil gå over til internetforbindelser, der altid er åbne, hvilket øger mulighederne for angribere, gør ubeskyttede terminaler mere sårbare og gør det nemmere for angribere at undgå at blive opdaget.

   - I hjemmene vil der i vid udstrækning blive installeret net, der forbinder mange forskellige apparater. Herved opstår nye angrebsmuligheder, og brugernes sårbarhed øges (f.eks. vil alarmsystemer måske kunne slås fra via nettet).

   - Med indførelsen af trådløse net (f.eks. trådløse abonnentnet, trådløse lokalnet (LAN), tredjegenerationsmobilnet) i stor skala står vi over for den udfordring at

sikre en effektiv kryptering af data, der sendes via radiosignaler. Det bliver derfor stadig mere problematisk at stille lovkrav om svag kryptering af disse signaler.

- Der vil være net og informationssystemer overalt, der kombinerer faste og trådløse forbindelser og tilbyder 'intelligente omgivelser', dvs. selvorganiserende systemer, der fungerer automatisk og træffer beslutninger, der tidligere blev truffet af brugeren. Udfordringen består i at undgå uacceptable svagheder og integrere sikkerhedsløsninger i systemarkitekturen.

3. En europæisk strategi

3.1. Grundlaget for en offentlig politik

At beskytte kommunikationsnettene betragtes i stigende grad som en særlig vigtig opgave for beslutningstagerne, hovedsagelig på grund af kravet om databeskyttelse, behovet for at sikre en velfungerende økonomi, hensynet til den nationale sikkerhed og ønsket om at fremme e-handelen. Det har medført omfattende retlige sikkerhedsforanstaltninger i EU-direktiverne om databeskyttelse og i EU-lovrammerne for telekommunikation (som det fremgår af afsnit 3.6). Disse foranstaltninger skal imidlertid anvendes i et hurtigt skiftende miljø med nye teknologier, konkurrence på markedet, sammenvoksende net og globalisering. Og dertil kommer det problem, at markedet har tendens til at underinvestere i sikkerhed af en række årsager, der analyseres nedenfor.

Net- og informationssikkerhed er en handelsvare, der købes og sælges på markedet, og en del af den kontraktlige aftale mellem parterne. Markedet for sikkerhedsprodukter er vokset betydeligt i de senere år. Ifølge undersøgelser var markedet for internetsikkerhedssoftware verden over ca. $4,4 mia. værd ved udgangen af 1999[11], og det vil vokse med 23 % om året, så det når op på $8,3 mia. i 2004. I Europa forventes markedet for sikkerhed i elektronisk kommunikation at vokse fra $465 mio. i 2000 til $5,3 mia. i 2006[12], mens markedet for IT-sikkerhed forventes at vokse fra $490 mio. i 1999 til $2,74 mia. i 2006[13].

Normalt antages det stiltiende, at prismekanismen vil sørge for, at omkostningerne ved at yde sikkerhed afbalanceres over for det konkrete sikkerhedsbehov. Visse brugere vil kræve høj sikkerhed, mens andre vil være tilfredse med et lavere niveau – om end staten måske sørger for, at der tilvejebringes et minimum af sikkerhed. Brugernes ønsker vil afspejles af den pris, de er villige til at betale for sikkerhedsfunktioner. Imidlertid er mange sikkerhedsrisici – som det fremgår af analysen i kapitel 2 – fortsat uløste, eller løsningerne slår kun langsomt igennem på markedet på grund af visse ufuldkommenheder på markedet:

i) **Samfundsmæssige omkostninger og fordele:** Investering i øget netsikkerhed genererer samfundsmæssige omkostninger og fordele, der ikke afspejles tilstrækkeligt i markedspriserne. **På omkostningssiden** drages markedsaktørerne ikke til ansvar for alle aspekter af deres sikkerhedsadfærd. Brugere og udbydere med et lavt sikkerhedsniveau skal ikke betale erstatning til tredjeparter. Det svarer til, at en skødesløs bilist ikke drages til ansvar for omkostningerne ved en trafikprop, der opstår som følge af en ulykke, bilisten har forårsaget. På samme måde er adskillige angreb på Internettet blevet iværksat

---

11 IDC: Internet security market forecast and analysis, 2000-2004 Report #W23056 - oktober 2000

12 Frost&Sullivan: The European Internet communication security markets, rapport 3717 - november 2000

13 Frost&Sullivan: The European Internet system security markets, rapport 3847 - juli 2000

via skødesløse brugeres dårligt beskyttede maskiner. **Sikkerhedsfordelene afspejles heller ikke fuldt ud i markedspriserne**. Når operatører, leverandører eller tjenesteudbydere forbedrer sikkerheden i deres produkter, kommer en stor del af udbyttet af denne investering ikke blot deres kunder til gode, men også alle dem, der direkte eller indirekte påvirkes af elektronisk kommunikation – dvs. stort set hele økonomien.

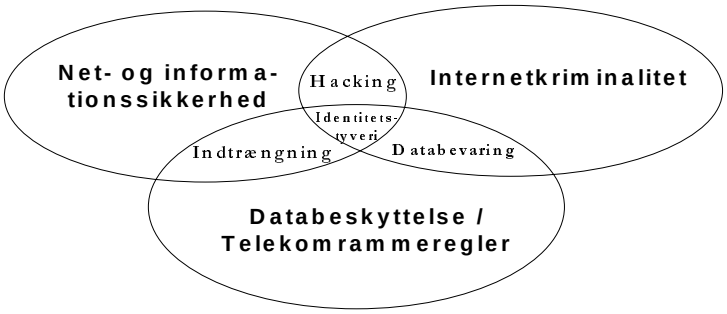
ii) **Informationsasymmetri:** Nettene bliver mere og mere komplekse og når et bredere marked, der omfatter mange brugere med ringe kendskab til teknologien og de mulige farer. Det betyder, at brugerne ikke er fuldt klar over alle sikkerhedstruslerne, og mange operatører, leverandører og tjenesteudbydere har svært ved at bedømme, hvilke svagheder der er, og hvor udbredte de er. Mange nye tjenester, applikationer og programmer tilbyder attraktive faciliteter, men ofte er disse en kilde til nye svagheder (f.eks. skyldes World Wide Web's succes delvis det brede udvalg af multimedieapplikationer, der nemt kan downloades, men 'plug-ins' er samtidig en indfaldsvej for angreb). Mens fordelene er synlige, er risikoen det ikke, og der er flere incitamenter for leverandørerne til at tilbyde nye produkter end større sikkerhed.

iii) **Problemet med offentlig handling:** Operatørerne indfører i stigende grad internetstandarder eller forbinder på en eller anden måde deres net med Internettet. Internettet blev imidlertid ikke udformet med tanke på sikkerheden, men blev derimod udviklet for at sikre adgang til information og lette udveksling af information. Dette har været grundlaget for dets succes. Internettet er blevet et globalt net af net, der repræsenterer en rigdom og mangfoldighed, som ikke kender nogen lige. At investere i sikkerhed kan ofte kun betale sig, hvis tilstrækkelig mange mennesker gør det samme. Derfor er det nødvendigt at **samarbejde** for at skabe sikkerhedsløsninger. Men samarbejde fungerer kun, hvis der er en kritisk masse af aktører, der deltager, og dette er vanskeligt at opnå, eftersom der kan tjenes penge ved at 'køre frihjul'. Interoperabilitet mellem produkter og tjenester skaber mulighed for konkurrence mellem sikkerhedsløsninger. Men det indebærer betydelige koordineringsomkostninger, hvis der skal findes globale løsninger, og nogle aktører fristes til at påtvinge markedet lukkede, leverandørspecifikke løsninger. Da et væld af produkter og tjenester stadig bruger leverandørspecifikke løsninger, er der ingen fordel ved at bruge sikre standarder, der kun giver ekstra sikkerhed, hvis alle andre også tilbyder dem.

For at råde bod på disse ufuldkommenheder har man i lovrammerne for telekommunikation og databeskyttelse allerede indført retlige forpligtelser for operatører og tjenesteudbydere til at sikre et vist niveau af sikkerhed i kommunikations- og informationssystemer. Grundlaget for en europæisk strategi for net- og informationssikkerhed kan beskrives som følger: For det første må de retlige bestemmelser på EU-plan anvendes effektivt, hvilket kræver en **fælles forståelse af de bagvedliggende sikkerhedsspørgsmål og de specifikke foranstaltninger der skal træffes.** Lovrammerne må også videreudvikles fremover, således som der allerede er taget skridt til med forslaget til et nyt regelsæt for elektroniske kommunikation og de kommende forslag i forbindelse med drøftelserne om internetkriminalitet. For det andet må man drage den konklusion, at markedskræfterne ikke sikrer tilstrækkelige investeringer i sikkerhedsteknologi og –praksis. **Politiske tiltag kan styrke markedsprocessen og samtidig bidrage til, at lovrammerne kommer til at fungere bedre.** Endelig må der tages hensyn til, at kommunikations- og informationstjenester udbydes på tværs af grænserne. Derfor har vi brug for en europæisk strategi for at **skabe et indre marked for sådanne tjenester, så vi kan drage fordel af fælles løsninger og handle effektivt på globalt plan**.

De politiske tiltag, der foreslås vedrørende net- informationssikkerhed, skal ses ikke blot i sammenhæng med den eksisterende lovgivning om telekommunikation og databeskyttelse,

men også med de politiske tiltag af nyere dato med hensyn til internetkriminalitet. Kommissionen har for nylig offentliggjort en meddelelse om internetkriminalitet[14], hvoraf det fremgår, at man bl.a. påtænker at oprette et EU-forum for internetkriminalitet med det formål at øge den gensidige forståelse og samarbejdet på EU-plan mellem alle berørte parter. En strategi for net- og informationssikkerhed vil udgøre det manglende led i de politiske rammer. Følgende diagram viser de tre politikområder og illustrerer med nogle eksempler, hvordan de er forbundet med hinanden:



3.2. Oplysning

For mange brugere er stadig ikke klar over, hvilke risici de løber, når de bruger kommunikationsnet, eller hvilke løsninger der allerede eksisterer for at imødegå truslerne. Sikkerhedsproblemerne er komplekse, og det er ofte vanskeligt at vurdere risikoen, selv for eksperter. Mangel på information er en af de ufuldkommenheder på markedet, som sikkerhedsstrategien bør tage op. Der er risiko for, at nogle brugere lader sig afskrække af de mange rapporter om sikkerhedstruslerne og simpelthen vælger helt at undgå elektronisk handel. Andre, der enten er uvidende om problemerne eller undervurderer risikoen, bliver måske for skødesløse. Nogle virksomheder vil måske underdrive den mulige risiko for ikke at miste kunder.

Paradoksalt nok er der en enorm mængde information om net- og informationssikkerhed til rådighed på Internet, og IT-tidsskrifterne dækker også dette spørgsmål i vid udstrækning. Problemet for brugerne er at finde relevante oplysninger, der er forståelige, ajourførte og som opfylder deres behov. Automobilindustrien er et godt eksempel på, hvordan komplekse sikkerhedsspecifikationer kan forvandles til et vigtigt markedsføringsaktiv. Endelig er udbyderne af offentligt tilgængelige teletjenester ifølge EU-lovgivningen forpligtet til at informere deres abonnenter om særlige risici for brud på netsikkerheden samt om, hvordan sådanne brud på nogen måde kan forebygges, herunder om omkostningerne i den forbindelse (jf. artikel 4 i direktiv 97/66/EF).

Målet for en oplysningsindsats over for borgere, offentlige instanser og virksomheder er derfor at levere tilgængelig, neutral og pålidelig information om net- og informationssikkerhed. Der er brug for en åben debat om sikkerhed. Når brugerne forstår

[14] Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet, KOM (2000) 890, http://europa.eu.int/ISPO/eif/internetPoliciesSite/Crime/crime1.html

sikkerhedstruslerne, kan de træffe deres egne valg og finde frem til det beskyttelsesniveau, der passer dem.

Forslag:

- Medlemsstaterne bør lancere en offentlig informations- og uddannelseskampagne, og det igangværende arbejde må forbedres. Indsatsen bør omfatte en kampagne i massemedierne og målrettede tiltag over for alle berørte parter. En veltilrettelagt og effektiv informationskampagne er ikke billig. Det kræver omhyggelig planlægning at udarbejde indhold, der beskriver risikoen uden at gøre folk unødigt bekymrede og give potentielle hackere gode ideer.

  Europa-Kommissionen vil medvirke til udveksling af bedste praksis og sikre et vist niveau af koordinering af de forskellige nationale informationskampagner på EU-plan, navnlig hvad angår indholdet af de oplysninger, der skal formidles. Et element i denne foranstaltning vil være en portal for websteder både på nationalt og europæisk plan. Man kunne også forestille sig, at der skabes forbindelser fra disse portaler til pålidelige websteder hos internationale partnere.

- Medlemsstaterne bør fremme brugen af bedste praksis inden for sikkerhed, baseret på eksisterende midler såsom ISO/IEC 17799 (adfærdskodeks for forvaltning af informationssikkerhed, www.iso.ch). Der bør især sættes ind over for små og mellemstore virksomheder. Kommissionen vil støtte medlemsstaterne i deres bestræbelser.

- Uddannelsessystemerne i medlemsstaterne bør lægge større vægt på kurser, der specielt vedrører sikkerhed. Der bør udformes uddannelsesprogrammer på alle niveauer, og skolernes IT-undervisning bør omfatte sikkerhedstruslerne i åbne net samt effektive løsninger.

  Der skal også være uddannelsesprogrammer for underviserne. Europa-Kommissionen støtter udviklingen af nye moduler til læseplanerne som led i forskningsprogrammet.

3.3. Et europæisk varslings- og informationssystem

Selv om brugerne er opmærksomme på sikkerhedsproblemerne, vil de stadig have behov for at blive advaret om nye trusler. Angribere vil næsten uundgåeligt finde nye svagheder, så de kan omgå de mest avancerede beskyttelsesforanstaltninger. Industrien udvikler løbende nye softwareapplikationer og tjenester, tilbyder øget tjenestekvalitet og gør således Internettet mere attraktivt. Men i denne proces skaber de samtidig utilsigtet nye svagheder og risici.

Selv erfarne netdesignere og sikkerhedseksperter overraskes ofte over opfindsomheden i visse angreb. Derfor er der brug for et varslingssystem, der hurtigt kan advare alle brugere, samt en kilde til hurtig og pålidelig rådgivning om, hvordan man tackler angrebene. Erhvervslivet har desuden brug for en ordning, hvor de kan rapportere om angreb i fortrolighed, så de ikke risikerer at miste offentlighedens tillid. Dette skal suppleres af en mere vidtgående fremsynet sikkerhedsanalyse, der samler det forskellige dokumentationsmateriale og vurderer risikoen ud fra en bredere synsvinkel.

Der er gjort en stor indsats på dette område af offentlige og private IT-alarmtjenester, kaldet "Computer Emergency Response Teams" (CERT) eller lignende organisationer. For eksempel har man i Belgien oprettet et virusalarmsystem, der betyder, at indbyggerne informeres om

nye virustrusler inden for to timer. CERT-tjenesterne fungerer imidlertid forskelligt i de forskellige medlemsstater, hvilket vanskeliggør et samarbejde. De eksisterende alarmtjenester er ikke altid ordentligt udstyret, og deres opgaver er ofte ikke klart defineret. Koordineringen på verdensplan sker gennem CERT/CC, der delvis finansieres af den amerikanske regering, og CERT-tjenesterne i Europa er afhængige af den informationsfrigivelsespolitik, der føres af CERT/CC og andre.

Som følge af disse kompleksiteter har det europæiske samarbejde hidtil været begrænset. Samarbejde er nødvendigt for at sikre en tidlig varsling i hele EU ved hjælp af øjeblikkelig udveksling af information ved de første tegn på angreb i et land. Derfor haster det med at styrke samarbejdet med CERT-systemet i EU. Det første tiltag, der sigter mod at styrke det offentlig-private samarbejde om pålidelighed i informationsinfrastrukturer (herunder udvikling af et varslingssystem) og mod at styrke samarbejdet mellem CERT-tjenesterne, er blevet vedtaget som led i *e*Europe-handlingsplanen.

Forslag:

- Medlemsstaterne bør revurdere deres CERT-systemer og sigte mod at styrke de eksisterende CERT-tjenester, hvad angår udstyr og kompetence. For at støtte tiltagene på nationalt plan vil Europa-Kommissionen udarbejde et konkret forslag om styrket samarbejde i EU. Dette vil omfatte projektforslag under TEN-Telekom-programmet med henblik på at sikre en effektiv brug af nettene, samt ledsageforanstaltninger under IST-programmet for at lette informationsudvekslingen.

- Når der er etableret et CERT-net på EU-plan, bør det forbindes med lignende systemer verden over, f.eks. det planlagte G8-system til rapportering af sikkerhedshændelser.

- Kommissionen påtænker i samarbejde med medlemsstaterne at undersøge, hvordan man bedst på europæisk plan tilrettelægger dataindsamling, analyse og planlægning af fremsynede reaktioner på eksisterende og nye sikkerhedstrusler. Hvilken form en eventuel organisation skal have, er et spørgsmål, der skal drøftes med medlemsstaterne.

3.4. Teknologistøtte

Der investeres for tiden ikke nok i net- og informationssikkerhedsløsninger. Det gælder både ibrugtagning af teknologi og forskning i nye løsninger. I en situation, hvor ny teknologi hele tiden medfører ny risiko, er løbende forskning en nødvendighed.

Net- og informationssikkerhed er allerede et forskningsemne i IST-programmet (informationssamfundets teknologier) under EU's femte forskningsrammeprogram (3,6 mia. EUR over fire år), og der forventes brugt ca. 30 mio. EUR på forskningssamarbejde om sikkerhedsrelateret teknologi i 2001-2002.

Teknisk forskning i kryptering er man nået langt med i Europa. Den belgiske algoritme ved navn 'Rijndael' har vundet en konkurrence om avancerede krypteringsstandarder afholdt af det amerikanske standardiseringsinstitut, NIST. IST-projektet NESSIE (New European Schemes for Signature, Integrity and Encryption) har lanceret en udvidet konkurrence om krypteringsalgoritmer, der opfylder krav i forbindelse med nye multimedieapplikationer, m-handel og smartkort.

Forslag:

- Kommissionen foreslår, at sikkerhedsspørgsmål bliver omfattet af det kommende sjette rammeprogram, som for tiden drøftes i Rådet og Parlamentet. Hvis disse udgifter skal

udnyttes optimalt, bør de knyttes sammen med en bredere strategi for bedre net- og informationssikkerhed. Forskning, der får støtte fra dette program, bør være rettet mod de centrale sikkerhedsproblemer i en "gennemdigitaliseret" verden og nødvendigheden af at sikre enkeltpersoners og persongruppers rettigheder. Den vil fokusere på grundlæggende sikkerhedsmekanismer og disses interoperabilitet, dynamiske sikkerhedsprocesser, avanceret kryptografi, teknik, der forbedrer beskyttelsen af privatlivets fred, teknik til håndtering af digitale aktiver og pålidelighedsfremmende teknik til støtte for erhvervsmæssige og organisatoriske funktioner i dynamiske og mobile systemer.

- Medlemsstaterne bør aktivt fremme brugen af stærke krypteringsprodukter, der er lige til at sætte ind på eksisterende operativsystemer[15]. Sikkerhedsløsninger, der bygger på 'plug in'-kryptering, skal foreligge som alternativ til dem, der er indbygget i operativsystemer.

3.5. Støtte til markedsorienteret standardisering og certificering

Hvis sikkerhedsfremmende løsninger skal være effektive, skal de implementeres i fællesskab af markedets aktører, og det er bedst, hvis de bygger på internationale standarder. En af hovedhindringerne for ibrugtagning af mange sikkerhedsløsninger, f.eks. elektroniske signaturer, har været at der savnes driftskompatibilitet mellem forskellige implementeringer. Ønsker to brugere at kommunikere sikkert mellem forskellige tekniske miljøer, er interoperabilitet en forudsætning. Der bør derfor tilskyndes til brug af standardiserede protokoller og grænseflader, herunder anvendelse af overensstemmelsesprøvning og afholdelse af interoperabilitetsarrangementer. Åbne standarder, der helst skal bygge på programmer med åben kildekode, kan bidrage til både hurtigere afhjælpning af fejl og bedre gennemskuelighed.

Desuden øger evaluering af informationssikkerheden brugernes tryghed. Brugen af fælles kriterier har gjort gensidig anerkendelse lettere som vurderingsmetode i mange lande[16], og disse lande har også aftalt ordninger for gensidig anerkendelse af IT-sikkerhedscertifikater med USA og Canada.

Certificering af forvaltningssystemer for forretningsprocesser og informationssikkerhed får støtte fra det europæiske akkrediteringssamarbejde (EA)[17]. Ved akkreditering af certificeringsorganer øges tilliden til deres kompetence og upartiskhed, og dermed fremmes accepten af deres certifikater på hele det indre marked.

Men certificering er ikke nok; der er også behov for interoperabilitetsprøvning. Et eksempel herpå er European Electronic Signatures Standardisation Initiative (EESSI), som udvikler konsensusløsninger til støtte for EU-direktivet om elektroniske signaturer. Andre eksempler er smartkort-initiativet i *e*Europe og initiativerne til implementering af infrastruktur til offentlige krypteringsnøgler, som er iværksat som led i IDA-programmet om dataudveksling mellem administrationerne.

Det skorter ikke på standardiseringsbestræbelser, men mange konkurrerende standarder og specifikationer resulterer i opsplitning af markedet og løsninger, der ikke kan fungere sammen. Derfor er der behov for bedre samordning af standardiserings- og certificeringsarbejdet og for at holde trit med indførelsen af nye sikkerhedsløsninger. Ved at

---

[15] Kaldes 'pluggable', dvs. at krypteringsprogrammet let kan installeres og gøre fuldt operationelt oven i operativsystemer.

[16] Rådets henstilling 95/144/EF om ensartede kriterier for vurdering af informationsteknologisk sikkerhed (gennemført i de fleste EU-medlemsstater).

[17] European co-operation for Accreditation, et samarbejde mellem organer fra 25 lande i EU, EFTA og kandidatlandene.

harmonisere specifikationerne kan man øge samfunktionsevnen og samtidig give markedsaktørerne mulighed for hurtig implementering.

Forslag:

- De europæiske standardiseringsorganisationer opfordres til at sætte mere fart i arbejdet på at tilvejebringe driftskompatible og sikre produkter og tjenesteydelser og opstille en ambitiøs og fast tidsplan. Om nødvendigt bør der arbejdes med nye former for projektleverancer og nye procedurer for at fremskynde arbejdet og styrke samarbejdet med forbrugerrepræsentanter og øge markedsaktørernes engagement i sagen.

- Kommissionen vil fortsat, navnlig gennem IST- og IDA-programmerne, støtte brugen af elektroniske signaturer, indførelsen af brugervenlige og driftskompatible PKI-løsninger og fortsat udbygning af IPv6 og IPSec[18] (som omhandlet i handlingsplanen *e*Europe 2002).
- Medlemsstaterne opfordres til at fremme brugen af certificerings- og akkrediteringsprocedurer i forbindelse med alment accepterede europæiske og internationale standarder, som fremmer gensidig anerkendelse af certifikater. Kommissionen vil vurdere behovet for et lovgivningsinitiativ om gensidig anerkendelse af certifikater inden udgangen af 2001.
- Aktørerne på det europæiske marked tilskyndes til at deltage mere aktivt i det europæiske (CEN, CENELEC, ETSI) og internationale standardiseringsarbejde (Internet Engineering Task Force (IETF) , World Wide Web Consortium (W3C)).

- Medlemsstaterne bør gennemgå alle relevante sikkerhedsstandarder. Der bør i samarbejde med Kommissionen organiseres konkurrencer om europæiske krypterings- og sikkerhedsløsninger for at stimulere fremkomsten af internationalt aftalte standarder.

3.6. Retsgrundlag

Der er flere retsakter, som har betydning for sikkerheden på kommunikationsnet og i informationssystemer. Det mest omfattende sæt af bestemmelser findes i regelsættet for telekommunikation. Konvergensen mellem forskellige typer net gør, at sikkerhedsproblemerne nu fører regler og reguleringstraditioner fra forskellige sektorer sammen. For det første er der **telekommunikation**ssektoren (omfattende alle kommunikationsnet), der reguleres og liberaliseres på en gang; dernæst er der den stort set uregulerede **computerindustri**[19]; der er **Internettet**, som hovedsagelig har fungeret uden myndighedsindgreb, og der er **e-handel**, som nu mere og mere underkastes specifik regulering. På sikkerhedsområdet er bestemmelser om tredjepartsansvar, cyberkriminalitet, elektroniske signaturer, databeskyttelse og eksportregulering relevante. Af særlig relevans er bestemmelserne i databeskyttelsesdirektiverne, lovrammen for telekommunikation og forskellige lovgivningsinitiativer vedrørende cyberkriminalitet.

Beskyttelse af privatlivets fred er et politisk hovedmål i EU Den er anerkendt som en grundrettighed i den europæiske menneskerettighedskonventions artikel 8[20]. Artikel 7 og 8 i

---

[18] IPv6 er en internetprotokol, der øger antallet af mulige IP-adresser, optimerer trafikdirigeringen og øger mulighederne for udbygning med IPSec. IPSec er en anden internetprotokol, som sigter mod at yde fortrolighed, forhindre pakker i at blive set af andre end modtagerværten og yde autentificering og integritet for at garantere, at dataene i pakken er autentisk og stammer fra den rigtige afsender.

[19] Der stilles mange sikkerhedskrav til computeres elektriske komponenter, men ingen til sikkerheden for de data, computeren behandler.

[20] http://europa.eu.int/comm/internal_market/en/media/dataprot/inter/con10881.htm#HD_NM_15

Den Europæiske Unions charter om grundlæggende rettigheder[21] slår fast, at enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation og til beskyttelse af personoplysninger.

I databeskyttelsesdirektiverne[22], og særlig artikel 5 i direktivet om databeskyttelse på teleområdet[23], forpligtes medlemsstaterne til at sikre kommunikationshemmeligheden i offentlige telenet og offentligt tilgængelige teletjenester. Desuden foreskriver samme direktivs artikel 4 som gennemførelsesmiddel til artikel 5, at leverandører af offentligt tilgængelige telenet og -tjenester skal træffe passende tekniske og organisationsmæssige foranstaltninger for at beskytte deres tjenester. Disse foranstaltninger skal desuden, under hensyn til teknologiens stade og omkostningerne i forbindelse med gennemførelsen, garantere et sikkerhedsniveau, der står i forhold til risikoen. Det betyder, at alle netoperatører har pligt efter loven til at beskytte kommunikation mod ulovlig opfangning. Tjenesternes tværeuropæiske karakter og den øgede konkurrence på tværs af grænserne vil kræve større harmonisering af disse bestemmelser.

I det generelle databeskyttelsesdirektiv, 95/46/EF, kræver artikel 17, at registeransvarlige og registerførere skal træffe foranstaltninger til at tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes, navnlig hvis behandlingen omfatter datatransmission gennem et net. De skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger mod hændelig eller ulovlig tilintetgørelse, mod hændeligt tab, mod forringelse, ubeføjet udbredelse eller ikke-autoriseret adgang, navnlig hvis behandlingen omfatter fremsendelse af oplysninger i et net, samt mod enhver anden form for ulovlig behandling. Disse bestemmelser har betydning for sikkerhedskravene til net og informationssystemer, der bruges af personer og organisationer som f.eks. udbydere af e-handelstjenester. Tjenesternes tværeuropæiske karakter og den øgede konkurrence på tværs af grænserne medfører større behov for specificering af midler til at opfylde disse bestemmelser.

EU's regelsæt for teletjenester indeholder adskillige bestemmelser om 'sikker netdrift' (i den forstand, at nettene skal være til rådighed i nødsituationer) og 'netintegritet' (hvad der skal sikre normal drift af sammenkoblede net)[24]. Kommissionen stillede i juli 2000 forslag om et nyt regelsæt for elektroniske kommunikationstjenester (som nu er på vej gennem den fælles beslutningsprocedure og altså til drøftelse i Europa-Parlamentet og Rådet). I hovedsagen genoptager kommissionsforslaget de eksisterende bestemmelser om netsikkerhed og -integritet, om end med visse ændringer.

Ud over de specifikke emner, som hver af retsakterne omhandler, retter den eksisterende lovramme sig også mod visse aspekter af net og informationssystemer, som tages op i denne meddelelse.

Meddelelsen om internetkriminalitet har udløst debat i EU om, hvordan man skal reagere på kriminel aktivitet, der udøves ved hjælp af computere og elektroniske net. Debatten vil blive videreført mellem alle berørte parter i det EU-forum, der skal etableres inden længe som annonceret i Kommissionens meddelelse om internetkriminalitet. Medlemsstaternes strafferet

---

21 EFT C 364 af 18.12.2000, http://ue.eu.int/df/default.asp?lang=da

22 Direktiv 95/46/EF (EFT L 281 af 23.11.1995), Direktiv 97/66/EF (EFT L 24 af 30.01.1998) http://europa.eu.int/ISPO/infosoc/telecompolicy/en/9766en.pdf

23 'Medlemsstaterne sikrer via nationale forskrifter telekommunikationshemmeligheden ved brug af offentlige telenet og offentligt tilgængelige teletjenester. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge loven, jf. artikel 14, stk. 1.'.

24 Kommissionens liberaliseringsdirektiv 90/388/EF, samtrafikdirektivet 97/33/EF og taletelefonidirektivet 98/10/EF.

bør omfatte ubeføjet indtrængen i edb-net, herunder krænkelse af beskyttede persondata. Der er ikke i øjeblikket nogen indbyrdes tilnærmelse af strafferetlige bestemmelser i EU på dette område. Dette kan give problemer i efterforskningen af sådanne forbrydelser, og det betyder, at den afskrækkende virkning på potentielle hackere og lignende bliver svag. Også af hensyn til det retlige samarbejde mellem medlemsstaterne er en indbyrdes tilnærmelse af strafferetlige bestemmelser om indbrud i edb-net vigtig.

Den berettigede uro over for internetkriminalitet kræver, at man kan gennemføre effektiv retshåndhævende efterforskning. Men disse retlige betænkeligheder bør ikke give anledning til løsninger, hvor retlige krav svækker kommunikations- og informationssystemernes sikkerhed.

Forslag:

- Der er behov for, at man når frem til en fælles forståelse af, hvad sikkerhed inden for elektronisk kommunikation indebærer i retlig henseende. Derfor vil Kommissionen opstille en oversigt over de nationale foranstaltninger, der er truffet i overensstemmelse med relevante EF-bestemmelser.
- Medlemsstaterne og Kommissionen bør fortsat støtte fri omsætning af krypteringsprodukter og -tjenester gennem tættere harmonisering af de administrative eksportprocedurer og yderligere lempelse af eksportkontrollen.
- Kommissionen vil stille et retsaktsforslag i medfør af EU-traktatens afsnit VI om indbyrdes tilnærmelse af nationale strafferetsregler om angreb på edb-systemer, herunder hacking og 'ude af drift'-angreb (denial of service attacks).

3.7. Sikkerhed i offentlige instanser

Handlingsplanen *e*Europe 2002 skal effektivisere samspillet mellem borgere og myndigheder. Hvis det mål skal nås, kræves der stærke sikkerhedsforholdsregler, for megen af den information der udveksles mellem borgere og den offentlige forvaltning er personlig og fortrolig (lægelige, økonomiske, juridiske forhold osv.) Dertil kommer, at udviklingen af elektronisk forvaltning både gør myndighederne til potentielle **forbilleder, når de demonstrerer effektive og sikre løsninger**, og til markedsaktører, der **kan påvirke udviklingen gennem deres indkøbsbeslutninger**.

For disse myndigheder gælder det ikke kun om at etablere informations- og kommunikationsteknologiske systemer, der opfylder krav til sikkerhed, men også om at udvikle en sikkerhedskultur i organisationen. Det kan gøres ved at udforme 'organisatoriske sikkerhedsstrategier', der passer til institutionens behov.

Forslag:

- Medlemsstaterne bør sørge for, at effektive og driftskompatible informationssikkerheds-løsninger indgår som et fundamentalt krav i deres aktiviteter vedrørende e-forvaltning og e-udbud.
- Medlemsstaterne bør indføre elektroniske signaturer, når der tilbydes offentlige online-tjenester.
- Som led i arbejdet med e-Kommissionen vil Kommissionen tage en række initiativer til at skærpe sikkerhedskravene til dens egne informations- og kommunikationssystemer.

3.8. Internationalt samarbejde

Ganske som kommunikation via nettene krydser også de dermed følgende sikkerhedsproblemer uden videre grænserne på en brøkdel af et sekund. Et net er kun så

sikkert som dets svageste led, men Europa kan ikke isolere sig fra resten af det globale net. Derfor kræver en løsning af sikkerhedsproblemet internationalt samarbejde.

Europa-Kommissionen medvirker allerede i internationale fora som G8, OECD og FN. Den private sektor arbejder med sikkerhedsspørgsmål i dens internationale organisationer som f.eks. Global Business Dialogue (www.GBDe.org) og Global Internet Project (www.GIP.org). En fortsat dialog mellem disse organisationer har afgørende betydning for den globale sikkerhed.

Forslag:

- Kommissionen vil styrke dialogen med internationale organisationer og partnere om netsikkerhed, herunder navnlig om den stigende afhængighed af elektroniske net.

4. Det videre forløb

I denne meddelelse opridses de strategiske hovedtræk i indsatsen på dette område. Den er kun et første skridt og endnu ikke en endelig handlingsplan for netsikkerhed i Europa. Den indeholder dog forslag til, hvad der kan gøres for at tilrettelægge en ramme for en fælles europæisk strategi. I næste fase skal rammen og forslagene drøftes af medlemsstaterne og Europa-Parlamentet. Det Europæiske Råd kan på mødet i Göteborg den 15.-16. juni udstikke retningslinjer for vejen frem.

Kommissionen foreslår, at der iværksættes en grundig drøftelse med industrien, brugerne og databeskyttelsesmyndighederne om den nærmere praktiske gennemførelse af forslagene. Kommentarer kan sendes til eeurope@cec.eu.int frem til udgangen af august 2001. Denne meddelelse er således en opfordring til interesserede parter om at indsende kommentarer med henblik på den endelige fastlæggelse af konkrete tiltag. Det kunne ske ved udarbejdelse af en køreplan hen mod slutningen af 2001.

***