KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 19.04.2002
KOM(2002) 173 endelig

2002/0086 (CNS)

Forslag til

RÅDETS RAMMEAFGØRELSE

om angreb på informationssystemer

(forelagt af Kommissionen)

BEGRUNDELSE

1. INDLEDNING

Elektroniske kommunikationsnet og informationssystemer udgør nu en vigtig del af EU-borgernes dagligdag og er af afgørende betydning for udviklingen af økonomien i EU. Netværk og informationssystemer smelter sammen og forbindes i stigende grad med hinanden. På trods af de mange indlysende fordele har denne udvikling skabt bekymring for truslen om bevidste angreb på informationssystemer. Sådanne angreb kan antage en lang række former, som f.eks. ulovlig adgang, spredning af skadelige koder og såkaldte "denial of service"-angreb. Man kan starte et angreb fra et hvilket som helst sted på kloden rettet mod et hvilket som helst andet sted når som helst. Der kan blive tale om nye uventede former for angreb i fremtiden.

Angreb på informationssystemer er en trussel mod etableringen af et sikrere informationssamfund og et område med frihed, sikkerhed og retfærdighed og kræver derfor indgriben på EU-plan. En del af Kommissionens bidrag hertil er dette forslag til en rammeafgørelse om indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler om angreb på informationssystemer.

1.1. Forskellige typer angreb på informationssystemer

Ordet "informationssystem" bruges bevidst her i sin bredeste betydning, idet man erkender, at elektroniske netværk og de forskellige systemer, de forbinder, efterhånden smelter sammen. I dette forslag omfatter informationssystemer derfor enkeltstående pc'er, PDA'er, mobiltelefoner, intranet, extranet og naturligvis de netværk, servere og anden infrastruktur, der udgør internettet.

I sin meddelelse Net- og informationssikkerhed: Forslag til en europæisk strategi[1] foreslog Kommissionen følgende beskrivelse af truslerne mod computersystemer:

(a) **Uautoriseret adgang til informationssystemer.** Begrebet omfatter blandt andet **"hacking"**. Hacking betyder uautoriseret adgang til en computer eller et netværk af computere. Det kan ske på en lang række måder, der spænder fra blot at udnytte interne oplysninger til direkte indtrængningsangreb og opsnapning af kodeord. Det sker ofte - men ikke altid - med henblik på at forvolde skade ved at kopiere, ændre eller ødelægge data. Bevidst forvanskning af websteder eller adgang til tjenester, der er beskyttet af adgangsstyring, uden at betale kan være et af målene for den uautoriserede adgang.

(b) **Forstyrrelse af informationssystemer.** Der findes forskellige måder, hvorpå man kan forstyrre informationssystemer ved destruktive angreb. En af de bedst kendte metoder til at blokere for eller forringe de tjenester, der udbydes via internettet, er et såkaldt **"denial of service"**-angreb (DoS). Denne type angreb svarer på en måde til at sende lange, gentagne beskeder til en fax. Ved DoS-angreb forsøger man at overbelaste webservere eller internetudbydere med automatisk genererede

---

[1] Meddelelse fra Kommissionen til Rådet, Europa-Parlamentet, Det Økonomiske og Sociale Udvalg og Regionsudvalget, Net- og informationssikkerhed: Forslag til en europæisk strategi, KOM (2001) 298 endelig, af 6.6.2001.

meddelelser. Af andre typer angreb kan nævnes forstyrrelse af servere, der forvalter domænenavnesystemet (DNS) og angreb mod "routere". Angreb, der skal forstyrre systemer, har været skadelige for visse fremtrædende websteder som f.eks. portaler. Nogle beregninger viser, at et angreb for nylig forrettede skade for flere hundrede millioner euro ud over den uhåndgribelige skade på omdømmet. Virksomhedernes omsætning er i stigende grad afhængig af deres websteder, og dem, der er afhængige af deres websted som kanal for "just in time"-levering, er særligt sårbare.

(c) **Hærværkssoftware, som ændrer eller ødelægger data**. Den bedst kendte form for hærværkssoftware er virus. Af berygtede eksempler kan nævnes "I Love You", "Melissa" og "Kournikova". Ca. 11 % af alle europæiske brugere har haft en virus på deres hjemme-pc. Der findes andre former for hærværkssoftware. Nogle skader selve pc'en, mens andre bruger pc'en til at angribe andre komponenter i netværket. Nogle programmer (som ofte kaldes "logiske bomber") kan ligge i dvale, indtil de udløses af en bestemt hændelse eller på en bestemt dato, hvor de kan forvolde omfattende skade ved at ændre eller slette data. Andre programmer er tilsyneladende godartede, men når de åbnes, udløser de et hærværksangreb (kaldes ofte "trojanske heste"). En anden variant er et program (ofte kaldet en orm), der ikke inficerer andre programmer som en virus, men i stedet kopierer sig selv i en uendelighed, indtil systemet kvæles.

(d) **Opfangning af kommunikation**. Destruktiv opfangning af kommunikation gør det umuligt at opfylde brugernes krav om fortrolighed og integritet. Det kaldes ofte "sniffing".

(e) **Identitetsforfalskning**. Informationssystemer giver nye muligheder for identitetsforfalskning og svindel. Overtagelse af en andens identitet på internettet og destruktiv anvendelse heraf kaldes ofte "spoofing".

1.2. Truslens karakter

Der er et klart behov for at indsamle pålidelige oplysninger om omfanget og karakteren af angreb på informationssystemer.

Nogle af de alvorligste angreb på informationssystemer rettes mod operatører af elektroniske kommunikationsnet og internetudbydere eller mod elektroniske salgsvirksomheder. Mere traditionelle områder kan også blive hårdt ramt på grund af den stadigt stigende interkonnektivitet i det moderne kommunikationsmiljø. Det kan dreje sig om fremstillingsindustrien, serviceindustrien, hospitaler, andre offentlige organer og myndighederne selv. Ofrene for angreb er imidlertid ikke blot organisationer, da angrebene også kan få meget direkte, alvorlige og skadelige følger for enkeltpersoner. Nogle af disse angreb pålægger offentlige organer, virksomheder og enkeltpersoner en væsentlig økonomisk byrde, som truer med at gøre informationssystemer dyrere og dermed forringe brugernes muligheder for at købe dem.

Den type angreb, der er beskrevet ovenfor, udføres ofte af enkeltpersoner, der handler på egen hånd. Der er ofte tale om mindreårige, som måske ikke er helt klar over, hvilke alvorlige følger deres handlinger kan få. Angrebene kan dog blive mere sofistikerede og ambitiøse. Der er stigende bekymring for, at organiserede kriminelle skal bruge kommunikationsnet til at iværksætte angreb mod informationssystemer for at gavne deres egen sag. Organiserede grupper af hackere, som er specialiseret i at hacke sig ind på og ødelægge websteder, bliver mere og mere aktive på verdensplan. Som eksempler kan nævnes Brazilian Silver Lords og

Pakistan Gforce, som søger at presse penge ud af deres ofre ved at tilbyde dem eksperthjælp efter at have hacket sig ind i deres informationssystemer. Anholdelse af store grupper hackere tyder på, at hacking er ved at blive en del af den organiserede kriminalitet. Der er for nylig rettet sofistikerede, organiserede angreb på intellektuel ejendomsret og gjort forsøg på at stjæle større beløb fra netbanker[2].

Brud på sikkerheden i databaser for e-handel, hvor man får adgang til kundeoplysninger, blandt andet kreditkortnumre, er også foruroligende. Denne form for angreb giver større mulighed for bedrageri med betalinger og tvinger under alle omstændigheder banksektoren til at annullere og genudstede tusindvis af kort. En yderligere konsekvens er den uhåndgribelige skade på virksomhedens rygte og forbrugerens manglende tillid til e-handel. Præventive foranstaltninger som minimumssikkerhedskrav for onlinevirksomheder, der modtager kreditkort, drøftes som led i handlingsplanen for at forebygge svig og forfalskning af andre betalingsmidler end kontanter[3].

Dette forslag er også en del af Kommissionens bidrag til imødegåelsen af truslen om et terroristangreb på vitale informationssystemer i EU. Det supplerer Kommissionens forslag om at erstatte udlevering fra et EU-land til et andet med en europæisk arrestordre[4] og om at foretage en tilnærmelse af medlemsstaternes lovgivning om terrorisme[5], som man nåede til politisk enighed om på Det Europæiske Råds møde i Laeken den 14. og 15. december 2001. Sammen vil disse instrumenter sikre, at EU's medlemsstater får effektive strafferetlige regler til at bekæmpe cyberterrorisme, og de vil samtidig styrke det internationale samarbejde om at bekæmpe terrorisme.

Dette forslag vedrører ikke blot handlinger rettet mod medlemsstaterne. Det gælder også handlinger inden for EU rettet mod informationssystemer i tredjelande. Det afspejler Kommissionens engagement i bekæmpelse af angreb på informationssystemer ikke blot i EU, men i hele verden.

I den senere tid har der allerede flere gange været tale om internationale spændinger, som har ført til et væld af angreb på informationssystemer, ofte også på websteder. Mere alvorlige angreb kunne medføre ikke blot alvorlige økonomiske tab, men i visse tilfælde endog tab af menneskeliv (f.eks. hospitalssystemer, kontrol med flytrafik etc.). At medlemsstaterne lægger stor vægt på dette spørgsmål, fremgår af den vigtighed, de tillægger en række initiativer vedrørende beskyttelse af kritisk infrastruktur. F.eks. har man i forbindelse med EU's program for informationssamfundsteknologier (IST)[6] i samarbejde med det amerikanske udenrigsministerium oprettet en fælles EU-USA-taskforce for beskyttelse af kritisk infrastruktur[7].

---

2 Ifølge en undersøgelse offentliggjort af Communications Management Association (CMA) har en tredjedel af alle britiske store virksomheder og organisationer i den offentlige sektor, herunder offentlige myndigheder, været udsat for angreb fra hackere. Skaden varierer fra infiltrering af bankkonti til tyveri af information. Undersøgelsen kan ses på http://www.cma.org

3 Kommissionens meddelelse: Forebyggelse af svig og forfalskning i forbindelse med andre betalingsmidler end kontanter, KOM (2001) 11 endelig. Vedtaget af Kommissionen den 9.2.2001.

4 Forslag til Rådets rammeafgørelse om den europæiske arrestordre og overgivelsesprocedurerne mellem medlemsstater, KOM (2001) 522 endelig. Vedtaget af Kommissionen den 19.9.2001.

5 Forslag til Rådets rammeafgørelse om bekæmpelse af terrorisme, KOM (2001) 521 endelig. Vedtaget af Kommissionen den 19.9.2001.

6 IST-programmet forvaltes af Kommissionen. Det indgår i det femte rammeprogram, der løber fra 1998 til 2002. Yderligere oplysninger kan fås på http://www.cordis.lu/ist

7 Under den fælles rådgivende gruppe nedsat i henhold til samarbejdsaftalen om videnskab og teknologi mellem EU og USA (EC/US Science and Technology Co-operation Agreement).

1.3. Behovet for nøjagtige oplysninger og statistikker

Der findes kun få pålidelige statistikker om det fulde omfang af den it-relaterede kriminalitet. Antallet af krænkelser, der hidtil er opdaget og anmeldt, viser næppe hele problemets omfang. Ifølge en amerikansk undersøgelse[8] var det i 1999 kun 32 % af dem, der havde været udsat for en krænkelse i det foregående år, der anmeldte krænkelsen til politiet. Det var imidlertid en forbedring i forhold til året før, hvor kun 17 % indgav anmeldelse. Der er anført en lang række grunde til ikke at indgive anmeldelse. På grund af begrænset indsigt og erfaring hos systemadministratorer og brugere opdages mange krænkelser ikke. Desuden er mange virksomheder ikke interesserede i at anmelde misbrug af deres computere, fordi de vil undgå dårlig omtale og kommende angreb. Mange politikorps fører endnu ikke statistikker over brug af computere og kommunikationssystemer i forbindelse med denne og andre former for kriminalitet[9]. Politiet mangler den rigtige uddannelse til at opdage, identificere og efterforske it-relaterede lovovertrædelser. EU er imidlertid begyndt at tackle emnet ved at indsamle tal om angreb på informationssystemer. I én medlemsstat anslog man, at der skete mellem 30 000 og 40 000 angreb på informationssystemer i 1999, mens der blot blev registreret 105 officielle anmeldelser på området. I 1999 registrerede syv medlemsstater kun i alt 1 844 officielle anmeldelser af kriminalitet mod informationssystemer og computerdata. Det er dog dobbelt så mange som i 1998, hvor der kun blev registreret 972 tilfælde i de syv medlemsstater[10].

Det fremgår desuden af en ny undersøgelse[11], at 13 % af de virksomheder, der har været udsat for økonomisk kriminalitet, betegner overgrebet som cyberkriminalitet. Undersøgelsen viser også øget bekymring for cyberkriminalitet, idet 43 % af de adspurgte mener, at cyberkriminalitet bliver en risiko i fremtiden. En anden undersøgelse konkluderer, at hackere og virus nu er den største trussel inden for cyberkriminalitet mod organisationer. Af gerningsmændene udgør hackere 45 %, tidligere ansatte 13 %, organiseret kriminalitet 13 % og nuværende ansatte 11 %[12]. Disse tal vil antagelig fortsat vokse i takt med den øgede brug af informationssystemer og den stigende sammensmeltning samt med en større villighed til at anmelde angreb. Det er dog klart, at der er behov for et hurtigt indgreb for at sikre et statistisk værktøj, som alle medlemsstater kan bruge til at måle it-relateret kriminalitet i EU såvel kvantitativt som kvalitativt. Udgangspunktet for en sådan analyse er en fælles EU-definition af de lovovertrædelser, der indgår i angreb på informationssystemer.

1.4. Baggrund for EU-politikken

På grundlag heraf understregede Det Europæiske Råd på sit møde i Lissabon i marts 2000, hvor vigtigt det er at overgå til en konkurrencebaseret, dynamisk og videnbaseret økonomi, og opfordrede Rådet og Kommissionen til at udarbejde en handlingsplan for *e*Europe for at udnytte mulighederne bedst[13]. Denne handlingsplan, der blev udarbejdet af Kommissionen og Rådet og vedtaget på Det Europæiske Råds møde i Feira i juni 2000, indeholder

---

8 Computer Security Institute (CSI) og FBI udgiver i begyndelsen af hvert år en oversigt med titlen "Computer Crime and Security Survey". Der kan hentes yderligere oplysninger om undersøgelsen på CSI's websted http://www.gocsi.com

9 Det italienske indenrigsministerium offentliggjorde for nylig statistikker over deres aktiviteter i kampen mod it-relateret kriminalitet i 1999 og 2000 (http://www.mininterno.it/dip_ps/dcpsffp/index.htm). I 2000 blev der registreret 98 tilfælde af hacking, hvilket er fire gange så mange som i 1999, hvor der kun var 21 officielt registrerede tilfælde.

10 Rådsdokument 8123/01 ENFOPOL 38. Kan findes på Rådets websted http://db.consilium.eu.int/jai

11 European Economic Crime Survey 2001, PricewaterhouseCoopers 2001 (http://www.pwcglobal.com)

12 The Cybercrime Survey 2001, Confederation of British Industry (http://www.pwcglobal.com)

13 Formandskabets konklusioner fra Det Europæiske Råds møde i Lissabon den 23. og 24. marts 2000 kan findes på http://ue.eu.int/en/Info/eurocouncil/index.htm

foranstaltninger for at øge netsikkerheden og udforme en koordineret og sammenhængende strategi til bekæmpelse af cyberkriminalitet inden udgangen af 2002.

Som en del af sit bidrag til opfyldelse af dette mandat inden for cyberkriminalitet offentliggjorde Kommissionen meddelelsen "Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet"[14]. Heri foreslog man en afbalanceret strategi for løsning af problemerne med cyberkriminalitet, hvor man tager fuldt hensyn til alle de implicerede parters mening, herunder politiet, tjenesteydere, netoperatører, andre erhvervsgrupper, forbrugerrepræsentanter, databeskyttelsesmyndigheder og grupper, der kæmper for at bevare privatlivets fred. Kommissionen foreslog en række lovgivningsmæssige og ikke-lovgivningsmæssige initiativer.

Et godt eksempel på en igangværende foranstaltning er Ida-programmet, hvor medlemsstaterne og Kommissionen allerede arbejder på at udarbejde en fælles sikkerhedspolitik og oprette et sikkert netværk til udveksling af administrative oplysninger.

Et af de vigtige spørgsmål, der blev behandlet i meddelelsen, var behovet for en effektiv indsats for at afværge truslerne for autenticiteten, integriteten, fortroligheden og disponibiliteten af informationssystemer og netværk. Der er allerede opnået meget inden for fællesskabsretten. Der er således indført flere retlige foranstaltninger på EU-plan med specifikke implikationer for netværks- og informationssikkerhed.

Denne rammeafgørelse supplerer det, der allerede er opnået inden for EU-retten med hensyn til beskyttelse af informationssystemer, f.eks. direktiv 95/46/EF, 97/66/EF og 98/84/EF om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester. Især indeholder EU's rammebestemmelser for telekommunikations- og databeskyttelse (direktiv 95/46/EF og 97/66/EF[15]) en sikring af, at udbydere af offentligt tilgængelige teletjenester træffer de nødvendige tekniske og organisatoriske foranstaltninger for at beskytte sikkerheden og fortroligheden af deres tjenester, og at disse foranstaltninger garanterer en grad af sikkerhed, der står i forhold til den foreliggende risiko.

En af de vigtigste og mest effektive måder, hvorpå man kan løse disse problemer, er gennem forebyggelse og uddannelse. I meddelelsen understreges vigtigheden af disponibilitet, udvikling, ibrugtagning og effektiv anvendelse af præventiv teknologi. Det understreges, at der er behov for at øge befolkningens bevidsthed om, hvilke risici it-relateret kriminalitet indebærer, for at fremme god praksis med hensyn til it-sikkerhed, for at udvikle effektive redskaber og procedurer til bekæmpelse af it-relateret kriminalitet samt for at tilskynde til videreudvikling af mekanismer til tidlig varsling og krisestyring. EU's program for informationssamfundsteknologier (IST)[16] skaber rammerne om udvikling af evnen og teknologierne til at forstå og imødegå nye udfordringer i forbindelse med it-kriminalitet.

På Det Europæiske Råds møde i Stockholm den 23.-24. marts erkendte man, at der er behov for en yderligere indsats inden for net- og informationssikkerhed og konkluderede: *"Rådet [vil] sammen med Kommissionen udarbejde en samlet sikkerhedsstrategi for elektroniske netværk, herunder praktiske gennemførelsesforanstaltninger. Dette bør forelægges inden Det Europæiske Råd i Göteborg"*. Kommissionen imødekom denne opfordring med sin

---

14 KOM (2000) 890 endelig.

15 EFT L 281 af 23.11.1995, s. 31-50, EFT L 24 af 30.1.1998, s. 1-8.

16 IST-programmet forvaltes af Kommissionen. Det indgår i det femte rammeprogram, der løber fra 1998 til 2002. Yderligere oplysninger kan fås på http://www.cordis.lu/ist

meddelelse Net- og informationssikkerhed: Forslag til en europæisk strategi[17]. Heri analyserede man de nuværende problemer inden for netværkssikkerhed og skitserede en strategi for initiativer på området. Den blev fulgt af en rådsresolution af 6. december 2001 om en fælles fremgangsmåde og specifikke aktioner i forbindelse med net- og informationssikkerhed.

Disse initiativer er ikke i sig selv tilstrækkelige til at afværge alvorlige angreb på informationssystemer. I begge Kommissionens meddelelser erkender man, at der er et presserende behov for indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler om angreb på informationssystemer. Dette fremgår af konklusionerne på Det Europæiske Råds møde i Tammerfors i oktober 1999[18], hvor højteknologikriminalitet nævnes blandt det begrænsede antal områder, hvor man bør søge at nå til enighed om fælles definitioner, fælles regler for, hvad der udgør lovovertrædelser, og fælles straffe. Højteknologikriminalitet nævnes også i henstilling nr. 7 i EU-strategien for begyndelsen af det nye årtusind om forebyggelse og kontrol af organiseret kriminalitet, som Rådet (RIA) vedtog i marts 2000[19]. Dette forslag til rammeafgørelse indgår også i Kommissionens arbejdsprogram for 2001[20] og den resultattavle for oprettelse af et område med frihed, sikkerhed og retfærdighed, som Kommissionen fremlagde den 30. oktober 2001[21].

1.5. Behovet for tilnærmelse af de strafferetlige regler

Medlemsstaternes love på dette område indeholder nogle betydelige lakuner og udviser store forskelle, som kan hæmme bekæmpelsen af organiseret kriminalitet og terrorisme samt enkeltpersoners alvorlige angreb på informationssystemer. Tilnærmelse af den materielle ret inden for højteknologikriminalitet vil sikre, at den nationale lovgivning er tilstrækkeligt omfattende til, at alle former for alvorlige angreb på informationssystemer kan efterforskes ved hjælp af de teknikker og metoder, der kan benyttes inden for strafferetten. Gerningsmændene bag sådanne lovovertrædelser skal udpeges og bringes for en dommer, og domstolene skal kunne benytte passende og forholdsmæssige sanktioner. Det vil have en kraftig afskrækkende virkning for dem, der overvejer angreb på informationssystemer.

Desuden kunne disse lakuner og forskelle virke som en hindring for effektivt politimæssigt og retligt samarbejde i forbindelse med angreb på informationssystemer. Angreb på informationssystemer vil ofte være af grænseoverskridende karakter og kræve internationalt samarbejde mellem politi og retlige myndigheder. En tilnærmelse af lovgivningen vil derfor forbedre dette samarbejde ved at sikre, at kravet om dobbelt strafbarhed er opfyldt (dvs. at en handling skal være strafbar i begge lande, for at gensidig retlig bistand kan ydes i forbindelse med strafferetlig forfølgning). Det vil styrke EU-landene i deres interne samarbejde og samtidig forbedre samarbejdet med tredjelande (hvis der findes en passende aftale om gensidig retlig bistand).

Der er desuden behov for at supplere de eksisterende EU-instrumenter. Rammeafgørelsen om den europæiske arrestordre[22], bilaget til Europol-konventionen[23] og Rådets afgørelse om

---

17 KOM (2001) 298 endelig af 6.6. 2001.

18 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm

19 Forebyggelse og bekæmpelse af organiseret kriminalitet: en EU-strategi for begyndelsen af det nye årtusind (EFT C 124 af 3.5.2000, s. 1).

20 http://europa.eu.int/comm/off/work_programme/index_da.htm

21 http://europa.eu.int/comm/dgs/justice_home/pdf/scoreboard_30oct01_da.pdf

22 EFT C ... s....

oprettelse af Eurojust[24] indeholder alle henvisninger til it-relateret kriminalitet, som skal defineres nærmere. I forbindelse med sådanne instrumenter omfatter it-relateret kriminalitet angreb på informationssystemer, som defineret i denne rammeafgørelse, der vil føre til en langt større grad af tilnærmelse mellem sådanne lovovertrædelsers forskellige bestanddele. Samtidig supplerer denne rammeafgørelse rammeafgørelsen om bekæmpelse af terrorisme[25], der omfatter terroristangreb, som fører til omfattende ødelæggelse af en infrastrukturfacilitet, herunder et informationssystem, der må forventes at bringe menneskeliv i fare eller at medføre store økonomiske tab.

1.6. Anvendelsesområde for og mål med den påtænkte rammeafgørelse

Målsætningerne for denne rammeafgørelse er derfor at foretage en tilnærmelse af medlemsstaternes strafferetlige regler i forbindelse med angreb på informationssystemer og at sikre det størst mulige politimæssige og retlige samarbejde om lovovertrædelser i forbindelse med angreb på informationssystemer. Samtidig indgår dette forslag i EU's bestræbelser for at bekæmpe organiseret kriminalitet og terrorisme. Hensigten er ikke at kræve, at medlemsstaterne skal kriminalisere mindre eller ubetydelige forseelser.

Det fremgår af EU-traktatens artikel 47, at denne rammeafgørelse ikke berører fællesskabsretten. Især berører den ikke fællesskabsrettens bestemmelser om rettigheder og forpligtelser i forbindelse med privatlivets fred eller databeskyttelse, som f.eks. direktiv 95/46 og 97/66. Den skal ikke kræve, at medlemsstaterne skal kriminalisere overtrædelse af regler om adgang til/afgivelse af oplysninger om persondata, fortrolig kommunikation, sikkerhed ved behandling af persondata, elektroniske signaturer[26] eller krænkelse af intellektuel ejendomsret, og den tilsidesætter ikke direktiv 98/84/EF om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester[27]. Der er tale om vigtige emner, men de er allerede omfattet af gældende fællesskabslovgivning. Enhver tilnærmelse af de strafferetlige regler inden for disse områder for at opfylde målsætningerne for fællesskabsretten, f.eks. med hensyn til beskyttelse af persondata, betaling til tjenesteudbydere, der benytter adgangsstyring, eller intellektuel ejendomsret, skal derfor ske på baggrund af fællesskabsretten frem for afsnit VI i EU-traktaten. Derfor er denne rammeafgørelse begrænset til den adfærd, der er beskrevet i afsnit 1.1, punkt (a)-(c).

I forbindelse med lovgivningsinitiativer på EU-plan skal der også tages hensyn til udviklingen i andre internationale fora. Hvad angår tilnærmelse af den materielle strafferet om angreb på informationssystemer, er Europarådet i øjeblikket længst fremme. Europarådet begyndte at forberede en international konvention om cyberkriminalitet i februar 1997. Denne konvention blev formelt vedtaget og åbnet for undertegnelse i november 2001[28]. I konventionen søger man at tilnærme omfanget af lovovertrædelser, herunder krænkelser af computersystemers og -datas fortrolighed, integritet og disponibilitet. Denne rammeafgørelse skal stemme overens

---

23 Rådets retsakt af 26. juli 1995 om udarbejdelse af en konvention på grundlag af artikel K.3 i traktaten om Den Europæiske Union om oprettelse af en europæisk politienhed (Europol-konventionen), EFT C 316 af 27.11.1995, s. 1.

24 EFT C ... s...

25 EFT C ... s...

26 Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer, EFT L 13 af 19.1.2000, s. 12.

27 EFT L 320 af 28.11.1998, s. 54-57.

28 Teksten kan findes på internettet på to sprog, nemlig fransk: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm og engelsk http://conventions.coe.int/treaty/en/projets/cybercrime.htm

med den fremgangsmåde, Europarådet har valgt i sin konvention om sådanne lovovertrædelser.

Under drøftelser af højteknologikriminalitet i G8 har man udpeget to hovedkategorier af trusler. Den første er trusler mod computerinfrastrukturer, som vedrører forsøg på at forstyrre, nægte adgang til, forvanske eller ødelægge data lagret i computere og computernetværk eller selve computerne og netværkene. Den anden er computerstøttede trusler, der vedrører skadelige aktiviteter som svindel, hvidvaskning af penge, børnepornografi, krænkelse af intellektuelle ejendomsrettigheder og narkosmugling, som gøres lettere ved hjælp af en computer. Dette forslag vedrører første kategori af trusler.

Tilnærmelse på EU-plan bør tage hensyn til udviklingen i internationale fora og være i overensstemmelse med nugældende fællesskabspolitikker. Dette forslag søger også at skabe større tilnærmelse i EU, end det har været muligt i andre internationale fora.

2. RETSGRUNDLAG

Målsætningen om at oprette et område med frihed, sikkerhed og retfærdighed skal opfyldes ved at forebygge og bekæmpe organiseret og generel kriminalitet, herunder terrorisme, gennem samarbejde mellem politi og retlige myndigheder i medlemsstaterne og indbyrdes tilnærmelse af medlemsstaternes regler om strafferetlige forhold. Dette forslag til en rammeafgørelse tager derfor sigte på at tilnærme medlemsstaternes love og administrative bestemmelser om strafferetligt samarbejde mellem politi og domstole. Det vedrører mindsteregler for, hvad der udgør en kriminel handling, især inden for organiseret kriminalitet og terrorisme. Det omhandler også "sikring af forenelighed mellem medlemsstaternes gældende regler" for at fremme og fremskynde samarbejde mellem de retlige myndigheder. Det retsgrundlag, der er anført i præamblen til forslaget, er derfor EU-traktatens artikel 29, 30, stk. 1, litra a), 31 og 34, stk. 2, litra b). Forslaget får ingen finansielle virkninger for De Europæiske Fællesskabers budget.

3. RAMMEAFGØRELSEN: ARTIKLERNE

Artikel 1- Rammeafgørelsens anvendelsesområde og mål

I denne artikel hedder det udtrykkelig, at målsætningerne med denne rammeafgørelse er at tilnærme medlemsstaternes strafferetlige regler om alvorlige angreb på informationssystemer, især med henblik på at bidrage til bekæmpelsen af organiseret kriminalitet og terrorisme, og dermed sikre det størst mulige retlige samarbejde om lovovertrædelser i forbindelse med angreb på informationssystemer. I overensstemmelse med EU-traktatens artikel 47 berører denne rammeafgørelse desuden ikke fællesskabsretten. Mere specifikt udelukker dette rettigheder og forpligtelser i forbindelse med privatlivets fred eller databeskyttelse i henhold til direktiv 95/46 og 97/66. Det er ikke tanken, at medlemsstaterne skal kriminalisere overtrædelse af regler om adgang til/afgivelse af oplysninger om persondata, fortrolig kommunikation, sikkerhed ved behandling af persondata, elektroniske signaturer[29] eller

---

[29] Europa-Parlamentets og Rådets direktiv 1999/93/EF af 13. december 1999 om en fællesskabsramme for elektroniske signaturer, EFT L 13 af 19.1.2000, s. 12.

krænkelse af intellektuel ejendomsret, og rammeafgørelsen tilsidesætter ikke direktiv 98/84/EF om retlig beskyttelse af adgangsstyrede og adgangsstyrende tjenester[30].

Denne rammeafgørelse skal ikke tvinge medlemsstaterne til at kriminalisere mindre eller ubetydelige forseelser. I artikel 3 og 4 fastlægges de kriterier, en handling skal opfylde for at blive betragtet som kriminel. Disse kriterier stemmer overens med mulighederne for undtagelser og forbehold i Europarådets udkast til en konvention om cyberkriminalitet.

Alle de lovovertrædelser, der er omhandlet af rammeafgørelsen, skal begås forsætligt. Ordet "forsætlig" bruges eksplicit i artikel 3, 4 og 5. Det skal fortolkes i overensstemmelse med medlemsstaternes normale strafferetlige principper om forsætlighed. Denne rammeafgørelse stiller således ikke krav om kriminalisering af handlinger, hvor der er tale om grov uagtsomhed eller anden form for uforsvarlighed, men ikke om forsætlighed. Et forsæt om at få ulovlig adgang til eller at gribe ind i informationssystemer generelt burde også være tilstrækkeligt. Det skulle ikke være nødvendigt at bevise, at forsættet gjaldt et specifikt informationssystem.

Artikel 2 - Definitioner

Forslaget til Rådets rammeafgørelse indeholder følgende definitioner:

(a) *"Elektronisk kommunikationsnet"*. Denne definition er den samme, som den, Rådet og Europa-Parlamentet vedtog den 14. februar 2002 i direktivet om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester[31].

(b) *"Computer"*. Denne definition er baseret på artikel 1 i udkastet til Europarådets konvention om cyberkriminalitet. Definitionen omfatter f.eks. enkeltstående pc'er, PDA'er, digitale settopbokse, personlige videooptagere og mobiltelefoner (hvis de har visse databehandlingsfunktioner, f.eks. WAP og tredje generation), der ikke ville være dækket alene af definitionen af elektroniske kommunikationsnet.

(c) *"Computerdata"*. Denne definition er baseret på ISO's[32] definition af data. Det er ikke tanken, at den skal omfatte fysiske genstande som bøger. Den omfatter dog en bog, der er lagret som computerdata (dvs. gemt i elektronisk form som en tekstbehandlingsfil) eller konverteret til computerdata ved hjælp af en scanner. Derfor gør denne definition det klart, at computerdata skal være skabt eller konverteret til et format, der egner sig til at blive behandlet i et informationssystem, eller som egner sig til at udføre en funktion i et informationssystem.

(d) *"Informationssystem"*. Denne definition af informationssystem er oprindelig taget fra den, OECD brugte i 1992 i sine retningslinjer for sikkerhed i informationssystemer og de tidligere definitioner, hvor der henvises til elektroniske kommunikationsnet, computere og computerdata. Dette ord er også blevet brugt i tidligere fællesskabsretsakter, f.eks. Rådets afgørelse af 31. marts 1992 om informationssystemers sikkerhed og Rådets henstilling af 7. april 1995 om ensartede kriterier for vurdering af informationsteknologisk sikkerhed. Det skal være

---

30 EFT L 320 af 28.11.1998, s. 54-57.

31 Den endelige tekst kan findes på http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg

32 International Organization for Standardization (ISO) er en verdensomspændende sammenslutning af nationale standardiseringsorganer fra ca. 100 lande.

teknologineutralt og nøjagtigt afspejle begrebet sammenkoblede net og systemer, der indeholder data. Det dækker såvel systemets hardware som software, men ikke selve indholdet i form af information. Det dækker også enkeltstående systemer. Efter Kommissionens opfattelse er det ønskværdigt at udvide den beskyttelse, strafferetten giver, til også at omfatte enkeltstående pc'er og ikke begrænse den til sammenkoblede systemer.

(e) *"Juridisk person"*. Der er tale om en standarddefinition fra Rådets tidligere rammeafgørelser.

(f) *"Autoriseret person"*. Enhver person, som i kraft af en kontrakt, ved lov eller med retmæssig tilladelse har ret til at bruge, forvalte, kontrollere, teste, udføre legitim videnskabelig forskning ved hjælp af eller på anden måde drive et informationssystem, og som handler i overensstemmelse med denne ret eller tilladelse. Det omfatter personer, som handler efter et retmæssigt samtykke fra en person, som har modtaget en sådan eksplicit autorisation. Det er særlig vigtigt, at følgende kategorier af personer og legitime aktiviteter (inden for grænserne for vedkommendes rettigheder, tilladelser og ansvarsområder og i overensstemmelse med fællesskabsrettens bestemmelser om databeskyttelse og fortrolig kommunikation) ikke kriminaliseres, når denne rammeafgørelse gennemføres i national lovgivning:

- almindelige brugere, såvel private som erhvervsbrugere, herunder deres brug af kryptering til at beskytte deres kommunikation og data
- baglænskonstruktion (reverse engineering), inden for de grænser, der er afstukket i direktiv 91/250 af 14. maj 1991 om retlig beskyttelse af edb-programmer[33]
- handlinger udført af forvaltere, kontrollører og operatører af netværk og systemer
- handlinger udført af autoriserede personer for at teste et system; enten selskabets egne ansatte eller eksterne personer, som er udpeget og har fået tilladelse til at teste et systems sikkerhed
- legitim videnskabelig forskning.

(g) *"Uretmæssigt"*. Der er tale om et bredt begreb, hvilket giver medlemsstaterne en vis fleksibilitet ved fastsættelsen af lovovertrædelsens nøjagtige omfang. For at medvirke til gennemførelsen af Rådets rammeafgørelse i national lovgivning finder Kommissionen det dog nødvendigt at påpege, at visse aktiviteter ikke bør falde ind under lovovertrædelsen. Det er ikke muligt, og antagelig ikke ønskværdigt, at udarbejde en udtømmende eksklusiv liste over undtagelser på EU-plan. Ordet "uretmæssigt" er imidlertid baseret på tidligere definitioner for at udelukke autoriserede personers handlinger. Det udelukker også enhver anden handling, der anerkendes som retmæssig i national ret, herunder standardiserede svarskrifter og andre former for bemyndigelse, der anerkendes i national ret.

---

[33] EFT L 122 af 17.5.1991, s. 42-46.

Artikel 3 - Alvorlige angreb gennem ulovlig adgang til informationssystemer

Denne lovovertrædelse skal dække ulovlig adgang til informationssystemer. Den omfatter blandt andet begrebet at "hacke" sig ind i et informationssystem. Medlemsstaterne kan frit udelukke mindre eller trivielle sager fra lovovertrædelsens anvendelsesområde, når de gennemfører rammeafgørelsen i national lovgivning.

Lovovertrædelsen skal kun fastslås i medlemsstaternes lovgivning i den udstrækning, den er begået:

(i) mod en del af et informationssystem, som er udstyret med specifikke beskyttelsesforanstaltninger

(ii) for at forvolde en fysisk eller juridisk person skade, eller

(iii) for at opnå en økonomisk gevinst.

Kommissionen ønsker ikke på nogen måde at udhule den betydning, den tillagde brug af effektive tekniske foranstaltninger til beskyttelse af informationssystemer. Det er dog en uheldig kendsgerning, at en stor del af brugerne udsætter sig selv for angreb ved ikke at have passende teknisk beskyttelse (eller slet ingen beskyttelse). For at afskrække hackere fra at angribe sådanne brugere, skal straffeloven dække uautoriseret adgang til deres systemer, selv om deres systemer måske ikke er teknisk beskyttet i tilstrækkelig grad. Hvis der enten er tale om et forsøg på at forvolde skade eller på at opnå en økonomisk gevinst, er der derfor ikke noget krav om, at sikkerhedsforanstaltninger skal være omgået, for at lovovertrædelsen er begået.

Artikel 4 - Ulovlig forstyrrelse af informationssystemer

Denne lovovertrædelse dækker uretmæssig, overlagt adfærd af en af følgende former:

(a) Alvorlig uretmæssig hindring eller afbrydelse af et informationssystems drift ved at tilføre eller tilsende det computerdata eller ved at beskadige, slette, forvanske, ændre eller tilsløre dets computerdata. Tilførelse eller tilsendelse af computerdata vedrører specifikt problemet med såkaldte "denial of service"-angreb, hvor der gøres et bevidst forsøg på at overvælde et informationssystem. Lovovertrædelsen dækker også "afbrydelse" af et informationssystems drift, hvilket kunne udledes af ordet "hindring", men det er nævnt eksplicit for at fjerne enhver tvivl. De øvrige elementer i lovovertrædelsen (beskadigelse, sletning, forvanskning, ændring eller tilsløring af computerdata) vedrører specifikt problemet med virus og andre former for angreb, som har til formål at hindre eller afbryde driften af selve informationssystemet.

(b) Sletning, forvanskning, ændring, tilsløring eller hindring af adgang til computerdata i et informationssystem, der foretages med henblik på at forvolde en fysisk eller juridisk person skade. Dette dækker virusangreb på et informationssystems indhold (eller computerdata) samt forvanskning af websteder.

I litra a) bruges udtrykket "alvorlig hindring eller afbrydelse" som et element i lovovertrædelsen for at beskrive virkningerne af et sådant angreb. Betydningen af ordet "alvorlig hindring" er ikke defineret, da hindringen kan komme til udtryk på forskellig måde, og omfanget kan variere afhængigt af angrebets form og de tekniske specifikationer af det informationssystem, der angribes. De enkelte medlemsstater fastsætter selv, hvilke kriterier

der skal opfyldes for, at der er tale om en "alvorlig hindring" for et informationssystem drift. Dog bør mindre gener eller forstyrrelser af driften af tjenester ikke betragtes som alvorlige.

Som ovenfor kan medlemsstaterne frit udelukke mindre eller trivielle sager fra at være omfattet af lovovertrædelsen, når de gennemfører rammeafgørelsen i national ret.

Artikel 5 - Medvirken, tilskyndelse og forsøg

I artikel 5, stk. 1, forpligtes medlemsstaterne til at sikre, at overlagt medvirken eller tilskyndelse til lovovertrædelser mod informationssystemer, som beskrevet i artikel 3 og 4, er strafbare.

Artikel 5, stk. 2, vedrører specifikt forsøg. Heri forpligtes medlemsstaterne til at sikre, at forsøg på at begå nogen af de lovovertrædelser mod informationssystemer, der er beskrevet i artikel 3 og 4, er strafbare.

Artikel 6 – Sanktioner

I stk. 1 kræves det, at medlemsstaterne træffer de nødvendige foranstaltninger for at sikre, at de lovovertrædelser, der er defineret i artikel 3-5, straffes med effektive sanktioner, der står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning[34]. I henhold til dette stykke skal medlemsstaterne indføre sanktioner, der står i forhold til lovovertrædelsens grovhed, hvilket udelukker frihedsstraffe med en maksimal straframme på under et år i alvorlige tilfælde. Alvorlige tilfælde kan ikke omfatte tilfælde, hvor adfærden ikke forvoldte skade eller førte til økonomisk gevinst.

Maksimumsstraffen på mindst et års fængsel i alvorlige tilfælde betyder, at lovovertrædelserne er omfattet af den europæiske arrestordre samt andre instrumenter som Rådets rammeafgørelse af 26. juni 2001[35] om hvidvaskning af penge, identifikation, opsporing, indefrysning eller beslaglæggelse og konfiskation af redskaber og udbytte fra strafbart forhold.

I overensstemmelse med karakteren af alle rammeafgørelser, som er bindende for medlemsstaterne med hensyn til de resultater, der skal opnås, men som lader dem selv fastlægge formen og midlerne, bevarer medlemsstaterne en vis fleksibilitet til at tilpasse deres lovgivning til disse regler og afgøre, hvor strenge sanktioner de vil anvende, inden for de grænser, der er fastsat i rammeafgørelsen, især de skærpende omstændigheder i artikel 7. Kommissionen understreger, at medlemsstaterne selv fastsætter kriterierne for at fastslå, hvor alvorlig en lovovertrædelse er, på grundlag af deres respektive retssystemer.

Straf behøver ikke altid at være i form af fængsling. I stk. 2 åbnes der mulighed for, at medlemsstaterne kan benytte bøder oven i eller som alternativ til frihedsstraf i overensstemmelse med deres respektive traditioner og retssystemer.

Artikel 7 - Skærpende omstændigheder

I denne artikel får medlemsstaterne mulighed for under visse omstændigheder at skærpe de sanktioner, der er fastsat i artikel 6. Kommissionen understreger, at listen over skærpende omstændigheder i denne artikel ikke berører andre omstændigheder, der i medlemsstaternes

---

34 Formuleringen er taget fra Domstolens dom af 21. september 1989 i sag C 68/88, Sml. 1989, s. 2965.

35 EFT L 182 af 5.7.2001, s. 1.

lovgivning betragtes som skærpende. Ved udarbejdelsen af listen er der taget hensyn til de skærpende omstændigheder, der er beskrevet i medlemsstaternes nationale bestemmelser, og som er fastsat i tidligere kommissionsforslag til rammeafgørelser.

Hvis en af følgende betingelser, som er opført i stk. 1, er opfyldt, kan den maksimale fængselsstraf ikke være mindre end fire år:

(a) lovovertrædelsen blev begået inden for rammerne af en kriminel organisation, som defineret i den fælles aktion 98/733 RIA, dog uden anvendelse af de strafferammer, der nævnes heri

(b) lovovertrædelsen skabte eller førte til betydelige direkte eller indirekte økonomiske tab, tilføjede en fysisk person fysisk skade eller tilføjede en del af medlemsstatens kritiske infrastruktur betydelig skade, eller

(c) lovovertrædelsen førte til en betydelig gevinst.

Medlemsstaterne skal endvidere sikre, at de lovovertrædelser, der nævnes i artikel 3, 4 og 5, straffes med frihedsstraf, der er strengere end straffen i henhold til artikel 6, når lovovertræderen har modtaget en endelig dom for en sådan lovovertrædelse i en medlemsstat.

Artikel 8 - Særlige omstændigheder

Denne artikel omhandler omstændigheder, hvorunder en medlemsstat kan beslutte at mildne de sanktioner, der er nævnt i artikel 6 og 7, når den kompetente retlige myndighed finder, at lovovertræderen kun har forvoldt mindre skade.

Artikel 9 - Juridiske personers ansvar

I overensstemmelse med den fremgangsmåde, der er benyttet ved udarbejdelsen af en række EU-retsakter for at bekæmpe forskellige former for kriminalitet, er det også nødvendigt at dække den situation, hvor juridiske personer deltager i angreb på informationssystemer. Artikel 9 indeholder derfor bestemmelser om at holde en juridisk person ansvarlig for de lovovertrædelser, der er omhandlet i artikel 3, 4 og 5, og som begås til deres fordel af en person med en vis ledelsesmæssig position, som handler enten individuelt eller som en del af den juridiske persons organisation. Begrebet ansvar skal omfatte enten strafferetligt eller civilretligt ansvar.

I overensstemmelse med almindelig praksis hedder det endvidere i stk. 2, at en juridisk person også kan drages til ansvar, når en person i en position, der gør det muligt at udøve kontrol, ikke har ført tilsyn eller kontrol, og dermed har åbnet mulighed for at begå lovovertrædelserne til den juridiske persons fordel. I stk. 3 fastslås det, at retsforfølgning af en juridisk person ikke udelukker sideløbende retsforfølgning af en fysisk person.

Artikel 10 - Sanktioner over for juridiske personer

I artikel 10 fastsættes et krav om sanktioner over for juridiske personer, der er ansvarlige for de lovovertrædelser, som omtales i artikel 3, 4 og 5. Man kræver effektive, forholdsmæssige og afskrækkende sanktioner, og mindstekravet er strafferetlige eller ikke-strafferetlige bøder. Der nævnes også andre sanktioner, som typisk kan anvendes over for juridiske personer.

Artikel 11 - Domstolskompetence

Da lovovertrædelser i forbindelse med angreb på informationssystemer er internationale af natur, kræver et effektivt juridisk modsvar proceduremæssige bestemmelser om domstolskompetence og udlevering, som er klare og langtrækkende på EU-plan, for at sikre, at lovovertræderne ikke kan undgå at blive retsforfulgt.

I stk. 1 fastsættes en række kriterier for at give de nationale retlige myndigheder domstolskompetence til retsforfølgning og efterforskning i sager, der omhandler de lovovertrædelser, der er nævnt i denne rammeafgørelse. En medlemsstat vil få domstolskompetencen i tre situationer:

(a) når lovovertrædelsen er begået helt eller delvis på dens område, uanset hvilken status den juridiske person har, og uanset hvilken nationalitet den pågældende fysiske person har (territorialprincippet)

(b) når lovovertræderen er statsborger i denne medlemsstat (personalitetsprincippet), og handlingen berører enkeltpersoner eller grupper af personer fra dette land; medlemsstater, som ikke har indført udleveringsbestemmelser, er ansvarlige for at retsforfølge egne statsborgere, der har begået lovovertrædelser i andre lande

(c) når lovovertrædelsen begås til fordel for en juridisk person, som er etableret på medlemsstatens område.

Stk. 2 skal sikre, at medlemsstaterne, når de fastsætter deres domstolskompetence over de lovovertrædelser, der er baseret på territorialprincippet, jf. stk. 1, litra a), sørger for, at kompetencen omfatter sager:

(a) hvor lovovertræderen begår lovovertrædelsen, mens han fysisk befinder sig på landets område, uanset om lovovertrædelsen er rettet mod et informationssystem på dets område; en person kan f.eks. få ulovlig adgang til (hacke) et informationssystem i et tredjeland fra medlemsstatens område, eller

(b) lovovertrædelsen begås mod et informationssystem på landets område, uanset om lovovertræderen på gerningstidspunktet fysisk befinder sig på landets område; en person kan f.eks. få ulovlig adgang til (hacke) et informationssystem i medlemsstaten fra et tredjeland.

Eftersom ekstraterritoriel kompetence for alle former for overtrædelser af straffeloven ikke anerkendes i alle medlemsstaternes juridiske tradition, får de i stk. 3 mulighed for ikke at anvende reglerne om kompetence i stk. 1 i de situationer, der er omfattet af stk. 1, litra b) og c).

I stk. 4 hedder det, at medlemsstaterne skal træffe de nødvendige foranstaltninger til også at fastsætte deres domstolskompetence i forbindelse med de lovovertrædelser, der nævnes i artikel 3-5 i tilfælde, hvor de afviser at udlevere en person, der er mistænkt eller dømt for en sådan lovovertrædelse, til en anden medlemsstat eller et tredjeland.

Stk. 5 omhandler tilfælde, der falder ind under flere landes kompetence, og skal sikre fuldstændigt samarbejde mellem medlemsstaterne for om muligt at centralisere sagsbehandlingen i en enkelt medlemsstat. Med henblik herpå mindes der om, at alle medlemsstaterne kan benytte de organer eller ordninger, der er oprettet i EU til at styrke

samarbejdet mellem retsmyndighederne og koordinere deres arbejde. Dette omfatter også Eurojust og det europæiske retlige netværk.

I stk. 6 hedder det, at medlemsstaterne skal underrette Rådets Generalsekretariat og Kommissionen, hvis de beslutter at anvende stk. 3.

Artikel 12 – Udveksling af oplysninger

Formålet med artikel 12 er at fremme udveksling af oplysninger ved at sikre, at der findes operationelle kontaktpunkter. Det er vigtigt for et effektivt politisamarbejde. Rådet (RIA) understregede den 19. marts 1998 og igen for nylig, hvor det vedtog en henstilling om kontaktpunkter, der fungerer 24 timer i døgnet, til bekæmpelse af højteknologikriminalitet, især at det er nødvendigt, at medlemsstaterne tilslutter sig G8-nettet af kontaktpunkter[36].

Artikel 13 - Gennemførelse

Artikel 13 vedrører gennemførelse og opfølgning af denne rammeafgørelse. Medlemsstaterne skal træffe de nødvendige foranstaltninger for at efterleve denne rammeafgørelse inden den 31. december 2003.

Medlemsstaterne skal inden denne dato underrette Rådets Generalsekretariat og Kommissionen om, hvilke bestemmelser de har indført for at overholde deres forpligtelse til at gennemføre denne rammeafgørelse i national lovgivning. Rådet vurderer i løbet af et år på grundlag af disse oplysninger og en skriftlig rapport fra Kommissionen, i hvilken udstrækning medlemsstaterne har opfyldt de forpligtelser, der blev pålagt dem med rammeafgørelsen.

Artikel 14 – Ikrafttræden

I artikel 14 hedder det, at rammeafgørelsen vil træde i kraft på tyvendedagen efter sin offentliggørelse i *De Europæiske Fællesskabers Tidende*.

---

36 EFT C 187 af 3.7.2001, s. 5.

2002/0086 (CNS)

Forslag til

RÅDETS RAMMEAFGØRELSE

om angreb på informationssystemer

RÅDET FOR DEN EUROPÆISKE UNION HAR -

under henvisning til traktaten om Den Europæiske Union, særlig artikel 29, 30, stk. 1, litra a), 31 og 34, stk. 2, litra b),

under henvisning til forslag fra Kommissionen[1],

under henvisning til udtalelse fra Europa-Parlamentet[2], og

ud fra følgende betragtninger:

(1) Der er beviser for, at der er foretaget angreb på informationssystemer, især som led i organiseret kriminalitet, og der er voksende bekymring for mulige terroristangreb på informationssystemer, der udgør en del af medlemsstaternes kritiske infrastruktur. Dette er en trussel mod skabelsen af et sikrere informationssamfund og et område med frihed, sikkerhed og retfærdighed og kræver derfor en reaktion fra EU.

(2) En effektiv reaktion på disse trusler kræver en samlet strategi til forbedring af net- og informationssikkerheden, som det blev understreget i handlingsplanen for eEurope og i Kommissionens meddelelse "Net- og informationssikkerhed: Forslag til en europæisk strategi"[3] og i Rådets resolution af 6. december 2001 om en fælles fremgangsmåde og specifikke aktioner i forbindelse med net- og informationssikkerhed.

(3) Behovet for en yderligere forbedring af kendskabet til problemerne i forbindelse med informationssamfundet og for at yde praktisk bistand blev desuden understreget i Europa-Parlamentets beslutning af 5. september 2001[4].

(4) Betydelige lakuner og forskelle mellem medlemsstaternes love på dette område hæmmer bekæmpelsen af den organiserede kriminalitet og terrorismen og lægger sig i vejen for effektivt samarbejde mellem politi og retsvæsen i forbindelse med angreb på informationssystemer. Den grænseoverskridende og -løse karakter af moderne elektroniske kommunikationsnet betyder, at angreb på informationssystemer ofte foregår internationalt, hvilket understreger det presserende behov for yderligere initiativer for en indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler på dette område.

---

1 EFT C ...
2 EFT C ...
3 KOM (2001) 298 endelig.
4 [2001/2098(INI)].

(5) Rådets og Kommissionens handlingsplan for, hvorledes Amsterdam-traktatens bestemmelser om indførelse af et område med frihed, sikkerhed og retfærdighed bedst kan gennemføres[5], Det Europæiske Råds møde i Tammerfors den 15.-16. oktober 1999, Det Europæiske Råds møde i Santa Maria da Feira den 19.-20. juni 2000, Kommissionens resultattavle[6] og Europa-Parlamentets beslutning af 19. maj 2000[7] peger på eller opfordrer til lovgivningsinitiativer for at bekæmpe den højteknologiske kriminalitet, herunder fælles definitioner, fælles regler for, hvad der udgør lovovertrædelser, og fælles straffe.

(6) Det er nødvendigt at supplere det arbejde, der er udført af internationale organisationer, især Europarådets arbejde med at tilnærme landenes strafferetlige regler og G8's arbejde med grænseoverskridende samarbejde inden for højteknologisk kriminalitet ved at finde en fælles EU-fremgangsmåde på dette område. Dette blev yderligere uddybet i Kommissionens meddelelse til Rådet, Europa-Parlamentet, Det Økonomiske og Sociale Udvalg og Regionsudvalget med titlen Et sikrere informationssamfund: Højnelse af sikkerheden i informationsinfrastrukturerne og bekæmpelse af computerrelateret kriminalitet[8].

(7) Der skal foretages en indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler i forbindelse med angreb på informationssystemer for at sikre det bedst mulige samarbejde mellem politi og retlige myndigheder vedrørende lovovertrædelser i forbindelse med angreb på informationssystemer og for at bidrage til bekæmpelsen af organiseret kriminalitet og terrorisme.

(8) Rammeafgørelsen om den europæiske arrestordre[9], bilaget til Europol-konventionen og Rådets afgørelse om oprettelse af Eurojust indeholder alle henvisninger til it-relateret kriminalitet, som skal defineres nærmere. I forbindelse med sådanne instrumenter omfatter it-relateret kriminalitet angreb på informationssystemer, som defineret i denne rammeafgørelse, der vil føre til en langt større grad af tilnærmelse mellem sådanne lovovertrædelsers forskellige bestanddele. Samtidig supplerer denne rammeafgørelse rammeafgørelsen om bekæmpelse af terrorisme[10], der omfatter terroristangreb, som fører til omfattende ødelæggelse af en infrastrukturfacilitet, herunder et informationssystem, der må forventes at bringe menneskeliv i fare eller at medføre store økonomiske tab.

(9) Alle medlemsstaterne har ratificeret Europarådets konvention af 28. januar 1981 om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger. De personoplysninger, der behandles i forbindelse med gennemførelsen af denne rammeafgørelse, vil blive beskyttet i overensstemmelse med denne konventions principper.

(10) Fælles definitioner på dette område, især af informationssystemer og computerdata, er vigtige for at sikre en ensartet holdning i medlemsstaterne til anvendelsen af denne rammeafgørelse.

---

5 EFT C 19 af 23.1.1999.
6 KOM (2001) 278 endelig.
7 A5-0127/2000.
8 KOM (2000) 890.
9 EFT C ... s....
10 EFT C ... s...

(11) Der er behov for en fælles definition af de elementer, straffelovsovertrædelser består af, ved at fastlægge en fælles definition af ulovlig adgang til et informationssystem og ulovlig forstyrrelse af et informationssystem.

(12) Det er nødvendigt at undgå overkriminalisering, især af triviel eller mindre alvorlig adfærd, og for at undgå at kriminalisere rettighedshavere og autoriserede personer, som f.eks. legitime private brugere og erhvervsmæssige brugere, ledere, kontrollører og operatører af netværk og systemer, legitime videnskabelige forskere og autoriserede personer, der tester et system, det være sig selskabets egne ansatte som eksterne personer, der er udpeget og har fået tilladelse til at teste et systems sikkerhed.

(13) Medlemsstaterne bør indføre sanktioner for angreb på informationssystemer, der er effektive, forholdsmæssige og afskrækkende, herunder frihedsstraf i alvorlige tilfælde.

(14) Der er behov for strengere sanktioner, når visse omstændigheder i forbindelse med et angreb på et informationssystem gør angrebet til en endnu større trussel mod samfundet. I sådanne tilfælde bør sanktionerne mod gerningsmændene være tilstrækkelige til, at angreb mod informationssystemer kan falde ind under anvendelsesområdet for instrumenter, der allerede er vedtaget til bekæmpelse af organiseret kriminalitet, som f.eks. fælles aktion 98/733/RIA af 21. december 1998 vedtaget af Rådet på grundlag af artikel K.3 i traktaten om Den Europæiske Union om at gøre det strafbart at deltage i en kriminel organisation i Den Europæiske Unions medlemsstater[11].

(15) Der bør træffes foranstaltninger for at gøre det muligt at drage juridiske personer til ansvar for de lovovertrædelser, der omhandles i denne afgørelse, som begås til deres fordel, og for at sikre, at hver enkelt medlemsstat har kompetence over lovovertrædelser begået mod informationssystemer i situationer, hvor gerningsmanden fysisk befinder sig på dens område, eller hvor informationssystemet befinder sig på dens område.

(16) Der bør også træffes foranstaltninger med henblik på samarbejde mellem medlemsstaterne for at sikre effektive indgreb mod angreb på informationssystemer. Der bør oprettes operationelle kontaktpunkter med henblik på udveksling af oplysninger.

(17) Eftersom målsætningerne om at sikre, at angreb på informationssystemer i alle medlemsstater straffes med effektive strafferetlige sanktioner, der står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning, og at det retlige samarbejde skal forbedres og styrkes ved at fjerne potentielle hindringer, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne alene, idet reglerne skal være fælles og sammenlignelige, og derfor bedre kan udarbejdes på EU-plan, kan EU i overensstemmelse med subsidiaritetsprincippet som omhandlet i EU-traktatens artikel 2 og EF-traktatens artikel 5 træffe foranstaltninger. I overensstemmelse med proportionalitetsprincippet, som er beskrevet i sidstnævnte artikel, går denne rammeafgørelse ikke ud over, hvad der er nødvendigt for at nå disse mål.

(18) Denne rammeafgørelse berører ikke Det Europæiske Fællesskabs beføjelser.

---

[11] EFT L 351 af 29.12.1998, s. 1.

(19) Denne rammeafgørelse respekterer de grundlæggende rettigheder og overholder især de principper, der er nævnt i EU-charteret om grundlæggende rettigheder, især dets kapitel II og VI -

TRUFFET FØLGENDE RAMMEAFGØRELSE:

Artikel 1

Rammeafgørelsens anvendelsesområde og formål

Formålet med denne rammeafgørelse er at forbedre samarbejdet mellem de retlige og andre kompetente myndigheder, herunder politiet og andre specialiserede retshåndhævende myndigheder i medlemsstaterne, ved at foretage en indbyrdes tilnærmelse af medlemsstaternes strafferetlige regler vedrørende angreb på informationssystemer.

Artikel 2

Definitioner

I denne rammeafgørelse gælder følgende definitioner:

(a) *"Elektronisk kommunikationsnet"* betyder transmissionssystemer og, hvor det er relevant, koblings- og dirigeringsudstyr og andre ressourcer, som giver mulighed for at overføre signaler ved hjælp af trådforbindelse, radiobølger, lyslederteknik eller andre elektromagnetiske midler, herunder satellitnetværk, faste (kredsløbs- eller pakkekoblede net, herunder internettet) og mobile jordbaserede netværk, elkabelsystemer, der anvendes til fremføring af signaler, netværk til radio- og tv-spredning og kabel-tv-net, uanset hvilken type information der overføres.

(b) *"Computer"* betyder enhver anordning eller gruppe af indbyrdes forbundne eller beslægtede anordninger, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af computerdata.

(c) *"Computerdata"* betyder enhver form for gengivelse af facts, information eller begreber, som er redigeret i eller omdannet til et format, der egner sig til behandling i et informationssystem, herunder et program, som kan anvendes til at få et informationssystem til at udføre en funktion.

(d) *"Informationssystem"* betyder computere og elektroniske kommunikationsnet samt computerdata, som de lagrer, behandler, kalder frem eller overfører i forbindelse med deres drift, brug, beskyttelse og vedligeholdelse.

(e) *"Juridisk person"* betyder enhver enhed, der har denne status i henhold til gældende lovgivning, med undtagelse af stater eller andre offentlige organer, der udøver offentlig myndighed, og offentlige internationale organisationer.

(f) *"Autoriseret person"* betyder enhver fysisk eller juridisk person, som i kraft af en kontrakt, ved lov eller i kraft af en retmæssig tilladelse har ret til at bruge, forvalte, kontrollere, teste, udføre legitim videnskabelig forskning ved hjælp af eller på anden måde drive et informationssystem, og som handler i overensstemmelse med denne ret eller tilladelse.

(g) *"Uretmæssigt"* betyder, at autoriserede personers adfærd eller anden adfærd, der anerkendes som retmæssig i national lovgivning, er udelukket.

Artikel 3

Ulovlig adgang til informationssystemer

Medlemsstaterne sikrer, at det er strafbart forsætligt at skaffe sig uretmæssig adgang til et informationssystem eller en del heraf, når handlingen:

(i) er rettet mod en del af et informationssystem, som er udstyret med specifikke beskyttelsesforanstaltninger, eller

(ii) begås for at forvolde en fysisk eller juridisk person skade, eller

(iii) begås for at opnå en økonomisk gevinst.

Artikel 4

Ulovlig forstyrrelse af informationssystemer

Medlemsstaterne sikrer, at følgende former for uretmæssig forsætlig adfærd er strafbare, når denne adfærd udgør et alvorligt angreb:

(a) alvorlig hindring eller afbrydelse af et informationssystems drift ved at tilføre eller sende det computerdata eller ved at beskadige, slette, forvanske, ændre, tilsløre eller hindre adgang til dets computerdata

(b) sletning, forvanskning, ændring, tilsløring eller hindring af adgang til computerdata i et informationssystem, der foretages med henblik på at forvolde en fysisk eller juridisk person skade.

Artikel 5

Medvirken, tilskyndelse og forsøg

1. Medlemsstaterne sikrer, at forsætlige lovovertrædelser og medvirken eller tilskyndelse til lovovertrædelser, som omtalt i artikel 3 og 4, er strafbare.

2. Medlemsstaterne sikrer, at forsøg på at begå de lovovertrædelser, der er omtalt i artikel 3 og 4, er strafbart.

Artikel 6

Sanktioner

1. Medlemsstaterne sikrer, at de lovovertrædelser, der henvises til i artikel 3, 4 og 5, straffes med effektive sanktioner, der står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning, herunder en maksimal frihedsstraf på mindst et år i alvorlige tilfælde. Alvorlige tilfælde omfatter ikke tilfælde, hvor den udviste adfærd ikke forvoldte skade eller medførte økonomisk gevinst.

2. Medlemsstaterne skal åbne mulighed for idømmelse af bøder som supplement eller alternativ til frihedsstraf.

Artikel 7

Skærpende omstændigheder

1. Medlemsstaterne sikrer, at de lovovertrædelser, der er nævnt i artikel 3, 4 og 5, straffes med frihedsstraf med en maksimal straframme på mindst fire år, når der er tale om følgende omstændigheder:

   (a) lovovertrædelsen er begået inden for rammerne af en kriminel organisation, som defineret i den fælles aktion 98/733/RIA om at gøre det strafbart at deltage i en kriminel organisation i Den Europæiske Unions medlemsstater, dog uden anvendelse af de strafferammer, der nævnes heri

   (b) lovovertrædelsen skabte eller førte til betydelige direkte eller indirekte økonomiske tab, tilføjede en fysisk person fysisk skade eller tilføjede en del af medlemsstatens kritiske infrastruktur betydelig skade

   (c) lovovertrædelsen førte til en betydelig gevinst.

2. Medlemsstaterne skal sikre, at de lovovertrædelser, der nævnes i artikel 3 og 4, straffes med frihedsstraf, der er strengere end straffen i henhold til artikel 6, når lovovertræderen har modtaget en endelig dom for en sådan lovovertrædelse i en medlemsstat.

Artikel 8

Særlige omstændigheder

Uden at det berører artikel 6 og 7, sikrer medlemsstaterne, at de sanktioner, der er omtalt i artikel 6 og 7, kan nedsættes, når den kompetente retsmyndighed finder, at gerningsmanden kun forvoldte mindre skade.

Artikel 9

Juridiske personers ansvar

1. Medlemsstaterne sikrer, at juridiske personer kan drages til ansvar for de lovovertrædelser, der er omtalt i artikel 3, 4 og 5, og som begås til deres fordel af en person med en vis ledelsesmæssig position, som handler enten individuelt eller som en del af den juridiske persons organisation, på grundlag af:

   (a) en bemyndigelse til at repræsentere den juridiske person

   (b) en beføjelse til at træffe beslutninger på den juridiske persons vegne

   (c) en beføjelse til at udøve kontrol med den juridiske person.

2. Ud over de tilfælde, der er omhandlet i stk. 1, sørger medlemsstaterne for, at en juridisk person kan drages til ansvar, når manglende tilsyn eller kontrol af en person,

som omtalt i stk. 1, har gjort det muligt for en person, der er underlagt den juridiske persons myndighed, at begå de lovovertrædelser, der er nævnt i artikel 3, 4 og 5, til fordel for den juridiske person.

3. En juridisk persons ansvar i henhold til stk. 1 og 2 udelukker ikke retsforfølgning af fysiske personer, som begår lovovertrædelser eller udviser den adfærd, der er nævnt i artikel 3, 4 og 5.

Artikel 10

Sanktioner over for juridiske personer

1. Medlemsstaterne sikrer, at en juridisk person, der drages til ansvar i medfør af artikel 9, stk. 1, straffes med effektive sanktioner, der står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning, og som skal omfatte strafferetlige eller ikke-strafferetlige bøder samt eventuelt andre sanktioner, som f.eks.:

   a) fratagelse af retten til at modtage offentlige ydelser eller støtte

   b) midlertidigt eller permanent forbud mod at udøve erhvervsaktiviteter

   c) retsligt opsyn

   d) likvidation efter retskendelse.

2. Medlemsstaterne sikrer, at en juridisk person, der drages til ansvar i medfør af artikel 9, stk. 2, straffes med effektive sanktioner, der står i rimeligt forhold til overtrædelsen og har en afskrækkende virkning.

Artikel 11

Domstolskompetence

1. Den enkelte medlemsstat fastsætter sin domstolskompetence vedrørende de lovovertrædelser, der er nævnt i artikel 3, 4 og 5, når lovovertrædelsen er begået:

   (a) helt eller delvis inden for dens område

   (b) af en af dens statsborgere, og handlingen berører enkeltpersoner eller grupper af personer fra denne stat

   (c) til fordel for en juridisk person, som har sit hovedsæde på den pågældende medlemsstats område.

2. Når den enkelte medlemsstat fastsætter sin domstolskompetence i medfør af stk. 1, litra a), sikrer den sig, at den omfatter tilfælde, hvor:

   (a) gerningsmanden begår lovovertrædelsen, mens han fysisk befinder sig på landets område, uanset om lovovertrædelsen er rettet mod et informationssystem på dets område

(b) lovovertrædelsen begås mod et informationssystem på landets område, uanset om gerningsmanden på gerningstidspunktet fysisk befinder sig på landet område.

3. En medlemsstat kan beslutte ikke at anvende reglen om domstolskompetence i stk. 1, litra b) og c), eller kun at anvende den i særlige tilfælde eller under særlige omstændigheder.

4. Medlemsstaterne skal træffe de nødvendige foranstaltninger til også at fastsætte deres domstolskompetence i forbindelse med de lovovertrædelser, der nævnes i artikel 3-5 i tilfælde, hvor de afviser at udlevere en person, der er mistænkt eller dømt for en sådan lovovertrædelse, til en anden medlemsstat eller et tredjeland.

5. Når en lovovertrædelse er omfattet af mere end én medlemsstats domstolskompetence, og når en hvilken som helst af de berørte medlemsstater kan rejse tiltale på grundlag af de samme forhold, samarbejder de berørte medlemsstater om at afgøre, hvem af dem der skal rejse tiltale mod gerningsmændene for om muligt at centralisere sagsbehandlingen i en enkelt medlemsstat. Med henblik herpå har medlemsstaterne adgang til alle organer eller ordninger, der er oprettet i EU, for at styrke samarbejdet mellem retsmyndighederne og koordinere deres arbejde.

6. Medlemsstaterne underretter Rådets Generalsekretariat og Kommissionen, hvis de beslutter at anvende stk. 3, når det er nødvendigt med en angivelse af de specifikke tilfælde eller omstændigheder, hvor beslutningen gælder.

Artikel 12

Udveksling af oplysninger

1. Med henblik på udveksling af oplysninger om de lovovertrædelser, der er nævnt i artikel 3, 4 og 5, skal medlemsstaterne i overensstemmelse med reglerne om databeskyttelse oprette operationelle kontaktpunkter, der fungerer 24 timer i døgnet, syv dage om ugen.

2. Den enkelte medlemsstat underretter Rådets Generalsekretariat og Kommissionen, når de har oprettet kontaktpunkter til udveksling af oplysninger om lovovertrædelser i forbindelse med angreb på informationssystemer. Generalsekretariatet viderebringer disse oplysninger til de øvrige medlemsstater.

Artikel 13

Gennemførelse

1. Medlemsstaterne træffer de nødvendige foranstaltninger for at efterleve denne rammeafgørelse senest den 31. december 2003.

2. De sender Rådets Generalsekretariat og Kommissionen teksten til de bestemmelser, de har indført, og oplysninger om eventuelle andre foranstaltninger, de har truffet, for at efterleve denne rammeafgørelse.

3. På grundlag heraf forelægger Kommissionen senest den 31. december 2004 Europa-Parlamentet og Rådet en rapport om efterlevelsen af denne rammeafgørelse, som i givet fald kan ledsages af lovgivningsmæssige forslag.

4. Rådet vurderer, i hvilken udstrækning medlemsstaterne har efterlevet denne rammeafgørelse.

Artikel 14

Ikrafttrædelse

Denne rammeafgørelse træder i kraft på tyvendedagen efter sin offentliggørelse i *De Europæiske Fællesskabers Tidende*.

Udfærdiget i Bruxelles, den

På Rådets vegne
Formand