EUROPA-KOMMISSIONEN

Bruxelles, den 30.9.2010
KOM(2010) 517 endelig

2010/0273 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om angreb på informationssystemer og om ophævelse af Rådets rammeafgørelse 2005/222/RIA

{SEK(2010) 1122 final}
{SEK(2010) 1123 final}

BEGRUNDELSE

1. FORSLAGETS BEGRUNDELSE OG FORMÅL

Formålet med forslaget er at erstatte Rådets rammeafgørelse 2005/222/RIA af 24. februar 2005 om angreb på informationssystemer[1]. Denne rammeafgørelse er som anført i betragtningerne en konsekvens af ønsket om 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 om angreb på informationssystemer. Med rammeafgørelsen blev der indført EU-lovgivning om lovovertrædelser, såsom ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer og ulovligt indgreb i data, samt særlige regler om juridiske personers ansvar, straffemyndighed og udveksling af oplysninger**.** Medlemsstaterne skulle træffe de nødvendige foranstaltninger for at efterkomme rammeafgørelsen senest den 16. marts 2007.

Den 14. juli 2008 offentliggjorde Kommissionen en beretning om gennemførelsen af rammeafgørelsen[2]. I beretningens konklusioner blev det anført, at der var gjort betydelige fremskridt i de fleste medlemsstater, og at gennemførelsesgraden var relativt god, men at gennemførelsen endnu ikke var tilendebragt i visse medlemsstater. Senere henne i beretningen anførtes det, at "de nylige angreb på tværs af Europa har sat fokus på adskillige nye trusler, siden rammeafgørelsen blev vedtaget, navnlig de nye massive simultane angreb på informationssystemer og øget kriminel brug af såkaldte botnet". Der var ikke særlig opmærksomhed på disse angreb, da rammeafgørelsen blev vedtaget. På foranledning af denne udvikling vil Kommissionen overveje at træffe foranstaltninger med henblik på at udtænke bedre metoder til at imødegå truslen (med hensyn til en forklaring af "botnet" henvises der til næste underafsnit).

Vigtigheden af at træffe yderligere foranstaltninger til at øge bekæmpelsen af it-kriminalitet blev fremhævet i Haagprogrammet af 2004 om styrkelse af frihed, sikkerhed og retfærdighed i Den Europæiske Union og i Stockholmprogrammet af 2009 og handlingsplanen hertil[3]. Endvidere blev der erkendt et behov for at takle de nye former for kriminalitet, der opstår, særligt it-kriminalitet på EU-plan, i den digitale dagsorden for Europa[4], det første flagskibsinitiativ vedtaget under Europa 2020-strategien, der for nylig blev fremlagt. På indsatsområdet vedrørende tillid og sikkerhed har Kommissionen givet tilsagn om foranstaltninger til bekæmpelse af it-angreb på informationssystemer.

På internationalt plan anses Europarådets konvention om it-kriminalitet (herefter "konventionen om it-kriminalitet"), der blev undertegnet den 23. november 2001, for at indeholde de mest dækkende internationale standarder til dags dato, idet den giver en omfattende og sammenhængende ramme for de forskellige aspekter af it-kriminalitet[5]. Indtil videre er konventionen blevet undertegnet af alle 27 medlemsstater, men kun ratificeret af

---

1 EUT L 69 af 16.3.2005, s. 68.

2 Beretning fra Kommissionen til Rådet i henhold til artikel 12 i Rådets rammeafgørelse af 24. februar 2005 om angreb på informationssystemer, KOM(2008) 448 endelig.

3 EUT C 198 af 12.8.2005, EUT C 115 af 4.5.2010, KOM(2010) 171 af 20.4.2010.

4 Kommissionens meddelelse af 19.5.2010, KOM(2010) 245.

5 Europarådets konvention om it-kriminalitet, Budapest, den 23.11.2001, CETS nr. 185.

15 medlemsstater[6]. Konventionen trådte i kraft den 1. juli 2004. EU har ikke undertegnet konventionen. På grund af konventionens vigtighed tilskynder Kommissionen aktivt de resterende medlemsstater til at ratificere den snarest muligt.

- **Generel baggrund**

Hvad angår it-kriminalitet, er sårbarhed på grund af en række faktorer den vigtigste årsag til fænomenet. Utilstrækkelige retshåndhævelsesforanstaltninger er en medvirkende årsag til udbredelsen af fænomenet og bidrager til vanskelighederne, idet visse former for lovovertrædelser begås på tværs af landegrænserne. Anmeldelse af denne type kriminalitet er ofte utilstrækkelig, dels fordi visse forbrydelser ikke opdages, dels fordi ofrene (erhvervsdrivende og virksomheder) ikke anmelder forbrydelserne af frygt for at få et dårligt rygte og for, at fremtidsudsigterne for deres virksomhed bliver skadet af, at deres sårbarhed bliver offentligt kendt.

Endvidere kan forskelligheder i national strafferet og strafferetspleje give anledning til forskelle i efterforskningen og retsforfølgningen, hvilket kan føre til, at disse forbrydelser behandles forskelligt. Udviklingen i informationsteknologi har gjort disse problemer større, idet det er blevet lettere at fremstille og distribuere værktøjer ("malware" og "botnet"), samtidig med at forbryderne kan bevare deres anonymitet, og ansvaret spredes over flere jurisdiktioner. På grund af de vanskeligheder, der er forbundet med retsforfølgning, kan organiseret kriminalitet være særdeles indbringende, uden at der løbes nogen større risiko.

Forslaget tager hensyn til de nye metoder til at begå it-kriminalitet, navnlig brug af botnet. Udtrykket "botnet" betyder et netværk af computere, der er blevet inficeret af ondsindet software (computervirus). Et sådant netværk af inficerede computere ("zombier") kan aktiveres, så de udfører nærmere bestemte handlinger, såsom at angribe informationssystemer (it-angreb). "Zombierne" kan styres - ofte uden at brugerne af de inficerede computere har kendskab til det - fra en anden computer. Den "styrende" computer kaldes også "kommando- og kontrolcentret". De personer, der kontrollerer centret, er blandt gerningsmændene, idet de bruger de inficerede computere til at angribe informationssystemer. Det er meget vanskeligt at opspore gerningsmændene, fordi de computere, der udgør botnettet og udfører angrebet, kan befinde sig et andet sted end gerningsmanden selv.

Angreb, der foretages ved hjælp af botnet, er ofte meget omfattende. Omfattende angreb er angreb, der enten udføres ved hjælp af værktøjer, der griber ind i et betydeligt antal informationssystemer (computere), eller angreb, der volder betydelig skade, såsom i form af afbrydelse af systemtjenester, økonomiske omkostninger eller tab af personlige data. Skade, som forvoldes ved omfattende angreb, har betydelige konsekvenser for funktionen af det, der er målet for angrebet, og/eller påvirker dets arbejdsomgivelser. På den baggrund forstås der ved "et stort botnet" et botnet, der er i stand til at volde betydelig skade. Det er svært nærmere at afgrænse størrelsen af botnet, men de største, der er set, har man anslået havde mellem 40 000 og 100 000 forbindelser (dvs. inficerede computere) i døgnet[7].

---

6 En oversigt over ratificeringen af konventionen (CETS nr. 185) findes her: http://conventions.coe.int/Treaty/Commun/ListeTraites.asp?CM=8&CL=ENG.

7 Antallet af forbindelser i døgnet er det mål, der sædvanligvis anvendes til at angive størrelsen af botnet.

- **Gældende bestemmelser på det område, som forslaget vedrører**

På EU-plan indførte rammeafgørelsen et minimumsniveau for den indbyrdes tilnærmelse af medlemsstaternes lovgivning med henblik på at strafbelægge en række it-forbrydelser, herunder tiltvingelse af ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer, ulovligt indgreb i data og anstiftelse heraf, medvirken og tilskyndelse hertil samt forsøg herpå.

Selv om bestemmelserne i rammeafgørelsen generelt er blevet gennemført af medlemsstaterne, har afgørelsen en række mangler på grund af tendensen i overtrædelsernes omfang og antal (it-angreb). Rammeafgørelsen medfører kun en tilnærmelse af lovgivningen, for så vidt angår et begrænset antal lovovertrædelser, men tager ikke i fuldt omfang højde for den potentielle trussel, som omfattende angreb udgør for samfundet. Den tager heller ikke tilstrækkeligt hensyn til forbrydelsernes grovhed og sanktionerne mod dem.

Andre EU-initiativer og programmer, der er gældende eller planlagt, takler i et vist omfang problemer vedrørende it-angreb eller spørgsmål som netsikkerhed og sikkerhed for internetbrugere, heriblandt aktioner, der støttes gennem programmer som "forebyggelse og bekæmpelse af kriminalitet"[8], "strafferet"[9] og "sikrere brug af internettet"[10] samt "initiativet vedrørende kritisk informationsinfrastruktur[11]. Ud over rammeafgørelsen findes der en anden relevant gældende retsakt, nemlig Rådets rammeafgørelse 2004/68/RIA om bekæmpelse af seksuel udnyttelse af børn og børnepornografi.

På det administrative plan er inficering af computere, hvorved de bliver gjort til "botnet", allerede forbudt i henhold til EU's regler om beskyttelse af privatlivets fred og databeskyttelse[12]. Navnlig samarbejder nationale administrative organer allerede med hinanden inden for rammerne af det europæiske kontaktnetværk for myndigheder med ansvar for spam. I henhold til de pågældende regler skal medlemsstaterne forbyde opfangning af kommunikationer ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester uden de pågældende brugeres samtykke og uden tilladelse i henhold til loven.

Nærværende forslag er i overensstemmelse med disse regler. Medlemsstaterne bør være opmærksomme på, at samarbejdet mellem administrative myndigheder og retshåndhævende myndigheder skal forbedres, for så vidt angår sager, hvor der både kan ifaldes forvaltningsretlige og strafferetlige sanktioner.

- **Overensstemmelse med andre EU-politikker og -mål**

Formålene er i overensstemmelse med EU's politik med hensyn til at bekæmpe organiseret kriminalitet, øge edb-nettenes modstandskraft, beskytte kritisk informationsinfrastruktur og databeskyttelse. Målene er også i overensstemmelse med programmet for sikrere brug af internettet, som blev udarbejdet for at fremme en sikrere brug af internettet og nye onlineteknologier og bekæmpe ulovligt indhold.

---

8 Se: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm.

9 Se: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm.

10 Se: http://ec.europa.eu/information_society/activities/sip/index_en.htm.

11 Se: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

12 Direktivet om databeskyttelse inden for elektronisk kommunikation, EFT L 201 af 31.7.2002, senest ændret ved direktiv 2009/136/EF, EUT L 337 af 18.12.2009.

Forslaget er blevet grundigt undersøgt for at sikre, at dets bestemmelser fuldt ud er forenelige med de grundlæggende rettigheder og særligt med beskyttelsen af personoplysninger, ytrings- og informationsfriheden, adgangen til en upartisk domstol, uskyldsformodningen og forsvarets rettigheder samt legalitetsprincippet og princippet om, at forbrydelse og straf skal stå i et rimeligt forhold til hinanden.

2. HØRING AF INTERESSEREDE PARTER OG KONSEKVENSANALYSE

- **Høring af interesserede parter**

Et vidt spektrum af sagkyndige på området er blevet hørt under en række forskellige møder, hvor man har behandlet forskellige aspekter af bekæmpelsen af it-kriminalitet, herunder det retslige efterspil af disse forbrydelser (retsforfølgelsen). De omfattede særligt repræsentanter for medlemsstaternes regeringer og den private sektor, specialkyndige dommere og anklagere, internationale organisationer, EU-agenturer og ekspertgrupper. En række eksperter og organisationer har efterfølgende indsendt bemærkninger og oplysninger.

Hovedkonklusionerne af høringen er, at der er behov for:

– at EU handler på dette område

– at visse former for lovovertrædelser, som ikke er omfattet af den nuværende rammeafgørelse, gøres strafbare, navnlig nye former for it-angreb (botnet)

– at hindringer for efterforskning og retsforfølgning i sager, der går på tværs af landegrænserne, fjernes.

I konsekvensanalysen er der taget hensyn til de bemærkninger, der er modtaget under høringen.

Indhentning og brug af ekspertbistand

Ekstern ekspertise er blevet indhentet under en række møder med interesserede parter.

Konsekvensanalyse

Der er set på forskellige politiske løsninger på, hvordan målet kan opfyldes.

- Løsning 1: Status quo/Ingen nye EU-foranstaltninger

Denne løsning indebærer, at EU ikke træffer nogen yderligere foranstaltninger til at bekæmpe denne særlige type it-kriminalitet, dvs. angreb på informationssystemer. De igangværende foranstaltninger fortsættes, navnlig programmet til styrkelse af beskyttelsen af kritisk informationsinfrastruktur og forbedring af samarbejdet mellem det offentlige og det private til bekæmpelse af it-kriminalitet.

- Løsning 2: Udvikling af et program til at øge indsatsen for at bekæmpe angreb på informationssystemer ved hjælp af ikke-lovgivningsmæssige foranstaltninger

Ikke-lovgivningsmæssige foranstaltninger vil i forlængelse af programmet til beskyttelse af kritisk informationsinfrastruktur fokusere på retshåndhævelse og samarbejde mellem det offentlige og det private på tværs af landegrænserne. Disse "soft law"-instrumenter bør sigte

mod at fremme en yderligere koordineret indsats på EU-plan, herunder en styrkelse af de eksisterende døgnbemandede netværk af kontaktpunkter for de retshåndhævende myndigheder, oprettelse af et EU-netværk af offentlig-private kontaktpunkter, der involverer eksperter i it-kriminalitet og retshåndhævende myndigheder, udarbejdelse af en EU-standardaftale om serviceniveauet for de retshåndhævende myndigheders samarbejde med operatører i den private sektor og støtte til tilrettelæggelsen af programmer for uddannelse af de retshåndhævende myndigheder i efterforskning af it-kriminalitet.

- Løsning 3: Målrettet ajourføring af reglerne i rammeafgørelsen (et nyt direktiv til erstatning for den nuværende rammeafgørelse) for at imødegå truslen om omfattende angreb på informationssystemer (botnet) og - når lovovertrædelsen begås ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører - fremme effektiviteten af medlemsstaternes retshåndhævende myndigheders kontaktpunkter og afhjælpe manglen på statistiske oplysninger om it-angreb.

Anvendes denne løsning, skal der indføres særlig målrettet (dvs. begrænset) lovgivning for at forebygge omfattende angreb på informationssystemer. En sådan styrket lovgivning ville blive ledsaget af ikke-lovgivningsmæssige foranstaltninger til at styrke det operationelle samarbejde over landegrænserne om sådanne angreb, hvilket ville lette gennemførelsen af de lovgivningsmæssige foranstaltninger. Formålet med disse foranstaltninger ville være at fremme den kritiske informationsinfrastrukturs beredskab, sikkerhed og modstandsdygtighed og udveksle erfaringer om den bedste praksis.

- Løsning 4: Indførelse af omfattende EU-lovgivning til bekæmpelse af it-kriminalitet

Denne løsning ville indebære omfattende ny EU-lovgivning. Ud over at indføre de "soft law"-foranstaltninger, der er nævnt under løsning 2, og foretage den i løsning 3 nævnte ajourføring, ville denne løsning også takle andre juridiske problemer i forbindelse med brug af internettet. Disse foranstaltninger ville ikke alene omfatte angreb på informationssystemer, men også spørgsmål som økonomisk it-kriminalitet, ulovligt internetindhold, indsamling/lagring/overførsel af elektroniske beviser, og mere detaljerede regler om jurisdiktionskompetence. Lovgivningen ville gælde sideløbende med Europarådets konvention om it-kriminalitet og ville omfatte de dermed forbundne ikke-lovgivningsmæssige foranstaltninger, der er nævnt ovenfor.

- Løsning 5: Ajourføring af Europarådets konvention om it-kriminalitet

Denne løsning ville kræve betydelig genforhandling af den nuværende konvention, hvilket er en langsommelig proces og uforeneligt med den tidsramme for handling, som foreslås i konsekvensanalysen. Der er tilsyneladende ingen international vilje til at genforhandle konventionen. En ajourføring af konventionen kan derfor ikke anses for en mulig løsning, da den falder uden for den ønskede tidsramme for handling.

Den foretrukne politiske løsning: En kombination af ikke-lovgivningsmæssige foranstaltninger (løsning 2) med en målrettet ajourføring af rammeafgørelsen (løsning 3)

Ifølge analysen af de økonomiske og sociale konsekvenser og konsekvenserne for de grundlæggende rettigheder udgør løsning 2 og 3 den bedste tilgang til at løse problemerne og opfylde målene i forslaget.

I forbindelse med udarbejdelsen af dette forslag har Kommissionen foretaget en konsekvensanalyse.

3. FORSLAGETS RETLIGE ASPEKTER

- **Resumé af forslaget**

Selv om direktivet ophæver rammeafgørelse 2005/222/RIA, vil det bevare rammeafgørelsens gældende bestemmelser og indeholde følgende nye elementer:

– Vedrørende materiel strafferet generelt gør direktivet følgende:

A. Det strafbelægger fremstilling, salg, erhvervelse med henblik på brug, import, distribution eller på anden måde stillen til rådighed af anordninger eller værktøj, der anvendes til at begå lovovertrædelserne.

B. Det indeholder bestemmelser om skærpende omstændigheder:

- Omfattende angreb - der vil blive taget hensyn til botnet eller tilsvarende værktøjer, idet der indføres et nyt forhold som skærpende omstændighed, således at det, at der etableres et botnet eller et tilsvarende værktøj, vil være en skærpende omstændighed, når de forbrydelser, der er opført i den gældende rammeafgørelse, begås.

- Når angrebene begås ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører. Disse regler ville skulle være i overensstemmelse med legalitetsprincippet og princippet om, at straffen skal stå i et rimeligt forhold til lovovertrædelsens grovhed, og være i overensstemmelse med gældende lovgivning om beskyttelse af personoplysninger[13].

C. Det indfører "ulovlig opfangning" som en lovovertrædelse.

D. Det indfører foranstaltninger til at forbedre EU-samarbejdet om strafferetspleje ved at styrke den eksisterende struktur med døgnbemandede kontaktpunkter[14]:

- Det foreslås, at der indføres en forpligtelse til at efterkomme anmodninger om bistand fra de operationelle kontaktpunkter (jf. direktivets artikel 14) inden en vis tidsfrist. Konventionen om it-kriminalitet indeholder ikke nogen bindende bestemmelse herom. Formålet med denne foranstaltning er at sikre, at kontaktpunkterne inden en nærmere fastsat frist oplyser, om de kan finde en løsning på anmodningen om bistand, og hvornår det kontaktpunkt, der fremsætter anmodningen, kan forvente, dette sker. Det angives ikke nærmere, nøjagtigt hvori løsningerne skal bestå.

E. Det opfylder behovet for at skaffe statistiske oplysninger om it-forbrydelser ved at gøre det obligatorisk for medlemsstaterne at sikre, at der findes et passende system til registrering, fremstilling og fremlæggelse af statistiske oplysninger om de lovovertrædelser, der er nævnt i den eksisterende rammeafgørelse, samt den nye overtrædelse "opfangning".

---

[13] Såsom Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12.7.2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), EUT L 201 af 31.7.2003, s. 37 (p.t. under revision) og det generelle databeskyttelsesdirektiv 95/46/EF.

[14] Indført ved konventionen og rammeafgørelse 2005/222/RIA om angreb på informationssystemer.

I definitionerne af de strafbare forhold i artikel 3, 4 og 5 (ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer, ulovligt indgreb i data) indeholder direktivet en bestemmelse, der giver adgang til kun at kriminalisere "grovere tilfælde" i forbindelse med gennemførelsen af direktivet i national ret. Dette element af fleksibilitet skal gøre det muligt for medlemsstaterne ikke at dække tilfælde, som ud fra en generel betragtning ville være omfattet af den grundlæggende definition, men som anses for ikke at være til skade for den beskyttede retlige interesse, særligt handlinger begået af unge mennesker, der forsøger at bevise deres ekspertviden i it-teknologi. Denne mulighed for at begrænse kriminaliseringsområdet bør dog ikke føre til, at der indføres yderligere elementer i gerningsindholdet af lovovertrædelserne ud over dem, der allerede er medtaget i direktivet, da dette ville føre til den situation, at kun lovovertrædelser, der begås under skærpende omstændigheder, dækkes. Under gennemførelsen bør medlemsstaterne særligt afholde sig fra at indføje yderligere elementer i gerningsindholdet for de grundlæggende lovovertrædelser, såsom særligt forsæt til at opnå ulovlig vinding fra forbrydelsen eller særlig virkning, såsom at der er forvoldt væsentlig skade.

- **Retsgrundlag**

Artikel 83, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde[15].

- **Nærhedsprincippet**

Nærhedsprincippet gælder for Den Europæiske Unions foranstaltninger. Målene med forslaget kan ikke i tilstrækkelig grad opfyldes af medlemsstaterne af følgende grunde:

It-kriminalitet og navnlig angreb på informationssystemer har en væsentlig grænseoverskridende dimension, som er mest påfaldende i forbindelse med omfattende angreb, hvor de indbyrdes forbundne elementer af angrebet ofte befinder sig på forskellige steder og i forskellige lande. Dette kræver handling fra EU's side, navnlig for at være på forkant med den nuværende tendens til omfattende angreb i Europa og verden over. Der er også blevet opfordret til handling fra EU's side og til en ajourføring af rammeafgørelse 2005/222/RIA i Rådets konklusioner fra november 2008[16], da formålet om effektivt at beskytte borgerne mod it-kriminalitet ikke i tilstrækkeligt omfang kan nås af medlemsstaterne alene.

Målene med forslaget kan opfyldes bedre gennem foranstaltninger på EU-plan af følgende årsager:

Forslaget vil medføre en yderligere indbyrdes tilnærmelse af medlemsstaternes materielle strafferet og retsplejeregler, hvilket vil have en positiv virkning på bekæmpelsen af disse forbrydelser. For det første er det en måde at forebygge, at lovovertræderne flytter til medlemsstater, hvor lovgivningen om it-angreb er mindre streng. For det andet er det muligt at udveksle oplysninger og indsamle og sammenligne relevante data, når de defineres på samme måde. For det tredje fremmes også effektiviteten af forebyggende foranstaltninger over hele EU og det internationale samarbejde.

Forslaget er derfor i overensstemmelse med nærhedsprincippet.

---

[15] EUT C 83 af 30.3. 2010, s. 49.

[16] "Fælles arbejdsstrategi og konkrete foranstaltninger til bekæmpelse af cyberkriminalitet", 2987. møde i Rådet (retlige og indre anliggender), Bruxelles, den 27. og 28. november 2008.

- **Proportionalitetsprincippet**

Forslaget er i overensstemmelse med proportionalitetsprincippet af følgende grunde:

Dette direktiv omfatter kun, hvad der er strengt nødvendigt for at opfylde disse mål på EU-plan, og er ikke mere vidtgående, end hvad der er nødvendigt til dette formål under hensyn til behovet for præcision i straffelovgivningen.

- **Reguleringsmiddel**

Foreslået reguleringsmiddel: direktiv.

Andre midler vil ikke være hensigtsmæssige af følgende grund:

I henhold til hjemlen skal der vedtages et direktiv.

Foranstaltninger af ikke-lovgivningsmæssig karakter og selvregulering ville forbedre situationen på visse områder, hvor gennemførelse er meget vigtig. Men inden for andre områder, hvor ny lovgivning er altafgørende, ville fordelene være begrænsede.

4. BUDGETMÆSSIGE KONSEKVENSER

Forslagets konsekvenser for EU's budget er begrænsede, idet medlemsstaterne ville bære. over 90 % af de anslåede omkostninger på 5 913 000 EUR ville bæres af medlemsstaterne, og det er muligt at ansøge om EU-finansiering til at nedbringe omkostningerne.

5. YDERLIGERE OPLYSNINGER

- **Ophævelse af gældende retsforskrifter**

Vedtagelse af forslaget vil indebære ophævelse af de gældende retsforskrifter.

- **Territorialt anvendelsesområde**

Direktivet er rettet til medlemsstaterne i overensstemmelse med traktaterne.

2010/0273 (COD)

Forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

om angreb på informationssystemer og om ophævelse af Rådets rammeafgørelse 2005/222/RIA

EUROPA-PARLAMENTET OG RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde, særlig artikel 83, stk. 1,

under henvisning til forslag fra Europa-Kommissionen[17],

efter fremsendelse af udkast til lovgivningsmæssig retsakt til de nationale parlamenter,

under henvisning til udtalelse fra Det Europæiske Økonomiske og Sociale Udvalg,

under henvisning til udtalelse fra Regionsudvalget,

efter den almindelige lovgivningsprocedure og

ud fra følgende betragtninger:

(1) Direktivets formål er at tilnærme medlemsstaternes strafferetlige regler til hinanden med hensyn til angreb på informationssystemer og at forbedre samarbejdet mellem de retlige og andre kompetente myndigheder, herunder politiet og andre specialiserede retshåndhævende myndigheder i medlemsstaterne.

(2) Angreb på informationssystemer, især som led i organiseret kriminalitet, er en voksende trussel, og der er i stigende grad bekymring for mulige terrorangreb eller politisk motiverede angreb på informationssystemer, der indgår i medlemsstaternes og Den Europæiske Unions kritiske infrastruktur. Dette er en trussel mod etableringen af et sikrere informationssamfund og et område med frihed, sikkerhed og retfærdighed og kræver derfor en reaktion fra Den Europæiske Unions side.

(3) Der er en klar tendens til, at angrebene på informationssystemer af afgørende betydning for staterne eller for enkelte funktioner i den offentlige eller private sektor bliver stadig farligere, sker hyppigere og er mere omfattende. Denne tendens falder sammen med udviklingen af stadigt mere avancerede værktøjer, der kan bruges af forbrydere til at foretage forskellige typer angreb over internettet.

(4) Fælles definitioner på dette område, især af informationssystemer og edb-data, er vigtige for at sikre samme holdning i alle medlemsstaterne til anvendelsen af dette direktiv.

---

[17] EUT C […] af […], s. […].

(5) Der er behov for at nå frem til en fælles tilgang til gerningsindholdet af strafbare handlinger ved at indføre fælles definitioner af lovovertrædelser med hensyn til ulovlig adgang til informationssystemer, ulovligt indgreb i informationssystemer, ulovligt indgreb i data og ulovlig opfangning.

(6) Medlemsstaterne bør træffe bestemmelse om sanktioner for angreb på informationssystemer. Sanktionerne bør være effektive, stå i et rimeligt forhold til overtrædelsernes grovhed og have afskrækkende virkning.

(7) Der bør fastsættes strengere straffe, når det er en kriminel organisation som defineret i Rådets rammeafgørelse 2008/841/RIA af 24. oktober 2008 om bekæmpelse af organiseret kriminalitet[18], der har begået angrebet på informationssystemet, når angrebet er meget omfattende, og når lovovertrædelsen begås ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører. Der bør også indføres strengere sanktioner, når et sådant angreb har forvoldt alvorlig skade eller har berørt væsentlige interesser.

(8) I sine konklusioner fra mødet den 27. og 28. november 2008 udtalte Rådet, at der burde udvikles en ny strategi sammen med medlemsstaterne og Kommissionen, hvori der skulle tages hensyn til indholdet af Europarådets konvention om it-kriminalitet af 2001. Konventionen udgør den retlige referenceramme for bekæmpelse af it-kriminalitet, herunder angreb på informationssystemer. Dette direktiv bygger på konventionen.

(9) Under hensyn til de forskellige måder, hvorpå angreb kan foretages, og på grund af den hurtige udvikling i hardware og software, bør direktivet omhandle "værktøj", som kan bruges til at begå de lovovertrædelser, der er opført i direktivet. Ved værktøj forstås f.eks. ondsindet software, herunder botnet, der bruges til at begå it-angreb.

(10) Det er ikke hensigten, at direktivet skal pålægge strafferetligt ansvar, når lovovertrædelserne begås uden forsæt til at begå en forbrydelse, f.eks. i forbindelse med tilladt testning eller beskyttelse af informationssystemer.

(11) Direktivet øger vigtigheden af netværk, såsom G8 og Europarådets netværk af kontaktpunkter, der står til disposition døgnet rundt på alle ugens dage, til udveksling af information for at sikre, at der straks ydes bistand i forbindelse med efterforskning eller procedurer vedrørende lovovertrædelser i forbindelse med informationssystemer og data eller indsamling af beviser for en lovovertrædelse i elektronisk form.. På grund af den hastighed, hvormed der kan foretages omfattende angreb, bør medlemsstaterne være i stand til straks at reagere på hastende anmodninger fra netværket af kontaktpunkter. Denne bistand bør bl.a. bestå i at fremme eller sikre, at der træffes foranstaltninger, såsom teknisk rådgivning, opbevaring af data, indsamling af beviser, tilvejebringelse af juridiske oplysninger og opsporing af mistænkte.

(12) Der er behov for at indsamle oplysninger om lovovertrædelser omfattet af dette direktiv med henblik på at få et mere fuldstændigt billede af problemet på EU-plan og dermed bidrage til at finde mere effektive løsninger på problemet. Oplysningerne vil derudover hjælpe specialiserede organer, såsom Europol og Det Europæiske Agentur

[18] EUT L 300 af 11.11.2008, s. 42.

for Net- og Informationssikkerhed, til at foretage en bedre vurdering af it-kriminalitetens omfang og af net- og informationssikkerhedssituationen i Europa.

(13) Betydelige mangler i og forskelle mellem medlemsstaternes lovgivning om angreb på informationssystemer kan hæmme bekæmpelsen af organiseret kriminalitet og terrorisme og kan vanskeliggøre et effektivt samarbejde mellem politi og retsvæsen på dette område. Den omstændighed, at moderne informationssystemer går på tværs af landene og landegrænserne, betyder, at angreb på sådanne systemer har en grænseoverskridende dimension, hvilket understreger det presserende behov for yderligere initiativer med henblik på en indbyrdes tilnærmelse af de strafferetlige regler på området. Derudover bør koordineringen af retsforfølgningen i forbindelse med tilfælde af angreb på informationssystemer være lettet ved vedtagelsen af Rådets rammeafgørelse 2009/948/RIA om forebyggelse og bilæggelse af konflikter om udøvelse af jurisdiktion i straffesager.

(14) Da målene med dette direktiv, dvs. at sikre, at angreb på informationssystemer i alle medlemsstaterne straffes med sanktioner, der er effektive, står i et rimeligt forhold til overtrædelsernes grovhed og har afskrækkende virkning, og at forbedre og fremme det retlige samarbejde ved at fjerne potentielle komplikationer, ikke i tilstrækkelig grad kan opfyldes af medlemsstaterne - idet reglerne skal være fælles og indbyrdes forenelige - og derfor bedre kan gennemføres på EU-plan, kan EU vedtage foranstaltninger i overensstemmelse med nærhedsprincippet, jf. EU-traktatens artikel 5. Dette direktiv går ikke ud over, hvad der er nødvendigt for at nå disse mål.

(15) Alle personoplysninger, der behandles i forbindelse med gennemførelsen af dette direktiv, bør beskyttes i overensstemmelse med reglerne i Rådets rammeafgørelse 2008/977/RIA af 27. november 2008 om beskyttelse af personoplysninger i forbindelse med politisamarbejde og retligt samarbejde i kriminalsager[19], for så vidt angår den databehandling, der er omfattet af rammeafgørelsens anvendelsesområde, og Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger[20].

(16) I dette direktiv overholdes de grundlæggende rettigheder og de principper, som bl.a. er anerkendt i Den Europæiske Unions charter om grundlæggende rettigheder, herunder beskyttelse af personoplysninger, ytrings- og informationsfrihed, ret til en upartisk domstol, uskyldsformodning og ret til et forsvar samt legalitetsprincippet og princippet om proportionalitet mellem lovovertrædelse og straf. Dette direktiv tilsigter især at sikre, at disse rettigheder og principper respekteres fuldt ud, og skal gennemføres i overensstemmelse med dem.

(17) [I medfør af artikel 1, 2, 3 og 4 i protokollen om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed, der er knyttet som bilag til traktaten om Den Europæiske Unions funktionsmåde, har Det Forenede Kongerige og Irland meddelt, at de ønsker at deltage i vedtagelsen og anvendelsen af dette direktiv]/[Med forbehold af artikel 4 i protokollen om Det Forenede Kongeriges og Irlands stilling for så vidt angår området med frihed, sikkerhed og retfærdighed

---

19 EUT L 350 af 30.12.2008, s. 60.

20 EFT L 8 af 12.1.2001, s. 1.

deltager Det Forenede Kongerige og Irland ikke i vedtagelsen af dette direktiv, som derfor ikke er bindende for og ikke finder anvendelse i Det Forenede Kongerige og Irland].

(18) I overensstemmelse med artikel 1 og 2 i protokollen om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Unions funktionsmåde, deltager Danmark ikke i vedtagelsen af dette direktiv, som derfor ikke er bindende for og ikke finder anvendelse i Danmark —

VEDTAGET DETTE DIREKTIV:

Artikel 1

Genstand

Dette direktiv fastsætter nærmere bestemmelser om de strafbare handlinger i forbindelse med angreb på informationssystemer og fastsætter minimumsregler for straffe herfor. Det indfører endvidere fælles bestemmelser om forebyggelse af angrebene og forbedring af EU-samarbejdet om strafferetspleje på dette område.

Artikel 2

Definitioner

I dette direktiv forstås ved:

a) "informationssystem": enhver enhed eller gruppe af indbyrdes forbundne eller beslægtede enheder, hvoraf en eller flere ved hjælp af et program udfører automatisk behandling af edb-data samt edb-data, som lagres, behandles, fremfindes eller overføres i forbindelse med systemernes drift, brug, beskyttelse og vedligeholdelse

b) "edb-data": enhver form for gengivelse af fakta, informationer eller begreber i 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

c) "juridisk person": enhver enhed, der har denne status i henhold til den lovgivning, der finder anvendelse, med undtagelse af stater eller andre offentlige organer, der udøver offentlig myndighed, og offentlige internationale organisationer

d) "uretmæssig": adgang eller indgreb, som ejeren eller en anden retmæssig indehaver af systemet eller en del af det ikke har givet tilladelse til, eller som ikke er tilladt i henhold til national lovgivning.

Artikel 3

Ulovlig adgang til informationssystemer

Medlemsstaterne træffer de nødvendige foranstaltninger for at gøre det strafbart forsætligt at skaffe sig uretmæssig adgang til et informationssystem eller en del heraf, i det mindste i grovere tilfælde.

Artikel 4

Ulovligt indgreb i informationssystemer

Medlemsstaterne træffer de nødvendige foranstaltninger til at gøre det strafbart forsætligt og uretmæssigt at forårsage en alvorlig hindring eller afbrydelse af et informationssystems drift ved at indlæse eller overføre edb-data eller ved at beskadige, slette, forvanske, ændre, tilbageholde eller hindre adgang til dets edb-data, i det mindste i grovere tilfælde.

Artikel 5

Ulovligt indgreb i data

Medlemsstaterne træffer de nødvendige foranstaltninger til at gøre det strafbart forsætligt og uretmæssigt at slette, beskadige, forvanske, ændre, tilbageholde eller hindre adgang til edb-data i et informationssystem, i det mindste i grovere tilfælde.

Artikel 6

Ulovlig opfangning

Medlemsstaterne træffer de nødvendige foranstaltninger til at gøre det strafbart forsætligt og uretmæssigt at opfange ikke-offentlige overførsler af edb-data til, fra eller inden for et informationssystem, herunder elektromagnetisk stråling fra et informationssystem, der indeholder disse edb-data, ved hjælp af tekniske hjælpemidler

Artikel 7

Værktøjer, der anvendes til at begå de strafbare handlinger

Medlemsstaterne træffer de nødvendige foranstaltninger til at gøre det strafbart forsætligt og uretmæssigt at fremstille, sælge, erhverve med henblik på brug, importere, være i besiddelse af, distribuere eller på anden måde foretage tilrådighedsstillelse af følgende, med henblik på at begå en af de strafbare handlinger i artikel 3-6:

a) anordninger, herunder edb-programmer, der hovedsagelig er beregnet eller tilpasset til at begå en af de strafbare handlinger i artikel 3-6

b) edb-password, adgangskoder eller tilsvarende data, hvorved der kan opnås adgang til et helt informationssystem eller en del heraf.

Artikel 8

Anstiftelse, medvirken, tilskyndelse og forsøg

1. Medlemsstaterne sikrer, at det er strafbart at anstifte, medvirke og tilskynde til at begå en strafbar handling som omhandlet i artikel 3-7.

2. Medlemsstaterne sikrer, at det er strafbart at forsøge at begå en strafbar handling som omhandlet i artikel 3-6.

Artikel 9

Sanktioner

1. Medlemsstaterne træffer de nødvendige foranstaltninger for at sikre, at de i artikel 3-8 omhandlede strafbare handlinger kan straffes med strafferetlige sanktioner, der er effektive, står i et rimeligt forhold til den strafbare handlings grovhed og har afskrækkende virkning.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-7 kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst to år.

Artikel 10

Skærpende omstændigheder

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-7 kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås inden for rammerne af en kriminel organisation som defineret i rammeafgørelse 2008/841/RIA.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-6 kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås ved hjælp af et værktøj, der er beregnet til at foretage angreb, der berører et betydeligt antal informationssystemer, eller angreb, der volder betydelig skade, såsom afbrydelse af systemtjenester, økonomiske omkostninger eller tab af personlige data.

3. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at de strafbare handlinger i artikel 3-6 kan straffes med strafferetlige sanktioner med en maksimal fængselsstraf på mindst fem år, når de begås ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører.

Artikel 11

Juridiske personers ansvar

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at juridiske personer kan drages til ansvar for strafbare handlinger, jf. i artikel 3-8, som for at skaffe dem vinding begås af en person, der handler enten alene eller som medlem af et organ under den juridiske person, og som har en ledende stilling inden for den juridiske person baseret på:

   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 intern kontrol.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at den juridiske person kan drages til ansvar, hvis manglende tilsyn eller kontrol fra en af de i stk. 1 omhandlede personers side har gjort det muligt for en person, der er underlagt den juridiske persons myndighed, at begå de strafbare handlinger i artikel 3-8 for at skaffe den juridiske person vinding.

3. Juridiske personers ansvar i henhold til stk. 1 og 2 udelukker ikke strafferetlig retsforfølgning af fysiske personer, der begår eller medvirker til de strafbare handlinger i artikel 3-8.

Artikel 12

Sanktioner over for juridiske personer

1. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at der over for juridiske personer, der kendes ansvarlige i henhold til artikel 11, stk. 1, kan iværksættes sanktioner, der er effektive, står i et rimeligt forhold til lovovertrædelsens grovhed og har afskrækkende virkning, omfatter strafferetlige og andre bøder og kan omfatte andre sanktioner, såsom:

   a) udelukkelse fra offentlige ydelser eller tilskud

   b) midlertidigt eller varigt forbud mod at udøve erhvervsvirksomhed

   c) anbringelse under retsligt tilsyn

   d) likvidation efter retskendelse

   e) midlertidig eller permanent lukning af forretningssteder, der er blevet brugt til at begå den strafbare handling.

2. Medlemsstaterne træffer de nødvendige foranstaltninger til at sikre, at der over for juridiske personer, der kendes ansvarlige i henhold til artikel 11, stk. 2, kan iværksættes sanktioner eller foranstaltninger, der er effektive, står i et rimeligt forhold til lovovertrædelsens grovhed og har afskrækkende virkning.

Artikel 13

Jurisdiktionskompetence

1. Hver medlemsstat fastlægger sin jurisdiktionskompetence i forbindelse med de strafbare handling, der er nævnt i artikel 3-8, når den strafbare handling er begået:

   a) helt eller delvis på den pågældende medlemsstats område eller

   b) af en af dens statsborgere eller en person, som har sædvanlig bopæl på den pågældende medlemsstats område eller

   c) for at skaffe en juridisk person, der har hjemsted på den pågældende medlemsstats område, vinding.

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

   a) gerningsmanden begår den strafbare handling, mens vedkommende fysisk befinder sig på medlemsstatens område, uanset om den strafbare handling er rettet mod et informationssystem på dens område, eller

   b) den strafbare handling begås mod et informationssystem på medlemsstatens område, uanset om gerningsmanden på gerningstidspunktet fysisk befinder sig på dens område.

Artikel 14

Informationsudveksling

1. Med henblik på udveksling af oplysninger om de strafbare handlinger, der er omhandlet i artikel 3-8, skal medlemsstaterne i overensstemmelse med reglerne om databeskyttelse gøre brug af det bestående netværk af kontaktpunkter, der fungerer døgnet rundt, alle ugens dage. Medlemsstaterne sikrer endvidere, at der findes procedurer, så de kan besvare hasteanmodninger inden otte timer. Besvarelsen skal mindst angive, om anmodningen om hjælp vil blive imødekommet, hvordan det vil ske og hvornår.

2. Medlemsstaterne underretter Kommissionen om, hvilket kontaktpunkt de har udpeget til at udveksle oplysninger om de strafbare handlinger i artikel 3-8. Kommissionen videresender oplysningerne til de øvrige medlemsstater.

Artikel 15

Overvågning og statistik

1. Medlemsstaterne sikrer, at der er findes et system til registrering, fremstilling og fremlæggelse af statistiske oplysninger om de strafbare handlinger i artikel 3-8.

2. De statistiske oplysninger i stk. 1 skal mindst omfatte det antal strafbare handlinger, jf. artikel 3-8, der er anmeldt i medlemsstaten, og oplysninger om, hvad der er foretaget på foranledning af anmeldelserne, og skal for hvert år angive antallet af anmeldte forhold, der er efterforsket, antallet af personer, der er blevet retsforfulgt, og antallet af personer, der er blevet dømt for de strafbare handlinger omhandlet i artikel 3-8.

3. Medlemsstaterne fremsender de oplysninger, der er indsamlet i henhold til denne artikel, til Kommissionen. De sikrer tillige, at der offentliggøres en konsolideret oversigt over disse statistiske rapporter.

Artikel 16

Ophævelse af rammeafgørelse 2005/222/RIA

Rammeafgørelse 2005/222/RIA ophæves herved, idet dette dog ikke berører medlemsstaternes forpligtelser med hensyn til frister for gennemførelse i national lovgivning. Henvisninger til den ophævede rammeafgørelse betragtes som henvisninger til dette direktiv.

Artikel 17

Gennemførelse

1. Medlemsstaterne sætter de nødvendige love og administrative bestemmelser i kraft for at efterkomme dette direktiv senest [to år fra vedtagelsen]. De tilsender straks Kommissionen disse bestemmelser med en sammenligningstabel, som viser sammenhængen mellem de pågældende bestemmelser og dette direktiv.

   Bestemmelserne skal ved vedtagelsen indeholde en henvisning til dette direktiv eller skal ved offentliggørelsen ledsages af en sådan henvisning. De nærmere regler for henvisningen fastsættes af medlemsstaterne.

2. Medlemsstaterne tilsender Kommissionen de vigtigste nationale bestemmelser, som de udsteder på det område, der er omfattet af dette direktiv.

Artikel 18

Rapportering

1. Senest [FIRE ÅR FRA VEDTAGELSEN] og derefter hvert tredje år forelægger Kommissionen en beretning om anvendelsen af dette direktiv i medlemsstaterne samt eventuelle forslag for Europa-Parlamentet og Rådet.

2. Medlemsstaterne sender Kommissionen alle de oplysninger, der er relevante for udarbejdelsen af den i stk. 1 omhandlede rapport. Oplysningerne skal omfatte en detaljeret beskrivelse af lovgivningsmæssige og ikke-lovgivningsmæssige foranstaltninger, som er vedtaget i forbindelse med gennemførelsen af direktivet.

Artikel 19

Ikrafttræden

Dette direktiv træder i kraft på tyvendedagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Artikel 20

Adressater

Dette direktiv er rettet til medlemsstaterne i overensstemmelse med traktaterne.

Udfærdiget i Bruxelles, den

På Europa-Parlamentets vegne	*På Rådets vegne*
Formand	*Formand*