EUROPA-KOMMISSIONEN

Bruxelles, den 30.9.2010
SEK(2010) 1123 endelig

ARBEJDSDOKUMENT FRA KOMMISSIONENS TJENESTEGRENE

RESUMÉ AF KONSEKVENSANALYSEN

Ledsagedokument til

forslag til

EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV

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

{COM(2010) 517 final}
{SEC(2010) 1122 final}

RESUMÉ AF KONSEKVENSANALYSEN

1. PROBLEMSTILLING

Antallet af angreb på informationssystemer er steget væsentligt siden vedtagelsen af rammeafgørelsen om angreb på informationssystemer (herefter "rammeafgørelsen"). Et af de ledende internetsikkerhedsfirmaer har rapporteret, at truslerne mod fortrolige oplysninger (i modsætning til offentligt tilgængelige oplysninger) blev øget betydeligt i 2008, idet der var en stigning fra 624 267 til 1 656 227 konstaterede nye trusler i 2008[1]. Endvidere er der observeret en række angreb af hidtil uset stort og farligt omfang såsom angrebene i Estland og Litauen i henholdsvis 2007 og 2008. I marts 2009 blev edb-systemer i regeringsorganer og private organisationer i 103 lande angrebet af et netværk af inficerede computere, der uddrog fortrolige og klassificerede dokumenter[2]. Det blev gjort ved brug af "botnet"[3], dvs. netværk af inficerede computere, der kan styres på afstand. Endelig er verden for tiden vidne til udbredelsen af et botnet kaldet "Conficker" (også kendte som Downup, Downadup og Kido), der har spredt sig og virket i et hidtil uset omfang siden november 2008 og har indvirket på millioner af computere verden over[4].

For det andet gør det en koordineret og effektiv indsats over for disse angreb vanskelig, at der er utilstrækkeligt samarbejde mellem medlemsstaterne og særligt de retshåndhævende og retslige myndigheder inden for EU. Selv om rapporten om gennemførelsen af rammeafgørelsen viser, at størstedelen af medlemsstaterne har indført permanente kontaktpunkter som krævet i henhold til artikel 11 i rammeafgørelsen, er der stadig problemer med deres reaktionsevne og evne til at besvare hastende anmodninger om samarbejde[5].

Det, at der findes et kontaktpunkt, er ingen garanti for, at det fungerer hensigtsmæssigt. I deres meddelelser til Kommissionen har en række af medlemsstaterne anført, at selv om deres respektive kontaktpunkter var etableret, var de ikke i drift døgnet rundt som krævet i henhold til rammeafgørelsen. Det betyder, at de ikke kan reagere på hasteanmodninger uden for normal kontortid. Samarbejde mellem det offentlige og det private bliver ofte hæmmet af kontaktpunkternes ringe effektivitet eller deres manglende evne til at behandle anmodninger om samarbejde fra den private sektor.

For det tredje findes der stadig kun få oplysninger om it-angreb og om politiets og retsvæsnets opfølgning på angrebene. Ikke alle medlemsstaterne indsamler data om it-angreb. De, der gør,

---

1 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf, s.10.

2 www.theglobeandmail.com/servlet/story/RTGAM.20090328.wspy0328/BNStory/International/home?cid=al_gam_mostemail.

3 Udtrykket "botnet" betyder et netværk af computere, der er blevet inficeret at 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 fra en anden computer — ofte uden at brugerne af de inficerede computere har kendskab til det. 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.

4 http://www.lemonde.fr/technologies/article/2009/03/31/virus-conficker-catastrophe-ou-poisson-d-avril_1174916_651865.html.

5 Beretning fra Kommissionen til Rådet i henhold til artikel 12 i Rådets rammeafgørelse af 24. februar 2005 om angreb på informationssystemer, KOM(2008) 0448 endelig.

indsamler dem på en sådan måde, at det på grund af afvigende statistiske metoder i medlemsstaterne ikke er muligt at sammenligne dem.

Befolkningen, dvs. brugere af informationssystemerne, den statslige og lokale forvaltning, internationale organisationer og private virksomheder er blandt ofrene for omfattende angreb på informationssystemer.

Angreb på mål inden for EU kan foretages fra tredjelande og omvendt.

2. NÆRHEDSPRINCIPPET

It-kriminalitet er et egentligt internationalt problem, der kun sjældent kan løses i en rent national sammenhæng. Det er almindeligt accepteret, at handling er nødvendig i EU og internationalt for at forebygge og bekæmpe den. De fleste angreb sker på tværs af EU's grænser. Alle medlemsstaterne er berørt af dem, og der er tegn på, at en væsentlig del af dem indebærer aktiviteter fra en medlemsstat til en anden. Informationssystemerne er ofte teknisk forbundet indbyrdes og afhængige af hinanden på tværs af landegrænserne. Der er derfor enighed blandt de sagkyndige om, at der kræves såvel international som EU-handling, og at det formål effektivt at bekæmpe denne type kriminalitet ikke i tilstrækkeligt omfang kan opnås af medlemsstaterne hver for sig.

En national tilgang til it-kriminalitet indebærer en risiko for fragmentering og ineffektivitet i hele EU. Forskelle i de nationale metoder og mangel på et systematisk samarbejde på tværs af landegrænserne gør de indenlandske modforanstaltninger betydeligt mindre effektive. Det skyldes til dels den indbyrdes forbindelse mellem informationssystemerne, idet et lavt sikkerhedsniveau i et land kan føre til, at andre lande bliver mere udsatte.

3. HVAD ER MÅLENE?

3.1 Generelle, specifikke og operationelle mål

Det overordnede mål med EU-handling er at bekæmpe og retsforfølge kriminalitet, både organiseret og anden kriminalitet, i overensstemmelse med artikel 67 i traktaten om Den Europæiske Unions funktionsmåde ved at bekæmpe omfattende it-angreb på informationssystemer.

A. Specifikt mål: Retsforfølgelse og domfældelse af forbrydere, der er ansvarlige for omfattende angreb, gennem tilnærmelse af strafferetten med hensyn til angreb på informationssystemer.

B. Specifikt mål: Forbedring af samarbejdet på tværs af landegrænserne mellem de retshåndhævende myndigheder.

C. Specifikt mål: Indførelse af effektive overvågningssystemer og indsamling af data.

4. HVILKE LØSNINGSMODELLER FINDES DER?

4.1 Løsning 1: Status quo/ingen nye EU-foranstaltninger

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

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

Ikke-lovgivningsmæssige foranstaltninger ville i forlængelse af programmet til beskyttelse af kritisk informationsinfrastruktur fokusere på retshåndhævelse og samarbejde mellem det offentlige og det private og skulle fremme en yderligere koordineret indsats på EU-niveau. Et ikke-lovgivningsmæssigt forslag kunne omfatte foranstaltninger såsom styrkelse af det eksisterende døgnbemandede netværk af kontaktpunkter for de retshåndhævende myndigheder, oprettelse af et EU-netværk af offentlige og private kontaktpunkter for eksperter i it-kriminalitet og politiet samt udarbejdelse af en EU-standardaftale om serviceniveauet for samarbejde mellem de retshåndhævende myndigheder og den private sektor.

4.3 Løsning 3: Målrettet ajourføring af rammeafgørelsen med henblik på takling af den særlige trussel fra omfattende angreb på informationssystemer

Følges denne løsning, skal der indføres særlig målrettet (dvs. begrænset) lovgivning for at bekæmpe særligt farlige omfattende angreb på informationssystemer. Den målrettede lovgivning ville skulle knyttes til foranstaltninger til at styrke operationelt samarbejde på tværs af landegrænserne til bekæmpelse af angreb på informationssystemer og forhøje de minimumsstraffe, der allerede er fastsat. Denne løsning ville bestå i en ajourføring af den gældende rammeafgørelse samt en række ikke-lovgivningsmæssige foranstaltninger, såsom forbedring af beredskab, sikkerhed og modstandsdygtighed til beskyttelsen af den kritiske informationsinfrastruktur og en forstærkning af instrumenter og procedurer til samarbejde om retshåndhævelse på tværs af landegrænserne og udveksling af erfaringer om den bedste praksis.

4.4 Løsning 4: Omfattende ny EU-lovgivning til bekæmpelse af it-kriminalitet

Nu, hvor der er konstateret et behov for hurtigt at træffe foranstaltninger mod udvikling af avancerede angreb på informationssystemer, opstår spørgsmålet, om det også ville være relevant at indføre mere vidtrækkende EU-lovgivning om it-kriminalitet generelt. Regler herom ville ikke alene skulle 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. Denne EU-lovgivning ville gælde parallelt med Europarådets konvention om it-kriminalitet, som særligt ville blive suppleret med nye bestemmelser, der i EU anses for at være nødvendige.

4.5 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 ligger uden for den nødvendige tidsramme for handling og kan derfor ikke anses for at være en mulig løsning.

5. KONSEKVENSANALYSE

Løsningsmodeller	Økonomiske konsekvenser	Samfundsmæssige konsekvenser	Konsekvenser for de grundlæggende rettigheder	Konsekvenser for tredjelande	Relevans for målene under A, B, C	Overensstemmelse med folkeretten
Løsning 1: Status quo/ingen nye EU-foranstaltninger	0	0	0	-	0	0
Løsning 2: Udvikling af et program til at øge indsatsen for at imødegå angreb på informationssystemer ved hjælp af ikke-lovgivningsmæssige foranstaltninger	-/+	++	-/+	++	A + B ++ C +	-/+
Løsning 3: Målrettet ajourføring af rammeafgørelsen med henblik på takling af truslen fra omfattende angreb på informationssystemer	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Løsning 4: Omfattende ny EU-lovgivning til bekæmpelse af it-kriminalitet	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Fortrukken løsning (løsning 2 og 3) Kombination af ikke-lovgivningsmæssige foranstaltninger og en målrettet ajourføring af rammeafgørelsen	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. HVORVED UDSKILLER LØSNINGERNE SIG FRA HINANDEN?

6.1 Løsning 1: Status quo

Denne løsning vil uundgåeligt føre til, at private, medlemsstaterne og EU som helhed vil være ringere stillet med hensyn til at takle it-kriminalitet på grund af dens art og væksten i den. Selv hvis de eksisterende foranstaltninger blev ført videre på samme niveau, ville det kræve koordinering på EU-plan.

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

Denne løsning har alle de fordele og ulemper, som er forbundet med et "soft law"-reguleringsmiddel. Det positive aspekt er, at det ville være muligt at beskrive hver af løsningsmodellerne på en måde, der stemmer bedst overens med den bedste nationale praksis, og derved gøre det lettere at finde frem til de foranstaltninger, der er mest effektive.

Denne løsning er imidlertid mindre effektiv til at nå målene.

6.3 Løsning 3: Målrettet ajourføring af rammeafgørelsen med henblik på takling af truslen fra omfattende angreb på informationssystemer

Denne løsning giver en målrettet indgriben over for de konstaterede problemer på det rette tidspunkt. Den takler de strafferetlige spørgsmål, der er nødvendige for effektivt at retsforfølge gerningsmændene til denne forbrydelse. Den forbedrer endvidere det internationale samarbejde ved at indføre en mekanisme til straks at yde international bistand i tilfælde af hasteanmodninger om samarbejde og fremmer samarbejdet med den private sektor gennem ledsageforanstaltninger, såsom ekspertmøder. Ved denne løsning indføres der en række skærpende omstændigheder, såsom den omstændighed, at et angreb er særligt omfattende, eller at det er begået ved at skjule gerningsmandens rigtige identitet og skade den, som identiteten egentlig tilhører.

For at gøre det muligt at måle problemets omfang, indføres der endelig forpligtelser til overvågning.

6.4 Løsning 4: Omfattende ny EU-lovgivning til bekæmpelse af it-kriminalitet

Denne løsning har ligesom løsning 3 den fordel, at den fastsætter bindende bestemmelser, og der må derfor forventes et højere effektivitetsniveau, hvis den bliver gennemført fuldt ud. Det forventes også, at den positive virkning af både de lovgivningsmæssige og de ikke-lovgivningsmæssige reguleringsmidler vil blive udnyttet i størst muligt omfang i forbindelse med et bredere spektrum af spørgsmål angående it-kriminalitet end bare omfattende angreb. Derudover ville den takle de strafferetlige regler og samtidig forbedre samarbejde om retshåndhævelsen på tværs af landegrænserne. Denne samlede tilgang er der imidlertid på nuværende stadium ikke enighed om blandt alle interesserede parter, selv om gennemførelsen af den ville udgøre et større fremskridt i kampen mod it-kriminalitet end alle andre løsninger.

7. DEN FORETRUKNE LØSNINGSMODEL

På baggrund af analysen af økonomiske konsekvenser, de samfundsmæssige konsekvenser og konsekvenserne for de grundlæggende rettigheder udgør løsning 2 og 3 den bedste tilgang til problemerne, hvis de fastsatte mål skal nås.

Alt i alt ville den foretrukne løsning være en kombination af løsning 2 og 3, da de supplerer hinanden og derfor bedst opfylder de fastsatte mål, både med hensyn til indhold og timing.

8. OVERVÅGNING OG EVALUERING

Der bør offentliggøres en rapport om gennemførelsen senest to år efter direktivets ikrafttræden. Rapporten bør særligt omhandle den nøjagtige gennemførelse, medlemsstaterne har foretaget af direktivet.

Derudover bør der regelmæssigt foretages evalueringer med henblik på at vurdere, hvordan og i hvilket omfang direktivet har bidraget til at nå målsætningerne. Den første evaluering bør foretages inden fem år efter direktivets ikrafttræden. Kommissionen vil siden offentliggøre rapporter hvert femte år derefter, og de vil omfatte oplysninger om gennemførelsen. På grundlag af konklusionerne og henstillingerne i evalueringerne bør Kommissionen tage stilling til, om der skal foretages flere ændringer i direktivet, eller om der er en anden mulig udvikling i forhold til det.