EUROPEISKA KOMMISSIONEN

Bryssel den 30.9.2010
SEK(2010) 1123 slutlig

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSANALYSEN

Följedokument till

Förslag till

EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV

om angrepp mot informationssystem och om upphävande av rådets rambeslut 2005/222/RIF

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

SAMMANFATTNING AV KONSEKVENSANALYSEN

1. PROBLEMBESKRIVNING

Antalet angrepp mot informationssystem har ökat betydligt sedan rambeslutet om angrepp mot informationssystem antogs. Ett av de ledande it-säkerhetsföretagen har rapporterat att hoten mot konfidentiell information (i motsats till allmänt tillgänglig information) ökade avsevärt under 2008, från 624 267 till 1 656 227 konstaterade nya hot 2008.[1] Vidare har ett antal mycket omfattande och skadliga angrepp kunnat iakttas, till exempel i Estland och Litauen under 2007 respektive 2008. I mars 2009 utsattes datorsystem hos statliga och privata organisationer i 103 länder för angrepp av ett nätverk av infekterade datorer som användes för att komma åt känsliga och sekretessbelagda uppgifter.[2] Detta skedde med hjälp av så kallade botnät[3], nätverk av smittade datorer som kan fjärrstyras. Slutligen kunde världen nyligen bevittna spridningen av ett botnät kallat *Conficker* (även kallat *Downup*, *Downadup* och *Kido*), som sedan november 2008 har spritts i en tidigare okänd omfattning och påverkat miljoner datorer över hela världen.[4]

Det otillräckliga samarbetet mellan EU-medlemsstaterna, särskilt mellan ländernas brottsbekämpande och rättsliga myndigheter, gör det svårt att vidta samordnade och effektiva åtgärder för att möta dessa angrepp. Även om rapporten om genomförandet av rambeslutet om it-angrepp visar att flertalet medlemsstater har inrättat kontaktpunkter som kan nås dygnet runt alla dagar i veckan i enlighet med artikel 11 i rambeslutet om it-angrepp, kvarstår ändå problem som har att göra med deras förmåga att reagera på brådskande förfrågningar om samarbete.[5]

Även om det finns en kontaktpunkt är detta ingen garanti för att den fungerar som avsett. Ett antal medlemsstater har i sina meddelanden till kommissionen angivit att de visserligen har inrättat kontaktpunkter, men att dessa inte var i drift dygnet runt på det sätt som föreskrivs i rambeslutet om it-angrepp. De kan således inte besvara brådskande förfrågningar utanför kontorstid. Samarbetet mellan offentliga och privata organisationer hämmas ofta av kontaktpunkternas bristande effektivitet eller deras oförmåga att hantera förfrågningar om samarbete från den privata sektorn.

Det finns fortfarande inte särskilt mycket information om it-angrepp och om den polisiära och rättsliga uppföljningen av sådana angrepp. Inte alla medlemsstater samlar in information om

---

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

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

3 Begreppet botnät (botnet) beskriver ett nätverk av datorer som infekterats av sabotageprogram (datorvirus). Sådana nätverk av infekterade datorer (zombier) kan aktiveras för att utföra särskilda uppgifter, till exempel angripa informationssystem (*it-angrepp*). Dessa zombier kan styras via en annan dator, ofta utan att de som använder de infekterade datorerna är medvetna om det. Den ”styrande” datorn kallas även kommando- och styrcentral (*command-and-control centre*). De personer som kontrollerar denna ”central” är också gärningsmän, eftersom de använder infekterade datorer för att angripa informationssystem. Att spåra förövarna är mycket svårt, eftersom de datorer som bildar botnätet och utför attackerna kan finnas på en annan plats än gärningsmannen själv.

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

5 Rapport från kommissionen till rådet på grundval av artikel 12 i rådets rambeslut av den 24 februari 2005 om angrepp mot informationssystem, KOM(2008) 0488 slutlig.

it-angrepp. Om de samlar in sådana uppgifter sker det på ett sätt som inte medger några jämförelser, eftersom medlemsstaterna använder sig av olika statistiska metoder.

Bland offren för storskaliga angrepp mot informationssystem finns den allmänhet som använder sig av informationssystemen, statliga och lokala myndigheter, internationella organisationer och privata enheter.

Angreppen kan ske från tredjeländer mot mål i EU och omvänt.

2. SUBSIDIARITET

IT-relaterad brottslighet är verkligen ett internationellt problem som sällan kan bekämpas enbart på ett nationellt plan. Det är allmänt vedertaget att det behövs åtgärder på EU-nivå och internationellt för att förebygga och hantera denna typ av brottslighet. De flesta angrepp sträcker sig över gränserna i EU. De påverkar alla medlemsstater, och det finns bevis för att en avsevärd del av dem involverar verksamhet som sträcker sig från en medlemsstat till en annan. Informationssystemens tekniska sammanlänkning och ömsesidiga beroende sträcker sig ofta över gränserna. Den allmänna uppfattningen bland experter är därför att det behövs såväl internationella insatser som åtgärder på EU-nivå, och att målet att kunna bekämpa sådan brottslighet på ett effektivt sätt inte kan uppnås av medlemsstaterna på egen hand.

En nationell strategi mot it-relaterad brottslighet riskerar att leda till splittring och ineffektivitet ur ett EU-perspektiv. Olikheter mellan de nationella strategierna och avsaknad av ett systematiskt gränsöverskridande samarbete gör inhemska motåtgärder avsevärt mindre effektiva. Detta hänger delvis samman med graden av sammankoppling mellan informationssystemen, som medför att en låg säkerhetsnivå i ett land kan öka sårbarheten i andra länder.

3. MÅL

3.1 Allmänna, särskilda och operativa mål

Det övergripande målet med EU-insatserna är att förebygga och bekämpa brottslighet, organiserad eller ej, i enlighet med artikel 67 i fördraget om Europeiska unionens funktionssätt, genom att bekämpa storskaliga it-relaterade angrepp mot informationssystem.

A Särskilt mål: Åtala och döma gärningsmännen bakom storskaliga angrepp genom tillnärmning av strafflagstiftningen om angrepp mot informationssystem

B Särskilt mål: Förbättra det gränsöverskridande samarbetet mellan brottsbekämpande myndigheter

C Särskilt mål: Inrätta effektiva system för övervakning och informationsinsamling

4. POLITISKA ALTERNATIV

4.1 Alternativ 1: Status Quo / Inga nya åtgärder på EU-nivå

Detta alternativ innebär att EU inte vidtar några ytterligare åtgärder för att bekämpa denna särskilda form av it-brott. Pågående åtgärder ska fortsätta, särskilt programmen för att stärka skyddet av kritisk it-infrastruktur och förbättra samarbetet mot it-brottslighet mellan den offentliga och den privata sektorn.

4.2 Alternativ 2: Utveckling av ett program för att stärka insatserna för att möta angrepp mot informationssystem genom andra åtgärder än lagstiftning

Dessa åtgärder skulle, med undantag för programmet för skydd av kritiskt it-infrastruktur, vara inriktade på gränsöverskridande brottsbekämpning och samarbete mellan den offentliga och den privata sektorn samt bidra till att underlätta ytterligare samordnade insatser på EU-nivå. Ett förslag till andra åtgärder än lagstiftning skulle kunna inbegripa sådana åtgärder som att stärka det befintliga nätverket av ständigt tillgängliga kontaktpunkter för de brottsbekämpande myndigheterna, att införa ett EU-nätverk av offentlig-privata kontaktpunkter, bestående av it-brottsexperter och brottsbekämpande myndigheter, samt att utarbeta en tjänsteavtalsmodell för brottsbekämpande myndigheters samarbete med aktörer inom den privata sektorn.

4.3 Alternativ 3: En målinriktad uppdatering av bestämmelserna i rambeslutet för att möta hotet från storskaliga angrepp mot informationssystem

Detta alternativ innebär att man inför särskild och riktad (d.v.s. begränsad) lagstiftning för att förhindra särskilt farliga storskaliga angrepp mot informationssystem. En sådan riktad lagstiftning skulle kopplas till åtgärder för att stärka det operativa gränsöverskridande samarbetet för att bekämpa angrepp mot informationssystem och för att skärpa redan fastställda minimistraff. Detta alternativ skulle ha formen av en uppdatering av det befintliga rambeslutet om angrepp mot informationssystem, kompletterad med ett antal andra åtgärder, såsom att förbättra beredskapen, säkerheten och motståndskraften hos skyddsfunktionerna i kritisk it-infrastruktur och stärka instrument och förfaranden för gränsöverskridande samarbete mellan brottsbekämpande myndigheter och utbyte av bästa praxis.

4.4 Alternativ 4: Införande av övergripande EU-lagstiftning mot it-relaterad brottslighet

Konstaterandet av att snabba åtgärder bör vidtas för att möta utvecklingen av sofistikerade angrepp mot informationssystem ger upphov till frågan om huruvida det vore lämpligt att även införa en bredare EU-lagstiftning om it-relaterad brottslighet i allmänhet. En sådan lagstiftning skulle inte endast omfatta angrepp mot informationssystem, utan även sådana frågor som it-relaterad finansiell brottslighet, olagligt Internetinnehåll, insamling/lagring/överföring av elektronisk bevisning samt mer detaljerade behörighetsbestämmelser. EU-lagstiftningen i fråga skulle tillämpas parallellt med Europarådets konvention om it-relaterad brottslighet, som särskilt skulle kompletteras med de nya bestämmelser som anses nödvändiga i EU.

4.5 Alternativ 5: Uppdatering av Europarådets konvention om it-relaterad brottslighet

Detta alternativ skulle kräva en betydande omförhandling av den nuvarande konventionen. Det är en långdragen process som inte kan passas in i den tidsram för insatser som föreslås i

konsekvensanalysen. Inte heller tycks det finnas någon vilja från internationellt håll att omförhandla konventionen. En uppdatering av konventionen ligger alltså utanför tidsramen för insatser och kan därför inte betraktas som ett rimligt alternativ.

5. KONSEKVENSANALYS

Alternativ	Ekonomiska konsekvenser	Sociala konsekvenser	Konsekvenser för de grundläggande rättigheterna	Konsekvenser för tredjeländer	Relevans för mål A,B,C	Förenlighet med internationell rätt
Alternativ 1: Status quo / Inga nya åtgärder på EU-nivå	0	0	0	-	0	0
Alternativ 2: Utveckling av ett program för att stärka insatserna för att möta angrepp mot informationssystem genom andra åtgärder än lagstiftning.	-/+	++	-/+	++	A + B ++ C +	-/+
Alternativ 3: En målinriktad uppdatering av bestämmelserna i rambeslutet för att möta hotet från storskaliga angrepp mot informations-system.	--/++	-/+++	-/++	+++	A +++ B +++ C +++	++
Alternativ 4: Införande av övergripande EU-lagstiftning mot it-relaterad brotts-lighet.	---/+++	+++	--/++	++	A ++ B ++ C ++	-/++
Förespråkad lösning (alternativ 2 och 3): andra åtgärder än lagstiftning i kombination med en riktad uppdatering av rambeslutet om angrepp mot informationssystem	--/+++	+++	-/++	+++	A +++ B +++ C +++	++

6. JÄMFÖRELSE MELLAN ALTERNATIVEN

6.1 Alternativ 1: Status Quo

Med hänsyn till it-brottslighetens natur och ökande omfattning kommer detta alternativ ovillkorligen att försätta privata aktörer, medlemsstaterna och unionen som helhet i en mer utsatt position när det gäller möjligheterna att hantera sådan brottslighet. Även med bibehållen insatsnivå skulle det krävas samordning på EU-nivå.

6.2 Alternativ 2: Utarbetande av ett program för att stärka insatserna för att möta angrepp mot informationssystem genom andra åtgärder än lagstiftning

Detta alternativ har alla de fördelar och nackdelar som är förknippade med icke-lagstiftningsåtgärder (*soft law*). Till fördelarna hör att det ger möjlighet att utforma varje lösning på ett sätt som står i överensstämmelse med bästa nationella praxis, vilket underlättar identifieringen av de mest effektiva åtgärderna.

Detta alternativ är dock mindre effektivt när det gäller att uppnå målen.

6.3 Alternativ 3: En målinriktad uppdatering av bestämmelserna i rambeslutet för att möta hotet från storskaliga angrepp mot informationssystem

Detta alternativ gör det möjligt att i rätt tid vidta riktade åtgärder för att möta de konstaterade problemen. Det tar upp de straffrättsliga lösningar som krävs för effektiv en lagföring av gärningsmännen bakom dessa brott. Det bidrar också till att förbättra det internationella samarbetet genom att införa en mekanism för omedelbart internationellt bistånd vid brådskande förfrågningar om samarbete, och främjar samarbete med den privata sektorn genom kompletterande åtgärder i form av exempelvis expertmöten. Med detta alternativ införs även ett antal försvårande omständigheter, t.ex. om angreppet är storskaligt eller om angreppet utförs genom att gärningsmannens verkliga identitet döljs, till skada för den som identiteten faktiskt tillhör.

För att göra det möjligt att mäta problemets omfattning införs slutligen övervakningsskyldigheter.

6.4 Alternativ 4: Införande av en övergripande EU-lagstiftning mot it-brottslighet

Detta alternativ har i likhet med alternativ 3 de fördelar som ligger i att införa bindande bestämmelser, vilket gör att man kan man förvänta sig en högre grad av effektivitet om det genomförs till fullo. Det förväntas också bidra till att maximera de positiva verkningarna av såväl lagstiftning som andra typer av instrument i ett bredare sammanhang, där även andra it-brottsrelaterade frågor än storskaliga angrepp berörs. Dessutom skulle det ta upp den straffrättsliga ramen och samtidigt bidra till att förbättra samarbetet mellan medlemsstaterna på det brottsbekämpande området. Ett sådant helhetsperspektiv får dock för närvarande inget samlat stöd från de berörda aktörerna, trots att det skulle föra kampen mot it-brott ett steg längre än alla andra alternativ.

7. FÖRESPRÅKAT ALTERNATIV

Efter en analys av de ekonomiska och sociala konsekvenserna samt av påverkan på de grundläggande rättigheterna kan det konstateras att alternativ 2 och 3 innebär den bästa lösningen på problemen, om man vill uppnå de fastställda målen.

Sammantaget skulle det förespråkade alternativet bestå av en kombination av alternativ 2 och 3, eftersom de kompletterar varandra och därför bäst svarar mot de fastställda målen, både till sitt innehåll och tidsmässigt.

8. ÖVERVAKNING OCH UTVÄRDERING

En genomföranderapport bör offentliggöras inom två år från den dag då detta direktiv träder i kraft. Rapporten ska ta upp exakt vilka åtgärder medlemsstaterna har vidtagit för att genomföra direktivet.

Dessutom bör regelbundna utvärderingar genomföras för att bedöma hur och i vilken utsträckning direktivet har bidragit till att nå de uppställda målen. Den första utvärderingen bör genomföras inom fem år från ikraftträdandet av detta direktiv. Kommissionen kommer därefter att lägga fram utvärderingsrapporter vart femte år, med uppgifter om genomförandeläget. Kommissionen bör använda de slutsatser och rekommendationer som framkommer vid utvärderingarna som underlag för att ta ställning till om direktivet behöver ändras eller bli föremål för eventuella andra åtgärder.