KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 30.3.2009
KOM(2009) 149 endelig

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

om beskyttelse af kritisk informationsinfrastruktur

"Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed"

{SEK(2009) 399}
{SEK(2009) 400}

(forelagt af Kommissionen)

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

om beskyttelse af kritisk informationsinfrastruktur

"Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed"

1. INDLEDNING

Informations- og kommunikationsteknologi (ikt) indgår i stigende grad i alle aspekter af vores hverdag. Nogle af disse ikt-systemer, -net og -tjenester (i det følgende betegnet ikt-infrastruktur) spiller en helt afgørende rolle i den europæiske økonomi og det europæiske samfund som grundlag for levering af uundværlige varer og tjenesteydelser eller som basis for andre kritiske infrastrukturer. De anses typisk for kritisk informationsinfrastruktur[1], eftersom det vil have alvorlige følger for samfundets kritiske funktioner, hvis de bryder sammen eller bliver ødelagt. Eksempler af nyere dato på trusler mod kritisk informationsinfrastruktur er de storstilede cyberangreb rettet mod Estland i 2007 og bruddet på transkontinentale kabler i 2008.

Det Verdensøkonomiske Forum skønnede i 2008, at der er 10 - 20 procents sandsynlighed for et større sammenbrud i den kritiske informationsinfrastruktur inden for de næste 10 år, der potentielt kan medføre økonomiske omkostninger på verdensplan på omkring 250 mia. USD[2].

Denne meddelelse lægger især vægt på forebyggelse, beredskab og bevidstgørelse og opstiller en plan over øjeblikkelige tiltag, der skal styrke sikkerheden og robustheden i kritisk informationsinfrastruktur. Vægtningen afspejler den debat, der er igangsat på Rådets og Europa-Parlamentets anmodning, om udfordringerne og hovedmålene for politikken for net- og informationssikkerhed samt om, hvilke midler der er bedst egnet til at gribe udfordringerne an på EU-plan. De foreslåede tiltag skal supplere indsatsen for at forebygge, bekæmpe og retsforfølge kriminalitet og terrorisme rettet mod kritisk infrastruktur og indgår i et samspil med nuværende og planlagte EU-forskningsaktiviteter inden for net- og informationssikkerhed samt med internationale initiativer på dette område.

2. DEN POLITISKE BAGGRUND

Denne meddelelse bygger videre på EU's politik for at styrke sikkerheden i og tilliden til informationssamfundet. Allerede i 2005 fremhævede Kommissionen[3] det akutte behov for en koordineret indsats for at opbygge tillid til elektroniske kommunikationsnet og -tjenester blandt interesseparterne. Til dette formål blev der i 2006 vedtaget en strategi for et sikkert informationssamfund[4]. Hovedelementerne heri, der blandt andet omfatter ikt-infrastrukturens

---

1 En definition af kritisk informationsinfrastruktur blev foreslået i KOM(2005) 576 endelig.
2 Global Risks 2008.
3 KOM(2005) 229.
4 KOM(2006) 251.

sikkerhed og robusthed, blev godkendt af Rådet i dets resolution 2007/068/01. Imidlertid ser det ud til, at de berørte parter ikke i tilstrækkelig grad har taget strategien til sig og gjort en indsats for at føre den ud i livet. Strategien styrker også - både på det taktiske og det praktiske plan - den rolle, der varetages af Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA), der blev oprettet i 2004 med det formål at bidrage til at sikre et højt niveau af net- og informationssikkerhed i Fællesskabet og udvikle en net- og informationssikkerhedskultur til gavn for EU's borgere, virksomheder og administrationer.

I 2008 blev ENISA's mandat forlænget i uændret form indtil marts 2012[5]. Samtidig efterlyste Rådet og Europa-Parlamentet *"yderligere drøftelser af ENISA's fremtid [og] […] overvejelser om den generelle retning for EU's bestræbelser hen imod et udvidet net- og informationssamfund."* For at støtte denne debat iværksatte Kommissionen i november 2008 en offentlig høring på internettet[6]. Resultaterne af høringen vil blive offentliggjort snarest.

De aktiviteter, der skitseres i nærværende meddelelse, vil blive gennemført som led i og parallelt med det europæiske program for beskyttelse af kritisk infrastruktur (EPCIP)[7]. Et af nøgleelementerne i dette program er direktivet[8] om indkredsning og udpegning af europæisk kritisk infrastruktur[9], der peger på ikt-sektoren som et højt prioriteret område for fremtidige tiltag. Endnu et vigtigt element i programmet er informations- og varslingsnetværket vedrørende kritisk infrastruktur (CIWIN)[10].

På lovgivningssiden indeholder Kommissionens forslag om en reform af regelsættet for elektroniske kommunikationsnet og -tjenester[11] nye bestemmelser om sikkerhed og integritet, der navnlig har til formål at skærpe operatørerne forpligtelser til at sikre, at der træffes passende forholdsregler for at imødegå konstaterede risici, garantere kontinuitet i leveringen af tjenester og anmelde brud på sikkerheden[12]. Denne fremgangsmåde vil bidrage til at nå det overordnede mål om at gøre kritisk informationsinfrastruktur mere sikker og robust. Europa-Parlamentet og Rådet har bakket bredt op om disse bestemmelser.

De foranstaltninger, der foreslås i denne meddelelse, supplerer eksisterende og fremtidige tiltag på området politisamarbejde og retligt samarbejde, der går ud på at forebygge, bekæmpe og retsforfølge kriminalitet og terrorisme rettet mod ikt-infrastruktur, således som der lægges op til i blandt andet Rådets rammeafgørelse om angreb på informationssystemer[13] og den planlagte ajourføring heraf[14].

Som baggrund for meddelelsen indgår også NATO's tiltag vedrørende en fælles politik for forsvar mod cyberangreb, dvs. Cyber Defence Management Authority og Cooperative Cyber Defence Centre of Excellence.

---

5 Forordning (EF) nr. 1007/2008.
6 http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464
7 KOM(2006) 786 endelig.
8 Rådets direktiv 2008/114/EF.
9 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf
10 KOM(2008) 676 endelig.
11 KOM(2007) 697, KOM(2007) 698, KOM(2007) 699.
12 Artikel 13 i rammedirektivet.
13 2005/222/RIA.
14 KOM(2008) 712.

Endelig tages der passende hensyn til den politiske udvikling på internationalt plan, især G8-principperne om beskyttelse af kritisk informationsinfrastruktur[15], FN's generalforsamlings resolution 58/199 om en verdensomspændende internetsikkerhedskultur og beskyttelse af kritisk informationsinfrastruktur samt den nylige OECD-anbefaling om beskyttelse af kritisk informationsinfrastruktur.

3. HVAD STÅR DER PÅ SPIL?

3.1. Kritisk informationsinfrastruktur er uundværlig for økonomien og for samfundsmæssig vækst i EU

Ikt-sektorens og ikt-infrastrukturens økonomiske og samfundsmæssige rolle fremhæves i en række nylige rapporter om innovation og økonomisk vækst, herunder meddelelsen om midtvejsevalueringen af i2010-initiativet[16], Ahogruppens rapport[17] og EU's årlige økonomiske rapporter[18]. OECD understreger den vigtige rolle, ikt og internettet spiller som drivkraft for økonomisk fremgang og social velfærd og som middel til at styrke samfundets muligheder for at forbedre befolkningens livskvalitet verden over[19]. Desuden anbefaler OECD, at der gøres en indsats for at øge tilliden til internetinfrastrukturen.

Ikt-sektoren er af afgørende betydning for alle dele af samfundet. Virksomhederne er afhængige af ikt-sektoren, både i forbindelse med direkte salg, og når det gælder effektiviteten i de interne virksomhedsprocesser. Ikt er et afgørende element i innovation og kilde til næsten 40 % af produktivitetsstigningen[20]. Ikt er også et gennemgående element i regeringernes og de offentlige administrationers arbejde: indførelsen af e-forvaltning på alle niveauer samt nye anvendelser af ikt som f.eks. innovative løsninger på sundhedsområdet og energiområdet og deltagelse i den politiske beslutningsproces ad elektronisk vej, gør den offentlige sektor stærkt afhængig af ikt. Sidst men ikke mindst er borgerne i stigende grad afhængige af ikt i deres hverdag. Styrket sikkerhed omkring kritisk informationsinfrastruktur vil øge borgernes tillid til ikt, ikke mindst fordi det betyder bedre beskyttelse af personoplysninger og privatlivets fred.

3.2. Truslerne mod kritisk informationsinfrastruktur

De risici, der er forbundet med bevidste angreb, naturkatastrofer eller tekniske uheld, er ofte ikke fuldt afdækket og/eller tilstrækkeligt analyseret. Resultatet er, at de berørte parter ikke er tilstrækkeligt bevidste om risiciene til at udtænke virkningsfulde sikkerheds- og modforholdsregler.

Cyberangrebene er blevet mere sofistikerede end nogensinde før. Simple forsøg bliver til raffinerede aktiviteter, der udføres med økonomisk udbytte eller politiske mål for øje. De seneste storstilede angreb på Estland, Litauen og Georgien er de mest omtalte eksempler på en generel tendens. Det enorme antal virusser, orme og andre former for skadelig software,

---

15 http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf
16 KOM(2008) 199 endelig.
17 http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm
18 Økonomien i EU: oversigt 2007, http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf
19 http://www.oecd.org/dataoecd/1/29/40821707.pdf
20 http://epp.eurostat.ec.europa.eu/ - Videnskab og teknologi, informationssamfundet.

udbredelsen af botnet og den vedvarende stigning i mængden af spam bekræfter problemets alvor[21].

Samfundets afhængighed af kritisk informationsinfrastruktur og informationsinfrastrukturens sammenhæng på tværs af grænserne og med anden infrastruktur samt dens sårbarhed og truslerne mod den gør, at det som første skridt i et forsvar mod svigt og angreb er nødvendigt at drøfte spørgsmålet om sikkerhed og robusthed ud fra et systemisk perspektiv.

3.3. En sikker og robust kritisk informationsinfrastruktur skal styrke tilliden til informationssamfundet

For at sikre, at ikt-infrastrukturen udnyttes så intensivt som overhovedet muligt, og dermed, at informationssamfundets økonomiske og sociale muligheder udnyttes fuldt ud, er det nødvendigt, at alle berørte parter har tillid til infrastrukturen. Tilliden afhænger af forskellige faktorer, med den vigtigste er et højt niveau af sikkerhed og robusthed. De forskellige komponenters diversitet, åbenhed, interoperabilitet, anvendelighed, gennemskuelighed, ansvarlighed og kontrollerbarhed samt konkurrence er vigtige faktorer i udviklingen af sikkerhed og stimulerer udbredelsen af sikkerhedsfremmende produkter, processer og tjenester. Som Kommissionen allerede har påpeget[22], er ikt-infrastrukturens sikkerhed et fælles ansvar: ingen enkelt aktør har de nødvendige midler til at garantere sikkerheden og robustheden i samtlige dele af infrastrukturen og påtage sig de dermed forbundne ansvarsopgaver.

Disse opgaver kræver en risikostyringsstrategi og -kultur, der gør det muligt at reagere på kendte trusler og forudse ukendte fremtidige trusler uden at overreagere og kvæle nyopdukkende innovative tjenester og applikationer.

3.4. Udfordringerne for Europa

Ud over alle aktiviteterne i forbindelse med gennemførelsen af direktivet om indkredsning og udpegning af europæisk kritisk infrastruktur, særlig opstillingen af ikt-sektorspecifikke kriterier, må vi gribe en række bredere udfordringer an for at gøre den kritiske informationsinfrastruktur sikrere og mere robust.

3.4.1. Uens og ukoordinerede nationale strategier

Selv om medlemsstaterne står over for udfordringer og problemer af samme art, er det forskelligt, hvilke foranstaltninger og ordninger de iværksætter for at gøre ikt-infrastrukturen sikker og robust, og hvilken grad af ekspertise og beredskab de sætter ind.

En rent nationalt orienteret strategi risikerer at resultere i opsplitning og ineffektivitet i Europa. Forskellene mellem de nationale strategier og manglen på systematisk tværnationalt samarbejde gør de nationale forholdsregler væsentligt mindre virkningsfulde, blandt andet fordi sammenhængen mellem ikt-infrastruktur på tværs af grænserne betyder, at et lavt sikkerhedsniveau i ét land potentielt kan øge sårbarheden og risiciene i andre lande.

Derfor er der behov for en europæisk indsats, der kan give de nationale politikker og programmer merværdi ved at skabe øget bevidsthed om og en fælles forståelse af

---

21 KOM(2006) 688 endelig.

22 KOM(2006) 251 endelig.

udfordringerne, sætte gang i vedtagelsen af fælles politiske mål og indsatsområder, styrke samarbejdet mellem medlemsstaterne og integrere de nationale politikker i et mere europæisk og verdensomspændende perspektiv.

3.4.2. Behovet for en ny europæisk forvaltningsmodel for kritisk informationsinfrastruktur

At gøre ikt-infrastrukturen mere sikker og robust er en opgave, der byder på helt særlige forvaltningsmæssige udfordringer. Selv om det i sidste ende er medlemsstaterne, der er ansvarlige for at fastlægge politikken for kritisk informationsinfrastruktur, er gennemførelsen af politikken afhængig af den private sektor, der ejer eller kontrollerer store dele af infrastrukturen. På den anden side giver markederne ikke altid den private sektor tilstrækkelige incitamenter til at investere i beskyttelse af kritisk informationsinfrastruktur i det omfang, som staten normalt ville kræve.

Som en løsning på dette forvaltningsmæssige problem er der vokset offentlig-private partnerskaber frem på nationalt plan, der kan fungere som referencemodel. Men trods bred enighed om, at offentlig-private partnerskaber også ville være ønskelige på europæisk plan, er der endnu ikke etableret sådanne europæiske partnerskaber. En europadækkende forvaltningsramme, der involverer en række forskellige parter, og som blandt andet kunne omfatte en styrket rolle for ENISA, kan øge den private sektors engagement i fastlæggelsen af strategiske forvaltningspolitiske mål samt konkrete indsatsområder og foranstaltninger. En sådan ramme ville slå bro over kløften mellem den politiske beslutningsproces på nationalt plan og den praktiske virkelighed.

3.4.3. Begrænset europæisk forvarslings- og reaktionsevne

Forvaltningsordninger bliver kun virkelig effektive, hvis alle deltagere har pålidelige oplysninger at handle ud fra. Dette er særlig relevant for regeringerne, der bærer det endelige ansvar for borgernes sikkerhed og trivsel.

Imidlertid varierer processerne og fremgangsmåderne for overvågning og rapportering af sikkerhedshændelser på nettene betydeligt fra medlemsstat til medlemsstat. Nogle medlemsstater har ingen referenceorganisation for overvågningen. Endnu alvorligere er det, at samarbejdet og informationsudvekslingen mellem medlemsstaterne af pålidelige og brugbare oplysninger om sikkerhedshændelser ikke synes tilstrækkeligt udbygget, idet der kun er tale om et uformelt samarbejde eller bilaterale eller begrænset multilaterale forbindelser. Simulering af sikkerhedshændelser og beredskabsøvelser er strategisk vigtige foranstaltninger i indsatsen for at gøre ikt-infrastrukturen mere sikker og robust, særlig fordi de fremhæver betydningen af fleksible strategier og processer, der gør det muligt at håndtere uforudsigeligheden i potentielle kriser. I EU befinder sådanne foranstaltninger sig imidlertid på begynderstadiet. Beredskabsøvelserne på tværs af grænserne er yderst begrænsede. Som en række begivenheder for nylig har vist[23], er gensidig bistand et væsentligt element i en effektiv reaktion på storstilede trusler og angreb på kritisk informationsinfrastruktur.

En stærk europæisk forvarslings- og reaktionsevne forudsætter velfungerende landsdækkende/statslige it-beredskabsenheder (CERT - Computer Emergency Response Team), der har en fælles basiskapacitet. Disse beredskabsenheder skal mobilisere de berørte parter på nationalt plan og gennemføre forvaltningspolitiske aktiviteter (blandt andet

---

[23] http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/

oplysnings- og varslingsaktiviteter rettet mod borgerne og små og mellemstore virksomheder). Desuden skal de indgå i et effektivt samarbejde og i informationsudveksling på tværs af grænserne, eventuelt via eksisterende organisationer som EGC (European Governmental CERTs Group)[24].

3.4.4. Internationalt samarbejde

Internettet har indtaget en nøglerolle som kritisk informationsinfrastruktur, der betyder, at der må lægges særlig vægt på dets robusthed og stabilitet. Internettet har vist sig at være en meget robust infrastruktur takket være sin distribuerede og redundante opbygning. Dets enorme vækst har imidlertid medført en stigende fysisk og logisk kompleksitet samt et væld af nye tjenester og anvendelser. Derfor er det rimeligt at stille spørgsmålstegn ved, om internettet er i stand til at modstå det stigende antal cyberangreb og andre sikkerhedshændelser.

De divergerende meninger om, hvor kritiske internettets forskellige elementer er, forklarer delvis de mange forskellige regeringsholdninger, der kommer til udtryk i internationale fora, og de ofte indbyrdes modsigende opfattelser af, hvor vigtigt spørgsmålet om internettets robusthed er. Dette kan gøre det vanskeligt at forebygge, modstå og overvinde trusler mod internettet. For eksempel bør konsekvenserne af overgangen fra IPv4 til IPv6 også vurderes ud fra en sikkerhedsmæssig synsvinkel.

Internettet er et verdensomspændende og stærkt distribueret net af net med kontrolcentre, der ikke nødvendigvis følger landegrænserne. For at sikre et robust og stabilt internet skal der derfor en særlig målrettet strategi til, der bygger på to indbyrdes sammenhængende tiltag. For det første skal der skabes bred enighed om de vigtigste europæiske mål for den offentlige politik og den praktiske indsats, der skal sikre internettets robusthed og stabilitet. For det andet skal verdenssamfundet gennem den strategiske dialog og samarbejdet med tredjelande og internationale organisationer inddrages i opstillingen af et sæt principper for internettets robusthed og stabilitet, der afspejler europæiske kerneværdier. Disse aktiviteter skal bygge på resultaterne af verdenstopmødet om informationssamfundet[25] og dets anerkendelse af, hvor altafgørende et stabilt internet er.

4. VEJEN FREM: ØGET KOORDINERING OG SAMARBEJDE PÅ EU-PLAN

På grund af problemets europæiske og internationale dimension vil en integreret EU-strategi for øget sikkerhed og robusthed i kritisk informationsinfrastruktur supplere og øge værdien af de nationale programmer såvel som eksisterende bilaterale og multilaterale samarbejdsordninger mellem medlemsstaterne.

De forvaltningspolitiske drøftelser i kølvandet på begivenhederne i Estland tyder på, at konsekvenserne af lignende angreb kan begrænses ved forebyggende foranstaltninger og gennem koordinerede tiltag i løbet af selve krisen. En mere struktureret udveksling af oplysninger og god praksis i EU vil gøre det betydeligt lettere at bekæmpe grænseoverskridende trusler.

Det er nødvendigt at styrke de eksisterende samarbejdsorganer, herunder ENISA, og eventuelt skabe nye ordninger. Det er vigtigt, at samarbejdet omfatter mange forskellige parter og

---

24 http://www.egc-group.org/

25 Tunisdagsordenen for informationssamfundet, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

foregår på mange forskellige niveauer, idet det koordineres på europæisk plan men samtidig supplerer og fuldt ud respekterer de nationale ansvarsområder.

En indgående forståelse af rammerne og begrænsningerne er nødvendig. For eksempel er internettets distribuerede karakter et problem, fordi denne egenskab medfører, at kantknuder (edge nodes) kan udnyttes som bærere af angreb, f.eks. gennem botnet. Imidlertid er netop den distribuerede karakter et nøgleelement i internettets stabilitet og robusthed, som kan medvirke til en hurtigere genopretning end det normalt ville være tilfældet med overformaliserede topstyrede procedurer. Derfor må der i hvert enkelt tilfælde foretages en omhyggelig analyse af, hvilken forvaltningspolitik og hvilke praktiske procedurer der er de bedst egnede.

Tidsplanen er også vigtig. Der er klart behov for at skride til handling øjeblikkeligt og hurtigt få de elementer på plads, der er nødvendige for at opbygge en ramme, som vil sætte os i stand til at reagere på de nuværende udfordringer, og som kan indgå i den fremtidige strategi for net- og informationssikkerhed.

Med henblik på at løfte disse udfordringer foreslår Kommissionen fem indsatsområder:

1) Beredskab og forebyggelse: at sikre beredskabet på alle planer

2) Opdagelse og reaktion: at sørge for tilstrækkelige forvarslingsordninger

3) Afhjælpning og genopretning: at styrke EU's forsvarsmekanismer for kritisk informationsinfrastruktur

4) Internationalt samarbejde: at fremme EU's mål på internationalt plan

5) Kriterier for ikt-sektoren: at støtte gennemførelsen af direktivet om indkredsning og udpegning af europæisk kritisk infrastruktur[26].

5. HANDLINGSPLAN

5.1. Beredskab og forebyggelse

Basisniveau af kapacitet og tjenester med henblik på et europadækkende samarbejde. Kommissionen opfordrer medlemsstaterne til

- med støtte fra ENISA at fastlægge et minimumsniveau af kapacitet og tjenester, som de landsdækkende/statslige it-beredskabsenheder (CERT) og reaktionsforanstaltningerne skal opfylde, så samarbejdet på europæisk plan kan fungere bedre.

- sikre, at de landsdækkende/statslige CERT-enheder fungerer som nøglekomponent i det nationale beredskab og i informationsudveksling, koordinering og reaktion på sikkerhedshændelser.

[26] Rådets direktiv 2008/114/EF.

Mål: minimumstandarderne skal være fastlagt ved udgangen af 2010; der skal være oprettet velfungerende landsdækkende/statslige CERT-enheder i alle medlemsstater ved udgangen af 2011.

Et europæisk offentlig-privat partnerskab for en robust infrastruktur (EP3R). Kommissionen vil

- støtte samarbejdet mellem den offentlige og den private sektor om målene for sikkerhed og robusthed, basiskrav, god strategisk praksis og foranstaltninger. Partnerskabets hovedvægt skal ligge på den europæiske dimension, set ud fra både et strategisk perspektiv (dvs. vedrørende god praksis på det politiske plan) og et taktisk/operationelt perspektiv (dvs. vedrørende den praktiske gennemførelse i den private sektor). Partnerskabet bør bygge på og supplere eksisterende nationale initiativer og ENISA's operationelle aktiviteter.

Mål: der skal foreligge en køreplan for EP3R ved udgangen af 2009; EP3R skal være etableret midt i 2010; de første resultater af partnerskabet skal foreligge i slutningen af 2010.

Europæisk forum for informationsudveksling mellem medlemsstaterne. Kommissionen vil

- etablere et europæisk forum, hvor medlemsstaterne kan udveksle information og god strategisk praksis vedrørende sikkerheden og robustheden i kritisk informationsinfrastruktur. Dette forum skal udnytte resultaterne af andre organisationers aktiviteter, særlig ENISA's.

Mål: forummet skal være etableret ved udgangen af 2009; forummets første resultater skal foreligge i slutningen af 2010.

5.2. Opdagelse og reaktion

Europæisk informationsudvekslings- og varslingssystem (EISAS). Kommissionen støtter

udviklingen og indførelsen af et europæisk informationsudvekslings- og varslingssystem (EISAS), der når ud til borgerne og de små og mellemstore virksomheder, og som er baseret på medlemsstaternes og den private sektors informationsudvekslings- og varslingssystemer. Kommissionen yder økonomisk støtte til to indbyrdes supplerende prototypeprojekter[27]. ENISA opfordres til at gøre status over resultaterne af disse projekter og andre nationale initiativer og opstille en køreplan for at fremme udviklingen og indførelsen af EISAS.

Mål: prototypeprojekterne skal være afsluttet ved udgangen af 2010; køreplanen for et europæisk informationsudvekslings- og varslingssystem skal foreligge i slutningen af 2010.

5.3. Afhjælpning og genopretning

Nationale katastrofeplaner og -øvelser. Kommissionen opfordrer medlemsstaterne til at

[27] Som led i fællesskabsprogrammet "*Forebyggelse, beredskab og konsekvensstyring i forbindelse med terrorisme og andre sikkerhedsrelaterede risici*". http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm

- udforme nationale katastrofeplaner og afholde jævnlige øvelser i håndtering af omfattende netsikkerhedshændelser og efterfølgende genopretning som et skridt på vejen mod en europadækkende koordinering. De landsdækkende/statslige it-beredskabsenheder (CERT (Computer Emergency Response Team) eller CSIRT (Computer Security Incident Response Team)) kan få til opgave at lede katastrofeøvelser til afprøvning af de nationale katastrofeplaner med deltagelse af parter fra både den private og den offentlige sektor. ENISA bør støtte udveksling af god praksis mellem medlemsstaterne.

Mål: der skal være gennemført mindst én national katastrofeøvelse i hver medlemsstat inden udgangen af 2010.

Fælleseuropæiske øvelser i håndtering af omfattende netsikkerhedshændelser. Kommissionen vil

- yde økonomisk støtte til tilrettelæggelse af fælleseuropæiske øvelser i håndtering af hændelser, der truer internettets sikkerhed[28]; sådanne øvelser kan også udgøre det praktiske grundlag for fælleseuropæisk deltagelse i tilsvarende øvelser på internationalt plan, f.eks. den amerikanske "Cyber Storm".

Mål: den første fælleseuropæiske øvelse skal være tilrettelagt og gennemført inden udgangen af 2010; der skal være fælleseuropæisk deltagelse i internationale øvelser inden udgangen af 2010.

Styrket samarbejde mellem landsdækkende/statslige CERT-enheder. Kommissionen opfordrer medlemsstaternes til at

- styrke samarbejdet mellem de landsdækkende/statslige CERT-enheder, også ved at udnytte og udvide de eksisterende samarbejdsordninger såsom EGC[29]. ENISA bør aktivt stimulere og støtte det fælleseuropæiske samarbejde mellem de landsdækkende/statslige CERT-enheder, der bør resultere i et styrket beredskab, styrket europæisk evne til at reagere på sikkerhedshændelser samt fælleseuropæiske (og/eller regionale) øvelser.

Mål: antallet af nationale instanser, der deltager i ECG, skal være fordoblet inden udgangen af 2010; ENISA skal udarbejde referencemateriale til støtte for et fælleseuropæisk samarbejde inden udgangen af 2010.

5.4. Internationalt samarbejde

Et robust og stabilt internet. Der lægges op til tre indbyrdes supplerende aktiviteter:

- EU's vigtigste mål for langsigtet robusthed og stabilitet i internettet. Kommissionen vil sætte gang i en europadækkende debat med deltagelse af alle relevante offentlige og private parter med det formål at fastlægge EU's vigtigste mål for langsigtet robusthed og stabilitet.

Mål: EU's vigtigste mål vedrørende kritiske internetkomponenter og -spørgsmål skal ligge fast inden udgangen af 2010.

---

[28] Se fodnote 27.
[29] Se fodnote 24.

- Principper og retningslinjer for et robust og stabilt internet (europæisk plan). Kommissionen vil samarbejde med medlemsstaterne om at opstille retningslinjer for internettets robusthed og stabilitet, idet der lægges særlig vægt på regionale udbedrende foranstaltninger, aftaler om gensidig bistand, koordinerede genopretnings- og kontinuitetsstrategier, den geografiske fordeling af kritiske internetressourcer, teknologiske sikkerhedsforanstaltninger i internettets arkitektur og protokoller, reproducerbare og forskelligartede tjenester og data. Kommissionen finansierer allerede en taskforce vedrørende robusthed i domænenavnssystemet, der sammen med andre relevante projekter skal være med til at opbygge konsensus på europæisk plan[30].

Mål: der skal foreligge en europæisk køreplan for opstilling af principper og retningslinjer for et robust og stabilt internet inden udgangen af 2009; der skal være enighed om et første udkast til et sådant sæt principper og retningslinjer inden udgangen af 2010.

- Principper og retningslinjer for et robust og stabilt internet (verdensplan). Kommissionen vil samarbejde med medlemsstaterne om at opstille en køreplan for at fremme de europæiske principper og retningslinjer på verdensplan. Det strategiske samarbejde med tredjelande vil blive udbygget, navnlig drøftelserne om informationssamfundet, som et middel til at opbygge konsensus på verdensplan[31].

Mål: der skal opstilles en køreplan for det internationale samarbejde om principper og retningslinjer for robusthed og stabilitet i starten af 2010; det første udkast til internationalt anerkendte principper og retningslinjer skal drøftes med tredjelande og i relevante fora, herunder forummet for internetforvaltning (Internet Governance Forum), i slutningen af 2010.

Verdensomspændende øvelser i genopretning og afhjælpning ved omfattende internetsikkerhedshændelser. Kommissionen opfordrer de berørte europæiske parter til at

- overveje, hvordan afhjælpnings- og genopretningsøvelserne rent praktisk kan udvides og gennemføres på verdensplan, idet der tages udgangspunkt i katastrofeplanerne og beredskabskapaciteten på regionalt plan.

Mål: Kommissionen vil foreslå en ramme og en køreplan for europæisk engagement og deltagelse i verdensomspændende øvelser i genopretning og afhjælpning ved omfattende internetsikkerhedshændelser inden udgangen af 2010.

5.5. Kriterier for europæisk kritisk infrastruktur i ikt-sektoren

Ikt-sektorspecifikke kriterier. På grundlag af de indledende aktiviteter, der er gennemført i 2008 vil Kommissionen

- i samarbejde med medlemsstaterne og alle relevante parter videreføre arbejdet med at opstille kriterier for indkredsning af europæisk kritisk infrastruktur i ikt-sektoren. I den forbindelse vil den trække på relevante oplysninger fra en særlig undersøgelse, der er ved at blive sat i værk[32].

---

30 Se fodnote 27.
31 KOM(2008) 588 endelig.
32 Se fodnote 27.

Mål: Kommissionen vil fastlægge kriterier for europæisk kritisk infrastruktur i ikt-sektoren i første halvdel af 2010.

6. KONKLUSION

En sikker og robust kritisk informationsinfrastruktur er det bedste forsvar mod svigt og angreb. Det er derfor altafgørende, at sikkerheden og robustheden i ikt-infrastrukturen i hele EU styrkes, for at vi kan høste det fulde udbytte af informationssamfundet. For at nå dette ambitiøse mål foreslår Kommissionen en handlingsplan, der skal styrke det taktiske og praktiske samarbejde på europæisk plan. Handlingsplanens succes afhænger af, hvor godt den kan bygge videre på og bidrage til aktiviteter i den offentlige og den private sektor, og af medlemsstaternes, EU-institutionernes og de øvrige parters engagement og fulde samarbejde.

I dette øjemed vil der blive afholdt en ministerkonference den 27.-28. april 2009, hvor de foreslåede initiativer vil blive drøftet med medlemsstaterne. Ministerkonferencen skal desuden markere medlemsstaternes engagement i debatten om en moderniseret og styrket politik for net- og informationssikkerhed i Europa.

Forbedring af sikkerheden og robustheden i ikt-infrastrukturen er et langsigtet mål, og strategien og foranstaltningerne for at nå dette mål må jævnligt tages op til fornyet overvejelse. Som led i den overordnede debat om net- og informationssikkerhedspolitikkens fremtid i EU efter 2012 vil Kommissionen derfor hen imod slutningen af 2010 iværksætte en evaluering af den første fase af foranstaltninger og om nødvendigt foreslå yderligere tiltag.