

DA

DA

DA



EUROPA-KOMMISSIONEN

Bruxelles, den 31.3.2011
KOM(2011) 163 endelig

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

om beskyttelse af kritisk informationsinfrastruktur

"Resultater og næste skridt: vejen til global internetsikkerhed"

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

om beskyttelse af kritisk informationsinfrastruktur

"Resultater og næste skridt: vejen til global internetsikkerhed"

1. INDLEDNING

Den 30. marts 2009 vedtog Kommissionen en meddelelse om beskyttelse af kritisk informationsinfrastruktur – "Beskyttelse mod storstilede cyberangreb og sammenbrud: øget beredskab, sikkerhed og robusthed"¹, der indeholdt en plan ("handlingsplanen for beskyttelse af kritisk informationsinfrastruktur") for at styrke sikkerheden og robustheden i kritisk informations- og kommunikationsinfrastruktur. Målet var at stimulere og støtte tiltag for at opbygge et højt niveau af beredskab, sikkerhed og robusthed både på nationalt og europæisk plan. Denne strategi blev godkendt af Rådet med bred opbakning i 2009².

Handlingsplanen for kritisk informationsinfrastruktur (i det følgende benævnt "handlingsplanen") er bygget op omkring fem indsatsområder: beredskab og forebyggelse, opdagelse og reaktion, afhjælpning og genopretning, internationalt samarbejde og kriterier for kritisk informationsinfrastruktur i ikt-sektoren. Den beskriver, hvilke opgaver der skal udføres under hvert indsatsområde af henholdsvis Kommissionen, medlemsstaterne og/eller erhvervslivet med støtte fra Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA).

Den digitale dagsorden for Europa³, der blev vedtaget i maj 2010, og Rådets konklusioner i denne forbindelse⁴ fremhævede det fælles udgangspunkt, at tillid og sikkerhed er grundlæggende forudsætninger for en almen udbredelse af ikt og dermed for at nå målene om "intelligent vækst" ifølge Europa 2020-strategien⁵. Den digitale dagsorden understreger behovet for, at alle berørte parter forener kræfterne i en samordnet indsats for at gøre ikt-infrastrukturen sikker og robust ved at sætte fokus på forebyggelse, beredskab og bevidstgørelse, og for at udvikle effektive og koordinerede mekanismer som forsvar mod nye og stadig mere avancerede former for angreb på internettet og internetkriminalitet. Denne strategi sikrer, at der træffes både forebyggende og afhjælpende foranstaltninger.

Følgende tiltag, der blev varslet i den digitale dagsorden, er iværksat i løbet af de seneste måneder: Kommissionen fremlagde i september 2010 et direktivforslag om angreb på informationssystemer⁶. Forslaget sigter mod at styrke kampen mod internetkriminalitet gennem indbyrdes tilnærmelse af medlemsstaternes straffelovgivninger og forbedret samarbejdet mellem retlige og andre kompetente myndigheder. Det indfører også

¹ KOM(2009) 149.

² Rådets resolution af 18. december 2009 om en samordnet europæisk strategi for net- og informationssikkerhed (2009/C 321/01).

³ KOM(2010) 245.

⁴ Rådets konklusioner af 31. maj 2010 om den digitale dagsorden for Europa (10130/10).

⁵ KOM(2010) 2020 og Det Europæiske Råds konklusioner af 25. og 26. marts 2010 (EUCO 7/10).

⁶ KOM(2010) 517 endelig.

bestemmelser med henblik på bekæmpelse af nye former for angreb på internettet, særlig via botnet. Som supplement til dette fremsatte Kommissionen samtidig et forslag⁷ om at styrke og modernisere Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA) med det formål at øge netsikkerheden og tilliden til informationsnettene. Et styrket og moderniseret ENISA vil kunne hjælpe EU, medlemsstaterne og private berørte parter til at udvikle deres kapacitet og beredskab til at forebygge, afsløre og reagere på netsikkerhedsproblemer.

Sidst, men ikke mindst, understreger den digitale dagsorden for Europa, Stockholmprogrammet/-handlingsplanen⁸ og strategien for EU's indre sikkerhed i praksis⁹, at Kommissionen er fast besluttet på at skabe digitale rammer, der gør det muligt for alle europæere at udnytte deres økonomiske og sociale potentiale fuldt ud.

Nærværende meddelelse gør status over de resultater, der er nået, siden handlingsplanen for kritisk informationsinfrastruktur blev vedtaget i 2009. Den gennemgår, hvilke skridt der er planlagt fremover for hvert indsatsområde på både europæisk og internationalt plan. Meddelelsen lægger vægt på udfordringernes globale dimension og vigtigheden af at styrke samarbejdet mellem medlemsstaterne og den private sektor på nationalt, europæisk og internationalt plan, for at der kan tages højde for de indbyrdes afhængigheder på globalt plan.

2. ET SCENARIO I UDVIKLING

Konsekvensanalysen, der ledsagede handlingsplanen for kritisk informationsinfrastruktur¹⁰, og en bred vifte af analyser og rapporter fra private og offentlige parter fremhæver ikke blot Europas sociale, politiske og økonomiske afhængighed af it, men også den stadige vækst i antallet af trusler mod itk-infrastrukturen – det være sig natur- eller menneskeskabte - og i truslernes rækkevidde, kompleksitet og potentielle følger.

Der er dukket nye, teknologisk mere avancerede trusler op, og truslernes globale, geopolitiske dimension bliver stadig tydeligere. Vi oplever en tendens til at udnytte it til at opnå politisk, økonomisk og militær dominans, blandt andet gennem offensive tiltag. "Cyberkrigsførelse" og "cyberterrorisme" er begreber, der af og til dukker op i denne sammenhæng.

Desuden er visse regimer, som det ses af de seneste begivenheder i det sydlige Middelhavsområde, af politiske grunde indstillet på og i stand til vilkårligt at fratage deres egne borgere adgangen til elektroniske kommunikationsmidler, navnlig internettet og mobilkommunikation. Sådanne ensidige indenlandske indgreb kan få alvorlige virkninger i andre dele af verden¹¹.

For at nå til en bredere forståelse af disse forskellige trusler kan det være hensigtsmæssigt at inddele dem i kategorier baseret på formålet med truslerne:

⁷ KOM(2010) 521.

⁸ KOM(2010) 171.

⁹ KOM(2010) 673.

¹⁰ SEK(2009) 399.

¹¹ Partnerskab for demokrati og fælles velstand med det sydlige Middelhavsområde, KOM(2011) 200 af 8.3.2011.

- **Udnyttelsesformål**, f.eks. "avancerede vedholdende trusler"¹² med økonomisk og politisk spionage for øje (f.eks. GhostNet¹³), identitetstyveri, de nylige angreb på emissionshandelssystemet¹⁴ eller på offentlige it-systemer¹⁵.
- **Afbrydelsesformål**, f.eks. distribuerede "denial of service"-angreb eller udsendelse af spammail, der iværksættes via botnet (f.eks. Conficker-nettet med 7 mio. maskiner og det spanskbaserede Mariposa-net med 12,7 mio. maskiner¹⁶), Stuxnet¹⁷ og afbrydelse af kommunikationsforbindelser.
- **Ødelæggelsesformål**. Dette er et scenario, vi endnu ikke har oplevet endnu, men i betragtning af den stadig mere udbredte brug af it i kritisk infrastruktur (f.eks. intelligente elnet og vandforsyningssystemer), kan det ikke udelukkes, at det vil blive en realitet i de kommende år¹⁸.

3. EU OG DEN GLOBALE SAMMENHÆNG

Udfordringerne forude er ikke specifikke for EU, og de kan ikke løftes af EU alene. Den vide udbredelse af it og internettet giver mulighed for mere effektiv, virksomhedsfuld og økonomisk kommunikation, koordinering og samarbejde mellem interesserede parter og resulterer i et dynamisk økosystem af innovation i alle områder af livet. Imidlertid kan truslerne nu også komme fra alle egne af verden, og på grund af kommunikationsnettenes verdensomspændende sammenhæng kan de få følger overalt i verden.

En rent europæisk strategi er ikke tilstrækkelig til at løfte de kommende udfordringer. Det er stadig så vigtigt som nogensinde at lægge en sammenhængende og samarbejdsorienteret strategi inden for EU, men det er nødvendigt, at en sådan strategi indgår i en verdensomspændende koordineringsstrategi, der involverer centrale partnere, såvel enkelte lande som relevante internationale organisationer.

Vi er nødt til at arbejde på at nå til en global forståelse af de risici, der er forbundet med en udbredt, massiv brug af it i alle kroge af samfundet. Og vi må udtænke strategier for, hvordan vi på en passende og effektiv måde styrer – dvs. forebygger, modvirker, afhjælper og reagerer på – disse risici. Den digitale dagsorden for Europa opfordrer til, at *"samarbejdet mellem de relevante aktører tilrettelægges på verdensplan, for at truslerne mod sikkerheden kan bekæmpes og afbødes effektivt"*, og sætter det mål at *"samarbejde med relevante parter verden over om navnlig at styrke **den globale risikostyring** i den digitale og den fysiske verden og iværksætte internationalt koordinerede målrettede tiltag mod it-kriminalitet og angreb på sikkerheden"*.

¹² Dvs. vedvarende og koordinerede angreb rettet mod statslige organer og den offentlige sektors it-systemer. Denne form for trussel er nu også ved at blive et problem for den private sektor (se "RSA 2011 cybercrime trends report").

¹³ Se rapporter fra projektet Information Warfare Monitor: "Tracking GhostNet: investigating a Cyber Espionage Network" (2009) og "Shadows in the Cloud: Investigating Cyber Espionage 2.0" (2010).

¹⁴ Se <http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/34&format=HTML&aged=0&language=EN&guiLanguage=fr>.

¹⁵ F.eks. de seneste angreb mod den franske regering.

¹⁶ Se OECD/IFP-projektet vedrørende "Future Global Shocks", "Reducing systemic cyber-security risks", 14. januar 2011, <http://www.oecd.org/dataoecd/3/42/46894657.pdf>.

¹⁷ Se <http://www.enisa.europa.eu/media/press-releases/stuxnet-analysis>

¹⁸ Se World Economic Forum, Global Risks 2011.

4. GENNEMFØRELSEN AF HANDLINGSPLANEN FOR BESKYTTELSE AF KRITISK INFORMATIONSFRASTRUKTUR: DE VIGTIGSTE RESULTATER

Den fulde rapport om resultaterne og de næste skridt i handlingsplanen findes i bilaget. I de følgende afsnit fremhæves de vigtigste punkter i statusopgørelsen.

4.1. Beredskab og forebyggelse

- **Det europæiske forum af medlemsstater (EFMS)** har bidraget væsentligt til at fremme debat og informationsudveksling mellem medlemsstaterne om god politisk praksis vedrørende sikkerhed og robusthed i ikt-infrastrukturen. EFMS anerkendes af medlemsstaterne som et vigtigt forum for drøftelser og udveksling af god politisk praksis¹⁹. EFMS's fremtidige arbejde vil fortsat blive støttet af ENISA og vil blive koncentreret om at styrke samarbejdet mellem landsdækkende/statslige it-beredskabsenheder (CERT), opstille minimumskrav for netsikkerhed i forbindelse med offentlige indkøb, udpege økonomiske og lovgivningsmæssige incitamenter til at gøre internettet mere sikkert og robust (under overholdelse af de gældende konkurrence- og statsstøtteregler), evaluere netsikkerhedsniveauet i Europa, udstikke retningslinjer for fælleseuropæiske it-beredskabsøvelser og drøfte målene for et internationalt samarbejde om sikkerhed og robusthed.
- **Det europæiske offentlig-private partnerskab for en robust infrastruktur (EP3R)** blev lanceret som en fælleseuropæisk styringsramme for en robust ikt-infrastruktur. Dets mål er at fremme samarbejdet mellem den offentlige og den private sektor om spørgsmål vedrørende sikkerhed og robusthed af strategisk betydning for EU. ENISA har spillet en formidlende rolle i EP3R's aktiviteter og skal ifølge Kommissionens forslag fra 2010 om modernisering af ENISA skabe en langsigtet og holdbar ramme for EP3R. EP3R vil også fungere som platform for et internationalt samarbejde om forvaltningspolitiske, økonomiske og markedsmæssige spørgsmål af betydning for sikkerhed og robusthed, især med det mål at styrke den globale risikoforvaltning for ikt-infrastruktur.
- Der er fastlagt et **minimumssæt af basiskapaciteter og -tjenester**²⁰ og tilhørende **politiske anbefalinger**²¹ for de landsdækkende/statslige CERT-enheder, for at de kan fungere effektivt og udgøre en nøglekomponent i det nationale beredskab og i informationsudveksling, koordinering og reaktion på netsikkerhedshændelser. Disse resultater danner grundlag for, at der med ENISA's støtte kan skabes et netværk af velfungerende landsdækkende/statslige CERT-enheder i alle medlemsstater inden 2012. Et sådant netværk vil danne rygraden i det europæiske informationsudvekslings- og varslingsystem (EISAS) for borgere og SMV'er, der skal opbygges med nationale ressourcer inden 2013.

¹⁹ Ifølge den britiske regerings svar på den femte rapport fra Underhusets EU-udvalg om handlingsplanen for kritisk informationsinfrastruktur har EFMS været en succes og har opfyldt et reelt behov hos de politiske beslutningstagere for at have et forum for udveksling af erfaringer.

²⁰ Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs>.

²¹ Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations>.

4.2. Opdagelse og reaktion

- ENISA har udarbejdet en køreplan på højt niveau for udvikling af et europæisk informationsudvekslings- og varslingsystem (EISAS) inden 2013²² baseret på indførelse af *basis tjenester* i de landsdækkende/statslige CERT-enheder og *interoperabilitetstjenester* til integrering af de nationale informationsudvekslings- og varslingsystemer i EISAS. En af de centrale opgaver i denne forbindelse bliver at sikre en tilstrækkelig beskyttelse af personoplysninger.

4.3. Afhjælpning og genopretning

- Foreløbig har kun 12 medlemsstater afholdt øvelser i håndtering af omfattende netsikkerhedshændelser og efterfølgende genopretning²³. ENISA har udarbejdet en **vejledning i god praksis for nationale beredskabsøvelser**²⁴ samt udsendt **anbefalinger** om udvikling af nationale strategier²⁵ for at støtte medlemsstaternes indsats og tilskynde til, at den optrappes.
- Den første **fælleseuropæiske øvelse i håndtering af omfattende netsikkerhedshændelser** (Cyber Europe 2010) fandt sted den 4. november 2010 og involverede alle medlemsstater, hvoraf 19 deltog aktivt i selve øvelsen, plus Schweiz, Norge og Island. Det vil uden tvivl styrke fremtidige fælleseuropæiske beredskabsøvelser, hvis der tilvejebringes en fælles ramme, der er baseret på og forbinder de nationale beredskabsplaner, og som omfatter grundlæggende mekanismer og procedurer for kommunikation og samarbejde mellem medlemsstaterne.

4.4. Internationalt samarbejde

- **De europæiske principper og retningslinjer for et robust og stabilt internet**²⁶ er blevet drøftet og fastlagt i EFMS-regi. Kommissionen vil udbrede kendskabet til principperne og drøfte dem med relevante interesseparter, særlig den private sektor (via EP3R), på bilateralt plan med centrale internationale partnere, især USA, såvel som på multilateralt plan. Den vil gøre dette i den udstrækning, den har kompetence til det, i fora som G8, OECD, NATO (navnlig på grundlag af NATO's nye strategiske koncept, der blev vedtaget i november 2010 og aktiviteterne i Cooperative Cyber-defense Center of Excellence), ITU (i forbindelse med kapacitetsopbygning på området internetsikkerhed), OSCE (via forummet for sikkerhedssamarbejde), ASEAN, Meridian²⁷ mv. Det er målet at anvende disse principper og retningslinjer som en fælles ramme for et fælles internationalt engagement i at skabe et vedvarende robust og stabilt internet.

²² http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap.

²³ Kilde: ENISA.

²⁴ Se http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

²⁵ Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations>.

²⁶ Se http://ec.europa.eu/information_society/policy/nis/index_en.htm

²⁷ Meridianprocessen har til formål at give regeringer verden over et redskab til at drøfte, hvordan de kan samarbejde på politisk plan om beskyttelse af kritisk informationsinfrastruktur. Se <http://meridianprocess.org/>

4.5. Kriterier for europæisk kritisk infrastruktur i it-sektoren

- De tekniske drøftelser i EFMS har resulteret i et **første udkast til it-sektorspecifikke kriterier** for udpegning af europæisk kritisk informationsinfrastruktur med fokus på **fast- og mobilnetkommunikation og internettet**. Drøftelserne vil fortsætte og blive suppleret af høringer af den private sektor om kriterieudkastet, både på nationalt og europæisk plan (via EP3R). Kommissionen vil også drøfte med medlemsstaterne, hvilke it-sektor-specifikke elementer der skal tages op i forbindelse med revurderingen i 2012 af direktivet om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre²⁸.

5. DET VIDERE FORLØB

Gennemførelsen af handlingsplanen for kritisk informationsinfrastruktur er præget af positive resultater, ikke mindst anerkendelsen af, at der er behov for en samarbejdsbaseret tilgang til net- og informationssikkerhed, der involverer alle parter. De milepæle og den tidsplan, der blev fastlagt i 2009, er i det store hele blevet overholdt. Vi bør dog ikke slække på indsatsen, for der er stadig masser af opgaver at udføre på både nationalt og europæisk plan, for at de hidtidige bestræbelser kan bære frugt.

Det er også særdeles vigtigt, at bestræbelserne indgår i en global koordineringsstrategi, og derfor at de udstrækkes til internationalt plan og til at omfatte alle relevante berørte parter, regioner, lande eller organisationer, der beskæftiger sig med lignende spørgsmål. Der bør opbygges partnerskaber med henblik på at fastlægge fælles strategier og tilhørende aktiviteter og undgå overlappning af indsatsen.

Vi må fremme en global risikostyringskultur. Der bør først og fremmest tilskyndes til koordinerede tiltag for at forebygge, opdage, afhjælpe og reagere på alle former for brud på netsikkerheden, natur- såvel som menneskeskabte, samt på at retsforfølge tilfælde af internetkriminalitet. Dette indebærer, at der iværksættes målrettede foranstaltninger mod sikkerhedstrusler og it-baseret kriminalitet.

Til dette formål vil **Kommissionen**:

- **fremme principperne for et robust og stabilt internet:** Der bør opstilles internationale principper for et robust og stabilt internet i samarbejde med andre lande, internationale organisationer og, hvor det er hensigtsmæssigt, verdensomspændende organisationer i den private sektor. Til dette formål bør man udnytte de eksisterende fora og processer, f.eks. dem, der har at gøre med forvaltningen af internettet. De internationale principper bør danne ramme om alle berørte parters aktiviteter vedrørende internettets stabilitet og robusthed. De europæiske principper og retningslinjer kunne danne grundlag for sådanne internationale principper
- **opbygge strategiske internationale partnerskaber:** Der bør opbygges strategiske partnerskaber med udgangspunkt i de aktiviteter, der allerede gennemføres inden for vigtige områder som håndtering af netsikkerhedshændelser, herunder beredskabsøvelser og samarbejde mellem CERT-enheder. Det er altafgørende, at den private sektor, der opererer på globalt plan, inddrages. EU-USA-arbejdsgruppen om internetsikkerhed og

²⁸ Rådets direktiv 2008/114/EF.

internetkriminalitet, der blev oprettet under topmødet mellem EU og USA i november 2010, er et vigtigt skridt i denne retning. Denne arbejdsgruppe vil rette opmærksomheden mod håndtering af netsikkerhedshændelser, offentlig-private partnerskaber, bevidstgørelse og internetkriminalitet. Den kunne også tænkes at undersøge mulighederne for at udvide samarbejdet til andre regioner eller lande og navnlig drøfte relevante spørgsmål med henblik på at fastlægge fælles strategier og tilhørende aktiviteter og undgå overlappning af indsatsen. Der bør tilstræbes yderligere samarbejde og koordinering i internationale fora, især G8. På europæisk side er hovedbetingelsen for succes en effektiv koordinering mellem alle EU-institutionerne, de relevante agenturer (særlig ENISA og Europol) og medlemsstaterne

- **opbygge tillid til "cloud computing":** Det er afgørende at styrke drøftelserne om, hvordan man bedst forvalter ny teknologi, der har global virkning, som f.eks. cloud computing. Drøftelserne bør under alle omstændigheder omfatte, men ikke begrænse sig til, passende forvaltningsrammer for beskyttelse af personoplysninger. Tillid er en forudsætning for, at vi kan høste det fulde udbytte af ny teknologi²⁹.

Eftersom sikkerhed er et fælles ansvar for alle, er alle medlemsstater nødt til at sikre, at deres nationale foranstaltninger tilsammen bidrager til en koordineret europæisk strategi for forebyggelse, opdagelse, afhjælpning og reaktion på alle former for forstyrrelse af og angreb på internettet. I den henseende bør **medlemsstaterne forpligte sig til at:**

- **styrke EU's beredskab ved at etablere et netværk af velfungerende landsdækkende/statslige CERT-enheder inden 2012.** Tilsvarende vil EU-institutionerne også oprette deres egen CERT-enhed inden 2012. Disse bestræbelser bør bygge på det minimumssæt af basiskapaciteter og -tjenester samt tilhørende strategiske anbefalinger, der er udformet af ENISA, som fortsat vil yde bistand til disse initiativer. Indsatsen vil også fremme udviklingen af det europæiske informationsudvekslings- og varslingssystem (EISAS), der skal være på plads til gavn for offentligheden i 2013
- **fastlægge en europæisk beredskabsplan for netsikkerhedshændelser inden 2012 samt jævnlige fælleseuropæiske beredskabsøvelser:** It-beredskabsøvelser er et vigtigt led i en sammenhængende strategi for håndtering af netsikkerhedshændelser på både nationalt og europæisk plan. Fremtidige fælleseuropæiske it-beredskabsøvelser bør være baseret på en europæisk beredskabsplan, der bygger på og forbinder de nationale beredskabsplaner. En sådan plan bør omfatte grundlæggende mekanismer og procedurer for kommunikation mellem medlemsstaterne og ikke mindst støtte udformningen og tilrettelæggelsen af fremtidige fælleseuropæiske øvelser. ENISA vil samarbejde med medlemsstaterne om at udarbejde en sådan europæisk beredskabsplan for netsikkerhedshændelser inden 2012. Inden for samme tidshorisont skal alle medlemsstater udforme almindelige nationale beredskabsplaner og beredskabs- og genopretningsøvelser
- **tilstræbe en koordineret europæisk indsats i internationale fora og drøftelser om forbedring af internettets sikkerhed og robusthed.** Medlemsstaterne bør samarbejde med hinanden og med Kommissionen om at fremme udviklingen af en princip- eller

²⁹ Se f.eks. ENISA's rapporter "Cloud Computing Information Assurance Framework" (2009): http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework/at_download/fullReport) og "Security and resilience in governmental clouds" (2011): <http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/>).

normbaseret tilgang til spørgsmålet om internettets globale stabilitet og robusthed. Målet bør være at styrke forebyggelsen og beredskabet på alle niveauer og blandt alle berørte parter og rette op på den nuværende tendens til at fokusere på militære aspekter og/eller national sikkerhed.

6. KONKLUSION

Erfaringen viser, at rent nationale eller regionale tiltag for at løfte de udfordringer, der er forbundet med at udvikle en sikker og robust informationsinfrastruktur, ikke slår til. Det europæiske samarbejde har udviklet sig betydeligt siden 2009 med opmuntrende resultater, især beredskabsøvelsen Cyber Europe 2010. Men Europa bør gå videre i bestræbelserne på at udvikle en sammenhængende og samarbejdsorienteret strategi for hele EU. Et moderniseret ENISA bør yde mere omfattende støtte til medlemsstaterne, EU-institutionerne og den private sektor i denne langsigtede indsats.

For at den europæiske indsats kan bære frugt, må den indgå i en koordineret strategi på globalt plan. Derfor vil Kommissionen fremme drøftelser om internetsikkerhed i alle relevante internationale fora.

En ministerkonference om beskyttelse af kritisk informationsinfrastruktur, der er tilrettelagt af det ungarske EU-formandskab, vil finde sted den 14.-15. april 2011. Denne konference er en afgørende lejlighed til at styrke engagementet i øget samarbejde og koordinering mellem medlemsstaterne, både på europæisk og internationalt plan.

BILAG

Handlingsplanen for kritisk informationsinfrastruktur: Detaljeret oversigt over resultaterne og de næste skridt

Resultaterne af de aktiviteter, der er gennemført som led i handlingsplanen for kritisk informationsinfrastruktur, er i det store hele i overensstemmelse med de milepæle og den tidsplan, som Kommissionen fastlagde i 2009. I det følgende beskrives resultaterne og de næste skridt for hvert af handlingsplanens indsatsområder. Dette øjeblicsbillede tager med i betragtning, at nogle af aktiviteterne er blevet yderligere udbygget som led i gennemførelsen af den digitale dagsorden for Europa og strategien for EU's indre sikkerhed i praksis.

1. Beredskab og forebyggelse

Basisniveau af kapacitet og tjenester med henblik på et europadækkende samarbejde

Resultater

- I 2009 indkredsede og fastlagde ENISA sammen med it-beredskabsenhederne (CERT) i Europa et minimumssæt af basiskapaciteter og -tjenester, som de landsdækkende/statslige CERT-enheder skal råde over for at kunne fungere effektivt i et fælleseuropæisk samarbejde. Man nåede til enighed om en liste over ufravigelige krav på områderne drift, teknisk kapacitet, mandat og samarbejde³⁰.
- I 2010 arbejdede ENISA sammen med CERT-enhederne i Europa på at omsætte de ovennævnte praktisk orienterede krav i et sæt politiske anbefalinger³¹, der skal sikre, at de landsdækkende/statslige CERT-enheder fungerer som nøglekomponent i det nationale beredskab og i informationsudveksling, koordinering og reaktion på netsikkerhedshændelser.
- Foreløbig har 20 medlemsstater³² etableret landsdækkende/statslige CERT-enheder, og næsten alle de øvrige har planer om at oprette en sådan enhed. Som varslet i den digitale dagsorden og yderligere uddybet i strategien for EU's indre sikkerhed har Kommissionen fremsat forslag om etablering af en CERT-enhed for EU-institutionerne inden 2012.

Næste skridt

- ENISA vil fortsat yde støtte til de medlemsstater, som endnu ikke har en landsdækkende/statslige CERT-enhed, der opfylder de vedtagne basiskrav, for at sikre, at målet om, at alle medlemsstater ved udgangen af 2011 råder over velfungerende landsdækkende/statslige CERT-enheder, nås. Denne milepæl skal bane vej for et velfungerende netværk af CERT-enheder på nationalt plan i **2012**, således som planlagt i den digitale dagsorden.

³⁰ Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-for-national-governmental-certs>.

³¹ Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations>.

³² Kilde: ENISA.

- ENISA vil i samarbejde med de landsdækkende/statslige CERT-enheder drøfte, om og hvordan basiskapaciteten kan udvides for at styrke CERT-enhedernes evne til at støtte medlemsstaternes indsats for robusthed og stabilitet i livsvigtig ikt-infrastruktur, og for at CERT-enhederne kan blive rygraden i det europæiske informationsudvekslings- og varslingsystem (EISAS) for borgere og SMV'er, der skal opbygges med nationale ressourcer inden 2013, som varslet i strategien for EU's indre sikkerhed.

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

Resultater

- I 2009 blev EP3R lanceret som en fælleseuropæisk styringsramme for en robust ikt-infrastruktur, der skal fremme samarbejdet mellem den offentlige og den private sektor om målene for sikkerhed og robusthed, basiskrav, god politisk praksis og foranstaltninger. Som det fremgår af strategien for EU's indre sikkerhed, skal EP3R også "*involvere internationale partnere for at styrke den globale risikostyring af it-netværk.*" ENISA har ydet støtte til partnerskabets aktiviteter.
- Private og offentlige interesseparter har været med til at fastlægge mål og principper for EP3R samt partnerskabets struktur og til at finde ud af, hvordan man kan tilskynde de relevante parter til at engagere sig aktivt i partnerskabet³³. De vigtigste indsatsområder for EP3R er udpeget i forslaget om modernisering af ENISA³⁴.
- Parallelt med udformningen af EP3R's struktur blev der i slutningen af 2010 oprettet tre arbejdsgrupper om a) nøgleaktiver, -ressourcer og -funktioner for uafbrudt og sikker elektronisk kommunikation på tværs af landegrænserne, b) basiskrav til sikkerhed og robusthed i elektronisk kommunikation, c) koordinerings- og samarbejdsbehov og -mekanismer med henblik på beredskabet og evnen til at reagere på omfattende afbrydelser i elektronisk kommunikation.
- I 2010 er der med Kommissionens forslag om at modernisere ENISA skabt grundlag for en langsigtet og holdbar ramme for EP3R, idet ENISA ifølge forslaget bør støtte "*samarbejdet mellem offentlige og private interessenter på EU-plan, bl.a. ved at fremme informationsudveksling og oplysning og ved at lette parternes bestræbelser på at udvikle og indføre standarder for risikostyring og for sikkerhed i elektroniske produkter, net og tjenesteydelser.*"

Næste skridt

- I 2011 vil EP3R fortsat styrke samarbejdet mellem interesseparter i den offentlige og den private sektor for at forbedre sikkerheden og robustheden ved hjælp af innovative tiltag og midler og for at fastlægge parternes ansvarsområder. Med støtte fra ENISA, der vil spille en formidlende rolle, vil EP3R-arbejdsgrupperne forelægge deres første resultater. En af de fremtidige opgaver bliver at drøfte sikkerhedsproblemerne i forbindelse med intelligente net på grundlag af det forberedende arbejde, der er udført af Kommissionen og ENISA.

³³

Se

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

³⁴

KOM(2010) 521.

- EP3R vil fungere som platform for et globalt samarbejde om forvaltningspolitiske, økonomiske og markedsmæssige spørgsmål af betydning for sikkerhed og robusthed. Kommissionen agter at benytte sig af EP3R til at støtte arbejdet i EU-USA-arbejdsgruppen om internetsikkerhed og internetkriminalitet med det formål at skabe sammenhængende rammer for samarbejdet mellem den offentlige og den private sektor, idet de gældende konkurrence- og statsstøtteregler overholdes.
- På lang sigt og i overensstemmelse med forslaget om en ny forordning om ENISA er det tanken, at EP3R skal blive en af nøgleaktiviteterne i et moderniseret ENISA.

Europæisk forum for informationsudveksling mellem medlemsstaterne (EFMS)

Resultater

- I 2009 blev der oprettet et europæisk forum for informationsudveksling mellem medlemsstaterne, EFMS, der skal fremme drøftelser og informationsudveksling mellem de relevante offentlige myndigheder om god politisk praksis med det mål at opstille fælles politiske mål for sikkerhed og robusthed i ikt-infrastruktur, direkte støttet af ENISA. EFMS, der holder møde en gang i kvartalet, har siden midten af 2010 haft en særlig webportal, der forvaltes af ENISA.
- EFMS har gjort betydelige fremskridt på følgende områder: a) fastlæggelse af kriterier for indkredsning af europæisk kritisk ikt-infrastruktur som led i gennemførelsen af direktivet om indkredsning og udpegning af europæisk kritisk infrastruktur³⁵, b) fastlæggelse af europæiske mål, principper og retningslinjer for et robust og stabilt internet og c) udveksling af god politisk praksis, særlig for øvelser i håndtering af netsikkerhedshændelser.
- EFMS anerkendes af medlemsstaterne som et vigtigt forum for drøftelser og udveksling af god politisk praksis³⁶.

Næste skridt

- I 2011 vil EFMS afslutte de tekniske drøftelser om ikt-kriterierne for europæisk kritisk informationsinfrastruktur og udstikke langsigtede retningslinjer og mål for storstilede fælleseuropæiske øvelser vedrørende net- og informationssikkerhed.
- EFMS vil blive inddraget yderligere i drøftelserne om målene for et internationalt samarbejde om sikkerhed og robusthed, særlig i forbindelse med aktiviteterne i EU-USA-arbejdsgruppen om internetsikkerhed og internetkriminalitet.
- De vigtigste mål for EFMS's fremtidige arbejde, der vil blive støttet direkte af ENISA, er³⁷: at finde metoder til at styrke samarbejdet mellem landsdækkende/statslige CERT-enheder, at opstille minimumskrav for internetsikkerhed i forbindelse med offentlige indkøb, at udpege økonomiske og lovgivningsmæssige incitamenter til at gøre internettet mere sikkert

³⁵ Rådets direktiv 2008/114/EF.

³⁶ Ifølge den britiske regerings svar på den femte rapport fra Underhusets EU-udvalg om handlingsplanen for kritisk informationsinfrastruktur har EFMS været en succes og har opfyldt et reelt behov hos de politiske beslutningstagere for at have et forum for udveksling af erfaringer.

³⁷ KOM(2010) 251.

og robust (under overholdelse af de gældende konkurrence- og statsstøtteregler) og at evaluere netsikkerhedsniveauet i Europa.

2. Opdagelse og reaktion

Europæisk informationsudvekslings- og varslingsystem (EISAS)

Resultater

- Kommissionen har finansieret to prototypeprojekter (FISHAS og NEISAS), der nu er ved at være klar til at fremlægge deres endelige resultater.
- På grundlag af en gennemførlighedsundersøgelse i 2007³⁸ og en analyse af relevante projekter på nationalt og europæisk plan har ENISA udarbejdet en køreplan på højt niveau for udvikling af EISAS inden 2013³⁹.

Næste skridt

- I 2011 vil ENISA bistå medlemsstaterne i gennemførelsen af EISAS-køreplanen ved at udvikle de "basistjenester", som de behøver for at kunne opbygge et nationalt informationsudvekslings- og varslingsystem på grundlag af den landsdækkende/statslige CERT-enhed.
- I 2012 vil ENISA udvikle de "interoperabilitetstjenester", der skal gøre det muligt at integrere de enkelte nationale informationsudvekslings- og varslingsystemer i et samlet europæisk system. ENISA vil også bistå medlemsstaterne med at afprøve disse tjenester gennem en trinvis integration af de nationale systemer.
- I løbet af 2011-2012 vil ENISA bistå de landsdækkende/statslige CERT-enheder i arbejdet med at integrere informationsudvekslings- og varslingsfunktioner i deres tjenester.

3. Afhjælpning og genopretning

Nationale beredskabsplaner og -øvelser

Resultater

- Ved udgangen af 2010 havde 12 medlemsstater udarbejdet nationale beredskabsplaner og/eller tilrettelagt øvelser i håndtering af omfattende netsikkerhedshændelser og efterfølgende genopretning⁴⁰.
- På grundlag af nationale og internationale erfaringer har ENISA udarbejdet en vejledning i god praksis for nationale beredskabsøvelser⁴¹, afholdt arrangementer i samarbejde med medlemsstaterne og CERT-enheder verden over om nationale øvelser og for nylig udsendt anbefalinger om udvikling af nationale strategier, hvor landsdækkende/statslige

³⁸ Se http://www.enisa.europa.eu/act/cert/other-work/files/EISAS_finalreport.pdf

³⁹ http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/eisas_roadmap

⁴⁰ Se http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

⁴¹ Se http://www.enisa.europa.eu/act/res/policies/good-practices-1/exercises/national-exercise-good-practice-guide/at_download/fullReport.

CERT/CSIRT-enheder tildeles en central rolle i ledelsen af nationale beredskabsøvelser med inddragelse af både private og offentlige parter⁴².

Næste skridt

- ENISA vil fortsat bistå medlemsstaterne i arbejdet med at udforme nationale beredskabsplaner og afholde jævnlige øvelser i håndtering af omfattende netsikkerhedshændelser og efterfølgende genopretning som et skridt på vejen mod en europadækkende koordinering.

Fælleseuropæiske øvelser i håndtering af omfattende netsikkerhedshændelser

Resultater

- Den første fælleseuropæiske øvelse i håndtering af omfattende netsikkerhedshændelser (*Cyber Europe 2010*) fandt sted den 4. november 2010 og involverede alle medlemsstater, hvoraf 19 deltog aktivt i selve øvelsen, plus Schweiz, Norge og Island. Øvelsen blev tilrettelagt og evalueret⁴³ af ENISA med aktiv deltagelse i planlægningen fra otte medlemsstater og teknisk bistand fra Det Fælles Forskningscenter (FFC).

Næste skridt

- I 2011 vil medlemsstaterne blive inddraget i drøftelserne om målet for og omfanget af den næste fælleseuropæiske it-beredskabsøvelse, der er planlagt til 2012. Muligheden for en trinvis fremgangsmåde, hvor en mindre gruppe af medlemsstater gennemfører mere tilbundsående øvelser, eventuelt med deltagelse af internationale parter, vil blive overvejet. ENISA vil fortsat støtte denne proces.
- Kommissionen yder økonomisk støtte til EuroCybex-projektet, der vil gennemføre en skrivebordsøvelse i andet halvår af 2011.
- It-beredskabsøvelser er et vigtigt led i en sammenhængende strategi for håndtering af netsikkerhedshændelser på både nationalt og europæisk plan. Derfor bør fremtidige fælleseuropæiske beredskabsøvelser være baseret på en europæisk beredskabsplan, der bygger på og forbinder de nationale beredskabsplaner. En sådan plan bør omfatte grundlæggende mekanismer og procedurer for kommunikation mellem medlemsstaterne og ikke mindst støtte udformningen og tilrettelæggelsen af fremtidige fælleseuropæiske øvelser. ENISA vil samarbejde med medlemsstaterne om at udarbejde en sådan europæisk beredskabsplan for netsikkerhedshændelser inden 2012. Inden for samme tidshorisont skal alle medlemsstater udforme almindelige nationale beredskabsplaner og beredskabs- og genopretningsøvelser. Den koordinering, der er nødvendig for at nå dette resultat, vil blive varetaget af EFMS.

Styrket samarbejde mellem landsdækkende/statslige CERT-enheder

Resultater

⁴² Se <http://www.enisa.europa.eu/act/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations>.

⁴³ Se <http://www.enisa.europa.eu/>.

- Samarbejdet mellem landsdækkende/statslige CERT-enheder er blevet styrket. ENISA's arbejde med hensyn til den basiskapacitet, som landsdækkende/statslige CERT-enheder bør råde over, samt vedrørende CERT-øvelser og nationale øvelser og håndtering af netsikkerhedshændelser har været med til at sætte gang i og støtte et tættere fælleseuropæisk samarbejde mellem de landsdækkende/statslige CERT-enheder.

Næste skridt

- ENISA vil fortsat støtte samarbejdet mellem landsdækkende/statslige CERT-enheder. Til dette formål vil agenturet i 2011 forelægge en analyse af kravene og udsende vejledning om en passende sikker kommunikationskanal mellem CERT-enheder, herunder en køreplan for gennemførelse og fremtidig udvikling. ENISA vil også undersøge, hvilke huller der er i praksis i samarbejdet på europæisk plan, og aflægge rapport om, hvordan samarbejdet på tværs af grænserne mellem CERT-enheder og de relevante berørte parter kan styrkes, især med henblik på koordinering af indsatsen i tilfælde af sikkerhedshændelser.
- Ifølge den digitale dagsorden bør medlemsstaterne have etableret et velfungerende netværk af CERT-enheder på nationalt plan senest **i 2012**.

4. Internationalt samarbejde

Et robust og stabilt internet

Resultater

- Der er opstillet europæiske principper og retningslinjer for et robust og stabilt internet⁴⁴ på grundlag af det arbejde, der er udført i EFMS.

Næste skridt

- I 2011 vil Kommissionen udbrede kendskabet til principperne og drøfte dem både som led i det bilaterale samarbejde med internationale partnere, især USA, og i multilaterale drøftelser i G8, OECD, Meridian og ITU. Desuden vil den rådføre sig med relevante interesseparter, særlig den private sektor, på europæisk (via EP3R) og internationalt plan (via Internet Governance Forum og andre relevante fora) samt tilskynde til drøftelser med centrale internetaktører/organisationer.
- I 2012 vil der blive indledt drøftelser med de internationale partnere med henblik på at anvende principperne og retningslinjerne som en fælles ramme for et fælles internationalt engagement i at skabe et vedvarende robust og stabilt internet.

Verdensomspændende øvelser i genopretning og afhjælpning ved omfattende internet-sikkerhedshændelser

Resultater

- Syv medlemsstater⁴⁵ deltog i den amerikanske it-beredskabsøvelse Cyber Storm III som internationale partnere. Kommissionen og ENISA deltog som observatør.

⁴⁴

Se http://ec.europa.eu/information_society/policy/nis/index_en.htm

Næste skridt

- I 2011 vil Kommissionen i samarbejde med USA inden for rammerne af EU-USA-arbejdsgruppen om internetsikkerhed og internetkriminalitet udvikle et fælles program og en køreplan for fælles/synkroniserede transkontinentale it-beredskabsøvelser i 2012/2013. Mulighederne for at udvide samarbejdet til andre regioner eller lande, der drøfter lignende spørgsmål, med henblik på at fastlægge fælles strategier og aktiviteter vil også blive overvejet.

5. Kriterier for europæisk kritisk infrastruktur i ikt-sektoren

Sektorspecifikke kriterier for indkredsning af europæisk kritisk infrastruktur i ikt-sektoren

Resultater

- De tekniske drøftelser i EFMS om sektorspecifikke kriterier for ikt-området har resulteret i et udkast til kriterier for fast- og mobilnetkommunikation og internettet.

Næste skridt

- EFMS vil fortsætte de tekniske drøftelser om de sektorspecifikke kriterier for ikt-området og sigter mod at afslutte arbejdet ved udgangen af 2011. Sideløbende hermed er der planlagt drøftelser med den private sektor om udkastet til kriterier i nogle af medlemsstaterne og på europæisk plan via EP3R.
- Kommissionen vil drøfte med medlemsstaterne, hvilke ikt-sektorspecifikke elementer der skal tages op i forbindelse med revurderingen af direktiv 2008/114/EF om indkredsning og udpegning af europæisk kritisk infrastruktur i 2012.

—