KOMMISSIONEN FOR DE EUROPÆISKE FÆLLESSKABER

Bruxelles, den 31.5.2006
KOM(2006) 251 endelig

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

En strategi for et sikkert informationssamfund – "Dialog, partnerskab og myndiggørelse"

{SEK(2006) 656}

INDHOLD

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

En strategi for et sikkert informationssamfund – "Dialog, partnerskab og myndiggørelse""

1. INDLEDNING

I meddelelsen "i2010 – et europæisk informationssamfund som middel til vækst og beskæftigelse"[1] fremhævede Kommissionen net- og informationssikkerhed som en afgørende forudsætning for, at der kan skabes et europæisk samarbejdsområde for information. Det bliver stadig vigtigere for vores økonomier og samfundsstrukturen, at der står net og informationssystemer til rådighed, og at de er pålidelige og sikre.

Formålet med denne meddelelse er at puste nyt liv i den strategi, som Europa-Kommissionen udstak i 2001 med meddelelsen "Net- og informationssikkerhed: Forslag til en europæisk strategi"[2]. Nærværende meddelelse gennemgår de aktuelle trusler mod sikkerheden i informationssamfundet og fastslår, hvilke yderligere skridt der bør tages for at forbedre net- og informationssikkerheden.

Med udgangspunkt i de erfaringer, der er gjort i medlemsstaterne og på EU-plan, er det målet at videreudvikle en dynamisk, overordnet strategi i Europa, baseret på en sikkerhedskultur og på **dialog, partnerskab og myndiggørelse**.

I forsøget på at takle sikkerhedsudfordringerne i informationssamfundet har EU udviklet en tresidet strategi, der omfatter dels specifikke net- og informationssikkerhedsforanstaltninger, dels regelsættet for elektronisk kommunikation (der omfatter beskyttelse af privatlivets fred og databeskyttelse) og dels bekæmpelse af internetkriminalitet. Selv om disse tre aspekter til en vis grad kan behandles særskilt, gør de mange indbyrdes afhængigheder det naturligt at lægge en koordineret strategi. Denne meddelelse skitserer en sådan strategi og opstiller rammer for videreudvikling og finjustering af en sammenhængende måde at gribe net- og informationssikkerhed an på.

Meddelelsen af 2001 definerer net- og informationssikkerhed som "*et nets eller et informationssystems evne til, på et givet tillidsniveau, at modstå uheld og ondsindede handlinger, der er til skade for disponibiliteten, autenticiteten, integriteten og fortroligheden i forbindelse med lagrede og transmitterede data og de dermed forbundne tjenester, der tilbydes af eller er tilgængelige via dette net eller system*". I løbet af de senere år har Det Europæiske Fællesskab gennemført en række foranstaltninger for at forbedre net- og informationssikkerheden.

Regelsættet for elektronisk kommunikation, der i øjeblikket er til revision, omfatter sikkerhedsrelaterede bestemmelser. Navnlig kræver direktivet om databeskyttelse inden for elektronisk kommunikation[3], at udbydere af offentligt tilgængelige elektroniske

---

1 KOM(2005) 229 endelig af 1.6.2005.
2 KOM(2001) 298 endelig af 6.6.2001.
3 Direktiv 2002/58/EF.

kommunikationstjenester beskytter sikkerheden i deres tjenester. Der er fastlagt bestemmelser til bekæmpelse af spam[4] og spionsoftware[5].

Tillid og sikkerhed spiller også en vigtig rolle i Det Europæiske Fællesskabs programmer for forskning og udvikling. Det sjette rammeprogram behandler disse spørgsmål gennem en bred vifte af projekter. Forskning vedrørende sikkerhed vil blive styrket i det syvende rammeprogram med oprettelsen af et europæisk program for sikkerhedsforskning[6]. Endvidere støtter programmet *Safer Internet Plus* netværksprojekter og udveksling af bedste praksis, hvad angår bekæmpelse af skadeligt indhold på informationsnettene.

Som et led i indsatsen mod sikkerhedstrusler besluttede EU i 2004 at oprette et europæisk agentur for net- og informationssikkerhed, ENISA. ENISA medvirker til at skabe en net- og informationssikkerhedskultur til gavn for borgere, forbrugere, virksomheder og offentlige organisationer i hele EU.

EU spiller også en aktiv rolle i de internationale fora, der behandler disse emner, såsom OECD, Europarådet og FN. På verdenstopmødet om informationssamfundet i Tunis deltog EU aktivt i drøftelserne om disponibilitet, pålidelighed og sikkerhed i forbindelse med net og information. Tunis-dagsordenen[7], der sammen med Tunis-engagementet skitserer de videre skridt i den politiske debat om det globale informationssamfund, og som støttes af ledere verden over, fremhæver nødvendigheden af at fortsætte kampen mod internetkriminalitet og spam, samtidig med at privatlivets fred og ytringsfriheden beskyttes. Dokumentet påpeger, at det er nødvendigt at nå frem til en fælles forståelse af spørgsmålene om internetsikkerhed, og at der er behov for yderligere samarbejde for at lette indsamling og formidling af oplysninger om sikkerhed samt udveksling af god praksis mellem alle berørte parter, hvad angår foranstaltninger til bekæmpelse af sikkerhedstrusler.

2. ØGET SIKKERHED I INFORMATIONSSAMFUNDET: DE VIGTIGSTE UDFORDRINGER

Trods anstrengelserne på internationalt, europæisk og nationalt plan bliver sikkerheden ved med at være et problem.

For det første er angreb på informationssystemer i stigende grad motiveret af udbytte, snarere end af ønsket om blot at lave ravage for sjov skyld. Data indsamles ulovligt, stadig oftere uden brugerens viden, og antallet af varianter af ondsindet software[8] og udviklingsraten for denne type software stiger hastigt. Spam er et godt eksempel på denne udvikling: det er ved at blive et bæremiddel for virusser og bedragerisk og kriminel aktivitet, såsom spionsoftware, phishing[9] og andre former for ondsindet software. Den omfattende udbredelse af spam bygger

---

4 Ubuden reklame.

5 Spionsoftware ("spysoftware") er sporingssoftware, der anvendes uden brugerens samtykke, og uden at brugeren gøres tilstrækkeligt opmærksom på det eller har kontrol over det.

6 Programmet for sikkerhedsforskning er ved at blive udformet som led i en forberedende foranstaltning vedrørende sikkerhedsforskning i perioden 2004-2006.

7 *Mod et globalt partnerskab i informationssamfundet - Opfølgning på Tunis-fasen af verdenstopmødet om informationssamfundet,* KOM(2006) 181 endelig af 27.4.2006.

8 Også kendt som "malicious software" eller "malware", dvs. ødelæggende software.

9 Phishing er en form for internetbedrageri, hvor gerningsmanden stjæler værdifulde oplysninger som kreditkortnumre, bankkontooplysninger, bruger-id og kodeord.

i stigende grad på botnet[10], dvs. kompromitterede servere og pc'er, der benyttes som relæ uden ejernes viden.

Den voksende udbredelse af mobiludstyr (3G-mobiltelefoner, bærbare videospil osv.) og mobilnetbaserede tjenester fører nye udfordringer med sig, efterhånden som der i hastigt tempo udvikles IP-baserede tjenester. Disse kan i sidste ende blive en mere almindelig indfaldsvej for angreb end pc'er, som allerede er forsynet med en væsentlig grad af sikkerhedsbeskyttelse. Faktisk giver alle nye former for kommunikationsplatforme og informationssystemer uundgåeligt nye muligheder for ondsindede angreb.

Endnu en vigtig udvikling er de "intelligente omgivelser", hvor der overalt er intelligent udstyr baseret på edb- og netteknologi (f.eks. RFID[11], IPv6 og sensornet). En hverdag, hvor alt er koblet sammen i net, giver væsentlige nye muligheder. Men det vil også skabe yderligere sikkerhedsrisici og trusler mod privatlivet. Fælles platforme og applikationer bidrager positivt til interoperabilitet og udbredelse af informations- og kommunikationsteknologi, men kan samtidig medføre øgede risici. Jo mere "hyldevare"-software der sælges, jo mere omfattende er følgerne, når eventuelle sårbarheder udnyttes eller der forekommer fejl. Fremvæksten af visse "monokulturer" inden for softwareplatforme og applikationer kan i høj grad lette væksten og spredningen af sikkerhedstrusler som ondsindet software og virusser. **Mangfoldighed, åbenhed og interoperabilitet spiller en afgørende rolle for sikkerheden og bør fremmes.**

Ikt-sektorens betydning for den europæiske økonomi og det europæiske samfund som helhed er uomtvistelig. Ikt er et afgørende element i innovation og kilde til næsten 40 % af produktivitetsstigningen. Desuden tegner denne stærkt innovative sektor sig for mere end en fjerdedel af den samlede europæiske F&U-indsats, og sektoren er af central betydning for økonomisk vækst og jobskabelse i hele økonomien. Flere og flere europæere lever i et sandt informationsbaseret samfund, hvor brugen af ikt har vundet hastigt frem som et centralt led i de sociale og økonomiske aktiviteter. Ifølge Eurostat brugte 89 % af virksomhederne i EU aktivt internettet i 2004, og ca. 50 % af forbrugerne havde benyttet nettet inden for den seneste tid[12].

Brud på net- og informationssikkerheden kan have virkninger, der går ud over den økonomiske dimension. Der er rent faktisk udbredt bekymring for, at sikkerhedsproblemer kan afskrække brugerne og hæmme udbredelsen af ikt. Samtidig er disponibilitet, pålidelighed og sikkerhed en forudsætning for at sikre grundlæggende rettigheder på nettet.

Dertil kommer, at andre kritiske infrastrukturer (transport, energi, osv.) som følge af den stigende forbindelse mellem nettene også blive mere og mere afhængige af integriteten i deres respektive informationssystemer.

Både virksomhederne og borgerne i Europa undervurderer stadig risiciene. Der er forskellige årsager til dette, men den vigtigste, for så vidt angår virksomhederne, ser ud til at være, at afkastet af investeringer i sikkerheden ikke er særlig synligt. Hvad angår borgerne, er det den omstændighed, at de ikke er bevidste om deres ansvar i den globale sikkerhedskæde.

---

[10] Et botnet er et net af bots, som er applikationer, der udfører opgaver på vegne af en fjernkontrolenhed, og som installeres i det skjulte på offerets maskine.

[11] Radio Frequency Identification – radiofrekvensbaseret identifikation.

[12] Eurostat, *Internet activities in the European Union*, 40/2005.

I betragtning af, at der er informations- og kommunikationsteknologi og informationssystemer overalt, er net- og informationssikkerhed en udfordring for alle:

- **Offentlige administrationer** er nødt til at tage vare på sikkerheden i deres systemer, ikke bare for at beskytte den offentlige sektors informationer, men også for at tjene som et eksempel på bedste praksis for andre

- **Virksomheder** må behandle net- og informationssikkerhed som et aktiv og en konkurrencefordel, snarere end som en "negativ omkostning"

- **Private brugere** er nødt til at forstå, at sikkerhed i deres hjemmesystemer er kritisk for den samlede "sikkerhedskæde".

For at kunne gribe de beskrevne problemer effektivt an har alle berørte parter brug for pålidelige oplysninger om informationssikkerhedshændelser og -tendenser. Pålidelige og dækkende oplysninger om sådanne hændelser er imidlertid vanskelige at skaffe. Årsagerne hertil er mange og strækker sig fra den hastighed, som sikkerhedstruende hændelser udvikler sig med, til visse organisationers modvilje mod at offentliggøre brud på sikkerheden. Ikke desto mindre er en af hjørnestenene i udviklingen af en sikkerhedskultur **bedre viden om problemet.**

Det er vigtigt at oplysningsprogrammer, der har til formål at sætte fokus på sikkerhedstruslerne, ikke underminerer forbrugernes tillid ved kun at fremhæve de negative sider af sikkerheden. Hvor det overhovedet er muligt, bør **net- og informationssikkerhed derfor præsenteres som et gode og en mulighed** snarere end som en belastning og en omkostning. Det skal anskues som et aktiv i bestræbelserne på at opbygge tillid blandt forbrugerne, en konkurrencefordel for virksomheder, der har informationssystemer, og et tjenestekvalitetsspørgsmål for tjenesteudbydere i både den offentlige og den private sektor.

Den vigtigste udfordring for beslutningstagerne består i at udforme en helhedsstrategi. Denne strategi skal anerkende de forskellige berørte parters respektive roller. Den skal sikre en ordentlig koordinering af de mange forvaltningspolitiske og forskriftsmæssige bestemmelser, der enten direkte eller indirekte har indflydelse på net- og informationssikkerheden. Liberaliseringen, dereguleringen og konvergensudviklingen har skabt et væld af aktører blandt de forskellige interessegrupper, hvilket ikke gør denne opgave nemmere. ENISA's bidrag til dette mål kan få stor betydning. ENISA kan fungere som et center for udveksling af oplysninger, samarbejde mellem alle berørte parter og udveksling af anbefalelsesværdig praksis, både inden for Europa og med resten af verden, og dermed bidrage til de europæiske ikt-virksomheders konkurrenceevne og et velfungerende indre marked.

3. MOD EN DYNAMISK STRATEGI FOR ET SIKKERT INFORMATIONSSAMFUND

Et sikkert informationssamfund må være baseret på **øget net- og informationssikkerhed** og en almen **sikkerhedskultur**. I dette øjemed foreslår Europa-Kommissionen en **dynamisk og integreret strategi**, der involverer alle berørte parter og er baseret på **dialog, partnerskab og myndiggørelse**. I betragtning af den offentlige og den private sektors komplementære roller i etableringen af en sikkerhedskultur må politiske initiativer på dette område baseres på en **åben og inklusiv dialog mellem de forskellige parter**.

Denne strategi og de dermed forbundne tiltag skal supplere og berige Kommissionens plan om at fortsætte udviklingen af en samlet dynamisk politisk ramme gennem en række initiativer i 2006:

(1) Udviklingen på området spam og trusler som spionsoftware og andre former for ondsindet software vil blive behandlet i en særlig meddelelse.

(2) Kommissionen vil fremsætte forslag med henblik på at forbedre samarbejdet mellem de retshåndhævende myndigheder og bekæmpe nye former for kriminel aktivitet, der udnytter internettet og underminerer kritiske infrastrukturer. Dette vil være emnet for en særlig meddelelse om internetkriminalitet.

Disse politiske initiativer supplerer også de aktiviteter, der planlægges for at nå målene i Kommissionens grønbog om et europæisk program for beskyttelse af kritisk infrastruktur[13], der blev udarbejdet som svar på en anmodning fra Rådet i december 2004. Grønbogsprocessen vil sandsynligvis føre til en handlingsplan, der kombinerer en samlet "paraplystrategi" for beskyttelse af kritisk infrastruktur med de nødvendige sektorspecifikke politikker, herunder en politik for ikt-sektoren. Den sektorspecifikke politik for ikt-sektoren vil via en **dialog mellem forskellige berørte parter** skulle undersøge de relevante økonomiske, forretningsmæssige og samfundsmæssige drivkræfter med henblik på at øge sikkerheden og net- og informationssystemernes modstandsdygtighed.

Endvidere vil der i forbindelse med revisionen af regelsættet for elektronisk kommunikation i 2006 også blive drøftet elementer, der kan forbedre net- og informationssikkerheden, såsom tekniske og organisatoriske foranstaltninger, der skal træffes af tjenesteudbydere, regler for anmeldelse af brud på sikkerheden samt brug af specifikke midler og sanktioner, når forpligtelserne ikke overholdes.

Det er i høj grad op til den private sektor at levere løsninger, tjenester og sikkerhedsprodukter til slutbrugerne. Det er derfor af strategisk betydning, at **den europæiske industri er både en krævende bruger** af sikkerhedsprodukter og -tjenester **og en konkurrencedygtig leverandør** af sådanne produkter og tjenester.

De nationale regeringer må være i stand til at identificere og følge bedste praksis inden for politikudformning, og de må vise støtte til disse politiske mål ved at forvalte deres egne informationssystemer på en sikker måde. Offentlige myndigheder, både i medlemsstaterne og på EU-plan, har en central rolle at spille, når det gælder om at informere brugerne ordentligt, så de bliver i stand til selv at tage vare på sikkerheden. Det bør have høj prioritet at øge bevidstheden om net- og informationssikkerhed og levere passende oplysninger i rette tid via særlige e-sikkerhedswebportaler om trusler, risici og sikkerhedsalarmer samt om bedste praksis. I dette øjemed kunne det være et vigtigt mål for ENISA at **oprette et europæisk flersproget informationsudvekslings- og varslingssystem**, der bygger på og sammenkæder eksisterende eller planlagte nationale offentlige og private initiativer.

Den globale dimension af net- og informationssikkerhed betyder, at Kommissionen både på internationalt plan og i koordinering med medlemsstaterne må øge indsatsen for at **fremme et verdensomspændende samarbejde om net- og informationssikkerhed**, navnlig i

[13] KOM(2005) 576 endelig af 17.11.2005.

forbindelse med gennemførelsen af den dagsorden, der blev vedtaget på verdenstopmødet om informationssamfundet i november 2005.

Endelig vil forskning og udvikling, særlig på EU-plan, medvirke til, at der etableres nye og innovative partnerskaber for at fremme væksten i den europæiske ikt-sektor som helhed, og i den europæiske sektor for ikt-sikkerhed i særdeleshed. Kommissionen vil derfor søge at sikre, at der afsættes tilstrækkelige økonomiske ressourcer til forskning i net- og informationssikkerhed og pålidelighedsteknologier under det syvende rammeprogram.

3.1. Dialog

3.1.1. Som et første skridt på vej mod en bedre dialog mellem de offentlige myndigheder foreslår Kommissionen, at der iværksættes en ***benchmarkingundersøgelse af de nationale politikker for net- og informationssikkerhed****, herunder særlige sikkerhedspolitikker for den offentlige sektor. Denne undersøgelse vil medvirke til at udpege de mest effektive fremgangsmåder, så disse kan vinde udbredelse overalt i EU, hvor det er muligt, og bidrage til at gøre de offentlige administrationer til en drivkraft for bedste sikkerhedspraksis. Aktiviteterne vedrørende elektronisk identifikation, bl.a. som et led i den nyligt offentliggjorte handlingsplan for e-forvaltning, kan spille en vigtig rolle i den henseende.*

3.1.2. Benchmarkingundersøgelsen bør ***kortlægge bedste praksis for, hvordan man øger bevidstheden hos små og mellemstore virksomheder og borgerne*** *om, hvor vigtigt det er, at de selv gør noget ved deres egne specifikke net- og informationssikkerhedsproblemer og -behov og deres evne til at løse problemerne. ENISA bør opfordres til at spille en aktiv rolle i denne dialog og i indsatsen for at konsolidere og udveksle bedste praksis.*

3.1.3. Der er brug for en ***struktureret debat mellem de forskellige berørte parter*** *om, hvordan man bedst udnytter de eksisterende redskaber og lovgivningsinstrumenter til at skabe en passende balance i samfundet mellem sikkerhed og beskyttelse af grundlæggende rettigheder, herunder privatlivets fred. Den planlagte konference "i2010 – på vej mod et allestedsnærværende europæisk informationssamfund", der tilrettelægges af det kommende finske formandskab, vil bidrage til denne debat, og det samme gælder høringen om konsekvenserne af radiofrekvensbaseret identifikation (RFID) for sikkerheden og privatlivets fred, der er et led i den bredere høring, som Kommissionen har iværksat for nylig. Desuden vil Kommissionen afholde:*

- et arrangement for erhvervslivet for at tilskynde den private sektor til at indføre effektive strategier for etablering af en sikkerhedskultur **i erhvervslivet**.

- et seminar, hvor man overvejer forskellige midler til at øge sikkerhedsbevistheden og styrke **slutbrugernes** tillid til elektroniske net og informationssystemer.

3.2. Partnerskab

3.2.1. For at kunne udforme en effektiv politik må man have en klar forståelse af udfordringernes art og omfang. Derfor er der brug for pålidelige og ajourførte statistiske og økonomiske data, både om sikkerhedshændelser og om tillidsniveauet blandt forbrugere og brugere, men også ajourførte data om størrelsen af og

*tendenserne i ikt-sikkerhedssektoren i Europa. Kommissionen vil bede ENISA udvikle et **tillidsbaseret partnerskab med medlemsstaterne og de berørte parter** og at udforme en **passende ramme for dataindsamling**, herunder procedurer og ordninger for indsamling og analyse af EU-dækkende data om sikkerhedshændelser og forbrugertillid.*

På grund af det stærkt opsplittede marked i EU og markedets særlige karakter vil Kommissionen samtidig opfordre medlemsstaterne, den private sektor og forskersamfundet til at **etablere et strategisk partnerskab** for at sikre, at der foreligger data om ikt-sikkerhedssektoren og om markedsudviklingen for produkter og tjenester i EU.

*3.2.2. For at forbedre Europas evne til at reagere på trusler mod netsikkerheden vil Kommissionen bede ENISA undersøge **muligheden for at oprette et europæisk informationsudvekslings- og varslingssystem,** der skal gøre det lettere at reagere effektivt på eksisterende og kommende trusler mod elektroniske net. Et af kravene til et sådant system vil være en **flersproget EU-portal**, der giver adgang til skræddersyede oplysninger om trusler, risici og sikkerhedsalarmer.*

3.3. Myndiggørelse

For at der kan skabes øget bevidsthed om sikkerhedsbehovene og -risiciene og dermed øget net- og informationssikkerhed, er det nødvendigt, at alle berørte parter myndiggøres og påtager sig et ansvar for udviklingen.

*3.3.1. I den henseende opfordrer Kommissionen **medlemsstaterne** til at:*

- deltage aktivt i den foreslåede benchmarking af nationale politikker for net- og informationssikkerhed
- fremme – i tæt samarbejde med ENISA – oplysningskampagner om fordelene ved og udbyttet af at indføre effektive sikkerhedsteknologier og en effektiv sikkerhedspraksis og -adfærd
- benytte indførelsen af e-forvaltningstjenester som løftestang for formidling og fremme af god sikkerhedspraksis i andre sektorer
- stimulere udvikling af net- og informationssikkerhedsprogrammer som led i læseplanerne for de højere uddannelser.

***3.3.2.** Kommissionen opfordrer også parterne i **den private sektor** til at tage initiativ til at:*

- nå frem til en passende fordeling mellem softwareproducenter og internetudbydere af ansvaret for at tilvejebringe et tilstrækkeligt og auditerbart sikkerhedsniveau
- fremme mangfoldighed, åbenhed, interoperabilitet, brugervenlighed og konkurrence som nøgledrivkræfter for sikkerhed samt stimulere indførelse af sikkerhedsfremmende produkter, processer og tjenester for at forebygge og bekæmpe id-tyveri og andre angreb på privatlivets fred.

- udbrede god sikkerhedspraksis for netoperatører, tjenesteudbydere og små og mellemstore virksomheder for at sikre et basisniveau for sikkerhed og virksomhedskontinuitet.

- fremme uddannelsesprogrammer i den private sektor, især for små og mellemstore virksomheder, for at give de ansatte den viden og de kvalifikationer, der er nødvendige, for at de kan gennemføre sikkerhedsreglerne i praksis.

- arbejde henimod prismæssigt overkommelige sikkerhedscertificeringsordninger, der omfatter produkter, processer og tjenester, og som opfylder EU-specifikke behov (navnlig hvad angår beskyttelse af privatlivets fred).

- involvere forsikringsbranchen i udvikling af passende risikostyringsværktøjer og -metoder til at takle ikt-relaterede risici og fremme en risikostyringskultur i organisationer og virksomheder (især små og mellemstore virksomheder).

4. KONKLUSION

For at kortlægge og løse sikkerhedsproblemerne i informationssystemerne og nettene i EU er det nødvendigt at sikre alle berørte parters fulde engagement. Den strategi, der skitseres i denne meddelelse, søger at opnå dette ved at styrke en **fremgangsmåde, som inddrager alle de berørte parter**. Dette indebærer, at der bygges på fælles interesser, at parternes roller afgrænses klart, og at der udvikles en dynamisk ramme, der skal fremme en effektiv offentlig politikudformning og initiativer i den private sektor.

Kommissionen vil aflægge rapport til Rådet og Parlamentet midt i 2007 om de iværksatte aktiviteter, indledende konklusioner og status for de enkelte initiativer, herunder ENISA's initiativer og de initiativer, der træffes af medlemsstaterne og i den private sektor. Hvis det viser sig hensigtsmæssigt, vil Kommissionen fremsætte forslag til en henstilling om net- og informationssikkerhed.