

## Årsberetning for IT-Sikkerhedsrådet for 2001/2002

4. april 2002

Ifølge det kommissorium for IT-Sikkerhedsrådet, som forskningsministeren lagde fast ved Rådets udnævnelse i december 1998, skal Rådet årligt afgive en rapport over status på IT-sikkerheden i Danmark. Rapporten skal tage udgangspunkt dels i de konkrete sager, Rådet har behandlet det pågældende år, dels i en række konkrete statusindberetninger fra de enkelte medlemmer af ekspertpanelet.

### 1. Indledning

Ifølge det kommissorium for IT-Sikkerhedsrådet, som forskningsministeren lagde fast ved Rådets udnævnelse i december 1998, skal Rådet årligt afgive en rapport over status på IT-sikkerheden i Danmark. Rapporten skal tage udgangspunkt dels i de konkrete sager, Rådet har behandlet det pågældende år, dels i en række konkrete statusindberetninger fra de enkelte medlemmer af ekspertpanelet.

Hermed fremsendes Rådets årsberetning for året 2001/2002 som vedtaget under Rådets møde den 4. februar 2002. Årsberetningen er den tredje og - inden for den gældende udnævnelsesperiode - sidste årsberetning, idet det på beretningstidspunktet endnu er usikkert, hvorledes fremtiden tegner sig for IT-Sikkerhedsrådet.

Forud for folketingsvalget den 20. november besluttede den daværende IT- og forskningsminister, Birte Weiss, at forlænge IT-Sikkerhedsrådets beskikkelsesperiode, således at den ressortminister, der har ansvar for Rådets arbejde efter folketingsvalget, kunne stå frit i sin afgørelse af, hvorledes - hvis overhovedet - Rådets arbejde skal videreføres. Nærværende årsberetning indeholder derfor 15-månedersperioden fra 1. januar 2001 til 31. marts 2002.

I januar 2002 modtog regeringens IT-sikkerhedsråd den store IT-sikkerhedspris på 50.000 kr., som er indstiftet af en række danske organisationer på IT-området. Rådet har besluttet at anvende beløbet til en åben idé-konkurrence, der sætter fokus på, hvilke IT-sikkerhedsmæssige udfordringer, det danske samfund står overfor i dag og i fremtiden med særlig fokus på operative løsningsmuligheder.

Ved udløbet af IT-sikkerhedsrådets kommissorium den 1. april 2002 indbyder det afgående IT-sikkerhedsråd hermed alle med interesse for IT-sikkerhedsområdet til at deltage i denne konkurrence. Formålet med konkurrencen er at få konkrete idéer på bordet for, hvordan vi kan møde trusler og udfordringer. Ved bedømmelsen vil der dog i alle tilfælde blive lagt vægt på, om der også anvises konkrete veje til løsninger. Det er dermed rådets håb, at konkurrencebidragene kan være til nytte som debatoplæg og indlæg i de politiske og driftsmæssige beslutninger, der skal træffes i den kommende tid."

### 2. Sammensætning

I beretningsperioden har IT-Sikkerhedsrådet haft samme sammensætning som ved dets udpegning i december 1998, nemlig

Professor, dr. jur. Mads Bryde Andersen, København Universitet (formand)  
Advokat Janne Glæsel, Bech-Bruun Dragsted  
Direktør Peter Landrock, Cryptomatic A/S  
Konsulent Steffen Stripp  
Direktør Jan Carlsen, Ernst & Young e- Security Nordic  
Kommunaldirektør Estrid Oxlund, Holstebro kommunue  
Statsautoriseret revisor Carsten Heilbuth, KPMG C. Jespersen

I beretningsperioden har der fundet enkelte udskiftninger sted i det ekspertpanel, der hører til Rådet, idet Bankdirektør Søren Møller Nielsen i forbindelse med sin fratræden fra Danske Bank havde ønsket at udtræde af panelet. Der er ikke sket genbeskikkelse i forbindelse med denne udtræden, og ved årets udgang bestod ekspertpanelet således af følgende medlemmer:

Politimester Lars Rand Jensen, Odense Politi  
Sekretariatschef Vibeke Høeg, H:S Informatik  
IT-sikkerhedschef Stig Folkmar Andersen, Kommunedata A/S  
Direktør Ib Larsen, Energistyrelsen  
Systemrevisionschef Knud E. Kristiansen, SDC  
Kontorchef Torben Jerlach, Indenrigsministeriets CPR-kontor  
Koncernsikkerhedschef Jørgen Bo Madsen TDC  
Kontorchef Klaus K. Simonsen, A.P. Møller  
Konsulent Per Gjerløv  
IT-chef Ole Damsgaard, B&O  
IT-revisionschef Per Rhein Hansen, Post Danmark, Intern Revision  
Underdirektør Kim Østrup, IBM  
Advokat Martin von Haller Grønbæk, Fabritius Tengnagel & Heine  
Centerchef Jens Ole Bach, Kommunernes Landsforening  
IT-chef Jens Risgaard, Post Danmark  
Vicekriminalinspektør Troels Ørting Jørgensen, Rigspolitiet  
IT-chef Lasse Solgaard, Told & Skat  
Direktør Jørgen Abild Andersen, Telestyrelsen  
Bankdirektør Søren Møller Nielsen, Danske Bank (medlem til den 1.8.01)

Rådet har afholdt et enkelt møde med ekspertpanelet den 27. februar 2001. Ved dette møde drøftedes bl.a. årsberetningen for 2000. Herudover er ekspertpanelet blevet hørt i forbindelse med Rådets publikation Adgangskontrol til en hjemmeside. Der har derimod ikke været behov for at udnytte den adgang, der gives i Rådets kommissorium for at inddrage enkelte af ekspertpanelets medlemmer at bistå i konkrete sager.

Rådet har haft sekretariat i Ministeriet for Videnskab, Teknologi og Udvikling, hvor det har været bistået af chefkonsulent Palle H. Sørensen, fuldmægtig Birgitte Hagelskjær-Nielsen fra den 1-9-01 og kontorfuldmægtig Anni Grønlund.

### 3. Arbejdsform

Rådet har afholdt i alt 8 møder, nemlig den 27. februar 2001, 2. april 2001, 29. maj 2001, 21. juni 2001, 28. august 2001, 30. oktober 2001, 11. december 2001 og den 4. februar 2002. I beretningsåret har der den 4. februar 2002 været afholdt en offentlig høring om "Det offentlige rådgivning om IT-sikkerhed i dag og i fremtiden.

### 4. Projekter

I beretnings året har Rådet afsluttet 4 projekter

#### *Sikkerhed ved e-post og Internet - hacking og virus:*

En række begivenheder i nyere tid (herunder den såkaldte "I love you"-virus fra maj 2000) har sat berettiget fokus på de risici, der er forbundet med at benytte Internettet til f.eks. web-surfing og elektronisk post. Ved at åbne "inficerede" elektroniske postmeddelelser eller filer kan man utilsigtet komme til at ødelægge programmer og data. Da der ikke er udsigt til, at sådanne risici inden for en overskuelig årrække vil blive elimineret ad teknisk vej, men da langt de fleste af risici på den anden side kan fjernes eller reduceres ved en kombination af praktiske foranstaltninger, klarere regler og sund fornuft, er der et stort behov for synliggørelse.

Dette var baggrunden for, at IT-Sikkerhedsrådet allerede i 2000 tog initiativ til at udarbejde en pjece, der giver gode råd om, hvordan IT-brugeren kan begrænse risikoen for hacking og virus ved brug af e-post-programmer og Internet-browsere. Pjecen henvender sig til tre forskellige persongrupper: Den private bruger (der har en computer i sit hjem, og som selv er ansvarlig for at installere og vedligeholde programmer), medarbejderen (der anvender computeren på sin arbejdsplads, eventuelt i forbindelse med en hjemme-pc-ordning) og den IT-sikkerhedsansvarlige.

Pjecen udkom i marts måned i 4.000 eksemplarer. Allerede i maj viste det sig nødvendigt at trykke et nyt oplag, og ved beretningsårets udløb er pjecen blevet distribueret i mere end 6.500 eksemplarer.

#### *IT-Sikkerhedsrådets udredning om Internet sårbarhed:*

Allerede under sine første møder i begyndelsen af 1999 drøftede IT-Sikkerhedsrådet behovet for at foretage en mere omfattende kortlægning af samfundets IT-relaterede sårbarhed. Disse overvejelser har bl.a. ført til gennemførelsen af de statistik-undersøgelser, der omtales andet steds i denne årsberetning (samt i årsberetningen for 2000). Efter drøftelse med Rådets ekspertpanel besluttede Rådet herudover at foretage en mere specifik undersøgelse af samfundets generelle IT-betingede sårbarhed. Formålet med projektet skulle være at give et overblik over, hvor der gør sig infrastrukturelt betingede sikkerhedsmæssige risici gældende af betydning for tilgængelighed og driftsstabilitet, og som kan få væsentlige konsekvenser for brugere af Internet.

Resultatet af dette projekt foreligger i form af en udredning af februar 2001 om Internet-sårbarhed. Udredningen indeholder en række anbefalinger, som i god tid forud for udsendelsen har været drøftet med det eksterne ekspertpanel, bl.a. under en høring den 28. august 2000.

#### *Adgangskontrol til en hjemmeside - en vejledning for tjenesteudbydere:*

Den stigende anvendelse af Internettet har ført til, at talrige tjenester udbydes fra en hjemmeside med en eller anden form for adgangskontrol. Der er i sagens natur stor variation mellem disse tjenester (f.eks. adgang til e-mail, information, vareindkøb og bankforretninger), men typisk har de alle indbygget en eller anden form for adgangskontrol, hvor brugeren skal indtaste et password for at få adgang til tjenesten. Denne velkendte fremgangsmåde har en række sårbarheder, og med dette projekt - der førte til en vejledning udsendt i august 2001 - har IT-Sikkerhedsrådet sat fokus på disse problemer. Vejledningen skitserer, hvad der bør tages hensyn til ved udformningen af en adgangskontrol, og beskriver en række autentificeringsmetoder og sårbarheder ved de forskellige metoder.

#### *Brug af e-post og internet på arbejdspladsen:*

Brug af e-post og internettet på arbejdspladsen er blevet et dagligt og vigtigt arbejdsredskab på både offentlige og private arbejdspladser.

Vejledningen der henvender sig til såvel virksomhedens ledelse, den IT-ansvarlige som medarbejdere, gennemgår lovgrundlaget for området og indeholder en beskrivelse af nogle strategiske overvejelser, som typisk vil være relevante for ledelsen:

Endvidere indeholder vejledningen beskrivelse af emner, der typisk vil være relevante at overveje ved fastlæggelse af en e-post og internetpolitik.

## 5. Høringssager

*Udkast til standardregulativ for udførelse af ledningsarbejder og andre arbejder i og over veje:* Den 29. juni 2001 afgav Rådet høringssvar til Trafikministeriet over det udkast til standardregulativ for udførelse af ledningsarbejder og andre arbejder i og over veje, som Trafikministeriet havde sendt i høring. Rådets bemærkninger havde bl.a. baggrund i nogle drøftelser, der har været ført i Rådet og med Rådets ekspertpanel om den samfundsmæssige betydning af de IT- og telenedbrud, der har årsag i graveskader. I høringssvaret hedder det bl.a.:

"...

Det fremgår ikke klart af det udsendte udkast, hvilken hjemmel, der danner grundlag for denne retsforordning. I mangel af særlig lovhjemmel for udstedelse af normerende bekendtgørelser som de, regelsættet indeholder, lægger IT-Sikkerhedsrådet til grund, at forordningen skal læses som et udtryk for de standardbetingelser, der i almindelighed agtes lagt til grund som vilkår for godkendelser meddelt i henhold til vejlovens § 106.

Som sådan er det forståeligt, at reglerne ikke søger at normere andre retlige problemer i relation til risikoen for skader på graveskader på ledningsarbejder. Af den undersøgelse, IT-Sikkerhedsrådet netop har offentliggjort vedrørende danske virksomheders IT-sårbarhed (og hvoraf et eksemplar vedlægges), fremgår det, at et meget stort antal IT-nedbrud skyldtes telekommunikationsforstyrrelser (hvoraf en stor del må formodes forvoldt ved graveskader). På denne baggrund skal Rådet pege på behovet for en præventiv regulering, der nedbringer risikoen for sådanne skader. Det er ganske enkelt for "billigt" at forvolde de følelige nedbrud på IT-driften, som en graveskade kan være forbundet med.

En sådan regulering kunne *for det første* tage udgangspunkt i den pligt til at sikkerhedsstillelse, der findes i udkastets § 8, kombineret med en regel om, at sådanne sikkerheder ikke alene skal dække de direkte omkostninger ved et ledningsbrud, men også indirekte (som f.eks. driftstab mv.). Hvis man præsenterer den virksomhed, der står foran et gravearbejde, for et krav om, at der skal præsteres en følelig garanti, vil dette kunne synliggøre de betydelige økonomiske risici, som den ansvarlige påfører sine omgivelser. Det maksimum, der anføres i kommentaren til denne bestemmelse (500.000 kr.), må således i mange tilfælde - herunder ved gravearbejder i storbyområder - være helt utilstrækkeligt.

I forlængelse af denne bemærkning - og med samme begrundelse - vil IT-Sikkerhedsrådet *for det andet* anbefale, at bestemmelsen i udkastets § 7 ændres, således at sidste pkt. - der vil begrænse ansvaret til ikke at omfatte indirekte følger af skaden - udgår. Begrundelsen herfor er, at det utvivlsomt vil have betydelig generalpræventiv betydning, at risikoen for sådanne erstatningskrav består. Da forslaget imidlertid - umiddelbart - kan forekomme vidtgående, knytter Rådet følgende uddybende bemærkninger hertil:

1. Dansk rets udgangspunkt, hvorefter det fulde tab erstattes (og herunder også driftstab og andre direkte tab), er ikke udtryk for den praktiske regel. I praksis rejses sådanne krav sjældent, jf. nærmere Bo von Eyben: *Ansvar for graveskader* (1990) s. 82. Og når kravene rejses stiller domstolene ganske store krav til karakteren af den "adækvans", hvormed de pågældende tab skal kunne henføres til skadevolderens forhold.
2. Det forhold, at potentielle skadevoldere i kommercielle kontraktforhold ofte fraskriver sig erstatningsansvaret for sådanne afledte tab, bør ikke føre til tilsvarende begrænsninger af dansk rets almindelige erstatningsregler over for ikke-kontraktsparter, jf. det ovenfor nævnte generalpræventive synspunkt.
3. Retspraksis pålægger den skadelidte ganske store krav til at søge sit potentielle tab minimeret, jf. således Østre Landsrets dom i U 1973.844, der lod det komme ejeren af en kyllingefarm til skade, at han først efter 1½ times forløb tog skridt til at forsyne sine slagtefærdige kyllinger med frisk luft efter at ventilationsanlægget var ophørt med at fungere på grund af en (i øvrigt erstatningsdækket) påkørsel af en lysmast. I praksis vil skadevolderen derfor primært stå i risiko for at blive mødt med et omfattende erstatningskrav, hvis den pågældende skade notorisk måtte forventes

at medføre de indtrufne skader. Der er navnlig behov for en generalpræventiv effekt i relation til disse situationer.

*For det tredje* vil IT-Sikkerhedsrådet foreslå, at der indføres en tvungen forsikringsordning for entreprenører, der befatter sig med gravearbejder, i lighed med, hvad der gælder for øvrige erhverv, hvis handlinger og undladelser kan medføre meget store økonomiske erstatningskrav. En sådan ordning bør give skadelidte et direkte krav mod skadevolderen for at alle tab opstået ved graveskader kan dækkes, herunder også de ovenfor nævnte afledte tab. Ved at indføre en sådan ordning vil man dels tilgodese skadelidtes interesser, dels vil man - i kraft af de sikringsforskrifter, forsikringsselskaberne vil indføre - udvirke en højere grad af påpasselighed ved gravearbejder.

..."

*Kriminalisering af hackerværktøjer.* Under drøftelserne i en særlig arbejdsgruppe under Justitsministeriets udvalg om Økonomisk Kriminalitet og Datakriminalitet var der rejst spørgsmål om, hvorvidt det ville være muligt at foretage en sådan afgrænsning af visse programmer mv., der i praksis udelukkende - eller stort set udelukkende - kan anvendes til retsstridig indtrængen i IT-systemer mv. I forbindelse med sine overvejelser om eventuelt at kriminalisere sådanne værktøjer ønskede arbejdsgruppen at høre IT-Sikkerhedsrådet om, hvorvidt det på forhånd måtte anses muligt at foretage en sådan afgrænsning.

Efter at have drøftet problemstillingen under sine møder den 29. maj og 21. juni 2001 meddelte Rådet, at man ikke havde kunnet opnå fuldstændig enighed om sit svar. Den overvejende opfattelse i Rådet var, at en sådan afgrænsning ikke er mulig, selv om man kan nære sympati for den procesbesparelse, der kan ligge i således at fremrykke fuldbyrdelses-momentet for bl.a. bestemmelsen i straffelovens § 263, stk. 2. Men Rådet delte sig i spørgsmålet, idet et mindretal fandt, at det er både praktisk muligt og forsvarligt at foretage en sådan afgrænsning af et område for besiddelse, der som sådant bør være kriminaliseret.

Det hedder i udtalelsen:

"...

Baggrunden for flertallets betænkelighed er følgende overvejelser:

Den første overvejelse ligger måske en anelse uden for rammerne af det stillede spørgsmål. Den knytter sig nemlig ikke så meget til de pågældende værktøjers tekniske beskaffenhed men snarere til de psykologiske motiver, der kan ligge bag gerningsmandens besiddelse af dem. Selv om der ikke kan føres bevis herfor kan det ikke udelukkes, at der i visse IT-miljøer synes at være en særlig følelse forbundet med selve dette at være i besiddelse af programværktøjer, der rummer *potentialet* for retsstridige handlinger. Også selv om disse værktøjer der fra en umiddelbar betragtning kun synes at give brugeren mulighed for at foretage noget retsstridigt, kan tænkes anvendt - eller i det mindste opbevaret - på måder, der ikke vil bringe besidderen i nærheden af en straffelovsovertrædelse. Opfattelsen kan for så vidt svare til den, man finder hos våbensamlere mv., hvor besiddelsen - inden for våbenlovens grænser - af "værktøjet" er gjort ulovlig i sig selv. Men hvor man typisk vil vide, hvornår man har et våben i sin besiddelse, kan man meget vel tænkes at komme i besiddelse af de nævnte værktøjer, uden (fuldt ud) at kende deres potentiale.

Hertil kommer imidlertid et forhold, der spiller ind med en særlig vægt i vurderingen af det stillede spørgsmål. For ganske mange brugere, der vel at mærke ikke har forsæt til at begå kriminelle handlinger, kan der være en betydelig nyttevirkning forbundet med at kunne anvende sådanne værktøjer, der i øvrigt rummer potentialet

til at skaffe sig retsstridig adgang til IT-systemer. En sådan anvendelse kan således give indblik i, hvorledes sådanne retsstridige handlinger undgås.

Som nævnt indledningsvis har de fremhævede forhold ikke umiddelbart adresse til det stillede spørgsmål, idet de snarere knytter sig til forholdene omkring besiddelsen af de nævnte værktøjer. Til disse overvejelser kommer imidlertid en række betænkeligheder af praktisk-teknisk art.

For det første vil det være vanskeligt at foretage nogen afgrænsning af, hvad det nærmere bestemt er for værktøjer, der i givet fald vil skulle forbydes. Et forbud rettet mod bestemte *programmer* (defineret gennem varemærke eller anden produktbetegnelse) vil ramme alt for bredt og også forbyde funktionaliteter i disse programmer, der ingen relation har til det, man ønsker at forbyde. Således indeholder de fleste hackerværktøjer flere - for så vidt lovlige - funktionaliteter ved siden af de, der må formodes tiltænkt retsstridig anvendelse. Som eksempel kan det nævnes, at det navnkundige *Back Orifice*-program, der må siges at være et eksempel på et program med i hovedsagen ulovlige anvendelsesformer, udadtil fremtræder som et program, der gør det muligt for brugeren at betjene sit udstyr fra en fremmed terminal.

Skulle man derimod - omvendt - vælge at regulere ud fra værktøjernes funktionalitet, må det erkendes, at der vil være endog meget store vanskeligheder forbundet med at foretage en afgrænsning af de former for funktionalitet, som man måtte ønske at ramme. Ganske mange af de funktioner, der i deres kombination fremstår som et tilsyneladende retsstridigt værktøj, vil således hver for sig kunne rumme helt sædvanlige ingredienser i et styresystem eller et programværktøj. Det skyldes netop kombinationen - som alt efter programmørens ønsker kan kombineres på en mangfoldighed af måder - at programværktøjet får dette "retsstridige præg". En beskrivelse af området for et forbud vil således være forbundet med særdeles store vanskeligheder. Forholdet adskiller sig således mærkbart fra de programmer, der findes til at omgå kopispærreanordninger, og som har ført til en særlig regulering, bl.a. i ophavsretslovens § 78. Sådanne anordninger kan kun udføre denne ene funktion.

Selv om det imidlertid skulle kunne lade sig gøre at foretage en præcis afgrænsning af de hackerværktøjer, som ønskes omfattet af en strafferetlig regulering med en form for fremrykket fuldbyrdelses-moment, vil det efter flertallets opfattelse være så store praktiske vanskeligheder ved at følge en sådan regulering til dørs gennem effektiv håndhævelse, at et forsøg af denne art må mødes med betænkelighed. Mulighederne for at placere den slags værktøjer på internettet (f.eks. fra en lukket hjemmeside eller lignende) er så enkle, at gerningsmanden uden vanskelighed kan sikre sig, at værktøjet aldrig er i hans "besiddelse" udover de gange, han benytter det. Også muligheden for at kryptere værktøjet til ukendelighed (når dette ikke benyttes) vil gøre en effektiv retshåndhævelse særdeles vanskelig.

Disse medlemmer har stor sympati for bestræbelserne for at opdatere straffeloven, således at den sikrer et effektivt værn mod de forbrydelses-former, som det digitale samfund frembyder. Men af de nævnte grunde kan de ikke anbefale, at man kriminaliserer besiddelsen af program-værktøjer med det nævnte potentiale for retsstridig indtrængen i IT-systemer.

Et mindretal i Rådet (*Jan Carlsen*) mener, at det trods de anførte betænkeligheder er muligt at nå frem til en beskrivelse af visse typer af værktøjer, om hvilke det kan siges, at den blotte besiddelse afgiver en så stærk formodning for et kriminelt forsæt, at der er grundlag for at forbyde besiddelsen som sådan, medmindre de pågældende kan godtgøre et legitimt formål med besiddelsen. Dette medlem peger

på, at man i visse steder i lovgivningen, herunder navnlig i ophavsretslovens § 78, har gjort tilsvarende forsøg på at nå frem til at kriminalisere besiddelsen af et programværktøj baseret på dets formodede funktionalitet. Den pågældende bestemmelse henviser herved til "midler, hvis eneste formål er at lette ulovlig fjernelse eller omgåelse af tekniske indretninger, som måtte være anvendt til at beskytte et edb-program", uanset det - ud fra synspunkter som dem, flertallet gør gældende - netop i ophavsretten må siges at være noget nær umuligt at konstatere, hvornår en sådan fjernelse er ulovlig, eftersom ophavsretsloven giver brugeren en præceptivt beskyttet ret til at foretage sikkerhedskopiering mv. Dette medlem ser derfor ikke noget problematisk principielt skridt ved at gøre noget tilsvarende i relation til straffelovens §§ 193, 263 og 291 og foreslår, at tilsvarende besiddelse kriminaliseret i relation til programværktøjer, hvis eneste formål det er at opnå funktionalitet til:

1. snifning (aflytning) af kommunikationslinier,
2. opsamling af og/eller gætning af passwords, PIN-koder, telefonnumre og andre identifikationer og lign., samt
3. udarbejdelse og/eller massedistribution af virus.

..."

*Udkast til tre bekendtgørelser om elektronisk signatur:* I forbindelse med en større høring, foranstaltet af IT- og Forskningsministeriet i august måned over tre bekendtgørelser om elektronisk signatur, fremkom IT-Sikkerhedsrådet med en række bemærkninger til den sproglige udformning af de pågældende bekendtgørelsestekster samt til indholdet af den foreslåede regulering. I Rådets høringsvar hedder det bl.a.:

"...

1. IT-Sikkerhedsrådet foreslår, at den foreslåede bestemmelse i bekendtgørelsens § 2, stk. 4, omformuleres således, at det er nøglecentrets "øverste ansvarlige ledelse" og ikke den "daglige ledelse", der skal godkende CP og CPS. Vedtagelse af et dokument som dette må på forhånd antages at være en strategisk beslutning, som de fleste virksomheder ønsker placeret på øverste niveau. Som bestemmelsen er formuleret opstilles imidlertid en overraskende modsat regel, idet beslutningen synes anskuet som en dagligdags disposition.
2. IT-Sikkerhedsrådet foreslår, at det i udkastets § 3, stk. 2, sidste pkt., præciseres således, at pligten til at videreføre og tilbagekaldelsestjenester alene gælder 6 år efter ophør af nøglecentrets virksomhed. Som bestemmelsen står, kan man få det indtryk, at 6-årsreglen gælder fra aftaletidspunktet.
3. Den foreslåede § 4 henviser til, om den pågældende leder eller betroede medarbejder skal være "straffet" for overtrædelse af straffeloven eller tavsheds- eller hemmeligholdelsesforpligtelser. Som bestemmelsen er formuleret vil den ikke finde anvendelse i tilfælde, hvor der alene idømmes en betinget straf (hvilket ofte er tilfældet). Bestemmelsen bør derfor omformuleres, således "straffet" ændres til "dømt skyldig for".
4. I den foreslåede § 8 bør det stilles som krav, at den pågældende aftale indgås skriftligt. Et krav herom vil modvirke tvivl om, hvilke opgaver den pågældende registreringsenhed har, og hvilket ansvar den virker under. Et tilsvarende krav gælder ifølge persondatalovens § 42, idet kravet dog ikke antages at forstås som et krav om anvendelse af papirmediet. En tilsvarende aftalepligt bør gælde i de øvrige sammenhænge, hvor nogen udøver beføjelser på vegne et nøglecenter.

5. Den foreslåede § 11, stk. 3, kan læses således, at nøglecentret skal tilbyde en revocation service. Et krav herom er da også velbegrundet i de tilfælde, hvor validering af certifikater sker off-line. Da online-validering imidlertid frembyder en langt højere sikkerhed bør bestemmelsen afgrænses således, at den alene gælder tilfælde, hvor validering sker off-line. IT-Sikkerhedsrådet foreslår derfor, at bestemmelsen indledes som følger: "*Såfremt nøglecentret giver meddelelse om spærrede eller suspenderede kvalificerede certifikater gennem offentliggørelse af lister, skal sådanne lister offentliggøres senest hver tolvte time.*"

6. Som allerede forudsat ved den førnævnte foreslår IT-Sikkerhedsrådet endelig, at 12-timers-reglen i den førnævnte bestemmelse gøres til en minimumsregel.

..."

Høringssvaret er i sin helhed tilgængeligt fra Rådets hjemmeside, [www.it-sikkerhedsraadet.dk](http://www.it-sikkerhedsraadet.dk). *Samfundets sårbarhed som konsekvens af IT-anvendelsen*: Den 19. september afgav Rådet nogle bemærkninger til IT- og Forskningsministeriet i anledning af et udkast til rapport af 17. august 2000 som en arbejdsgruppe under Statens IT-råd havde afgivet om "Samfundets sårbarhed som konsekvens af IT-anvendelsen. I Rådets svar hedder det bl.a.:

"...

IT-Sikkerhedsrådet deler det hovedsynspunkt, der finder udtryk i rapporten: Rådet finder ikke alene at det er nyttigt med en nøje koordination mellem de meget forskelligartede initiativer, der udføres i det danske samfund. Interessen i at sikre den informationsteknologiske infrastruktur er så vital for det moderne samfund, at en sådan indsats må betragtes som en ren og skær nødvendighed, hvis der skal være mening i at anvende samfundsmæssige ressourcer på dette område.

De vanskeligheder, der måtte være med at koordinere den store indsats, der udfoldes ved forskellige myndigheder - med muligt forskelligartede IT-politiske ønsker og målsætninger - bør ikke stå til hinder for, at denne samlede indsats gøres. Hertil er interessen i at sikre samfundets sikkerhedsmæssige infrastruktur for væsentlig. Af samme grund ser IT-Sikkerhedsrådet et stort behov for, at sekretariatsfunktionen i et sådant initiativ forankres hos en myndighed, der ikke så let kan blive genstand for interne kompetencestridigheder myndighederne imellem. Til dette spørgsmål, der berøres på s. 11 f., skal IT-Sikkerhedsrådet derfor anbefale, at det foreslåede Koordinationscenter for IT-sikkerhed placeres organisatorisk under Statsministeriet.

Når idéerne fra rapporten skal føres ud i livet vil IT-Sikkerhedsrådet gerne tilbyde sin bistand i dette koordinerende arbejde. Rådet har, siden sin nedsættelse i 1995, samlet et vist erfaringsmateriale, ikke alene om de retlige, politiske og tekniske problemer med at drive IT-sikkerhedspolitik, men navnlig vedrørende den "pædagogiske" indsats med at bringe anbefalinger herom ud til den almindelige dansker. I det omfang disse erfaringer kan komme til nytte bør de gøre det.

..."

*Kommissionens meddelelse om net- og informationssikkerhed*: Den 19. september 2001 afgav Rådet følgende høringssvar til IT- og Forskningsministeriet i anledning af den meddelelse om Net- og informationssikkerhed (med forslag til en europæisk strategi), som Kommissionen havde udsendt i juni måned. I Rådets bemærkninger hedder det bl.a.:

"...

I et samfund, hvis vitale funktioner i stigende grad står og falder med sikkerheden af dets IT-infrastruktur, er der et åbenbart behov for at anlægge en overordnet - national såvel som regional - strategi for, hvilke risici man anser for mest væsentlige, hvem der skal have ansvaret for at afdække disse risici, samt ikke mindst hvordan dette skal ske. Det er derfor særdeles værdifuldt, at Kommissionen har taget dette initiativ, som ikke alene på god og klar vis adresserer de risiko-områder, der må anses for relevante, men som derudover anviser velegnede metoder til at håndtere disse risici. Og det er i enhver henseende glædeligt, at man har kunne præstere et dokument af en så høj kvalitet.

Som anført i meddelelsen på s. 4 har Kommissionen med dette første initiativ ønsker at fokusere på, hvilke "yderligere eller styrkede offentlige tiltag på europæisk eller national plan", der er brug for. I dette lys skal Rådet foreslå følgende supplerende indsatsområder:

- Når meddelelsen på s. 5 påpeger behovet for at sikre nettenes disponibilitet, ville det være hensigtsmæssigt om der ligeledes blev gjort en indsats for, at sikre en højere grad af transparens omkring de forhold, der kan gøre nettene indisponible, f.eks. ved almindelige overbelastninger. Det er almindelig kendt - og i sig selv helt angribeligt - at de teleleverandørers løfte om at stille kommunikationsfaciliteter til rådighed for brugere almindeligvis angives med et mål (et antal kilobit pr. sekund), der alene kan nås under forudsætning af, at netbelastningen har et vist, gennemsnitligt omfang. Udover det særlige behov, der består for at reservere telelinjer for særlige kommunikationsforhold under et katastrofeberedskab, vil det være til gavn for den almindelige telesikkerhed, hvis det i højere grad blev sikret, at den almindelige - offentlige, erhvervsmæssige eller private - bruger af disse net på forhånd kan overskue, hvilken kommunikationskapacitet, der reelt opnås og under hvilke omstændigheder denne kapacitet af en eller anden grund ikke kan nås.
- På s. 14 berøres et anliggende, der i den seneste tid har givet anledning til debat, og som efter IT-Sikkerhedsrådets opfattelse kunne fortjene en mere indgående retspolitisk behandling, nemlig spørgsmålet om IT-brugerens erstatningsansvar for de tab, der kan følge af en skødesløs IT-sikkerhed. Efter Rådets opfattelse er det væsentligt at inddrage erstatningsretlige sanktioner i en drøftelse om IT-sikkerhed, idet sådanne sanktioner i mange tilfælde kan indebære en meget væsentlig motiverende faktor for de personer, der har det i deres magt at undgå sikkerhedsmæssige trusler. Således har Rådet for nylig i forbindelse med en høring over et regulativ om gravearbejder argumenteret for, at der må pålægges den entreprenør mv., der på uagtensom vis har forårsaget telenedbrud på grund af kabelskader under gravearbejder, et fuldt erstatningsansvar for alle de tab - herunder driftstab og afledte tab - som en sådan skade giver anledning til. Ligeledes finder Rådet, at der bør tilvejebringes passende forsikringsordninger for at sikre dette tab. Rådet nærer imidlertid betænkelighed ved også at udstrække en sådan erstatningstankegang til at dække tilfælde, hvor en skade forvoldes ved passiv optræden - f.eks. ved undladt sikring af en server mod infektion (et forhold, der dog heller ikke bringes direkte frem som et forslag i meddelelsen). Det er i strid med udgangspunktet i den almindelige erstatningsret at skulle pålægge ansvar for passivitet, og for at gøre undtagelse herfor må der kunne identificeres et meget præcist pligtbrud, som erstatningssanktionen i givet fald rettes mod. IT-Sikkerhedsrådet nærer tvivl ved, om muligheden herfor er til stede i dag.
- IT-Sikkerhedsrådet vil gerne benytte lejligheden til at udtale støtte til det forslag, der er anført på s. 16 om at lancere en offentlig informations- og uddannelses-kampagne. Det nuværende råd, hvis kommissorium udløb ved årsskiftet, har ved en række lejligheder overvejet at tage skridt til en sådan bredere kampagne for at synliggøre de risici, der er forbundet med IT-anvendelsen, og anviser hjælp til selvhjælp mv. Hidtil har Rådet alene haft ressourcer til at gennemføre en sådan inden for et enkelt område - jf. Rådets meget læste 2001-vejledning om sikkerhed ved e-post og Internet. Med Kommissionens anbefaling kan der dog være grund til overveje, om ikke der på forhånd bør sikres det IT-Sikkerhedsråd,

der i givet fald skal udpeges med virkning fra januar 2002, ressourcer til at tage denne væsentlige opgave op.

..."

*Udkast til høring af Justitsministeriets anti-terrorpakke:* I anledning af den af Justitsministeren udarbejdede udkast til lovpakke om terrorbekæmpelse ("anti-terrorpakken") afgav Rådet den 22. november følgende høringssvar til Justitsministeriet:

"...

IT-Sikkerhedsrådet fremkommer hermed med følgende bemærkninger i anledning af det udkast til forslag til lov om ændring af straffeloven, retsplejeloven, telelovgivningen og udleveringsloven, som Justitsministeriet har udsendt til høring den 30. oktober d.å.

Den meget omfattende lovpakke indeholder en række forslag, der må anses for særdeles vidtgående i forhold til, hvad der hidtil har været dansk lovgivningstradition. Dette gælder både hvad angår reglernes materielle indhold og i henseende til det lovforberedelsesarbejde, der ligger til grund for forslaget. Om begivenhederne den 11. september giver grundlag for et sådant indgreb anser IT-Sikkerhedsrådet for at være et almindeligt retspolitisk spørgsmål, som det ikke tilkommer Rådet at forholde sig til.

Rådet finder dog anledning til at bemærke, at der ved en eventuel vedtagelse af disse regler også bør vedtages en procedure, hvorved der følges op på, om reglerne har tjent deres formål, om de på længere sigt - fortsat - må anses for nødvendige, og om der vil være behov for korrektioner, når der er indvundet et erfaringsgrundlag fra praksis. Denne tanke ligger bl.a. til grund for forslaget om, at de nærmere krav til tele- og internetvirksomheder om logning teletrafik skal fastsættes ved bekendtgørelse (jf. bemærkningerne herom s. 68, afsnit 3.1.3.3), men bør også gælde de forslag til en specifik lovregulering, der stilles.

Dernæst har Rådet følgende bemærkninger til enkelte af de foreslåede regler:

1. Når det som nævnt foreslås, at § 786, stk. 4, i overensstemmelse med en senere udstedt bekendtgørelse, skal give hjemmel for logning af teletrafik i en kortere eller længere periode (6 eller 12 måneder), etablerer man en ordning, hvorefter de pågældende virksomheder i denne periode vil råde over kundedata mv., der kan være både følsomme og sikkerhedskritiske. Når dette forslag stilles må det imidlertid også sikres, at de pågældende virksomheder rent faktisk sikrer, at de pågældende oplysninger ikke bliver anvendt til andre formål. Det må således antages, at en række af de virksomheder, man nu giver ansvaret for at passe på de pågældende teleoplysninger, som ellers var blevet slettet, måske ikke er indrettet til at løfte den sikkerhedsmæssige opgave, der ligger i at sikre oplysningerne mod retsstridig kompromittering, f.eks. forvoldt ved hacking, jf. straffelovens § 263, stk. 2. Et regelsæt af denne art bør derfor følges op med en kompetence for IT- og forskningsministeren til at have indseende med sikkerhedsrutinerne hos IT- og televirksomhederne med særligt henblik på sikringen af de pågældende trafikdata.

2. Flere af de - centrale - forhold, som man foreslår løst ved bekendtgørelsesregulering, synes ikke med sikkerhed at have hjemmel i de relevante foreslåede bemyndigelsesbestemmelser, jf. § 786, stk. 4 og 5. Ved bemærkningen på s. 71, 2. afsnit, er det f.eks. forudsat, at der vil kunne opstilles regler om sikkerhedsgodkendelse af personale. En hjemmel til denne vidtgående - men i sig selv velbegrundede - retsvirkning synes ikke at fremgå af

bemyndigelsesbestemmelsen med den fornødne klarhed. I den forbindelse bør det sikres, at også alle de personer, der har at gøre med håndteringen af politiets begæringer om aflytning mv. (og altså ikke kun dem, der er beskæftigede med selve lovgivningen), er sikkerhedsgodkendte. Ligeledes bør det udtrykkeligt fremgå, som nævnt s. 69, at aflytningsfaciliteterne skal være til rådighed 24 timer i døgnet. Rådet skal derfor foreslå, at det i givet fald skrives ind i hjemmelsbestemmelsen, at der kan træffes bestemmelse om disse forhold. Endelig bør det fremgå - eventuelt blot i de endelige lovbemærkninger - at tekniske krav til logningen af den art, der omtales s. 66 under midten og s. 67 foroven, skal fremgå udtrykkeligt af bekendtgørelsesreguleringen.

3. Med den foreslåede nye affattelse af retsplejelovens § 806, stk. 3, 1. pkt., vil der blive givet politiet kompetence til at begære edition uden først at skulle afvente indhentelse af retskendelse. Om en sådan fravigelse af udgangspunktet om retskendelse er reelt velbegrundet, skal IT-Sikkerhedsrådet ikke udtale sig om. Imidlertid finder Rådet anledning til at påpege, at der kan være et behov for at sikre, at der i disse tilfælde rent faktisk indhentes den fornødne retskendelse. Rådet har tidligere haft lejlighed til at vurdere indholdet af de sikkerhedsrutiner, Rigspolitiet har fastsat i forbindelse med etablering af aflytning "på øjemedet" efter retsplejelovens regler om indgreb i meddelelshemmeligheden. Det var Rådets opfattelse, at disse rutiner var adækvate. Tilsvarende rutiner bør imidlertid også etableres i forbindelse med de øjmeds-begæringer om edition, som der nu lægges op til.

4. Den foreslåede adgang til computerovervågning giver politiet mulighed for at få adgang til en lang række oplysninger mv., som politiet ikke tidligere har kunne forlange udleveret. Eksempelvis kan en persons bankkonti og diverse passwords etc. nu komme i politiets varetægt. Dette giver politiet en teoretisk mulighed for - retsstridigt - at træffe dispositioner, som man ikke tidligere har kunnet, f.eks. uden kontohaverens vidende fjerne penge i dennes navn. Selv om risikoen herfor kun må anses for rent teoretisk, er det nødvendigt, at der indføres kontrolmekanismer, der i højere grad end de nuværende giver mulighed for indseende med den anvendelse, politiet gør af de således indsamlede oplysninger. Regler herom er ikke foreslået i det nu udarbejdede lovforslag, men bør forberedes som led i den opfølgingsopgøveling, der er omtalt i det indledende ovenfor.

..."

## 6. Konkrete udtalelser

I beretningsåret har IT-Sikkerhedsrådet ikke modtaget henvendelser om at tage konkrete problemstillinger op til behandling.

I andet kvartal af 2001 blev computere verden over ramt af en Internet-orm, der i forskellige variationer gik under navnet "Code Red". Som nærmere anført nedenfor under 9. adskilte denne orm sig fra tidligere af de computervirus, der har ramt nettet. For det første fordi den kunne sprede sig uden en aktiv medvirken fra offerets side. For det andet fordi dens skadelige virkninger - som bl.a. indebar risiko for tab af fortrolighed - i mange tilfælde ville være ukendte for offeret. Dette forhold samt den lethed, hvormed sådanne angreb kunne imødegås rejste efter IT-Sikkerhedsrådets opfattelse et stort behov for at advare offentligheden. Derfor udsendte IT-Sikkerhedsrådet den 8. august følgende fælles opfordring, sammen med Andersen, Dansk Dataforening, KMD, KPMG C. Jespersen, PricewaterhouseCoopers, VIGILANTe, TDC og Tele2.

"...

Fælles opfordring til handling:

"Code Red" computer-orme skaber reelle problemer

De sejlivede Internetorme under betegnelsen "Code Red" skaber i forskellige versioner nu så store problemer på Internettet, at det er nødvendigt at private og professionelle computerbrugere gør en aktiv indsats for at bekæmpe det ondsindede computerprogram. Code Red kan ramme brugere af det meget udbredte Windows-styresystem fra Microsoft, men kun i visse nyere versioner, nemlig Windows 2000 og Windows NT. Brugere af de ældre udgaver af Windows, dvs. Windows 95, Windows 98, og Windows ME er på nuværende tidspunkt ikke direkte berørt.

Hvem trues?

Både private brugere og virksomheder kan risikere at få Code Red orm eller en nyere variant. Størstedelen af de inficerede maskiner befinder sig hos mindre og mellemstore virksomheder, men i den seneste variant berøres også private brugere. Langt størstedelen af de ramte maskiner er koblet på Internettet via ADSL-forbindelser, men flere af de inficerede maskiner benytter et almindeligt modem, så den røde orm har altså ramt meget bredt.

Hvem skal agere?

Alle - virksomheder, organisationer og private -, der har en Windows NT eller Windows 2000 computer med en Microsoft web-server, på bør agere. På Windows 2000 kan web-serveren være aktiv uanset om den anvendes eller ej.

IT-leverandører, Internet-udbydere og konsulentfirmaer bør aktivt medvirke til at bremse ormenes virkninger. Det kan ske igennem informationsformidling til deres kunder og/eller direkte aktiv hjælp.

Hvad er virkningen af ormene?

Code Red ormen findes i flere varianter, hvoraf den nyeste udsætter ofrene for en stor risiko for senere at blive hacket, ligesom den breder sig meget aggressivt. Vi vurderer, at udbredelsen nu er så stor, at en sårbar computer, der bliver tilsluttet Internettet for første gang, kan blive inficeret med Code Red Worm, inden der er gået 20 minutter. En inficeret computer medvirker til ormens videreudbredelse, og deltager i angreb imod andre computere.

Hvad skal man gøre?

Microsoft tilbyder en gratis opdatering (en såkaldt patch), der lukker det sikkerhedshul som de meget udbredte orme udnytter:

<http://www.microsoft.com/technet/security/bulletin/MS01-033.asp> . Opdateringen er gratis.

Brug af opdaterede anti-virus produkter anbefales.

Den nuværende nye variant af Code Red, oftest kaldet CodeRedII eller CodeRed.v3 kan give en hacker fuld kontrol over computeren, så der kan i princippet være sket hvad som helst med filerne på harddisken, imens computeren har været inficeret. Derfor bør ejere af de ramte computere downloade opdateringen og gemme den på en diskette og derefter lave en fuldstændig geninstallation af Windows, efterfulgt af en installation af Microsofts opdatering, inden man igen tilslutter computeren til Internettet. En computer er sandsynligvis inficeret hvis filen C:\EXPLORER.EXE eksisterer.

Internetudbydere anbefales nøje at holde øje med, om kundernes computere er inficeret af ormene og i givet fald yde kunden den fornødne hjælp med rådgivning. Endvidere opfordres til, hvis kunden ignorerer advarslerne at afbryde forbindelsen. For at få en holdbar løsning på problemet, opfordres IT-leverandørerne ligeledes til at medvirke aktivt til at udbedre og forebygge spredningen.

..."

#### 7. Sager optaget til behandling af egen drift:

I beretningsåret har IT-Sikkerhedsrådet valgt af egen drift at tage følgende problemstillinger op til behandling:

*Sikkerheden i GSM-systemet:* Ved forskellige lejligheder har der været rejst tvivl om, hvorvidt den kommunikationssikkerhed, der tilbydes i forbindelse med GSM-telefoni, er så høj som det almindeligvis antages. Spørgsmålet påkaldte sig navnlig Rådets interesse, da Telestyrelsen - foranlediget af et spørgsmål i Folketinget - i foråret 2000 udarbejdede en redegørelse om aflytningsmuligheder i GSM-systemet, der generelt konkluderede, at det i praksis ikke er muligt at foretage en sådan aflytning.

I en udtalelse af 19. september 2001 kommenterede Rådet Telestyrelsens redegørelse som følger:

"...

IT-Sikkerhedsrådet har ved flere møder haft lejlighed til at diskutere den redegørelse, som Telestyrelsen udarbejdede i februar 2001, om muligheden for uautoriserede aflytninger af telefonsamtaler og SMS-beskeder i det danske GSM-net. Med den udbredte anvendelse af GSM-mobiltelefoni til såvel taletelefoni som dataoverførsel har dette tema fået central samfundsmæssig betydning. Allerede derfor er det forståeligt, at Telestyrelsens konklusioner har givet anledning til generel interesse, jf. således bl.a. artiklen i Ingeniøren fredag den 25. maj d.å. De følgende bemærkninger må ses i dette lys. Med de følgende bemærkninger ønsker IT-Sikkerhedsrådet at kaste lys over enkelte af rapportens konklusioner.

For det første forekommer redegørelsens konklusioner vedrørende den krypteringsalgoritme (A5), der anvendes i GSM-systemet uklare på et par punkter. Af bemærkningerne s. 11 fremgår det, at A5/1-algoritmen ikke er blevet offentliggjort, og fremstillingen på denne og den følgende side lader formode, at det ikke vides, om algoritmen er blevet brudt. Heroverfor står det forhold, at flere af hinanden uafhængige videnskabelige artikler mener at have offentliggjort algoritmen og fremhævet en række svagheder af mere eller mindre fundamental karakter ved den. Det bør derfor som minimum påpeges, at det formentlig ikke har været muligt at hemmeligholde algoritmen, og at der tillige består en vis - ikke ubetydelig risiko - for, at den er brudt.

Samtidig kunne man ønske sig en mere indgående drøftelse af, hvilken reel sikkerhedsmæssig betydning det har, at man har reduceret bitestørrelsen i A5/1-algoritmen fra 56 til 54 bits - ikke mindst i lyset af, at netop denne bit-størrelse i DES-algoritmen markerer undergrænsen for, hvornår der skal søges om eksporttilladelse for visse krypterings-værktøjer. For udestående kan det sammenfattende være vanskeligt at forstå, hvordan det på den ene side kan antages, at det i anden kommunikation kan være nødvendigt med en større nøgle (fordi man her ikke benytter brute-force, men et angreb baseret på delvist kendskab til indhold), medens det samme steds - underforstået - siges, at dette angreb ingen betydning har i relation til A5/1-algoritmen.

Foruden disse bemærkninger kan der efter Rådets opfattelse rejses tvivl om, hvorvidt den risikovurdering, der lægges til grund i Telestyrelsens redegørelse, er rammende. Redegørelsen konkluderer således - forholdsvis bastant - at der ikke er praktisk mulighed for at foretage uautoriseret aflytning af GSM-samtaler gennem brud på A5/1-algoritmen. Imidlertid undlader den at sætte fokus på, hvilke andre punkter, GSM-systemet så er sårbart over for, herunder aflytning baseret på indgreb på sendemaster ("celler") eller andre faste terminalpunkter. I betragtning af at det - som bekendt - er muligt at få opsat autoriseret aflytning af GSM-telefoni (efter retskendelse), må det på forhånd forekomme givet, at der findes sådanne faktiske

aflytningsmuligheder. Det har ikke hidtil været muligt for IT-Sikkerhedsrådet at opnå noget klart billede af, hvilke sikkerheds-foranstaltninger, der iagttages omkring disse aflytningspunkter. Jeg kan i den forbindelse orientere dig om, at netop dette tema gennem længere tid været søgt afklaret gennem kontakt til vicerigspolitichefen.

I den førnævnte artikel fra Ingeniøren den 25. maj 2001 er der i øvrigt omtalt en række teknikker, der er tilgængelige, og som - angiveligt - muliggør uautoriseret aflytning på GSM-nettet. Det er muligt, at disse teknikker må anses for "nye" i forhold til redegørelsens dato. Imidlertid synes alene det forhold, at der mangler en sådan afklaring, at kunne begrunde en generel anbefaling til GSM-brugerne om - i hvert enkelt tilfælde - at foretage en afvejning af, om den trafik, man overvejer at lade transportere i GSM-nettet, er så kritisk, at den blotte risiko for uautoriseret aflytninger bør føre til tilbageholdenhed. Man kan i de forbindelse frygte, at Telestyrelsens vejledning indgyder brugere, for hvilke fuld sikkerhed for fortrolighed i GSM-nettet er kritisk, en falsk sikkerhed.

Som anført indledningsvis har disse spørgsmål været drøftet ved flere lejligheder i IT-Sikkerhedsrådet ligesom det generelle spørgsmål om sikkerhedsforanstaltningerne i forbindelse med den lovlige aflytning har været det. Jeg er ikke bekendt med, om Telestyrelsen forbereder en opdatering af sin redegørelse, endsige en fortsat bearbejdning af disse spørgsmål, men det kunne måske i alle tilfælde være nyttigt, at Rådet og styrelsen forsøgte at samle kræfterne for en højere synliggørelse af sikkerheden på denne væsentlige del af samfundets kommunikationsinfrastruktur.

..."

Udtalelsen gav anledning til en presseomtale, der ? modsat Rådets intention ? fortolkede denne udtalelse således, at Rådet hermed afgav en substantiel kritik af Telestyrelsens redegørelse. Efter ønske fra IT- og forskningsministeren afholdtes derfor et møde mellem Telestyrelsen og IT-Sikkerhedsrådet for at afklare disse mulige uenigheder. Mødet førte til følgende fælleserklæring:

"...

IT-Sikkerhedsrådet og Telestyrelsen har på et møde den 30. oktober 2001 gennemdrøftet redegørelsen og konklusionerne.

IT-Sikkerhedsrådet og Telestyrelsen er efter drøftelsen enige om, at redegørelsens konklusioner om sikkerheden mod aflytning i GSM-systemet samlet set er dækkende, idet det forholder sig sådan, at det netop er kombinationen af en række sikkerhedsforanstaltninger, der tilsammen udgør sikkerheden i systemet.

Tager man et enkelt element ud og betragter det isoleret, er situationen en anden. Således er det IT-Sikkerhedsrådets opfattelse, at A5/1-algoritmen ikke i sig selv (hverken ved anvendelse med 54 bit eller med alle de mulige 64 bit i nøglen) kan betegnes som en "stærk" kryptering. Som en illustration heraf kan nævnes, at A5/1-algoritmen anvendt uden samtidig anvendelse af andre sikkerhedsforanstaltninger - som f.eks. de, der anvendes i GSM-systemet - ikke ville være nok til effektiv beskyttelse af f.eks. finansielle transaktioner. IT-Sikkerhedsrådet finder det i den sammenhæng uheldigt, at der i den sammenfattende konklusion på redegørelsens kapitel 2, der er oplistet i sammenfatningen står "... den stærke A5/1-kryptering".

Telestyrelsen er enig i denne opfattelse af, at A5/1-algoritmen ikke i sig selv kan betegnes som en "stærk" kryptering. Denne sprogbrug er valgt, idet der i de folketingsspørgsmål (S 1040 - S 1042 fra januar 2001), der førte til udarbejdelsen af redegørelsen blev fokuseret meget på styrken af krypteringen. I de pågældende

spørgsmål blev der således skelnet mellem på den ene side en "svag" A5/2-algoritme og på den anden side en "stærk" A5/1 -algoritme. Ordet "stærk" skal således ses relativt- og A5/1-krypteringen anvendt i et GSM-system er "stærk nok", hvilket IT-Sikkerhedsrådet i øvrigt er enig i, jf. ovenfor. I redegørelsens gennemgang af A5/1-algoritmen er det således flere steder fremhævet, at A5/1 (både 54 og 64 bit-udgaven) er en "tilstrækkelig" kryptering set i forhold til, at det er A5/1-algoritmen sammen med de øvrige sikkerhedsforanstaltninger i GSM, der gør systemet sikkert. Det skal i øvrigt bemærkes, at Telestyrelsens redegørelse alene forholder sig til den del af GSM-systemet, hvor der sker transmission af data i luftsegmentet - dvs. på radiostrækningen mellem mobiltelefon og basestation eller på de radiokædestrækninger, der eventuelt benyttes internt i udbyderens GSM-system. Der er således ikke taget stilling til spørgsmålet om, hvorvidt GSM-telefoni kan aflyttes på den del af telenettet, der foregår via andre fysiske forbindelser.

IT-Sikkerhedsrådet og Telestyrelsen finder på baggrund af drøftelsen ikke anledning til at anbefale, at der på nuværende tidspunkt iværksættes yderligere undersøgelser eller udredninger om muligheden for uautoriseret aflytning i de danske GSM-net.

..."

*Henvendelse til Kulturministeriet om retten til at sikkerhedskopiere programmet:* Ved skrivelse af 21. december 2000 rettede IT-Sikkerhedsrådet henvendelse til Kulturministeriet i anledning af den rapport om implementering af EU's direktiv om retlig beskyttelse af edb-programmer (91/250/EØF), som Kommissionen havde fremlagt den 10. april 2000 (COM(00) 1999 final).(se årsberetningen for 2000).

Kulturministeriet svar af 26. september 2001 på Rådets henvendelse lyder som følger:

"...

Med henvisning til IT-Sikkerhedsrådets skrivelse af 21. december 2000 vedrørende spørgsmålet om sikkerhedskopier af edb-programmer skal man oplyse, at Kulturministeriet ikke kan være enig med Kommissionen i, at adgangen til at fremstille en sikkerhedskopi af et edb-program efter edb-programdirektivets art. 5, stk. 2, er begrænset til 1 kopi. Denne opfattelse har også fundet udtryk i forbindelse med den danske implementeringslov af 19. december 1992, hvor det i bemærkningerne til § 11a (nu § 36, stk. 2) udtales:

"Udtrykket "et sikkerhedseksemplar" betyder ikke, at det ikke er tilladt at fremstille flere sikkerhedseksemplarer, hvis dette er nødvendigt for benyttelsen af programmet."

Kommissionens implementeringsrapport har endnu ikke været genstand for forhandling med medlemslandene. Kulturministeriet vil under kommende drøftelser tilkendegive den danske holdning i sagen.

..."

*Initiativ om indførelse af system til uafhængig tidsstempning:* Ved en række lejligheder, bl.a. under den offentlige høring, Rådet afholdt i august 2000 har IT-Sikkerhedsrådet konstateret, at der kan være behov for at kunne føre bevis for, hvornår en hændelse, der er verificeret digitalt (f.eks. gennem en digital signatur) har fundet sted. Rådet har drøftet denne problemstilling under flere møder og besluttede den 1. oktober 2001 at afgive følgende anbefaling herom, der i første række er rettet til IT- og Forskningsministeriet:

"...

Et system til uafhængig tidsstempling indebærer, at en uafhængig tredjepart (herefter kaldet UT) ved at signere en meddelelse og offentliggøre denne signatur sammen med en meddelelse om tidspunktet herfor (et tidsstempel), kan præstere et bevis for, hvornår en begivenhed har fundet sted. Signaturen ledsages nemlig af et certifikat (en "konstaterende erklæring"), der knytter sig an til det tidspunkt, hvor meddelelsen er modtaget af UT. Når en person sender en meddelelse (evt. en hashværdi af en meddelelse) til UT, tilføjer UT meddelelsen et tidsstempel samt en digital signatur på denne meddelelse. De tre elementer udgør dermed tilsammen beviset for, at meddelelsen har eksisteret på det pågældende tidspunkt. Bevisets værdi står og falder dog med afgiverens troværdighed.

Det vil være en god idé hvis et sådant UT får udstedt gyldige certifikater fra en række CA'er f.eks. alle i landet. En sådan certificering vil således understøtte beviset for, at UT'ens tidsstempel ikke er et falsum, men at det rent faktisk er udstedt af UT'en.

Et system til uafhængig tidsstempling kan benyttes af såvel afsenderen som modtageren af en meddelelse. Hvis A modtager en signeret e-mail fra B, kan A sende B's digitale signatur på meddelelsen videre til UT. Når UT returnerer meddelelsen med sin signatur, opnår A et uafhængigt bevis for, at e-mailen må have været A's med netop det indhold B har signeret i hænde før det tidspunkt tidsstemplet angiver.

I princippet er der intet til hinder for, at enhver privat eller offentlig virksomhed etablerer en sådan tjeneste, f.eks. i forbindelse med virksomhed som certificeringstjenesteyder (i loven om elektroniske signaturer kaldet "nøglecentre", i det følgende kaldet CA). Det kan imidlertid også tænkes, at andre virksomheder kan ønske at melde sig på banen med sådanne services, f.eks. inden for advokat- og revisorsektoren.

Endvidere kan UT afhjælpe nogle af genererne, hvis et CA måtte ophøre med at fungere, f.eks. pga. konkurs. Hvis det kan fastslås, hvornår CA ophører med at fungere, f.eks. ved at dets offentlige nøgle tidsstempler ved brug af UT (Telestyrelsen kunne f.eks. have på en web-side eller det elektroniske Statstidende kunne offentliggøre en meddelelse om, at "Certificeringscentret NN er pr. dato ophørt med at drive CA virksomhed"), vil alle signaturer afgivet af brugere under dette CA, som med sikkerhed kan siges at være genereret før CA'et lukkede, være gyldige (hvis ellers signaturen er korrekt og certifikatet var tidsstemplet gyldigt). Tidsstemplingen ved UT godtgør således - bl.a. i kraft af den tillid, der forventes at bestå til UT - at signaturen er genereret før CA'et lukkede (stadig under forudsætning af at certifikatet var gyldigt på dette tidspunkt). Da alle brugere under alle omstændigheder bør benytte UT for vigtige signaturer, sker der i altså princippet intet alvorligt ved, at et CA lukker ud fra et rent sikkerhedsmæssigt synspunkt.

I en enkelt henseende kan sådanne sikkerhedsproblemer dog tænkes at opstå. Det kan således tænkes, at et certifikat forinden lukningen er blevet revokeret, men dette ikke er kommet nogen til kundskab, e.g. pga. sløseri fra CA'et side. Denne situation adskiller sig dog principielt ikke fra andre situationer, hvor CA begår fejl. Og da CA ifølge lovgivningen om e-signaturer skal have fornøden forsikring til dækning for sådanne fejl, rummer konkurssituationen ikke særlige problemer.

Som hermed antydnet burde det være en enkel sag at indbygge systemer til uafhængig tidsstempling i de funktioner, der i øvrigt tilbydes fra CA-virksomheder. En afgørende principiel beslutning herom må dog træffes ved valget af, hvilke tidsservere, der skal anses for officiel dansk/vesteuropæisk tid. I øjeblikket er dansk nationaltid fastsat som middelsoltiden, hvilket ikke er operationelt for IT-systemer.

Det anbefales derfor at anvende UTC-tiden (Coordinated Universal Time). UTC-tiden kan tilgås via kendte protokoller, og kan gælde for hele Danmark. ISP'er, e-handelssteder og andre IT-systemer kan synkronisere hermed, og det vil således være muligt at verificere tiden. Den eneste administrative foranstaltning, et sådant system kræver, er den beskrevne advarselsordning, som må formodes relativt enkelt at kunne implementeres via Telestyrelsen. Inden et sådant system sættes i værk bør det dog afklares, om de CA-virksomheder, der p.t. har gjort deres indtog på markedet, overhovedet er interesseret i at markedsføre en sådan service.

..."

Som det fremgår af årsberetningen for 2000 har IT-Sikkerhedsrådet den 29. maj 2000 rejst en række spørgsmål overfor Rigspolitiet om, hvilke sikkerhedsforanstaltninger, der følges i forbindelse med politiets aflytning af telekommunikation. Henvendelsen er besvaret af Rigspolitiet den 12. juli 2001 med en nærmere redegørelse, som Rigspolitiet anmoder om, at der ikke sker offentliggørelse af. IT-Sikkerhedsrådet drøftede dette materiale under sit møde den 28.8.2001, Rådet var enig i, at de opstillede sikkerhedsforanstaltninger indebar en rimelig sikkerhed, herunder sikkerhed for, at det ved aflytninger "på øjemedet" rent faktisk sikres at der efterfølgende indhentes retskendelse til den stedfundne aflytning. IT-Sikkerhedsrådet besluttede på denne baggrund ikke at foretage sig yderligere i sagen.

#### 8. Igangværende projekter

##### *Statistik-projektet:*

IT-Sikkerhedsrådet har i beretningsåret videreført den statistiske undersøgelse om IT-sikkerheden i Danmark som man igangsatte i 2000. Foruden den afrapportering af undersøgelsen, som fandt sted i januar måned med udsendelse i juni 2001 af delrapporten om "Datasikkerheden i Danmark år 2000", forelå også i beretningsåret resultaterne for 1. halvår af 2001. Disse resultater er baseret på besvarelser fra 391 deltagende virksomheder og institutioner. Dette er en tilbagegang på 27 besvarelser i forhold til det antal virksomheder der indgik i besvarelserne for undersøgelsen af datasikkerheden i år 2000. Det er forventeligt, at der vil være et vist frafald af deltagerne igennem den 3-årige periode. Dette søges kompenseres ved at lukke op for tilgang af nye virksomheder og institutioner fra årsskiftet 2001/2002.

IT-Sikkerhedsrådet anser dog besvarelserne og dermed tallene for 1. halvår for mere præcise end de tilsvarende tal for år 2000, idet de deltagende virksomheder og institutioner efter 1. runde ved hvilke spørgsmål der stilles, og forhåbentlig har indført de fornødne registreringer, der lægges til grund for rapporteringen. Endvidere omfatter perioden kun ½ år, hvor den første del af undersøgelsen omfattede et helt år.

Statistikken viser, at der, sammenlignet med tallene for år 2000, blandt andet er store procentvise stigninger i antallet af tilfælde med telekommunikationsproblemer og fejl i backup-rutinerne. Mere end hver tiende har endog konstateret alvorlige konsekvenser som følge af telekommunikationsproblemer, mens hver tolvte har haft alvorlige gener efter svigt i backup-funktionen.

IT-Sikkerhedsrådet tager dog i rapporten et forbehold med hensyn til den reelle udviklingstakt og anfører, at tallene for første halvår af 2001 formentlig er mere præcise end de tilsvarende tal for 2000.

Begrundelsen er, at det er anden gang undersøgelsen gennemføres, hvorfor de deltagende knap 400 virksomheder og myndigheder sandsynligvis har indført rutiner for registrering af IT-sikkerhedsproblemer og derfor nu kan opgøre antallet mere præcist.

Statistikken for første halvår af 2001 viser også en mere forventelig stigning i antallet af virusangreb, som hver anden virksomhed og myndighed har været udsat for. Men konsekvenserne af de mange virusangreb, som også har været flittigt omtalt i medierne, har været mindre alvorlige end året før, så den præventive indsats mod virusangreb har virket.

Derimod har hver tiende haft alvorlige gener som følge af telekommunikationsproblemer, og for en håndfuld er det gået helt galt: Fire virksomheder/myndigheder karakteriserer konsekvenserne som katastrofale. Kategorien telekommunikationsproblemer dækker eksempelvis afbrydelse af forbindelsen, fejl eller forsinkelse på datatransmission mv.

Ud fra et hyppighedskriterium er virusangreb, telekommunikationsproblemer og backup de væsentligste IT-sikkerhedsproblemer. Derefter følger indbrud, strømproblemer, e-mail og

internetproblemer. Alle fire kategorier rammer tæt på hver fjerde virksomhed og myndighed. Softwarefejl og hardware-afbrud har ramt næsten hver femte.

Deltagerne i undersøgelsen er blevet bedt om at karakterisere konsekvenserne af de tilfælde af IT-sikkerhedsproblemer, de har været udsat for. Hvor mange af dem, der var generende, alvorlige eller katastrofale.

Når der måles på antallet af generende tilfælde, er det de samme sikkerhedsproblemer, som nævnt ovenfor, der topper listen. Men hvis der måles på antal alvorlige tilfælde, ændres rækkefølgen. Så er telekommunikationsproblemer den væsentligste udfordring, fulgt af hardware-afbrud, softwarefejl, og problemer som følge af e-mail og backup-svigt.

IT-Sikkerhedsrådets overvejelser i lyset af disse konklusioner, er anført nedenfor under 9.

#### *Opdatering af Privatliv på internet:*

I 1998 udsendte IT-Sikkerhedsrådet en rapport med titlen "Privatliv på Internet", hvori Rådet dels kortlagde de dele af den danske del af Internet, som kunne tænkes at indebære særlige risici for tab af fortrolighed mv., dels gav nogle anbefalinger for, hvorledes man gennem forskellige tiltag kunne øge privatlivsbeskyttelsen på nettet.

I løbet af de år der er gået siden offentliggørelsen af denne rapport, har Internettet undergået en stærk udvikling, og i mange henseender har denne udvikling gjort rapportens konklusioner mindre relevante. På denne baggrund besluttede IT-Sikkerhedsrådet sig til at igangsætte arbejdet med en ny udgave af denne vejledning. Beslutningen blev truffet hen ved slutningen af beretningsåret og på et tidspunkt, hvor det var kendt, at ministeren ville forlænge Rådets mandat med yderligere tre måneder. Rådet påregner således at færdiggøre arbejdet med denne rapport i marts måned 2002, som det sidste af Rådets projekter.

#### 9. Rådets vurdering af IT-sikkerheden i Danmark

Ifølge kommissoriet for IT-Sikkerhedsrådet skal Rådet afgive en årlig rapport over status på IT-sikkerheden i Danmark. Det er bl.a. for at opfylde denne del af kommissoriet, at Rådet har igangsat sine løbende undersøgelser af IT-sikkerheden i Danmark, jf. bemærkningerne herom under pkt. 8. I det følgende skal gøres nogle bemærkninger om enkelte af de begivenheder, der udspillede sig i beretningsåret.

2001 kom i mange henseender til at sætte sikkerhedstemaet på den politiske dagsorden. I et tilbageblik står mest iøjnefaldende terrorangrebet mod USA den 11. september, men året bød også på andre hændelser, der har forrykket vort syn på sikkerhed i almindelighed og IT-sikkerhed i særdeleshed.

1. Når det gælder de specifikke *sikkerhedstrusler*, så vi i beretningsåret en type *computervirus*, der viste sig langt mere alvorlige end dem, vi har set tidligere. Hidtil har vira primært udløst deres destruktive funktioner, når brugerne selv foretog sig noget (f.eks. klikke på en vedhæftet fil). For så vidt har man kunnet sige, at de brugere, der er blevet ramt af virus - i en eller anden henseende - kunne siges at bære medansvaret herfor. Men en virus som f.eks. *code red worm* fungerer anderledes. Den spreder sig for første uden nogen form for aktiv medvirken fra brugeren (nemlig via en web-server). For det andet medfører den en risiko for *kompromittering* af de data, brugeren har liggende på sin web-server. Brugeren ved med andre ord ikke, at han er blevet ramt (f.eks. fordi data mistes), og han kan derfor risikere at leve videre, intetanende om de trusler, der nu er realiseret. Dernæst, for det tredje, var der tale om en virus, der var meget vanskelig at udrydde, hvis ikke alle ramte brugere foretog en koordineret indsats.

Dette aktualiserede et hidtil uset behov for en samlet koordineret indsats mellem ramte og truede brugere, nationalt såvel som internationalt. Og dette var baggrunden for, at IT-Sikkerhedsrådet tog det - set i forhold til tidligere, usædvanlige - skridt at gå ud med den fælles anbefaling, der er omtalt ovenfor i afsnit 6.

Sagen om *code red worm* har dermed fremhævet behovet for at koordinere den IT-sikkerhedsmæssige indsats, både nationalt og på internationalt plan. Problemerne slår ned på tværs af landegrænser, og de løsninger, der kan imødegå dem, er også de samme, uanset geografi og nationalitet. Man kan dermed sige, at den del af IT-sikkerhedsarbejdet, der gælder kampen mod virus, befinder sig i samme kategori som andre dele af sikkerhedsarbejdet, f.eks. sikring af persondata over landegrænser. Men hvor spørgsmål som det sidstnævnte har givet anledning til såvel politisk uenighed som retlig tvivl - nogle lande vil gerne regulere, andre ikke - burde der ikke være tvivl om retningen, når det gælder sikkerhedsindsatsen på dette område. Derfor er der et stort behov for, at man gør en indsats for at styrke den koordinerede indsats til bekæmpelse og afhjælpning af virusangreb mod IT-systemer.

2. Det andet område, hvor der kan synes at være behov for at styrke den koordinerende indsats, drejer sig om *backup*, eller sikkerhedskopiering. I beretningsåret har IT-Sikkerhedsrådet haft planer om at udforme en vejledning for sikkerhedskopiering. Det er rådets opfattelse, at der er et stort behov for ikke alene at synliggøre behovet backup-kopiering, men også at give vejledning om, hvorledes backup gennemføres. Behovet er måske størst blandt private brugere. For større IT-installationer er der som regel taget de forholdsregler, der er nødvendige, i form af spejling af diske, ved distribueret datalagring og ved andre adækvate tiltag. Men for private brugere er det at udføre backup-kopiering ikke nødvendigvis udtryk for en dagligdags rutine, som man uden videre sørger for sker. Mange programmanualer giver slet ikke vejledning herom - måske fordi der er tale om et alment problem, som ikke er særpræget for det pågældende program - og i de uddannelses tilbud, der gennemføres i forbindelse med PC-kørekortet, indgår emnet ikke (et forhold, som Dansk Dataforening dog - efter henvendelse fra IT-Sikkerhedsrådet - har ændret i det såkaldte "PC-erhverv").

Rådet nåede i beretningsåret ikke længere end til at konstatere, at der er et stort behov for at gøre noget ved problemerne vedrørende backup-kopiering, og at opgaven ikke er let. I denne beretning skal derfor blot lyde opfordringen til, at man i en fremtidig rådgivning på IT-sikkerhedsområdet er opmærksom på dette meget store problem.

3. Et tredje forhold, som der efter Rådets opfattelse ? igen baseret på de undersøgelser vedrørende datasikkerheden i Danmark, der er gennemført - er behov for at gøre noget ved, angår de problemer, der er forbundet med de relativt hyppige nedbrud af telekommunikations- og elektricitetsforsyningsforbindelser. Det er tænkeligt, at en del af disse problemer skyldes, at der ganske hyppigt sker brud på tele- og forsyningsforbindelser i forbindelse med gravearbejde (graveskader). Rådet har ved en enkelt lejlighed - nemlig i forbindelse med en konkret hørings sag, se herom ovenfor under pkt. 5 - rejst spørgsmålet overfor trafikministeriet. Men der kan være behov for at følge op på dette problem over en bredere front, i første omgang ved at søge problemets omfang og mere specifikke årsagsfaktorer klarlagt.

I lyset af begivenhederne den 11. september er det nærliggende afslutningsvis at gøre nogle tanker om, hvorvidt der i den verden, vi nu befinder os i, er grund til at se på IT-sikkerhedsarbejdet på en grundlæggende anderledes måde end tidligere.

Ser man bort fra de specifikke områder, der vil blive berørt af den lovgivning, der forventes vedtaget i 2002 som led i regeringens anti-terrorpakke (en lovgivning, som bl.a. vil betyde, at visse televirksomheder får pålagt nogle andre opgaver vedrørende registrering og overvågning mv.) er det Rådets opfattelse, at der ikke er grundlag for at anlægge et fundamentalt anderledes syn på sikkerhedsarbejdet. Et nøgternt blik på de *IT-sikkerhedsmæssige* skader, der indtrådte efter terrorangrebet i New York, viser således, at IT-systemerne i en vis forstand slap nådigst gennem katastrofen. Hovedparten af de IT-funktioner, der var blevet afviklet i the World Trade Center, kunne hurtigt videreføres på andet udstyr, idet man - bl.a. for at spare på den kostbare kvadratmeterleje - havde gjort brug af *remote centre*. IT-funktionerne blev derfor afviklet i lokaliteter adskilt fra de sammenstyrtede bygninger.

At et fly kolliderer med en skyskraber, der herefter bryder i brand og/eller styrter sammen, har altid stået som et muligt scenarie i læren om IT-sikkerhed. Og det har tilmed været kendt - bl.a. ved bombeangrebet på the World Trade Center i 1993 - hændelser af denne karakter, kunne tænkes udløst ved terrorisme. Terrorangrebet den 11. september 2001 har måske nok givet anledning til at omdefinere de sandsynlighedsgrader, efter hvilke man søger at indkalkulere sådanne risici i sit sikkerhedsarbejde. Men på det helt grundlæggende plan - forstået som netop dette: at kalkulere og kvantificere risici og foretage de hertil fornødne modforanstaltninger - er der efter IT-Sikkerhedsrådets opfattelse ikke bibragt noget afgørende nyt erfaringsmateriale med katastrofen den 11. september 2001.

I beretningsåret har Rådet - efter ønske fra det eksterne ekspertpanel - forsøgt at danne sig et overblik over, hvilken forskning, der foregår herhjemme på IT-sikkerhedsområdet. Det har været vanskeligt at få nogen til at påtage sig opgaven med at foretage en sådan udredning. Opgaven er nemlig vanskelig, fordi emnet ikke har nogen klar afgrænsning, og fordi en betydelig del af området drejer sig om forhold, som måske slet ikke egner sig for egentlig "akademisk" forskning (f.eks. udmøntet i ph.d.- og doktorafhandlinger mv.).

I Danmark IT-retten arbejdes der intenst med IT-retlige spørgsmål ved universiteterne i København og Aarhus og ved Handelshøjskolen i København. Der forskes i kryptering ved Aarhus Universitet (matematisk institut) og ved Danmarks Tekniske Universitet (Lars Ramkilde).

Derimod er der såvidt ses ingen forskning inden for områder, hvor problemerne gør sig gældende i praksis relation til specifikke applikationer. Dette kan i og for sig ikke overraske, og man må nok i det hele taget konstatere, at det vil være vanskeligt at definere et akademisk forskningsområde inden for sådanne applikationsområder.

Et enkelt område, som man dog kunne overveje om ikke kunne prioriteres højere, er det statistiske område. De undersøgelser, IT-Sikkerhedsrådet har foretaget om datasikkerheden i Danmark, synes at antyde et ganske stort behov for nærmere statistisk viden om, hvilke faktorer, der kan påvirke samfundets sårbarhed på dette punkt. Men netop i lyset af IT-Sikkerhedsrådets aktiviteter på dette område kan man overveje, om ikke denne opgave således varetages på god vis af en offentlig myndighed.

#### 10. Rådets fremtid

IT-Sikkerhedsrådet afsluttede sin årsberetning for 2000 med at gøre nogle betragtninger om, hvilke former en kommende organisering af Rådets arbejde kunne tænkes at antage

Rådets mandat udløb pr. 31. december 2001 men på grund af folketingsvalget den 20. november 2001 blev mandatet forlænget i 3 måneder og udløber således pr. 31. marts 2002. I den anledning har Ministeriet for Videnskab, Teknologi og Udvikling overvejet, hvordan behovet for offentlig rådgivning på IT-sikkerhedsområdet kan varetages i fremtiden.

For at kunne opnå det bedst mulige beslutningsgrundlag herfor tog ministeren for videnskab, teknologi og udvikling sammen med IT-Sikkerhedsrådet initiativ til at afholde en offentlig høring om det offentlige rådgivning om IT-sikkerhed i dag og i fremtiden. Til høringen, der afholdtes den 4. februar 2002, deltog foruden Rådets medlemmer, ministeren for videnskab, teknologi og udvikling, politiske ordførere på IT-sikkerhedsområdet samt særligt indbudte sagkyndige med berøring til IT-Sikkerhedsrådets arbejde.

Formålet med høringen var at afdække de konkrete behov og problemstillinger, der er på IT-sikkerhedsområdet og derigennem skabe et grundlag for en vurdering af behovet for den fremtidige offentlige rådgivning på området. Overvejelserne herom er i skrivende stund ikke afsluttet.