# Årsberetning 2004

RÅDET FOR IT-SIKKERHED

Udgivet af:

Rådet for it-sikkerhed
c/o IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Telefon 3545 0364
Telefax 3545 0014
e-mail raadet@rfits.dk
www.rftis.dk

Årsberetningen kan også ses på rådets netsted www.rfits.dk

Omslag: Gitte Blå Design
Opsætning og tryk: Schultz Grafisk

Digital ISBN: 87-91469-56-2

>

# Årsberetning 2004

Rådet for it-sikkerhed

# Indhold >

>

## Større opmærksomhed om it-sikkerhed >

Rådet for it-sikkerhed har nu eksisteret i to år. Rådet blev nedsat af videnskabsminister Helge Sander pr. 1. januar 2003 som afløser for det tidligere IT-Sikkerhedsråd.

Rådet for it-sikkerhed ser det som en af sine fornemmeste opgaver at fremme en egentlig it-sikkerhedskultur i Danmark.

Samtidig med at angrebene på it-netværk og computere i 2004 har været massive, kan rådet med stor tilfredshed konstatere en støt stigende opmærksomhed på og bevågenhed over for it-sikkerhed i den danske befolkning. Således har 32 pct. af virksomhederne nu en godkendt it-sikkerhedspolitik. 90 pct. af virksomhederne benytter antivirusprogrammer. I den offentlige forvaltning er tallet helt oppe på 97-100 pct. I befolkningen som sådan er situationen nu den, at mere end otte ud af ti med computer og internet derhjemme bruger it-sikkerhedsprodukter. F.eks. tager 37 pct. backup af vigtige filer.

Som et led i at få etableret en it-sikkerhedskultur i Danmark skal rådet arbejde for at:

> øge bevidstheden om risici ved anvendelse af it-systemer og netværk

> skabe større tillid til anvendelsen af it-systemer og netværk

> skabe rammer, der kan hjælpe interessenter til at forstå sikkerhedsproblemstillinger og respektere etiske værdier i forbindelse med disse politikker

> fremme samarbejde og videndeling mellem interessenter i forbindelse med udvikling og implementering af politikker og procedurer for it-sikkerhed

> fremme, at bevidstheden om it-sikkerhed indgår som et vigtigt mål for alle, der er involveret i udvikling eller implementering af standarder.

>

Rådet for it-sikkerhed sekretariatsbetjenes af IT- og Telestyrelsen.

Rådet er sammensat som følger:

**Formandskab**
Allan Fischer-Madsen, partner, Devoteam Fischer & Lorenz (formand)
Janne Glæsel, partner, Bech-Bruun Dragsted (næstformand)

**Øvrige medlemmer**
Per Buchwaldt, formand, Dansk IT
Martin von Haller Grønbæk, partner, Advokatfirmaet von Haller
Birgit Hansen, udviklingsdirektør, Scan-Jour
Carsten Heilbuth, partner, KPMG
Adser Leick, global it-sikkerhedschef, LEGO Koncernen
Estrid Oxlund, kommunaldirektør, Holstebro Kommune

## Sådan går det med it-sikkerheden i Danmark >

Den *offentlige forvaltning* i Danmark gør det generelt rigtig godt, når det drejer sig om it-sikkerhedsforanstaltninger. F.eks. har 9 ud af 10 myndigheder en ledelsesgodkendt it-sikkerhedspolitik.

For *virksomhedernes* vedkommende ligger Danmark sammen med de øvrige nordiske lande helt i spidsen internationalt og betydeligt bedre end EU-gennemsnittet.

Også *befolkningen* som sådan er ved at komme efter det: 83 pct. bruger it-sikkerhedsprodukter. Det er en stigning på 10 pct. i forhold til året før.

300.000 danskere har nu anskaffet sig en digital signatur.

Det er et generelt godt billede, der dog dækker over store variationer, såvel i forholdet mellem mindre og mellemstore og store virksomheder som mellem forskellige befolkningsgrupper og forskellige geografiske områder.

Den generelt større tilskyndelse til at beskytte sig modsvares af massive anslag mod it-sikkerheden i Danmark. I en situation hvor mere end 60 pct. oplyser, at de har opdateret et antivirusprogram inden for den seneste måned, har hele 31 pct. alligevel mistet data i forbindelse med virus.

Spam er det it-sikkerhedsproblem, som flest danskere føler sig ramt af. Studerende er den befolkningsgruppe, som it-sikkerhedsproblemer rammer hyppigst. Dette afspejler såvel hyppighed i brug af internettet, måden at bruge internettet på som graden af sikring. Funktionærer og selvstændige er de befolkningsgrupper, der er bedst til at sikre sig mod it-sikkerhedsproblemer. Således tager over halvdelen af de selvstændige jævnligt backup af vigtige filer.

Den aktuelle situation for it-sikkerheden i Danmark fremgår af afsnittet om it-sikkerhed i rapporten *Informationssamfundet Danmark – It-status 2004,* som Danmarks Statistik har udarbej-

det for Videnskabsministeriet. Rapporten viser, at jo mere man bruger pc og internet, jo mere oplever man de forskellige former for sikkerhedsproblemer. De unge er den mest udsatte gruppe, fordi de er de meste aktive brugere – og ældre er i flere henseender de mindst udsatte, fordi de er mere tilbageholdende i forhold til deres brug af pc og internet. Tilsvarende forskelle viser sig geografisk. Der er således flere mennesker vest for Storebælt end øst for, der ganske enkelt undlader at foretage visse handlinger på nettet. 56 pct. vest for Storebælt mod 46 pct. øst for undlader at bruge kreditkort på nettet, og 51 pct. vest for Storebælt mod 43 pct. øst for undlader at sende fortrolige oplysninger på nettet.

Det offentlige i Danmark giver it-sikkerhed høj prioritet:

> Firewalls og antivirusprogrammer anvendes af praktisk talt alle myndigheder. Spamfiltre anvendes af omkring hver anden.

> Der er også udbredt anvendelse af backup på anden lokalitet end driftsmiljøet og af nødstrømsanlæg.

> Ni ud af ti myndigheder har en it-sikkerhedspolitik, og de fleste af de hovedansvarlige for it-sikkerheden refererer direkte til ledelsen.

Men:

> Halvdelen af de offentlige myndigheder har oplevet problemer med it-sikkerheden, flest virusangreb men også fejl og nedbrud i serversoftware.

Virksomhederne bringer Danmark i front internationalt:

> 94 pct. af dem har en eller flere it-sikkerhedsforanstaltninger.

>

- Virksomhederne anvender mest teknologiske sikkerhedsforanstaltninger som antivirusprogrammer, firewalls, backup mv.

- Organisatoriske sikkerhedstiltag er betydeligt mindre udbredt. Kun hver tredje virksomhed med internetadgang har f.eks. udpeget en it-sikkerhedsansvarlig.

- Kun 14 pct. har en ajourført it-sikkerhedsvejledning til virksomhedernes pc-brugere.

- It-sikkerhedsforanstaltninger er mere udbredt i større virksomheder end i de små. Det afspejler dels at de større virksomheder har større økonomisk kapacitet og mere specialviden om området, dels at de større virksomheder oftere udsættes for problemer.

Her går det galt for virksomhederne:

- Virusangreb og nedbrud rammer mere end 30 pct. af dem.

- Tyveri og datatab på grund af manglende backup er også et stort problem.

- Større virksomheder rammes oftere end små virksomheder af de enkelte problemer. Og de rammes oftere af flere problemer samtidig.

Det samlede billede viser, at it-sikkerhed stadig er en helt afgørende udfordring i forhold til udvikling af viden- og netværkssamfundet. Det er tydeligt, at it-sikkerhed er kommet på dagsordenen, både for virksomheder, myndigheder og borgere – desværre ofte foranlediget af datatab eller andre former for sikkerhedsproblemer. Men antallet af virksomheder, myndigheder og borgere, der rammes af sikkerhedsproblemer, viser også, at der stadig er lang vej igen.

>

Links:

*Informationssamfundet Danmark – It-status 2004:*
www.vtu.dk//fsk/div/itsoejlen/ITstatus.9.11.04.pdf
Pressemeddelelse fra Rådet for it-sikkerhed vedr. rapporten:
www.rfits.dk/Befolkningen_sikrer.3347.0.html

**Hjælp mod computervirus og andre ondsindede programmer**
Orme, trojanske heste, makrovirus og hoax. Selv om de færreste umiddelbart ved, hvad der gemmer sig bag disse navne, har omkring hver tredje internetbruger stiftet et meget ubehageligt bekendtskab med dem, når deres computer rammes af en virus.

Rådet for it-sikkerhed har derfor sammen med IT- og Telestyrelsen udgivet en pjece med 10 gode råd om, hvordan man bedst beskytter sig mod computervirus. Pjecen *Beskyt dig mod computervirus* henvender sig til borgere og virksomheder og er en opfølgning på pjecen *Hvad du bør vide om computervirus*, som Rådet for it-sikkerhed og IT- og Telestyrelsen udgav i 2003.

Pjecen indeholder – ud over de 10 gode råd – en ordliste, der i et enkelt sprog forklarer, hvad der gemmer sig bag betegnelserne som hoax, orm, trojansk hest, antivirusprogram og opdatering af programmer. Den giver også en kort beskrivelse af, hvad computervirus er, og hvordan computeren inficeres med virus, og den fortæller, hvorfor det er så vigtigt at sikkerhedsopdatere programmerne jævnligt og at installere et antivirusprogram.

Der er udsendt omkring 10.000 eksemplarer af begge pjecer, og de ligger desuden tilgængelige i elektronisk udgave på rådets hjemmeside (www.rfits.dk ) sammen med andet af rådets oplysningsmateriale.

Rådet for it-sikkerhed prioriterer højt at udbrede så mange gode råd som muligt til den almindelige borger. Virus- og andre sikkerhedsproblemer fortsætter med at vokse, og det er derfor vigtigt, at så mange som muligt bliver aktiveret og inddraget i bestræbelserne på at gøre det trygt at bruge computere og netværk.

**Hjemmeside om firewalls**
Brugen af firewall er en af de vigtigste sikkerhedsforanstaltninger, når en computer er koblet til internettet. Den sikrer, at

computeren kun giver adgang til udefrakommende trafik, som man selv har bedt om. Dermed sørger en firewall for eksempel for, at ens computer ikke kan bruges af hackere og andre til angreb på websites og servere andre steder på nettet. Derfor er det af stor betydning for datasikkerheden generelt, at så mange som muligt installerer en firewall.

Rådet for it-sikkerhed og IT- og Telestyrelsen har som led i sit oplysningsarbejde etableret en hjemmeside (indgang fra www.rfits.dk), der indeholder gode råd om brugen af firewalls. Hjemmesiden henvender sig til borgere og mindre og mellemstore virksomheder. Den giver generelle og lettilgængelige informationer om, hvad en firewall er, og hvordan den installeres. For de mere teknisk interesserede er der mulighed for at læse mere og at finde links til endnu mere information.

Hjemmesiden er logisk opbygget, så den forudsætningsløse læser kan bevæge sig fra afsnittet om trusler på internettet, over en beskrivelse af firewalls til hvordan de virker og installeres. Desuden indeholder websiden en ordliste, der på almindeligt dansk forklarer de mange ord og begreber, man støder på, når det handler om computersikkerhed og firewalls. Almindelige brugere kan med hjælp fra hjemmesiden opsætte en firewall.

**Landsdækkende it-sikkerhedskampagne**
*Netsikker nu!* er titlen på den it-sikkerhedskampagne, som Videnskabsministeriet i samarbejde med Rådet for it-sikkerhed står bag. Kampagnen holdes over flere dage i marts 2005.

Målet med *Netsikker nu!* er at sætte tryghed og tillid til it-anvendelsen på dagsordenen. Kampagnen henvender sig til borgere og mindre og mellemstore virksomheder, og den skal bidrage til at give større opmærksomhed omkring it-sikkerhed.

Hele kampagnen skal være med til at gøre it-brugerne opmærksomme på deres ansvar i forhold til en it-sikkerhedskultur. At få opbygget en sådan sikkerhedskultur er i høj grad et spørgsmål om information, uddannelse og bevidsthed suppleret med de

teknologiske muligheder, der løbende udvikles. Opgaven er i langt højere grad at få borgere, virksomheder og offentlige myndigheder til at indøve nye vaner og adfærd, som passer til netværkssamfundet, hvor alle er forbundet med alle via internettet.

Kampagnen vil gennem en lang række aktiviteter, it-sikkerhedsmaterialer samt PR og markedsføring skabe så meget opmærksomhed som muligt om sikker it-adfærd. Kampagnen sigter på at nå ud til hele Danmarks befolkning og til de mindre og mellemstore virksomheder gennem forskellige målrettede arrangementer om it-sikkerhed, blandt andet besøg i folkeskoler, på-vej-hjem-møder på arbejdspladser, workshops, PR i lokalblade osv.

*Netsikker nu!* er et privat-offentligt samarbejde. Projektet er iværksat af en række offentlige og private aktører, som ønsker at skabe opmærksomhed om sikker adfærd på nettet. Alle interesserede offentlige og private aktører kan deltage.

Rådet har bidraget til de it-sikkerhedsfaglige rammer gennem en løbende dialog med Videnskabsministeriet.

**10 gode råd**
Rådet for it-sikkerhed vil i 2005 tage initiativ til, at der mellem en række interessenter i fællesskab udformes ”10 gode råd”, som anviser en vej til basal it-sikkerhedsbeskyttelse for borgere og mindre og mellemstore virksomheder.

Rådet ønsker med dette initiativ at bidrage til størst mulig synergi i kommunikationen om it-sikkerhed til borgere og de mindre og mellemstore virksomhed fra indholdsleverandører, internetudbydere, hardware- eller softwareproducent, myndigheder m.fl.

I det omfang de mange forskellige aktører ønsker at medvirke, vil det være muligt i en koordineret bestræbelse at lægge større kraft bag budskabet. I rådets øjne er det afgørende at etablere

>

netværksinitiativer af denne art, da en bedre it-sikkerhed kræver, at mange mennesker og virksomheder får mere viden og bedre sikkerhedsvaner og rutiner.

## Branchen og it-sikkerheden >

**Branchekodeks for it-sikkerhed**
En stor del af de danske internetudbydere vedtog i maj 2004 en fælles branchekodeks om frivilligt at arbejde på at bremse skadelig trafik på internettet[1]. Kodeksen blev tiltrådt af TDC, Cybercity, Telia, Tele 2, Tiscali, Sonofon, Webpartner og Netgroup.

Rådet for it-sikkerhed hilser oprettelsen af den fælles kodeks velkommen. Rådet har løbende været i dialog med udbyderne og deres brancheorganisationer om denne kodeks, og rådet er yderst tilfreds med, at branchen på denne måde er med til at tage hånd om de netværksmæssige aspekter af it-sikkerheden.

Det er rådets opfattelse, at internetudbyderne har en central rolle i kraft af deres placering som formidlere af forbindelse til internettet. Rådet har hele tiden været af den opfattelse, at de bedste resultater i forhold til it-sikkerheden opnås, hvis udbyderne selv står bag de initiativer, der skal beskytte den danske del af internettet.

Kodeksen indeholder fælles sigtelinier for, hvad der er god skik med henblik på internetsikkerhed. De udbydere, der tilslutter sig, forpligter sig til at efterleve kodeksen.

Udbyderne og deres organisationer understreger, at vedtagelsen af en fælles kodeks ikke fritager den enkelte bruger for at sikre egen hardware og software, og at brugere at internettet har det ubetingede ansvar for at sikre sig mod hackerangreb, virus og andre former for misbrug.

Ved at tilslutte sig kodeksen forpligter internetudbyderne sig til at tildele kvalificerede ressourcer til at håndtere trusler mod internettet, til bl.a. at arbejde effektivt for at begrænse trusler mod internettet og at begrænse komplikationer som følge af hacker- eller virusangreb og andre former for misbrug.

Senest er flere store udbydere begyndt at filtrere spam fra for deres kunder. Det ser Rådet for it-sikkerhed som en naturlig

1 http://billed.di.dk/wimpfiles/lores/image.asp?objno=/322108.pdf

fortsættelse af den fælles branchekodeks. Det er rådets holdning, at it-sikkerheden skal ind i alle produkter fra starten, så brugerne ikke skal være nødt til at tilvælge eller købe ekstra produkter. Udbydernes automatiske spamfiltrering er et godt eksempel på en sådan form for indbygget sikkerhed.

**Dialog med branchen og forbrugere**
Rådet for it-sikkerhed vil i tættere dialog med virksomheder, brancheorganisationer og forbrugere om it-sikkerhed.

Derfor tog rådet i august 2004 initiativ til at etablere et åbent og uformelt dialogforum, hvor der kan udveksles synspunkter om it-sikkerhed. Formålet med dialogforummet er, at det skal gøre opmærksom på aktuelle og kommende mulige it-sikkerhedsproblemer, som rådet bør fokusere på i rådgivningen over for offentlige myndigheder, ministerier og regeringen. Desuden er det formålet, at forummet skal afklare, om aktuelle sikkerhedsproblemer bør analyseres nærmere og tages op af rådet.

På forummets første møde blev der blandt andet rejst spørgsmål om de it-sikkerhedsproblemer, der opstår som konsekvens af den stadig større sammenkobling mellem forskellige firmaers netværk. Der blev peget på, at det er nødvendigt at tænke i nye baner for at imødekomme de trusler mod sikkerheden, som denne udvikling giver anledning til.

Også spørgsmålet om fysisk it-sikkerhed blev rejst. Mange mindre og mellemstore virksomheder har ensidigt fokus på andre sikkerhedsaspekter end det fysiske. Det er imidlertid nødvendigt også at forholde sig til og investere i den fysiske sikkerhed. It-sikkerhed, herunder den fysiske sikkerhed, kræver ledelsesmæssigt fokus. Som et aktuelt eksempel blev der peget på, at kommunalreformen er en god anledning til, at kommunerne tager de fysiske it-sikkerhedsproblemer op til revision.

Lovgivning eller vejledning var endnu et emne, der blev drøftet på dialogforummets første møde. Mange forskellige synspunkter blev fremført. Rådet for it-sikkerhed blev opfordret til at ud-

give flere konkrete vejledninger målrettet den enkelte bruger ud fra en betragtning om, at virksomhedernes ledelser ikke bør være den primære målgruppe for informationer om it-sikkerhed. Andre mente, at brugervenlige vejledninger ikke er løsningen. Som alternativ blev det foreslået at arbejde for at opnå bedre it-sikkerhed gennem lovgivning. Endnu et synspunkt var, at leverandørerne burde være den primære målgruppe. Argumentet var, at brugerne skal kunne have tillid til de systemer, de benytter, og at målgruppen derfor bør være dem, der laver systemerne.

Formanden for Rådet for it-sikkerhed understregede, at rådet tror på frivillighed gennem vedtagelse af kodeks, og at de forskellige synspunkter og forslag vil indgå i rådets videre arbejde.

**Manglende sikkerhed i MPLS-netværk**
Udbredelsen af MPLS-netværk bliver større og større. MPLS betyder *Multi-Protocol Label Switching* og er en fælles betegnelse for løsninger, hvor to eller flere lokationer forbindes via en logisk afgrænset del af internettet. Brugere af disse netværk har et stort ønske om at få indsigt i løsningernes it-sikkerhed. Dette tilbyder leverandørerne af MPLS-netværk ikke i dag.

MPLS-netværkene rummer sårbarheder, som ikke er belyst i tilstrækkelig grad. Som udgangspunkt giver MPLS-netværk således ikke sikkerhed for fortrolighed, og de beskytter ikke kundens netværk. I MPLS-standarden er der heller ikke indbygget beskyttelse mod fejlkonfigurationer i MPLS-nettet. Konfigurationen af MPLS-nettet sker på routere i netværket. Særligt de såkaldte kantroutere, der er de enkelte kunders indgang til netværket, er kritiske. Fejlkonfigurationer i disse kantroutere kan påvirke sikkerheden i hele MPLS-nettet.

Især finanssektoren, der har nogle af de største kunder til MPLS-netværk, har efterlyst større indsigt i it-sikkerheden. Finanssektoren har bl.a. udtrykt ønske om, at udbyderne blev pålagt et reguleret tilsyn. Rådet for it-sikkerhed mener, at en sådan fremgangsmåde vil være ude af takt med de grundlæggende

>

principper for regulering af telesektoren i Danmark og i EU. Rådet overvejer i stedet at formulere sit eget synspunkt på, hvad der er god it-sikkerhedsadfærd fra MPLS-leverandørernes side.

Rådet for it-sikkerhed ser det som en sund og naturlig udvikling, at virksomheder, der outsourcer datatransmissionen, tager ejerskab til it-sikkerhedsproblemerne og forsøger at sikre sig mod de risici, der er på området. Virksomhederne har en naturlig og stor interesse i at sikre høj it-sikkerhed, også når de outsourcer, og derudover hviler ansvaret for sikker elektronisk behandling af personoplysninger ifølge persondataloven fortsat på virksomheden, selv om den outsourcer.

Derfor har rådet skrevet til alle udbydere af MPLS-netværk og opfordret dem til at give deres kunder det indblik i it-sikkerhedsspørgsmål, som kunderne har brug for. En måde at gøre det på kunne være, at udbyderne tilbyder et uafhængigt tilsyn med it-sikkerheden.

## Det offentlige og it-sikkerheden >

**It-sårbarhed**
Den nationale sårbarhedsudredning, som Indenrigs- og Sundhedsministeriet har udarbejdet, giver et overblik over udfordringer, sårbarheder og beredskab på en række samfundsvigtige områder og kommer med en række anbefalinger til forbedring af sikkerheden.

Som opfølgning på sårbarhedsudredningen har Videnskabsministeriet ved IT- og Telestyrelsen iværksat projektet "Statsligt it- og teleberedskab", der har til formål at pege på et tidssvarende beredskab for elektronisk kommunikation. Projektet har primært beredskabsmyndighederne som målgruppe og fokuserer på deres behov for it-anvendelse og elektronisk kommunikation i en beredskabssituation. Projektet fokuserer også på den infrastruktur, der ejes af teleudbyderne.

Rådet for it-sikkerhed finder projektet "Statsligt it- og teleberedskab" af væsentlig betydning. Rådet peger derudover på det vigtige i at få belyst samfundets generelle afhængighed af it-infrastrukturen. Rådet finder det nødvendigt også at få belyst de sårbarheder, der ikke er direkte relateret til beredskabsmyndighedernes behov i en krise- eller krigssituation. Rådet vurderer, at det er afgørende, at der fremover også bliver set på de bredere aspekter af sårbarheder inden for it-området, for eksempel er sårbarheden inden for vigtige sektorområder som detailhandlen og finanssektoren endnu ikke tilstrækkeligt kortlagt. Derfor har Rådet for it-sikkerhed nedsat en arbejdsgruppe, der vil skitsere anbefalinger til yderligere sårbarhedsanalyser inden for it-anvendelsen i Danmark. Det kan eksempelvis dreje sig om initiativer af mere forskningsmæssig karakter, dels i forhold til samfundets generelle afhængighed af it og sårbarheder forbundet hermed, dels i forhold til enkeltsektorer, hvis funktioner er særligt kritiske for samfundet.

>

## Det internationale og it-sikkerhed >

EU-kommissionen har etableret *Det europæiske Agentur for Net- og Informationssikkerhed (ENISA).* ENISA vil få sæde i Grækenland. Agenturet skal fungere som et ekspertisecenter, hvor både medlemslandene og EU's institutioner kan søge rådgivning. Det skal bidrage til et bredt samarbejde mellem forskellige europæiske aktører på området for informationssikkerhed.

Med henblik på ENISAs første arbejdsprogram har Rådet for it-sikkerhed opfordret til, at ENISA arbejder for international interoperabilitet på området for digital signatur. Rådet mener, at det er vigtigt for den digitale signaturs succes, at der kan ske en ensartet og transparent udveksling af certifikater i EU. Rådets forslag bunder i en erkendelse af, at hidtidige tiltag i EU ikke har medført mærkbare fremskridt med henblik på at skabe løsninger, der kan være enighed om, og som fører til fælles konsensus og implementering. Rådets formand og næstformand har haft lejlighed til under et uformelt møde med agenturets direktør, Andrea Pirotti, at drøfte udfordringer og muligheder for ENISA. Rådet vil løbende bidrage til ENISAs arbejde.

>

# Sikker it i alt >

”Pervasive computing” – *it i alt* – er den tredje bølge af computerteknologi, som nogle gange også beskrives med ordene *ting der tænker.* Den nye teknologibølge udgør en betydelig strategisk udfordring for dansk erhvervsliv og en tilsvarende udfordring for samfundet. *It i alt* spænder vidt fra det, der i dag opfattes som ren science fiction, til nutidens dagligdags ting som mobiltelefoner. *It i alt* betyder, at der bliver indbygget computere i alt – fra sportstøj med indbygget pulsmåler, kontorstole der husker brugerens højde, interaktive rum, automatiserede lagersystemer og kasseapparater uden kassedamer til intelligente bandager, computerstyrede bremser, ubemandede kampfly og meget mere. Der findes mange teknologier, men den i øjeblikket mest kendte er den elektroniske stregkode, også kendt som RFID-tag’et.

Med *it i alt* vil de mange produkter og varer efterhånden have indlejret computerchips. En af de mest brugte funktioner vil være aflæsning af chippens unikke identitet på afstand. Går man f.eks. gennem kassen i et supermarked, vil det ikke længere være nødvendigt at tage varerne op af vognen. Varerne vil selv kunne kommunikere med kasseapparatet.

I forbindelse med denne konstant mulige kommunikation mellem mennesker og ting, mennesker og mennesker samt ting og ting, dukker en række væsentlige it-sikkerhedsspørgsmål op. Rådet for it-sikkerhed og Datatilsynet holdt derfor i november 2004 en offentlig høring om emnet. Høringen var meget velbesøgt.

Formålet med høringen var dels at få en kortlægning af it-sikkerhedsmæssige og juridiske problemstillinger om it i alt, dels at igangsætte en diskussion om og udfærdige et forslag til en adfærdskodeks for it i alt. Anvendelsen af elektroniske stregkoder i detailhandelen blev valgt som tema, fordi det er et af de områder, der hurtigst vil komme til at berøre alle borgere, og som derfor bliver afgørende for forbrugernes generelle tryghed og tillid i forhold til den nye allestedsnærværende teknologi.

>

Forud for høringen havde Rådet for it-sikkerhed inviteret Alexandra Instituttets Center for it-sikkerhed til – i samarbejde med professor Peter Blume, Københavns Universitet – at udarbejde en analyse af de it-sikkerhedsmæssige og juridiske aspekter ved it i alt. Peter Blume var blevet bedt om at udarbejde en råskitse til en adfærdskodeks for detailhandlen. Baggrunden for dette var, at Dansk Industri, Forbrugerrådet og Dansk Handel & Service havde indvilliget i forud for høringen at diskutere indholdet af en sådan kodeks og på høringen fremlægge resultatet af deres drøftelser samt efterfølgende at arbejde videre med oplægget. Rådets målsætning er at få udarbejdet en kodeks, som parterne kan enes om, og som Datatilsynet også kan tilslutte sig.

I forbindelse med høringen udtalte rådets formand, Allan Fischer-Madsen, at det er vigtigt, at få debatten om *it i alt* skudt i gang, inden det er for sent: ”Vi står over for en teknologi, der sandsynligvis vil ændre vores hverdag drastisk, på samme måde som mobiltelefonen har gjort det. Vi ved, at teknologien kommer, lige meget hvad vi hver især synes om det, men en debat kan være med til, at teknologien bidrager til en positiv udvikling i vores samfund”.

Under høringen fremlagde Rådet for it-sikkerhed rapporten *Pervasive computing – it-sikkerhed og privacy,* som Alexandra Instituttet havde udarbejdet for rådet. Rapporten tager udgangspunkt i en række scenarier for fremtidens udvikling af it i alt, og den beskriver de omfattende sikkerhedstemaer, som det er helt afgørende at forholde sig til, for at der blandt forbrugerne kan skabes tillid og tryghed til den nye teknologi. De tre væsentligste sikkerhedstemaer drejer sig om integritet, fortrolighed og tilgængelighed.

Efter høringen arbejder Forbrugerrådet, Dansk Handel og Service og Dansk Industri videre med kodeksen, og i forbindelse hermed vil de bl.a. give deres bud på, om myndighederne bør og kan inddrages i arbejdet med den. Datatilsynet holdes orienteret om resultaterne af dette arbejde.

>

Rådet håber, at en sådan kodeks for detailhandlen vil kunne udbredes til andre brancher og inspirere andre lande til tilsvarende initiativer.

Kodeksen kommer blandt andet til at fokusere på åbenhed i forhold til kunder og ansatte, skiltning i butikkerne samt varestyring frem for overvågning af kundernes adfærd mv.

Rådets opfølgning omfatter følgende punkter:

> Rapporten, som blev udarbejdet til høringen, er oversat til engelsk og sendt til International Chamber of Commerce (ICC). Med dette initiativ vil rådet bidrage til, at anbefalinger og analyseresultater gøres tilgængelige internationalt i samarbejdet om de it-sikkerhedsmæssige aspekter ved it i alt.

> Rådet har foreslået, at Datatilsynet tager emnet op i forhold til det internationale samarbejde på persondataområdet via "artikel-29"-gruppen.

> Rådet vil medvirke aktivt til, at brancheorganisationernes og Forbrugerrådets arbejde med et udkast til kodeks for brug af RFID-teknologien bliver afsluttet.

> Rådet vil bidrage til at it-sikkerheden ved *it i alt* bliver et tema i Netsikker Nu! kampagnen.

> Rådet har sendt den engelske oversættelse af rapporten fra høringen til Det europæiske Agentur for Net- og Informationssikkerhed (ENISA).

>

## Her bør der sættes ind i fremtiden >

Rådet for it-sikkerhed har efter to års virke og på baggrund af kontakt med leverandører, brancheorganisationer, virksomheder og andre aktører på it-sikkerhedsområdet konstateret, at vi både nationalt og internationalt har en række muligheder for at højne it-sikkerhedsniveauet generelt i samfundet. Rådets indsats i forhold til koordinerende initiativer og netværksinitiativer er blevet godt modtaget af producenter, brancheorganisationer og andre aktører.

It-markedet og internettet er internationale og grænseoverskridende. Det samme gælder flertallet af it-sikkerhedstruslerne. Forbedring af it-sikkerhedsforholdene drejer sig derfor i høj grad om at skabe internationale løsninger. Som et land med udbredt og relativ homogen brug af it har Danmark mulighed for at bidrage aktivt til international udbredelse af en it-sikkerhedskultur, som tager udgangspunkt i demokratiske traditioner.

**Det kan der gøres på nationalt plan**
På det nationale niveau ser rådet mulighed for en række fremtidige initiativer, som kan mindske risici og skadevirkninger og i et vist omfang dæmme op for de grænseoverskridende angreb.

En bedre it-sikkerhedskultur vil beskytte os bedst muligt både mod de trusler, der skyldes egen forsømmelse, og mod de trusler, der er udefrakommende og uforskyldte. Rådet vurderer derfor, at der er et betydeligt behov for at gennemføre flere brede og omfattende kampagner, således at viden og opmærksomhed højnes både hos den enkelte og hos virksomhederne. Bedre it-sikkerhed handler om at få samfundet som helhed til at skifte gear, således at flertallet af borgere og virksomheder, når det gælder computere, går fra ”maskintænkning” til ”netværkstænkning”. Vi står over for en meget stor kulturel og oplysningsmæssig udfordring.

Den fremtidige udvikling vil i meget høj grad afhænge af, hvorvidt store dele af befolkningen og virksomhederne føler sig trygge ved den nye teknologi. I det omfang utryghed kommer til at dominere, vil det sinke eller hindre udbredelsen af nye mere

>

effektive systemer både i erhvervslivet og hos det offentlige. Det vil i de kommende år blive tydeligt for alle, ikke kun for pionererne, hvordan mennesker, virksomheder, organisationer og myndigheder for alvor begynder at hænge sammen via elektroniske netværk. Det gælder, hvad enten vi taler om let og hurtig adgang til serviceydelser, eller sikkerhedsproblemer hvor en borgers ubeskyttede computer er med til at angribe hans egen kommune eller måske en virksomhed i Hongkong og et universitet i Argentina.

Når det gælder konkrete initiativer, vil rådet gerne have leverandører af software- og/eller hardware-systemer til at intensivere deres indsats for at forbedre sikkerheden, både i forbindelse med forebyggelse og ved indgreb når en aktuel trussel bliver opdaget. Vi er nået et stykke med internetleverandørernes frivillige spam- og virusfiltrering, ligesom softwareleverandører har øget tilbuddene om gratis og (halv-)automatisk opdatering af software for at fjerne sårbarheder.

Rådet forventer, at der vil blive behov for flere tilsvarende initiativer baseret på frivillige brancheløsninger. Rådet har i sit arbejde haft den principielle holdning, at it-sikkerhedsløsninger skal være baseret på fuld åbenhed, herunder at brugeren bevarer en mulighed for aktivt at fravælge muligheder for filtrering, opdatering osv.
I forhold til de generelle vilkår vedrørende it-sikkerhed, ser rådet følgende arbejdspunkter:

> For at styrke Danmarks it-sikkerhedsmæssige kompetencer generelt bør det it-sikkerhedsmæssige kompetenceniveau i de korte, mellemlange og lange videregående uddannelser hæves. Rådet mener herudover, at arbejdet med at etablere en Masteruddannelse på it-sikkerhedsområdet bør fremmes.

> Rådet mener, at brancheorganisationerne bør være kampagneførende over for egne medlemsvirksomheder – og dette ansvar synes de større brancheorganisationer efterhånden også at have taget på sig i 2004. Det er dog rådets vurde-

>

ring, at enkeltbrancher bør træde betydeligt mere i karakter med it-sikkerhedskampagner.

> Det er rådets opfattelse, at it-sikkerhed bør indgå som en eksplicit del af begrebet "Corporate Governance". Ved at nå virksomhederne og deres medarbejdere kan man samtidig opnå en afsmittende effekt over for borgerne, fordi medarbejderne vil kunne tage de gode vaner med hjem fra arbejde. Rådet har derfor rettet henvendelse til Nørby-udvalget herom.

Udover det allerede nævnte, ser rådet følgende mere konkrete indsatsområder vedrørende it-sikkerhed i Danmark:

> Rådet vil gerne i samarbejde med revisorbranchen fokusere på, om branchens kunder er tilstrækkeligt opmærksomme på betydningen af it-sikkerhed.

> Kommunalreformen vil uden tvivl sætte yderligere gang i udviklingen af digital forvaltning og elektroniske tjenesteydelser. I den forbindelse er det af betydning, at aktørerne i den offentlige sektor udvikler ensartede og høje sikkerhedskrav, således at brugerne – dvs. den enkelte borger og virksomhed – kan have tillid til og føle sig tryg ved de nye systemer.

> Rådet er bekymret over den stigende it-kriminalitet. Rådet finder det relevant, at de berørte myndigheder i fællesskab overvejer, hvordan stigende it-kriminalitet kan imødegås, og om en strategi eventuelt kunne være at etablere en særlig statsadvokatur for it-kriminalitet (som "Bagmandspolitiet").

> Rådet mener, at den digitale signatur skal videreudvikles hen mod et egentligt chipkort eller lignende til alle borgere. Kortet bør kunne bruges af ejeren over alt i det danske samfund.

> Rådet mener, at arbejdet med at kortlægge samfundets sårbarhed over for nedbrud af it-systemer skal fortsætte. Rådet vurderer, at der er behov for øget afklaring af sårbarheden i samfundet uden for de sædvanlige beredskabssektorer samt på tværs af sektorer (f.eks. imellem de forskellige sektorer i en værdikæde).

> Der bør arbejdes for W3C-certificering af offentlige hjemmesider[2].

**Det kan der gøres på internationalt plan**
International koordinering af it-sikkerhedsarbejdet er i dag sparsom. De fleste lande har arbejdet med disse spørgsmål hver for sig. Først nu er der på europæisk plan etableret et Agentur for Net- og Informationssikkerhed, ENISA, der åbner i Grækenland i 2005. Internationalt samarbejde om emnet vanskeliggøres af, at it-sikkerhed organisatorisk er placeret forskellige steder fra land til land, f.eks. indenrigsministerier, politimyndigheder, finansministerier og i Danmark bl.a. i Videnskabsministeriets IT- og Telestyrelse.

Danmark bør arbejde for at få såvel EU som FN og OECD til at tage en række emner op, der kan være med til at imødegå eller mindske it-sikkerhedstrusler. Rådet vurderer, at det vil være af betydning for Danmark, at der bliver bragt internationalt fokus på følgende områder:

> Etablering af en EU-norm med krav om at it-produkter som udgangspunkt har aktiveret indbyggede sikkerhedselementer, når de installeres eller tages i anvendelse af brugeren. Derved sikres det, at sikkerhedselementer er slået til og aktiveret, medmindre brugeren aktivt har fravalgt it-sikkerheden i produktet. I dag er det typisk omvendt – it-sikkerheden skal vælges til.

> Styrkelse af det internationale samarbejde om efterforskning af grænseoverskridende it-kriminalitet, både på EU-plan og på internationalt plan.



2 Hvis hjemmesider overholder W3C-retningslinier, vil de kunne læses af mange forskellige browsere, og dermed vil brugerne have mulighed for at vælge deres foretrukne browser, f.eks. den, der p.t. har færrest it-sikkerhedsproblemer.

>

- Hurtig etablering af effektive mekanismer for at benytte certifikater på tværs af landegrænser. Rådet vurderer, at certifikater (som det danske OCES digitale signatur-certifikat) får stigende betydning for etableringen af sikker kommunikation og bestræbelserne på at sikre åbne it-miljøer – og dermed muligheden for effektivt at blokere for it-kriminalitet. Udbredelsen af certifikater er imidlertid helt afhængig af, at de nationale grænser ikke bliver en barriere.

- Der bør arbejdes for, at enhver form for distribution af software eller andre elementer, der kan påvirke it-miljøet, er ledsaget af et afsendercertifikat. Herved kan risikoen for at modtage og aktivere utilsigtede elementer (virus, orme, spy-ware osv.) begrænses, idet certifikatet kan forhindre, at afsender er anonym eller giver sig ud for at være en anden.

- Der bør arbejdes for at fremme udarbejdelsen og anvendelsen af åbne standarder, der kan øge it-sikkerheden.

- Indsatsen for at styrke it-sikkerhed på mobilområdet bør øges, bl.a. for at imødegå mobil-hacking. En effektiv indsats kræver øget forskning og produktudvikling på internationalt niveau.

- Rådet mener, at der generelt er brug for øget fokus på, hvem der har ansvaret for it-sikkerheden. I den forbindelse kan der evt. gennemføres en international høring om hvilke krav, der kan stilles til virksomhedernes ansvar for it-sikkerheden.

>

# Er der stadig behov for uafhængig it-sikkerhedsrådgivning af regeringen? >

Rådet for it-sikkerhed går nu ind i sit tredje og indtil videre sidste år. Dette har givet rådet anledning til at overveje, om det fremover vil være hensigtsmæssigt, at der findes et eksternt råd, der rådgiver videnskabsministeren og dermed regeringen om it-sikkerhedsspørgsmål, og i givet fald hvilke rammer et sådant eksternt råd bør have.

Udgangspunktet for rådets etablering var, at videnskabsministeren og dermed regeringen havde en formodning om, at der på et så teknisk kompliceret og vanskeligt tilgængeligt område var behov for en uafhængig rådgivning, Det var også et mål, at rådet gennem sit virke kunne bidrage markant til udviklingen af en it-sikkerhedskultur, sådan som Danmark har tilkendegivet at ville i henhold til sin tilslutning til vedtagelser i OECD og EU.

Er behovet stadig det samme efter mere end otte år med det nuværende og tidligere it-sikkerhedsråd? Er udviklingen i den offentlige sektor og i virksomhederne nået til et punkt, hvor it-sikkerheden er en anerkendt og integreret del af it-tænkningen – og dermed også af it-tænkningen på samfundsmæssigt plan?

Ser man på det offentlige system er it-sikkerhed blevet en integreret del af mange forskellige myndigheders arbejdsfelter: Politiet, Forsvaret, Finanstilsynet, Økonomistyrelsen, Datatilsynet – bare for at nævne enkelte eksempler. Hver af disse myndigheder forholder sig aktivt til it-sikkerhed med udgangspunkt i deres kerneforvaltningsopgaver.

Videnskabsministeriet har i denne sammenhæng ansvaret for regeringens it-politik, herunder den overordnede og civile it-sikkerhedspolitik, og det er i denne sammenhæng, at Rådet for it-sikkerhed har fungeret og udøvet sin rådgivningsvirksomhed. I kraft af sin placering har rådet haft sit afsæt i de sager og it-sikkerhedsspørgsmål, som hører ind under Videnskabsministeriet ved IT- og Telestyrelsen. Rådet har i tæt samspil med IT- og Telestyrelsen arbejdet for at sikre, at de nødvendige spørgsmål blev rejst og belyst. Videnskabsministeriet har givet it-sikkerhe-

>

den særlig opmærksomhed gennem etableringen af et fagligt kontor i IT- og Telestyrelsen.

Rådet har haft et højt ambitionsniveau vedrørende it-sikkerhed generelt i det danske samfund. Disse ambitioner har ikke i tilstrækkelig grad kunnet komme til udtryk gennem vedvarende og markante tiltag. Dertil har de ressourcer, som rådet har fået tildelt, ikke været tilstrækkelige.

Rådet vurderer, at der fortsat er en række væsentlige udækkede behov og muligheder i forhold til it-sikkerhed i Danmark, og at der derfor fortsat er brug for en uafhængig rådgivningsfunktion:

> De forskellige forvaltningsmyndigheder, der i dag har it-sikkerhed som en del af deres myndighedsressort, har det alene i relation til de specifikke sektorer, som myndighederne arbejder med. Det gælder f.eks. Finanstilsynet, PET og FE og Datatilsynet. Der er ikke nogen anden offentlig aktør, der har fokus på den brede civilrettede og tværgående it-sikkerhed og dens samspil med den generelle samfundsudvikling, sådan som et uafhængigt råd for it-sikkerhed kan have det.

> Politisk kan der være en efterspørgsel efter en fagligt kompetent og uafhængig rådgivning i forhold til nuværende og kommende it-sikkerhedsproblematikker, som ikke naturligt bliver opfanget af eksisterende offentlige organer. Et uafhængigt råd kan være med til at sikre, at problemer af denne art kommer i fokus i tide, så den nødvendige politiske opfølgning sikres.

Forudsætningerne for at en evt. kommende uafhængig rådgivningsfunktion kan bringes til at fungere optimalt er følgende:

> Rådgivningsfunktionen bør sikres reel uafhængig, således at den f.eks. kan tage initiativer på egen hånd. Der bør afsættes tilstrækkeligt med ressourcer til at kunne gennemføre sådanne initiativer, herunder egne undersøgelser og

analyser. Dermed vil det være muligt at basere rådgivningen på et mere solidt analysegrundlag, end det har været muligt med de begrænsede ressourcer, som Rådet for it-sikkerhed har haft i dets hidtidige virke. Sekretariatsbetjeningen af en uafhængig rådgivningsfunktion bør på tilsvarende vis sikres uafhængighed, således at sekretariatet kan arbejde fuldt og helt for rådgivningsfunktionen.

> En uafhængig rådgivningsfunktion bør sikres reel mulighed for at gå på tværs af sektorområder, således at it-sikkerhedsspørgsmål kan tages op, hvor de end måtte opstå inden for et bestemt sektorområde eller i samspillet mellem forskellige sektorområder.

> Rådet for it-sikkerhed har i sit arbejde varetaget en rådgivningsfunktion. Rådet har også udført en oplysnings- og kampagnefunktion i forhold til befolkningen og erhvervslivet, men uden at det har fået tildelt særskilte midler til dette. Rådet anbefaler, at der til kampagner fremover bør bevilges midler i et omfang, som gør det muligt at opnå større gennemslagskraft, for eksempel via tv-annoncering. Hvis et fremtidigt råd skal have sit primære fokus på den rådgivende funktion, kan det udførende arbejde vedrørende kampagner varetages af for eksempel Videnskabsministeriets it-sikkerhedskontor.