Årsberetning 2005

RÅDET FOR IT-SIKKERHED

Udgivet af:

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

Telefon: 35 45 03 64
Telefax: 35 45 00 14
e-mail rfits@rfits.dk
www.rftis.dk

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

Omslag: Gitte Blå Design
Opsætning og tryk: Schultz Grafisk

Trykt ISBN: 87-91227-69-0
Digital ISBN: 87-91227-71-2

>

Årsberetning 2005

Rådet for it-sikkerhed

>

Indhold >

>

1. Alle skal kunne håndtere it-sikkerhed >

Tidligere var computere og internet specialisternes og nørdernes domæne. Nu er det blevet alment eje.

Hvornår kører toget? Bestilling af en bog på biblioteket. Tjek lige lægens åbningstid! Hvad går der i biografen i aften? Hov, her er en regning, som skulle have været betalt i går. Alt sammen dagligdags begivenheder, som for en meget stor del af befolkningen naturligt involverer brug af computer og internet.

Alle, som har gennemlevet internettets gennembrud de sidste 10 år, har været del af en vedvarende læreproces. De har fået nye computere og ny software mange gange. Og de har lært at bruge nye tjenester via nettet formodentlig endnu flere gange.

En stor del af denne indlæring har handlet om at lære, hvordan man lærer. Vi har måttet lære selv at håndtere problemer, vælge, vurdere og tage ansvar eller bede om hjælp, når vi fra vores trygge base i et velfærdssamfund begav os ud i en virtuel verden med tilbud fra både velmenende, kommercielle og kriminelle aktører fra hele kloden.

Sikkerhed har ikke været en drivende kraft i udviklingen. Tværtimod. Internettets entreprenør-drevne og anarkistiske dynamik er blevet båret frem af et internet og en teknologi, hvor sikkerheden grundlæggende har været og til dels stadig er fraværende. Krav om sikkerhed har ikke udgjort nogen barriere for kreativitet, hverken hos iværksættere eller kriminelle. Sikkerhed har heller ikke været højt på dagsordenen hos den enkelte bruger. Umiddelbar tilfredsstillelse af nysgerrighed og behov er kommet i første række.

Der er derfor populært sagt et underskud af sikkerhed, når en typisk internetbruger tænder sin computer. Det største problem er, at de fleste ikke er klar over det. Det ville svare til, at flertallet af trafikanter ikke var opmærksomme på nødvendigheden af, at deres bil kan bremse og styre - og at de ikke holdt øje med risiko for islag.

I virksomheder og hos offentlige myndigheder er udviklingen over de seneste år vendt, således at der nu er et fald i antallet af tabsgivende angreb fra vira og andre sikkerhedstrusler (se afsnit 3). Men i befolkningen som helhed, er der fortsat en generel mangel på viden om, hvor usikkert internettet egentlig er. Vi har faktisk en urimeligt høj "ulykkesfrekvens" for brug af computere og internet.

Der er heldigvis ikke som i trafikken tale om fysiske skader og dødsfald. Men effekten af it-ulykkerne er stor nok endda: mistede ressourcer, mistet tillid, tidsspilde, unødig frustration, økonomiske tab. Kort sagt: mistede muligheder, både individuelt og måske især for det danske samfund som helhed. Både i forhold til livskvalitet, kultur, erhvervsudvikling og international indflydelse.

Målet må være, at alle, som tænder en computer, har en basal viden om it-sikkerhed. De skal ikke kunne løse alle problemer, men de skal vide, at computere og især internettet byder på store - men også usikre - muligheder, netop fordi det grundlæggende har en fri og åben struktur. Brugeren skal hjælpes til at sætte ind, hvor behovet er størst. F.eks. er de færreste klar over, at det er langt mere risikabelt, at opbevare følsomme oplysninger i ukrypteret form på sin computer, end det er at sende dem som ukrypteret e-post. Forklaringen er, at de følsomme oplysninger er umiddelbart tilgængelige for alle, der kan skaffe sig adgang til computeren, mens det er betydeligt mere vanskeligt oprette en "lyttepost", som kan opfange e-post fra en bestemt bruger på nettet.

Brugerne skal have en viden om, hvad man altid bør gøre, og hvad man aldrig bør gøre, så de undgår at skade sig selv og andre. Vi har brug for en it-sikkerhedskultur, på samme måde som vi har brug for en trafiksikkerhedskultur.

Rådet for it-sikkerhed mener, at det er en samfundsmæssig opgave at igangsætte og udbrede denne form for oplysning. Rådet har, i overensstemmelse med sit kommissorium, gjort sit bedste

for at løfte en del af denne opgave med de midler, der har været til rådighed. Rådet må selv åbenhjertigt konstatere, at det ikke har været i stand til at indfri omverdenens forventninger til indsatsen.

Rådet har eksisteret i tre år, og dette er Rådets sidste årsberetning. Rådet blev nedsat af videnskabsminister Helge Sander pr. 1. januar 2003. Dets aktiviteter overtages pr. 1. januar 2006 af IT-Sikkerhedskontoret under IT- og Telestyrelsen, Teknologirådet og et nyt it-sikkerhedspolitisk panel nedsat af Videnskabsministeren.

Det afgående råd har været sammensat som følger:

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

Øvrige medlemmer
Per Buchwaldt, senior manager,
Deloitte Business Consulting A/S
Martin von Haller Grønbæk, partner, Advokatfirmaet Bender von Haller Dragsted
Birgit Hansen, udviklingschef, Scan-Jour A/S
Carsten Heilbuth, partner, KPMG
Adser Leick, global it-sikkerhedschef, LEGO Koncernen
Estrid Oxlund, kommunaldirektør, Holstebro Kommune

>

2. Sådan går det med it-sikkerheden i Danmark >

I løbet af 2005 har der været en jævnt fremadskridende udvikling af nye trusler mod it-sikkerheden:

> Vira, orme og spam har gennemløbet en jævn evolution. Der har været en tydelig acceleration af hastigheden, hvormed hackere og spammere udnytter nyopdagede sårbarheder. Det medfører behov for hurtigere rytme i sikkerhedsopdateringerne hos private, virksomheder og myndigheder. Tidligere gav ugentlige opdateringer af antivirus-definitioner en rimelig god sikkerhed. Nu bør det ske automatiseret med få dages mellemrum eller dagligt.
> Koblingen mellem virus og spam er blevet tydeligere. Det er nu en klar og betydende tendens, at spam distribueres via netværk af computere, som er inficeret via vira, orme m.m.
> Spyware og adware har i årets løb udviklet sig betydeligt og er nu et væsentligt sikkerhedsproblem, som alle brugere af internettet bør have viden om[1].
> Brugen af instant messaging er tiltagende. Da kommunikation via instant messaging foregår hurtigere end ved e-post, er hastigheden, hvormed sikkerhedsproblemer spreder sig, også tilsvarende større.

Blandt de problemer, der i 2006 og frem kan forventes at få større betydning, er:

> Vira, orme og spam på mobile platforme. Første tilfælde i Danmark blev konstateret i efteråret 2005.
> Phishing har i efteråret 2005 for første gang ramt svenske kunder i en stor nordisk bank. Phishing er forsøg på at lokke f.eks. en banks kunder til at opgive fortrolige oplysninger, herunder numre på bankkonti, betalingskort og pin-koder. Phishing har fået en vis omtale i danske medier i 2005, og det må forventes at dukke op i dansk sammenhæng i 2006.

Trusler mod it-sikkerheden er kendetegnet ved at have en hurtig spredningshastighed og ved, at de generelt går efter at udnytte de svagest beskyttede punkter på internettet. Generelt vurderer Rådet for it-sikkerhed, at der ville kunne opnås større effekt af

1 I tredje kvartal 2005 var 72 pct. af amerikanske private pc'ere inficeret med spyware. Det er et fald i forhold til året før, hvor 92 pct. var inficeret. Kilde: State of spyware report Q3 2005, www.webroot.com. Danske tal kendes ikke.

indsatsen for at forbedre it-sikkerheden, hvis der var større samordning og koordinering mellem de forskellige aktører, som er aktive på området. Det gælder både praktiske løsninger på sikkerhedsproblemer blandt internetudbyderne, i forhold til lovgivning, uddannelse, standardisering og kampagner og i det internationale samarbejde mellem myndigheder. Grundlaget for denne type samarbejde må efter Rådets mening være baseret på forståelsen af it-trusler og it-sikkerhed som massefænomener og komplekse størrelser, der kan påvirkes i fællesskab, men ikke direkte kontrolleres eller styres af enkelte instanser.

Danske internetudbydere har allerede på en række punkter etableret sådanne former for samarbejde (se afsnit 4). Rådet for it-sikkerhed hilser denne udvikling velkommen.

3. Borgerne og it-sikkerheden >

Opgørelser fra Danmarks Statistik viser udviklingen i antallet af brugere, der er udsat for virusangreb, som medfører tab af data eller arbejdstid.[2] :

Virusangreb med tab af data eller tid hos borgere, virksomheder og i den offentlige sektor			
	Borgere	Virksomheder	Offentlige sektor
2002	-	46 pct.	59 pct.
2003	29 pct.	32 pct.	58 pct.
2004	31 pct.	24 pct.	43 pct.
2005	35 pct.	-	-

Kilde: Danmarks Statistik. Befolkningens brug af internet, Danske virksomheders brug af it, Den offentlige sektors brug af it. For virksomheder og offentlige myndigheder er de omfattede virusangreb karakteriseret som "generende" eller "alvorlige". Forskel mellem virksomheder og offentlige sektor er forbundet med organisationernes størrelse.

En stigende andel af de borgere, der benytter internet, oplever tab af information eller tid som følge af virusangreb - og dermed sandsynligvis også øvrige sikkerhedstrusler, idet "virus" i folkemunde bruges om sikkerhedsproblemer i bred betydning. Da der i samme årrække har været en kraftig stigning i antallet af borgere, som har pc med internetadgang, betyder det, at den faktiske stigning i tabsgivende angreb er større end procenttallene umiddelbart indikerer.

Stigningen i antallet af tabsgivende virusangreb blandt borgere står i kontrast til udviklingen i virksomheder og i den offentlige sektor (se tabellen). Her er procentdelen, der oplever tabsgivende virusangreb, større end hos borgere, men tendensen i udviklingen er nu vendt. Blandt virksomheder har der fra 2002 til 2004 været et markant fald i procentdelen, der har oplevet skadesvoldende angreb, og hos offentlige virksomheder har der fra 2003 til 2004 været et tilsvarende markant fald.

Dette kan tages som udtryk for, at virksomheder og myndigheder over de sidste par år er begyndt at få etableret en generel forståelse for nødvendigheden af it-sikkerhed, mens denne erkendelse endnu ikke har indfundet sig i befolkningen som helhed.

2 Nølgetal om informationssamfundet - Danmark 2005 (s.45). http://www.vtu.dk/fsk/div/presse/2005/danske_tal_01_62.pdf

De høje tal for virusangreb med tab til følge kan umiddelbart undre, idet både borgere, virksomheder og myndigheder oplyser høje tal for brugen af sikkerhedsprodukter. Blandt borgerne er det, iflg. 2005-tallene fra Danmarks Statistik, 93 pct. af dem, som har adgang til internet, der har antivirusprogram. 70 pct. oplyser, at de har firewall. 80 pct. oplyser, at antivirus/firewall er opdateret inden for den sidste måned. Set under ét er det 77 pct. af dem, som har pc eller internet derhjemme, som bruger sikkerhedsprodukter. Men set i forhold til 2004, hvor tallet var 83 pct., er andelen faldet. Igen kan denne udvikling hænge sammen med den fortsatte stigning i udbredelsen af pc og internetforbindelse. Måske det forholder sig således, at færre af de nye brugere har kendskab til it-sikkerhed.

Samlet set kan det konkluderes, at der er betydelige problemer med it-sikkerheden i de danske hjem, og at der fortsat er en stigning i antallet af tabsgivende angreb. I maj-juni 2005 fik Rådet for it-sikkerhed gennemført en måling for at få en mere detaljeret viden på dette område. Analysen blev udført via telefoninterviews af analysevirksomheden Epinion.

Målingen viste, at et stort flertal af dem, som har egen pc (74 pct.), selv mener, at de har nogenlunde eller godt styr på it-sikkerheden inden for basale forhold som brug af antivirusprogrammer, firewall og sikre kodeord[3]. Men når man spørger til pc-brugernes viden om de nyeste sikkerhedstrusler og deres viden om, hvordan man genkender sikkerhedstrusler i forbindelse med e-post og usikre netsteder, så har 63 pct., baseret på deres egen vurdering, en utilstrækkelig sikkerhed.

Der er dermed i befolkningen som helhed en betydelig forskel på oplevet sikkerhed og faktisk sikkerhed. Brugerne tror, at de har sikret deres computer tilstrækkeligt, uden at det er tilfældet. Mange brugere har installeret antivirus og firewall, men er ikke bekendt med, hvordan man generelt genkender og herved undgår sikkerhedsproblemer på internettet.

3 http://www.rfits.dk/Daarling it-sikkerhed.3368.0.html

En nærmere analyse viser, at der blandt pc-brugerne i befolkningen er en række svage grupper, hvor både kendskab, forståelse og efterlevelse af it-sikkerhed ligger på et lavere niveau:

- Kvinder har stort set samme erfaring med it som mænd fra arbejde eller studier, men de anvender ikke nær så hyppigt it i hjemmet. De har generelt lavere kendskab til it-sikkerhed, og de søger hyppigere hjælp til at løse sikkerhedsproblemer end mænd. Kvinderne har især lavere opmærksomhed omkring it-sikkerhed i forhold til brug af netsteder og trådløs internetadgang.
- Personer over 60 år er mindre aktive brugere af it i hjemmet end andre. De har i stort omfang erfaring med it fra arbejdet, men de er ikke nær så opmærksomme på it-sikkerhed som yngre aldersgrupper. De ældre har især lavere opmærksomhed omkring it-sikkerhed i forhold til brug af netsteder og trådløs internetadgang.
- Personer under 30 år bruger mindre it i hjemmet og har mindre styr på it-sikkerhed end dem over 30 år, dog er de yngste i gruppen (under 20 år) mere opmærksomme på it-sikkerhed end de ældste.
- De lavere uddannede (afsluttet uddannelse under gymnasieniveau) har markant mindre opmærksomhed på it-sikkerhed end gruppen med studentereksamen eller højere uddannelse.
- De, der ikke arbejder med it på arbejde eller i studiesammenhæng, har ligeledes markant lavere opmærksomhed på it-sikkerhed. Det kan hænge sammen med, at gruppen omfatter en del ældre personer og en del personer, som har afsluttet deres uddannelse under gymnasieniveau.

Undersøgelsen af befolkningens holdninger viser overordnet, at der er stort behov for yderligere viden om og forståelse for betydningen af it-sikkerhed. Den viser også, at it-sikkerhedskulturen varierer betydeligt i befolkningen, og at en række grupper står særlig svagt.

Initiativer, som kan adressere de svage grupper, der i kraft af deres usikre computere og usikre adfærd påvirker alle, kan f.eks. være:

> Tilbud om pc-kørekort, hvori der indgår undervisning i it-sikkerhed.
> Øget oplysning i forbindelse med brugen af PC-bank, så brugerne bliver klar over at it-sikkerhed handler om andet og mere end kodeordsbeskyttelse.
> Øget fokus på it-sikkerhed i studie- og erhvervsmæssige sammenhænge.
> Øget fokus på it-sikkerhed i folkeskolen og på øvrige uddannelser.
> Større indsats i forhold til generelle og letforståelige informationskampagner med brug af kommunikationskanaler med stor gennemslagskraft.
> Øget fokus på it-sikkerhed fra internetudbydernes side.

Mangel på statistiske oplysninger
Meget af den hidtidige statistik vedrørende it-sikkerhed i Danmark giver ikke et reelt grundlag for at beskrive udviklingen på området. Ganske vist er der blevet stillet de samme spørgsmål år for år, men mange af de stillede spørgsmål har været udformet, så de i løbet af få år er blevet "teknologisk forældede". For eksempel var det for 4-5 år siden meningsfuldt at spørge, om et sikkerhedsprodukt var blevet opdateret inden for de sidste tre måneder. I dag indeholder svaret på dette spørgsmål ikke længere nogen reel indikation af sikkerhedsniveauet, idet opdateringer for at have effekt nu skal ske ugentligt eller dagligt og helst automatisk. Et andet eksempel er, at nye sikkerhedstrusler er længe om at blive inkluderet i de statistiske undersøgelser. For eksempel er den kraftige vækst i spyware endnu ikke blevet opfanget i officiel dansk statistik.

Rådet for it-sikkerhed var fra 2003 i dialog med Danmarks Statistik om disse problemer uden at finde en løsning. Danmarks Statistik har fastholdt behovet for at stille samme spørgsmål mange år i træk, da dette giver et nationalt og internationalt sammenligningsgrundlag.

I 2005 valgte Rådet derfor at iværksætte sin egen undersøgelse baseret på KFE-metoden, som er udviklet af analysevirksomheden Parkegaard og Kristensen Sikkerhed. (K=kendskab, F=forståelse, E=efterlevelse). Analysemetoden blev valgt, da den er velegnet til at undersøge en kultur, i dette tilfælde it-sikkerhedskulturen i Danmark, som er under stadig udvikling.

Undersøgelsen er designet, så den måler den enkelte brugers egenvurdering af kendskab /forståelse /efterlevelse op imod en antaget optimal viden og adfærd, som den f.eks. udtrykkes i gældende anbefalinger om god it-sikkerhed[4]. Undersøgelsesmetoden er på en række forskellige områder i stand til at følge "et mål i bevægelse" og giver samtidig detaljeret information om forskellige befolkningsgruppers egen oplevelse af it-sikkerhed.

Behov for skærpet informationsindsats

I sit treårige virke har Rådet for it-sikkerhed benyttet trykte og elektroniske pjecer samt udsendelse af pressemeddelelser som sine primære informationskanaler til offentligheden. Der er i perioden distribueret mere end 86.000 trykte pjecer og mere end 76.000 elektroniske udgaver af disse publikationer (se bilag 3). Rådets medlemmer har endvidere stillet sig til rådighed for interviews og medvirket i elektroniske mediers dækning af spørgsmål vedrørende it-sikkerhed.

Disse distributionskanaler er valgt ud fra en vurdering af emnernes karakter og de ressourcer Rådet har haft til rådighed samt ud fra en vurdering af målgruppen for Rådets informationsindsats i 2003. I takt med at Rådets publikationer er gjort tilgængelige via www.rfits.dk, har en del andre netsteder, både offentlige og private, linket til de elektroniske udgaver af Rådets pjecer. Rådet har i 2005 medvirket til at skabe bedre krydshenvisninger mellem forskellige offentlige netsteder med fokus på it-sikkerhed. De offentlige netsteder, der oplyser om it-sikkerhed, herunder www.it-borger.dk og www.netsikkernu.dk optræder samlet set med relativt gode placeringer på søgemaskiner ved søgning på f.eks. "it-sikkerhed".

[4] Bilag 4, "Gode råd om it-sikkerhed" er et eksempel på sådanne anbefalinger.

Rådet vurderer, at der fremover er behov for en betydeligt mere offensiv og dermed også ressourcekrævende informationsindsats i forhold til offentligheden. I løbet af de sidste 3-5 år er computere blevet hvermandseje, og it-sikkerhed er nu relevant for størstedelen af befolkningen. Det betyder, at der fremover skal kommunikeres på flere forskellige niveauer, og at den vigtigste kommunikation skal bringes ud i meget enkel og letforståelig form med den almindelige pc- og internetbruger som den typiske modtager.

Et godt udgangspunkt for en sådan enkel og letforståelig kommunikation er, at alle betydende aktører bliver enige om at arbejde sammen og koordinere deres kommunikationsindsats.

Som et første lille skridt i den retning har Rådet for it-sikkerhed i 2005 taget initiativ til at skabe en konsensusversion af "gode råd om it-sikkerhed". Hidtil har forskellige kampagneførende organisationer, myndigheder og private aktører haft en hel række forskellige versioner af "gode råd" om it-sikkerhed. Rådet har vurderet, at en konsensus-version af disse gode råd vil kunne give et godt udgangspunkt for en fremtidig styrket kommunikation i forhold til befolkningen. Alle aktører, som Rådet har spurgt, har udtrykt deres klare støtte til initiativet, og de har medvirket aktivt til at skabe den nu foreliggende konsensus-version (se bilag 1).

Rådet for it-sikkerhed har sideløbende udarbejdet "Gode råd om brug af digital signatur" (se bilag 2).

Rådet anbefaler, at kommende offentlige aktører på området for it-sikkerhed (IT- og Telestyrelsen m.fl.) tager ejerskab til en fortsat konsensusproces omkring "gode råd" og anden generel information om it-sikkerhed. Det centrale indhold, som kampagneførende organisationer har behov for, vil på den måde kunne udarbejdes med brug af færre ressourcer, og samtidig vil det kunne give synergi-effekter, at mange kommunikerer samme budskaber. Materiale udarbejdet i en fortløbende konsensusproces vil kunne annonceres aktivt og stilles frit til rådighed for alle, der ønsker at benytte det.

2005 var første år for netsikker-nu!-kampagnen, der gentages i 2006. Rådet for it-sikkerhed anser kampagnen for vigtig, fordi den giver mulighed for at koordinere mange forskellige aktørers indsats i forhold til it-sikkerhed. Rådet bidrog til kampagnen i 2005 gennem en løbende dialog med Videnskabsministeriet og ved deltagelse i enkelte af kampagnens aktiviteter.

Rådet har over for Videnskabsministeriet udtrykt sin bekymring i forhold til den valgte organiseringsform, hvor private aktørers interesse i at medvirke er tæt forbundet med deres interesse i at øge salget af egne produkter og ydelser. I lignende fremtidige kampagner anbefaler Rådet en form for organisering, som i højere grad fremmer og fokuserer på initiativer, der er frigjort af snævre partsinteresser. Et eksempel til inspiration kunne være Rådet for Større Færdselssikkerhed, som har formået både at fastholde en dagsorden, som er fri af særinteresser, og samtidig har vist, hvordan private virksomheder kan indgå i sponsoraktiviteter med navns nævnelse uden direkte at promovere egne produkter/ydelser.

Medierne og it-sikkerhed

Når det gælder kommunikation til befolkningen om it-sikkerhed har medierne en central rolle. Mange medier udviser stor interesse for it-sikkerhed på relativt højt fagligt niveau. De har stor gennemslagskraft, og deres nyhedsdækning af f.eks. virusudbrud fungerer uden tvivl som "vågn-op"-beskeder til borgere, virksomheder og myndigheder, som endnu ikke har beskyttet sig tilstrækkeligt.

Blandt især de brede medier er der en tendens til at give aktuelle sikkerhedstrusler en stor eksponering uden samtidig at være præcis med, hvem der risikerer at blive ramt under hvilke omstændigheder. Dette kan være et problem. Mange borgere vil således høre de bredt formulerede advarsler, samtidig med at de selv oplever ikke at blive ramt. Det kan medvirke til at skabe en ulven-kommer-effekt, som kan gøre det svært at få offentligheden i tale. Overdrevne advarsler kan også være unødigt skræmmende for befolkningsgrupper, som endnu ikke har taget computere og internet til sig.

Ofte udvikler en ulven-kommer-historie sig gradvist. Starten kan være en præcis og faktuelt korrekt beskrivelse af et nyopdaget sikkerhedsproblem i et fagmedie. Når historien videre-bringes af andre medier, kortes den ned, og detaljerne bliver færre, samtidig med at overskriften og vinklen måske skærpes. Det sker også, at dækningen af it-sikkerhed bliver upræcis, fordi den på de brede medier varetages af journalister uden faglig viden om it og it-sikkerhed. Der er endvidere en tendens til, at sikkerhedsproblemer, som rammer medierne selv, får større dækning end de berettiger til ud fra en almen betragtning. En sidste faktor, som bidrager til en ulven-kommer-effekt, er skarpt vinklede pressemeddelelser fra kommercielle aktører, som søger at skabe maksimal eksponering af deres virksomhed i medierne.

For at sætte fokus på disse fænomener udsendte Rådet for it-sikkerhed i juni 2005 et forslag til god skik og brug for medieomtale af it-sikkerhed. Forslaget indeholdt fire korte opfordringer til journalister og redaktører i forbindelse med mediernes omtale af sikkerhedstrusler:

> Fortæl altid, hvem der er berørt, og hvordan de er berørt.
> Fortæl altid, hvordan man som bruger finder ud af, om man er berørt.
> Fortæl altid, hvad man kan gøre, hvis man er berørt.
> Brug så vidt muligt uvildige kilder.

Rådets forslag blev omtalt i en række fagmedier og fremkaldte et bredt spektrum af reaktioner fra journalister og redaktører.

Identitetstyveri
Foranlediget af det første nordiske eksempel på phishing i efteråret 2005 har Rådet for it-sikkerhed vurderet de nuværende risici for, at danske borgere bliver udsat for identitetstyveri via internettet.

Det er Rådets vurdering, at danske borgere generelt er mindre udsatte for elektronisk identitetstyveri i forbindelse med phishing end borgere i mange andre lande. Dette hænger først og

fremmest sammen med, at det danske CPR-system giver en entydig identifikation af alle danske borgere og deres registrerede fysiske adresser, samtidig med at fortrolige adgangsoplysninger til f.eks. bankkonti og digitale signaturer meddeles via brev til den fysiske adresse. Endvidere benytter danske netbanker både kodeord, brugernavn og signaturfil, mens f.eks. amerikanske banker i stort omfang forlader sig alene på brugernavn/password.

Danske borgere er endvidere i kraft af lov om visse betalingsmidler godt beskyttet mod tab i forbindelse med uberettiget brug af deres betalingskort.

Indtil nu har danske mediers omtale af phishing især været baseret på eksempler fra andre lande (især USA), hvor borgerne er mindre godt beskyttet. En række af de problemer, som rapporteres fra udlandet, vil ikke umiddelbart kunne opstå i Danmark. Dette fremgår langt fra altid af de danske mediers dækning af phishing-fænomenet.

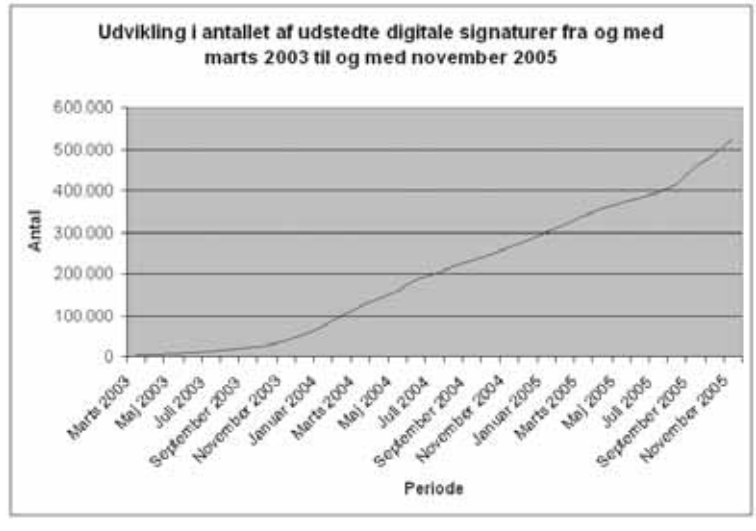
I takt med internettets stigende udbredelse inden for alle former for kommunikation og handel, kan man forestille sig, at der også i Danmark fremover vil blive flere forsøg på identitetstyverier. I dansk sammenhæng vil tyveri af en digital identitet som udgangspunkt forudsætte, at der også stjæles adgangskoder eller pinkoder via indbrud på bopælen eller i postkasser. Rådet anbefaler, at de danske myndigheder holder et vågent øje med, om disse typer kriminalitet bliver mere udbredt, men mener på nuværende tidspunkt ikke, at der er behov for skærpede foranstaltninger eller ændringer i den danske lovgivning.

Der er generelt behov for mere oplysning om, hvad phishing er, og hvordan det foregår, samt hvordan man som borger i Danmark skal forholde sig til fænomenet. Grundlæggende information om emnet findes på Rådets netsted[5].

5 http://www.rfits.dk/Pas_paa_identiteten.3384.0.html

Udvikling i brugen af digital signatur

I løbet af 2005 er der sket en vedvarende og relativt kraftig vækst i antallet af digitale signaturer. I november 2005 var der udstedt mere end en halv million digitale signaturer, hvilket er en fordobling på blot ét år. Antallet er udstedte digitale signaturer steg især kraftigt i august og september 2005, hvilket dels hænger sammen med den fælles offentlige kampagne for digitale selvbetjeningsløsninger, dels at portalen sundhed.dk i september begyndte at tilbyde borgere adgang til at se data om deres egne sygehusbehandlinger.



Kilde: Videnskabsministeriet

Udviklingen viser, at det faktisk er muligt for det offentlige at gå i front for udbredelse af en ny teknologi, som muliggør en generel højnelse af niveauet for sikkerhed blandt borgerne. Rådet finder udviklingen overordentlig positiv.

Der har i 2005 været eksempler på, at det er muligt at opsnappe en brugers kodeord til den digitale signatur ved hjælp en keylogger (trojansk hest)[6]. Disse former for sikkerhedsproblemer skyldes ikke den digitale signatur i sig selv, men generelle sårbarheder på brugernes computere.

6 Se Computerworld 22. juni http://www.computerworld.dk/art/24194?a=block&i=22 og 23. september http://www.computerworld.dk/art/29915?a=block&i=22

4. It-branchen og it-sikkerhed >

Rådet for it-sikkerhed har i sin levetid løbende været i dialog med internetudbyderne omkring forskellige former for selvregulerende initiativer. På en række områder er der nu etableret forskellige former for selvregulering ved hjælp af frivillige adfærdskodeks, samarbejdsaftaler m.m.[7]:

> En række danske internetudbydere (ISP'ere) enedes i august 2005 om et særligt adfærdskodeks, hvor selskaberne på forskellige områder forpligter sig til at gøre en indsats mod spam. Initiativet vil være implementeret senest 1. januar 2006, og er ifølge udbyderne det første af sin art i Europa.
> I maj 2004 vedtog internetudbyderne et første fælles branchekodeks om frivilligt at arbejde på at bremse skadelig trafik på internettet.
> I oktober 2005 har TDC aktiveret et filter, som spærrer for netadresser med børneporno. Filteret er etableret og opdateres i samarbejde med Rigspolitiet og Red Barnet. En række øvrige internetudbydere har taget filteret i brug eller tilkendegivet, at de vil gøre det.

Rådet er yderst tilfreds med, at branchen på denne måde er med til at tage hånd om de aspekter af it-sikkerheden, der vedrører internettet, og betragter det som en succes, at branchen over de sidste par år har iværksat flere forskellige former for selvregulering. 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.

Rådet opfordrer Videnskabsministeriet og regeringen til også i fremtiden at støtte og opmuntre aktører på den danske del af internettet til at etablere forskellige former for selvregulering.

Det er Rådets opfattelse, at selvregulering blandt markedets aktører er et af de stærkeste værktøjer til at sikre hurtige og adækvate reaktioner på nye sikkerhedstrusler. Det hænger sammen

7 Se http://www.isp-sikkerhedsforum.dk/

med, at tidshorisonten på at etablere selvregulering kan tælles i timer, uger eller måneder, mens det som regel tager måneder eller år at gennemføre en offentlig regulering. Rådet opfordrer derfor også til, at der i det kommende it-sikkerhedspanel, som VTU har inviteret brancheorganisationerne til at deltage i, arbejdes aktivt videre med branchens muligheder for selvregulering. Rådet har anbefalet Videnskabsministeren, at det kommende it-sikkerhedspanelet får en udefrakommende uafhængig formand.

Dialog med branchen

Rådet for it-sikkerhed afholdt i 2005 sit andet dialogforum, hvor temaet var it-sikkerhed og fremtiden.
En række indlægsholdere fra it-branchen var inviteret, og i alt deltog mere end 100 personer med tilknytning til it-branchen.
De fremførte synspunkter kan sammenfattes således[8]:

- Der er brug for et uvildigt offentligt råd, som forholder sig til it-sikkerhed.
- Et sådant offentligt råd skal være reelt uafhængigt og kunne agere frit i forhold til alle offentlige myndigheder. Ellers kan det være lige meget.
- Der skal afsættes tilstrækkelige ressourcer i forhold til opgaven, og et råd skal have den rette sammensætning (flere forskellige forslag, herunder at bruge Rådet for Større Færdselssikkerhed som model for et nyt råd).
- Mange forholdt sig kritisk til det nu afgående råd. Et generelt kritikpunkt var, at Rådet ikke har taget tilstrækkeligt mange initiativer og ikke har været synligt nok i offentligheden.
- Mange pegede på, at fokus for arbejdet med it-sikkerhed skal være i forhold til borgerne og de små og mellemstore virksomheder, idet det er her behovet og effekten af en indsats vil være størst.
- Mange af de fremmødte fagfolk udtrykte generel bekymring i forhold til persondatasikkerhed og påpegede den tætte sammenhæng mellem it-sikkerhed og sikkerhed omkring persondata.

8 Detaljeret referat findes her: http://www.rfits.dk/fileadmin/public/Filer/2._Dialogforum/Referat_dialogforum.pdf

Rådet for it-sikkerhed mener, at det er af stor betydning, at der også fremover inviteres til denne type tværgående fora, hvor iagttagelser fra de forskellige dele af it-branchen kan deles, diskuteres og perspektiveres. Initiativer af denne art bidrager til forståelse og større samarbejde omkring de dynamiske processer, som kan være med til at svække og fremme it-sikkerhed i netværkssamfundet.

I 2004 tog Rådet initiativ til møder med leverandører af MPLS-net i Danmark. 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 et netværk. Rådet forholdt sig til, at en række aktører inden for den finansielle sektor havde efterlyst større indsigt i sikkerheden ved brug af MPLS over internettet. Rådet fik via dialog med Cybercity og TDC etableret en fælles forståelse for nødvendigheden af, at sikkerheden ved MPLS-netværk beskrives og findes tilgængelig for de kunder, som har brug for det. Det er endvidere nu muligt for MPLS-kunder hos TDC at få erklæringer vedrørende it-sikkerhed udarbejdet af uafhængige revisorer.[9]

Det skal være nemmere for forbrugerne at "købe sikkerhed"

Generelt er der blandt private brugere af pc og internet et efterslæb i forhold til sikkerhed (se afsnit 3). Efterslæbet kan mindskes, hvis det bliver nemmere for forbrugerne at "købe sikkerhed" på en nem og overskuelig måde. Ideelt set, skulle det - ifølge Rådets opfattelse - som forbruger ikke være muligt at købe en pc eller internetadgang uden samtidig at få tilbudt rådgivning og tilkøb af de nødvendige sikkerhedsløsninger.

Rådet vurderer, at en række kommercielle aktører kunne have fordel af at etablere en mærkningsordning, som signalerer, at computere sælges "inklusive sikkerhed", og at markedskræfter således kunne være med til at højne sikkerhedsniveauet blandt almindelige brugere.

9 Se http://www.rfits.dk/Sikkerhed_i_MPLS-net.3362.0.html

Rådets forslag er, at der etableres en form for mærkningsordning for de butikker, der følger en ”sikker-når-den-tages-i-brug”-politik for salg af computere. Med en mærkningsordning vil de salgspunkter, som ønsker det, kunne dokumentere et vist kvalitetsniveau ift. it-sikkerhed.

Rådet h ar henvendt sig til e-handelsfonden med en opfordring om at tage initiativ til en sådan ”sikker-når-den-tages-i-brug”-mærkningsordning i stil med e-mærket, idet alle de relevante aktører inden for detailhandlen er samlet i e-handelsfondens bagland.

En mærkningsordning af denne type er eksempel på et initiativ, hvor branchen kan være med til at koordinere de markedskræfter, der trækker i retning af øget it-sikkerhed og øget viden blandt borgerne.

Rådet mener også, at det skal være nemmere for forbrugerne at få overblik over, hvilke internetudbydere, der tilbyder virus- og spamfiltre samt andre sikkerhedsydelser. Rådet har derfor opfordret redaktionen af teleprisguide.dk (IT- og Telestyrelsen) til i fremtidige versioner at inkludere oplysninger om netudbyderes sikkerhedsydelser.

Sammenligning af standarder for it-sikkerhed
Virksomheder og myndigheder kan fastlægge it-sikkerhed efter forskellige standarder. Den internationale standard på området er ISO 17799. Den danske standard på området er DS484.

Rådet for it-sikkerhed har igangsat udarbejdelse af en sammenligning af de nyeste versioner af de to standarder. Formålet er at hjælpe virksomheder, som har behov for at dokumentere, at de opfylder både den danske og den internationale standard. Sammenligningen udformes som et dokument på både dansk og engelsk.

Sammenligningen er udarbejdet i fællesskab af KPMG og Devoteam Fischer & Lorenz. Rådet for it-sikkerhed takker de to virksomheder for arbejdet, som er udført uden honorar.

>

Sammenligningen var ikke endeligt afsluttet ved færdiggørelsen af denne årsberetning. Den færdige version af sammenligningen vil blive overdraget til Videnskabsministeriet.

>

5. Det offentlige og it-sikkerheden >

I 2003 udarbejdede Indenrigs- og Sundhedsministeriet "Den nationale sårbarhedsudredning". Som opfølgning på dette arbejde har Videnskabsministeriet ved IT- og Telestyrelsen i 2004-2005 gennemført projektet "Statsligt it- og teleberedskab". Det opfølgende projekt 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.

Det er Rådets opfattelse, at en række aspekter af samfundets sårbarhed i relation til brug af it fortsat ikke er belyst. Rådet anser det for særdeles vigtigt, at også samfundets generelle afhængighed af it-infrastrukturen bliver undersøgt og beskrevet.

Blandt de faktorer, som mangler at blive undersøgt og beskrevet, er effekten af, at stadig flere it-systemer bliver koblet sammen. Brug af internet og andre former for netværk resulterer i øget og tættere datamæssig kobling mellem forskellige systemer samt øget brug af realtids-kommunikation. Konsekvensen er, at indbyggede svagheder i ét system uventet og hurtigere end tidligere kan forplante sig til andre systemer. Risikoen for at dette sker og de mulige konsekvenser og worst-case scenarier er ikke undersøgt.

Rådet for it-sikkerhed har opfordret Videnskabsministeriet til at gennemføre en udvidet sårbarhedsudredning med udgangspunkt i disse betragtninger. Ministeriet meddelte i starten af 2005, at det ikke har ressourcer til at iværksætte en udredning, og at ministeriet heller ikke har ressourcer til blot at iværksætte en projektbeskrivelse af en sådan udredning. Rådet finder den manglende prioritering beklagelig og ser den som udtryk for, at et enkelt ministerium har svært ved at igangsætte nødvendige tværgående initiativer vedrørende it-sikkerhed, når disse berører andre ministeriers ressortområder. Rådets opfattelse er, at effektiv fremme af it-sikkerhed og skabelse af en egentlig it-sikkerhedskultur i det danske samfund kræver vilje og midler til at tænke og handle tværgående.

>

6. Internationalt samarbejde om it-sikkerhed >

EU-kommissionen har etableret Det europæiske agentur for net- og informationssikkerhed (ENISA), og agenturet har i 2005 etableret sig på Kreta.

Rådet for it-sikkerhed mener, at der i øjeblikket sker for lidt i forhold til internationalt samarbejde om it-sikkerhed. Problemet er, at der stort set ikke er noget samarbejde mellem de relevante politisk-administrative enheder i EU-landene, når det gælder it-sikkerhed. Mange initiativer vedrørende it-sikkerhed etableres lokalt, uden at der sker en erfaringsudveksling landene imellem. Det betyder, at mulige synergifordele ikke synliggøres eller udnyttes, og det svækker også de nationale indsatser. It- og it-sikkerhed er grænseoverskridende, og derfor bør der tænkes og handles internationalt i langt højere grad, end det sker i dag.

Danmark har i de kommende år mulighed for at påvirke den internationale udvikling på området, f.eks. ved at delagtiggøre ENISA i de erfaringer, som indhøstes ift. it-sikkerhed og de forskellige former for selvregulering blandt danske internetudbydere. Danmark har også mulighed for at påvirke ENISA i spørgsmålet om digitale signaturer, hvor der er behov for international kompatibilitet. Endvidere er der behov for en forbedring af international sammenlignelig statistik om it-sikkerhed.

>

7. RFID kommer, men vi er ikke parate >

RFID er en ny teknologi, som populært sagt gør stregkoderne trådløse. Det betyder, at man som forbruger f.eks. kan undgå at stå i kø ved kassen i supermarkedet. RFID-teknologien gør det muligt for butikken trådløst at aflæse indholdet af ens indkøbsvogn eller kurv.

Den nye teknologi kan også bruges i en lang række andre sammenhænge. Den udvikler sig i øjeblikket hastigt, og den stiller samfundet over for en lang række nye spørgsmål om hvordan privatlivets fred skal beskyttes.

I udlandet har de første supermarkeder allerede introduceret RFID-teknologien, og den må forventes at komme i brug i Danmark inden for de nærmeste år. Ingen lande har endnu forholdt sig til, i hvilket omfang butikker og andre må aflæse og opbevare oplysninger indsamlet via RFID og lignende trådløs teknologi, og de internationale udredninger på området er fortsat generelle og undersøgende ift. evt. regulering af teknologien.

Rådet for it-sikkerhed afholdt sammen med Datatilsynet i 2004 en velbesøgt høring om RFID-teknologien, fordi den er den form for allestedsnærværende teknologi (også kaldet "it-i-alt", eng.: pervasive computing), der hurtigst kommer til at berøre alle borgere. Dermed får mødet med RFID stor betydning for, med hvilken grad af tillid befolkningen generelt modtager denne næste teknologi-bølge, hvor it og kommunikation bliver tilgængeligt i et utal af produkter.

En af konklusionerne på høringen i 2004 var, at gældende dansk lovgivning, først og fremmest persondataloven, generelt er robust og brugbar i forhold til allestedsnærværende teknologi, herunder RFID. En anden konklusion var, at der udover gældende lovgivning er behov for en form for adfærdskodeks, der beskriver, hvordan den enkelte borger bevarer retten til selv at bestemme over sine identitetsoplysninger. Det skal med andre ord være muligt for en kunde, der går ud af et supermarked, selv at bestemme om andre skal kunne aflæse indholdet i indkøbsposerne - og om oplysningerne skal kunne bruges hjemme i køleskabet til f.eks. at give besked, når mælken bliver for gammel.

Forud for høringen havde Rådet for it-sikkerhed inviteret professor Peter Blume, Københavns universitet, til at udarbejde en råskitse til et sådant adfærdskodeks for brug af RFID for detailhandlen. Forud for høringen var Dansk Industri, Forbrugerrådet og Dansk Handel & Service blevet inviteret til at diskutere forslaget.

Interesseorganisationerne tog imod invitationen og har også efterfølgende arbejdet videre med en konkret udformning af et sådant frivilligt RFID-kodeks. Parterne har i løbet af 2005 ikke kunnet nå til enighed, og Rådet for it-sikkerhed har måttet konstatere, at Dansk Handel & Service ikke synes at være aktive i konsensusprocessen.

Rådet beklager dette. Danmark har på nuværende tidspunkt gode chancer for at præge den internationale dagsorden i forhold til, hvordan de nye teknologier kan introduceres på en måde, som bidrager positivt til udviklingen af samfundet. Rådet opfordrer derfor Videnskabsministeriet og IT- og Telestyrelsen til at fortsætte den igangværende konsensusproces omkring RFID ved at inddrage flere parter, også selv om Dansk Handel & Service ikke ønsker at medvirke. Endvidere anbefaler Rådet, at Datatilsynet og Teknologirådet sætter emnet højt på dagsordenen, da det vil få afgørende indflydelse på it-sikkerheden i fremtiden, både ift. it-infrastrukturen og ift. beskyttelse af persondata. Aktører, som har mulighed for det, bør overveje at inddrage ENISA, da emnet i høj grad har internationale perspektiver.

Rådet for it-sikkerhed fik på basis af høringen i 2004 udarbejdet en rapport, som belyser de juridiske, teknologiske og sikkerhedsmæssige problemstillinger. Rapporten er i engelsk udgave sendt til diverse internationale aktører, herunder ENISA, i forsøg på at gøre dens anbefalinger og analyseresultater bredt tilgængelige[10].

10 For detaljer, se Rådets årsberetning for 2004, side 25.

8. Fremtidigt arbejde med it-sikkerhed >

Rådet ser med nogen bekymring på den fremtidige udvikling vedrørende it-sikkerhed, både i Danmark og internationalt. Den generelle it-udvikling aktiverer meget store kræfter, både i forhold til teknologi og økonomi. I forhold hertil er der relativt svage kræfter, som forholder sig til it-sikkerhed og borgernes tryghed ved de nye former for teknologi. Denne situation kan resultere i uforudsete begivenheder med stor effekt, som vores samfund ikke er forberedt på.

Når det gælder "simpel it-sikkerhed" (beskyttelse af enkeltpunkter i nettet vha. opdateringer, antivirus, antispam og antispyware) ser det ud til at markedskræfterne og de kommercielle aktører i relativt stort omfang har en direkte interesse i at udvikle løsninger, som skaber øget tryghed og sikkerhed. Dog ser der ud til at være en vis forudsigelighed i, at hver ny teknologisk bølge følges af en stribe sikkerhedsproblemer. Disse problemer accelererer til et vist niveau, hvorefter de bliver "opdaget" af de kommercielle kræfter, som udvikler og tilbyder forskellige løsninger. Der er altså et vedvarende efterslæb, hvor nye områder i en periode har meget lav sikkerhed. Det seneste og aktuelle eksempel af denne type er håndholdte computere (PDA'ere) og mobiltelefoner med datakommunikation, hvor sikkerheden endnu ikke er "indbygget". Det er klart, at innovation vil blive hæmmet, hvis alt fra start underkastes strenge sikkerhedskrav, men Rådet finder, at det ville være hensigtsmæssigt, hvis flere aktører generelt var mere opmærksom på sikkerhedsaspekterne, omkring de produkter og ydelser de udvikler og tilbyder. Rådet mener, at involverede myndigheder og organisationer kan støtte en sådan udvikling i retning af øget opmærksomhed på sikkerhedsproblemer ved at fokusere på innovation og forskning omkring it-sikkerhed.

Når det gælder "kompleks sikkerhed", er der i øjeblikket meget lidt viden og mangel på overblik. Kompleks sikkerhed omfatter de problemer, der kan opstå, ved at mange forskellige it-systemer kobles sammen, herunder også at systemer, der oprindeligt er udviklet til brug i lukkede miljøer åbnes op mod omverdenen via f.eks. de såkaldte web-applikationer. En metode til at øge

sikkerheden i komplekse systemer er at identificere og korrigere de svagheder, som har stor multiplikatoreffekt, og som er systemkritiske. Der er i øjeblikket meget lidt viden om disse forhold i forhold til det danske samfund. Sårbarheder af denne type vil kunne resultere i storskala-nedbrud i forbindelse med f.eks. naturkatastrofer, krig og terrorangreb. Rådets vurdering er, at samfundets parathed på dette område slet ikke står mål med samfundets fortsat stigende afhængighed af it. Som det fremgår (se afsnit 5), har Rådet i 2005 rejst spørgsmålet over for Videnskabsministeriet. Rådet opfordrer til, at det generelt undersøges, hvordan det offentlige kan bidrage til øget fokus på "kompleks sikkerhed".

Hvad der kan gøres nationalt

Rådet opfordrer i denne sin sidste årsberetning alle relevante aktører til at sætte it-sikkerhed højt på dagsordenen og medvirke til, at området holdes fri af særinteresser. Målet må være at vi som samfund betragtet finder et niveau for it-sikkerhed, som på den ene side giver borgerne den fornødne tryghed, og på den anden side støtter og drager nytte af internettets åbne struktur. I denne afvejning bør også indgå hensynet til borgernes krav på sikring af privatlivets fred. Det er Rådets opfattelse, at de initiativer, som Videnskabsministeren har iværksat i forbindelse med kommissoriets udløb, ikke er tilstrækkelige til at sikre et hensigtsmæssigt niveau for it-sikkerhed i det danske samfund. Rådet anser det for uhensigtsmæssigt, at den offentlige indsats vedrørende it-sikkerhed fra 1. januar spredes ud hos tre forskellige instanser.

Rådet anser det for afgørende, at der i fremtiden arbejdes mere målrettet og med brug af flere ressourcer for at skabe en it-sikkerhedskultur i Danmark. Sker dette ikke, er risikoen at en stor del af befolkningen bliver utryg ved it-teknologien, fordi den vil kollidere med rodfæstede danske værdier omkring retten til selvbestemmelse og privatlivets fred. Dette vil sinke eller hindre udbredelsen af nye og mere effektive systemer i erhvervslivet og hos det offentlige. Hertil kommer risikoen for større nedbrud og kompromittering eller tab af data, som vil kunne medføre økonomiske tab for borgere, virksomheder og samfundet som helhed.

I det følgende gives en opsummering af de vigtigste af de initiativer og arbejdspunkter, som er beskrevet i denne årsberetning.

I forhold til et fremtidigt nationalt arbejde vedrørende it-sikkerhed har Rådet følgende anbefalinger til Videnskabsministeriet og andre relevante aktører:

> Der er behov for en kraftigt øget folkeoplysning i forhold til it-sikkerhed. Flertallet af befolkningen har taget pc og internet til sig i dagligdagen, men har fortsat et betydeligt efterslæb i forhold til it-sikkerhed. 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. Bedre it-sikkerhed handler om at få samfundet som helhed til at skifte gear, således at flertallet af borgere og virksomheder går fra "maskintænkning" til "netværkstænkning." Det danske samfund står over for en meget stor kulturel og oplysningsmæssig udfordring, som der endnu ikke for alvor er taget fat på, og som regering og ministerier ikke kan løse alene.
> Det er Rådets mening, at it-produkter, som sælges til forbrugere, som udgangspunkt bør "være sikre", det vil sige, at produktets sikkerhedselementer skal være aktiveret, og at der i forbindelse med salg skal medfølge instruktion og eventuelle tillægsprodukter, som er nødvendige for at opnå tilstrækkelig sikkerhed. På grund af den dynamiske og internationaliserede handel med it-produkter kan noget sådant ikke gennemføres ved regulering. Rådet har (jvf. afsnit 4) opfordret e-handelsfonden til at tage initiativ til en mærkningsordning ("sikker-når-den-pakkes-ud"). Mærket vil kunne opnås af forhandlere, som tilbyder instruktion i, hvordan it-produkter gøres sikre at bruge. Rådet opfordrer IT- og Telestyrelsen til at tage en aktiv rolle i forhold til at få en sådan mærkningsordning etableret.
> Videnskabsministeriet, IT- og Telestyrelsen og Danmarks Statistik opfordres til sammen med DK-CERT og it-branchens organisationer at iværksætte en fast tilbagevendende måling af it-sikkerhedskulturen i Danmark, baseret på en metode sva-

rende til den, som er benyttet i Rådets undersøgelse fra 2005 (se afsnit 3). Rådet vurderer, at der for at kunne tilrettelægge kampagner og fremtidigt informationsmateriale generelt er behov for betydeligt mere viden om holdninger til it-sikkerheden i forskellige dele af den danske befolkning.

> Rådet opfordrer brancheorganisationer til i højere grad at være kampagneførende omkring it-sikkerhed i forhold til sine medlemmer. En række større brancheorganisationer har allerede påtaget sig et sådant ansvar. Det er Rådets opfattelse, at en række enkeltbrancher fortsat bør træde mere i karakter på området. Rådet anbefaler, at IT- og Telestyrelsen fortsætter arbejdet med at etablere konsensus omkring centrale anbefalinger (jvf. Rådets arbejde med at etablere konsensusudgave af "Gode råd om it-sikkerhed", se afsnit 3 og bilag 4) og stiller dette arbejde til rådighed for alle, der ønsker at benytte det.

> Rådet ser med bekymring på den fortsat stigende it-kriminalitet. Statistik på området er mangelfuld, men ud fra de sager, der har været offentligt omtalt, ser det ud som om kriminelle er en hel del foran myndighederne i forhold til at udnytte netværkssamfundets nye muligheder. Rådet henvendte sig i 2004 til Rigspolitiet og pegede på de mulige fordele ved at etablere en særlig statsadvokatur for it-kriminalitet, blandt andet at det ville gøre det nemmere at samle den nødvendige ekspertise inden for området. Rigspolitiet svarede, at forslaget ville indgå i fremtidige overvejelser. Rådet udtrykker sit håb om, at forslaget vil blive inddraget i de aktuelle reformer af politiets organisatoriske struktur.

> Rådet har med tilfredshed bemærket, at der nu er udstedt mere end en halv million digitale signaturer. Rådet anbefaler fortsat, at den danske digitale signatur bliver videreudviklet i retning mod et egentligt chipkort eller lignende til alle borgere, og at løsningen på længere sigt også skal kunne indeholde biometriske sikkerhedsløsninger. Kortet bør kunne bruges af ejeren overalt i det danske samfund. Rådet har bemærket, at den Digitale Taskforce arbejder med forslag om et chipbaseret kort, hvor der gradvist kan indlægges flere funktioner. Rådet støtter dette initiativ.

Hvad der kan gøres internationalt
Den internationale koordinering af arbejdet med it-sikkerhed er fortsat sparsom. Først i 2005 har EU etableret et Agentur for Net- og Informationssikkerhed (ENISA), og der er fortsat sparsom koordinering på området inden for andre internationale organer. 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 IT- og Telestyrelsen under Videnskabsministeriet.

På det internationale område har Danmark på nuværende tidspunkt gode muligheder for at være med til at præge udviklingen. 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. På en lang række områder har it-udviklingen en karakter, som gør, at national regulering ikke er hensigtsmæssig, hvorimod international regulering, f.eks. på EU-niveau, vil have den fornødne gennemslagskraft. Mange af de problemstillinger, der vedrører "kompleks sikkerhed" (se tidligere i dette afsnit), er i høj grad grænseoverskridende og adresseres derfor bedst i en international sammenhæng.

Rådet vurderer, at det vil være af betydning for Danmark, at der bliver bragt internationalt fokus på følgende områder:

> Der bør etableres en EU-norm med krav om, at it-produkter som udgangspunkt har indbyggede sikkerhedsforanstaltninger aktiveret, når de installeres eller tages i brug. Forslaget betyder, at brugeren aktivt skal fravælge tilgængelige sikkerhedsløsninger. I dag er det modsatte typisk tilfældet.
> Danmark bør arbejde for styrkelse af det internationale samarbejde om grænseoverskridende it-kriminalitet, både på EU-plan og på internationalt plan.
> Der er behov for effektive mekanismer til at benytte certifikater som f.eks. det danske OCES-certifikat (digital signatur) på tværs af landegrænser. Rådet vurderer, at brugen af

certifikater har afgørende betydning for etablering af sikker kommunikation og blokering af it-kriminalitet. Danmark har med sine pioner-erfaringer vedrørende digital signatur gode muligheder for at bidrage til den internationale udvikling på området.

> Der bør i international sammenhæng arbejdes for, at enhver form for distribution af software og andet, som påvirker it-miljøet, ledsages af et afsendercertifikat. Det vil forhindre, at afsenderen er anonym eller udgiver sig for at være en anden, hvilket vil kunne begrænse organiseret distribution af virus, orme, spyware og lignende. Rådet har ikke lagt sig fast på, om dette bedst gennemføres i form af adfærdskodeks eller via lovgivning.

> Danmark bør støtte og arbejde for at fremme udarbejdelsen og anvendelsen af åbne standarder, der kan øge it-sikkerheden.

> Indsatsen for at styrke it-sikkerhed i forhold til mobiltelefoner, pda'ere og andre mobile enheder bør øges. Der er behov for øget forskning på området og for at støtte og opmuntre til samarbejde mellem forskere og erhvervsliv i forhold til produktudvikling på internationalt niveau.

> Danmark bør opfordre ENISA til at arbejde videre med en international løsning på problemerne omkring it-sikkerhed og privatlivets fred i forhold til brug af RFID-teknologi.

BILAG 1

Rådets initiativer og anbefalinger 2003-2005 >

Udover generel informationsvirksomhed har Rådet for it-sikkerhed i sin levetid taget en række initiativer og givet en række anbefalinger vedrørende it-sikkerhed. Det følgende skema giver et overblik over de fleste af Rådets aktiviteter.

DIALOG MED	EMNE	RESULTAT
Undervisningsministeriet	It-sikkerhed som del af junior pc-kørekort	
Universiteter og Videnskabsministeren	Forslag om etablering af masteruddannelse inden for it-sikkerhedsområdet, herunder anbefaling til Videnskabsministeren.	Både DTU og Alexandra Instituttet har forsøgt at etablere masteruddannelse i it-sikkerhed, men indtil videre er det ikke lykkedes
Videnskabsministeriet	Anbefaling af dansk høring samt høringssvar vedrørende Common Criteria-standarden (ISO 15408) og Common Criteria Recognition Arrangement (CCRA).	Anbefalinger fulgt. Common Critiria er p.t. i international høringsproces, som forventes afsluttet ultimo 2005 eller i 2006
Videnskabsministeriet	Anbefaling af at vælge ISO17799 frem for DS484 som statens standard for it-sikkerhed	I det væsentlige ikke fulgt. Rådet har iværksat udarbejdelse af en sammenligning af de to standarder
EU-kommissionen	Høringssvar ift. EU-kommissionens meddelelse om "Betydningen af digital forvaltning for Europas fremtid", hvor Rådet bl.a. pegede på vigtigheden af, at it-sikkerhed fra start indtænkes i de digitale forvaltningsprojekter fra de lokale til de internationale	
EU-kommissionen	Høringssvar ift. EU-Kommisionens forslag vedrørende "Interoperabel levering af paneuropæiske e-forvaltningstjenester til offentlige myndigheder, virksomheder og borgere" (IDABC, 2005-2009), hvor Rådet anbefalede at it-sikkerhed af hensyn til troværdighed og borgernes tillid fik en mere central placering i forhold til projektets formålsbeskrivelse	

>

DIALOG MED	EMNE	RESULTAT
Internetnetudbydere	Opfordring og støtte til initiativ om koordineret indsats mod sikkerhedstrusler og spam	Koordineret indsats etableret af de største internetudbydere i Danmark
Justitsministeriet	Høringssvar vedr. udkast til bestemmelser om logning af teletrafik m.v., hvori Rådet bl.a. anbefalede at genoverveje omfanget af den foreslåede logning, idet Rådet frygter at store udgifter til logning kan gå ud over de generelle investeringer i øget it-sikkerhed	Ikke fulgt
Udbydere af MPLS-netværk (dvs. forbindelser mellem lokale netværk etableret via internettet)	Behov for større gennemsigtighed omkring it-sikkerheden i de udbudte løsninger	MPLS-kunder hos TDC kan nu få erklæringer vedrørende it-sikkerhed udarbejdet af uafhængige revisorer
Videnskabsministeriet	Anbefaling vedrørende "udvidet sårbarhedsudredning" eller evt. blot projektbeskrivelse af en sådan	Ikke fulgt
ENISA (Det europæiske agentur for net- og informationssikkerhed)	Opfordring til at ENISA arbejder for international interoperabilitet vedrørende digitale signaturer og orientering om Rådets analyse omkring RFID og pervasive computing	
Dansk Handel & Service, Dansk Industri, Forbrugerrådet	Opfordring og støtte til etablering af frivilligt kodeks for brug af RFID-tags ("trådløse stregkoder) i detailhandlen	Forhandlinger gået i stå i 2005. Dansk Handel & Service synes ikke at deltage i konsensusproces
IT-branchen	Uddeling af pjece om trådløst internet i forbindelse med salg/distribution	Pjecen distribueret af flere store leverandører
E-handelsfonden	Forslag om at etablere en "sikker-når-den-tages-i-brug"-mærkningsordning for it-udstyr, der sælges til forbrugere	

>

DIALOG MED	EMNE	RESULTAT
Danmarks Statistik m.fl.	Opfordring til at udvide og opdatere indholdet af statistik vedrørende it-sikkerhed	Rådets ønsker er ikke blevet imødekommet. Rådet har i 2005 selv gennemført en undersøgelse af befolkningens holdning til it-sikkerhed
Brancheorganisationer og kommercielle aktører	Konsensus-udgave af "Gode råd om it-sikkerhed" (se bilag 4) således at kampagneførende organisationer benytter samme grundmateriale i deres anbefalinger	Konsensus-tekst etableret og overdraget til IT- og Telestyrelsens videre forvaltning

>

BILAG 2

Kommissorium for Rådet for it-sikkerhed >

11. december 2002

Rådet for IT-sikkerhed skal gennem sit virke bidrage til at sikre offentlige myndigheder samt den private sektor og borgerne den højeste faglige viden inden for IT-sikkerhedsområdet. I den forbindelse skal rådet pege på de menneskelige og samfundsmæssige risici og interesser, som videnssamfundet skaber.

Rådet skal arbejde for:

> At fremme en sikkerhedskultur mellem alle interessenter som et middel til beskyttelse af IT-systemer og netværk.
> At øge bevidstheden om risici ved anvendelse af IT-systemer og netværk.
> At skabe større tillid til anvendelse af IT-systemer og netværk.
> At skabe rammer, der kan hjælpe alle interessenter til at forstå sikkerhedsproblemstillinger og respektere etiske værdier i forbindelse med udvikling og implementering af politikker og procedurer for sikkerheden i IT-systemer og netværk.
> At fremme samarbejde og videndeling mellem alle interessenter i forbindelse med udvikling og implementering af politikker og procedurer for sikkerhed i IT-systemer og netværk.
> At fremme, at bevidstheden om IT-sikkerhed indgår som et vigtigt mål for alle interessenter, der er involveret i udvikling eller implementering af standarder.

Rådets arbejde giver sig udslag i bl.a.:

> Igangsættelse af målrettede kampagner med henblik på at skabe en bevidsthed om IT-sikkerhed.
> Udarbejdelse af vejledninger og generel rådgivning til løsning af IT-sikkerhedsproblemer, der har en vis almen karakter.
> Initiativer til fastlæggelse af normer og standarder for IT-sikkerhed.
> Initiativer i forbindelse med forebyggelse og afhjælpning af virus- og hackerangreb.
> Initiativer i forbindelse med validering og sikring af kritisk infrastruktur samt koordinering af beredskabsplaner indenfor IT.

- Initiativer, der kan styrke og forbedre koordinationen af det internationale samarbejde.
- Initiativer til styrkelse af undervisning og forskningsprojekter inden for IT-sikkerhed.

Rådet kan afgive tekniske/juridiske udtalelser i relation til generelle og specifikke IT-sikkerhedsproblemstillinger.

Rådet ytrer sig gennem udtalelser, der enten fremkommer på baggrund af henvendelser fra borgere, private virksomheder og offentlige myndigheder eller på eget initiativ. Rådet udtaler sig endvidere løbende om samfundets IT-sikkerhed, bl.a. på baggrund af de målinger af IT-xsikkerheden, som gennemføres af Videnskabsministeriet.

Rådet udarbejder desuden en årlig arbejdsplan og skal afgive en årlig rapport over status på IT-sikkerheden i Danmark. Rapporten skal tage udgangspunkt dels i rådets arbejde i relation til rådgivning af Videnskabsministeriets Kompetencecenter for IT-sikkerhed i IT- og Telestyrelsen samt generelle sager i det pågældende år. De bevillingsmæssige rammer for rådets arbejde fastsættes på årets finanslov.

Rådet skal endvidere yde rådgivning til Kompetencecentret i forbindelse med centrets opgavevaretagelse. Rådets årlige arbejdsplan bidrager til Kompetencecentrets samlede prioriterede arbejdsplan. Rådet høres om Kompetencecentrets prioriterede arbejdsplan.

Rådet for IT-sikkerhed udgøres af et formandskab på 2 personer bestående af en formand og en næstformand, og 6 andre medlemmer, der er udpeget af ministeren for videnskab, teknologi og udvikling. Medlemmerne er personligt udpeget i kraft af deres sagkundskab om eller holdninger til IT-sikkerhedsområdet og er ikke repræsentanter for bestemte interesseorganisationer eller lignende. Rådet udpeges for en periode af 3 år, hvorefter rådet kan genbesættes. Genbeskikkelse af medlemmer kan finde sted.

>

Rådet er uafhængigt. Videnskabsministeriets Kompetencecenter for IT-sikkerhed i IT- og Telestyrelsen yder sekretariatsfunktion for rådet.

>

BILAG 3

Rådets udgivelser 2003-2005 >

TITEL	ÅR	DISTRIBUERET I TRYKT VERSION (ANTAL PJECER)	DISTRIBUERET ELEKTRONISK *(ANTAL DOWNLOADS)
Sikkerhed i trådløse netværk	2005/2003	27.017	15.226
Beskyt dit trådløse netværk	2005/2003	26.456	20.723
Hvad du bør vide om computervirus	2004	10.000	17.249
Beskyt dig mod computervirus	2004	19.332	3.764
Firewall - Beskyt din computer	2004	Ingen trykt version	19.192

* opgjort pr. 8. dec. 2005

Rådets årsberetninger for 2003, 2004 og 2005 er trykt og distribueret i 1000 eksemplarer og er tilgængelige via www.rfits.dk.

Følgende pjecer er derudover udgivet elektronisk eller videreført fra det tidligere IT-sikkerhedsråd:

> Spyware - hvad er det? Og hvordan undgår jeg det? (2004)
> Privatliv på internettet (2003)
> IT-sikkerhedsrådets redegørelse om brug af e-post og internet på arbejdspladsen (2003)
> Bilag til til Brug af af e-post og internet på arbejdspladsen (2003)
> Kortlægning af offentlige og private virksomheders behov for kompetencer på it-sikkerhedsområdet (2003)
> Datasikkerheden i Danmark (2003)

>

BILAG 4

Gode råd om it-sikkerhed >

Sådan beskytter du dig selv og undgår at sprede sikkerhedsproblemer til andre:

1. Brug et antivirusprogram med automatisk opdatering, en firewall og et antispywareprogram. Sammen beskytter programmerne din pc mod mange angreb og skadelige programmer.
2. Anvend opdaterede versioner af dit styresystem, din webbrowser og dit e-postprogram. Slå automatisk opdatering til, hvor det er muligt, så glemmer du det ikke.
3. Vær ekstra opmærksom, når du åbner vedhæftede filer. De kan indeholde virus. Pas især på filer med underlige eller lokkende navne, også hvis de kommer fra nogen, du kender.
4. Hvis du benytter trådløst internet, så slå kryptering til - ellers kan andre kigge med eller misbruge din internetforbindelse. Vælg stærk kryptering.
5. Bed andre om hjælp, hvis du er i tvivl, og brug i øvrigt din sunde fornuft. Selv om du har både antivirusprogram, firewall og et antispywareprogram, så forhold dig kritisk til de netsteder, du besøger.

... og sådan passer du på dine personlige og fortrolige oplysninger:

6. Adgangskoder er den vigtigste beskyttelse af dine personlige oplysninger. Gode råd om adgangskoder:

> De består af minimum 8 tegn
> Brug både små og store bogstaver
> Brug et eller flere tal
> Brug evt. specialtegn som #,!,? eller *
> Vær ekstra omhyggelig med adgangskoder til netbank, digital signatur og det trådløse netværk.

7. Vær påpasselig med at afgive personlige oplysninger via e-post. Det svarer til at sende åbne postkort. Hvis du sender fortroligt materiale som e-post, så brug kryptering og digital signatur. Hold øje med, om netsteder, der beder om fortrolige oplysninger, benytter kryptering (se efter hængelås nederst i browseren).
8. Slet spam uden at åbne det og svar ikke på spam. Hvis du åbner eller svarer på spam, kan afsenderen se det, og så får du sandsynligvis mere spam. Benyt eventuelt et spamfilter.

9. Hent kun programmer fra internettet, hvis du stoler på netstedet, du henter det fra. Undersøg om du siger ja til reklamer og afgivelse af private oplysninger, før du installerer. Vær især opmærksom over for fildelingsprogrammer og gratis programmer.
10. Undgå spyware og adware. Det er programmer, som opsamler oplysninger om din identitet og adfærd og udsætter dig for uønsket annoncering, samtidig med at de gør din computer langsommere. De bliver typisk installeret i det skjulte, hvis du klikker på lokkende tekst eller billeder eller uskyldigt udseende dialogbokse.
11. Reager ikke på e-post fra banker og betalingstjenester, hvis de indeholder links du skal klikke på eller anmoder dig om personlige og fortrolige oplysninger. Det kan være forsøg på "phishing", en form for svindel hvor der linkes til falske kopier af netsteder, som du har tillid til.
12. Brug adgangskode til log-in på din computer.
13. Indstil sikkerhedsniveauet i din browser, så du altid bliver spurgt, når informationer, filer og programmer overføres til din computer.
14. Vær påpasselig, når du bruger chat og instant messaging. Disse tjenester er nye og spreder sikkerhedsproblemer endnu hurtigere end e-post. Vær derfor særlig opmærksom, og klik kun på links, hvis du kan gennemskue, hvor de fører hen, og du har tillid til afsenderen.
15. Lav sikkerhedskopier af dine vigtige dokumenter og filer, og tjek, at de kan genindlæses.

Version 1.0
Sidst opdateret: december 2005

Flere oplysninger om netsikkerhed:
www.netsikkernu.dk
www.it-borger.dk
eller hos din internetudbyder.

Denne tekst er udarbejdet af Rådet for it-sikkerhed og IT- og Telestyrelsen i samarbejde med DANSK IT, DK-CERT, Finansrådet, IT-Brancheforeningen, ITEK, Prosa og 1984.dk samt TDC. Andre organisationer eller netsteder kan frit anvende teksten i sin helhed. Nyeste version findes på www.it-borger.dk. Forslag til opdatering kan sendes til sik@itst.dk.

>

BILAG 5

Gode råd om brug af digital signatur >

Med en digital signatur kan du identificere dig selv elektronisk og også underskrive dokumenter elektronisk. Vælg en leverandør af digital signatur, som du har tillid til. IT- og Telestyrelsen har godkendt TDC, som leverandør af OCES-certifikat, der er den type digitale signatur, du skal bruge for at kommunikere med danske myndigheder.

Du bevarer den høje sikkerhed, som er indbygget i selve den digitale signatur, hvis du følger disse gode råd:

1. Brug kun digital signatur fra sikre computere.
Den digitale signatur har i sig selv en høj sikkerhed, men du opnår kun den høje sikkerhed, hvis din computer også er sikker. Følg de almindelige gode råd om it-sikkerhed, dvs. brug et opdateret antivirus-program, firewall, antispywareløsning, opdateret styresystem og programmer samt kryptering af evt. trådløst netværk. Lad være med at bruge digital signatur, før disse forhold er i orden.

2. Hold adgangskoden hemmelig, og lær den udenad.
Når du opretter en digital signatur, får du anvisninger på, hvordan du sammensætter en sikker adgangskode. Lad være med at bruge denne adgangskode i andre sammenhænge overhovedet. Giv ikke adgangskoden til andre, for det er den, du skal bruge for at aktivere din elektroniske underskrift. Lær adgangskoden udenad, eller gem den et sikkert sted. Opbevar ikke adgangskoden på din computer.

3. Pas godt på selve den digitale signatur.
Tænk på din digitale signatur som var den et betalingskort. Selve den digitale signatur er en unik computerfil, som bl.a. indeholder din e-postadresse. Hvis du opbevarer, dvs. installerer, den digitale signatur på din computer, skal du i princippet passe lige så godt på din computer, som du gør på et betalingskort. Du kan nemmere passe på din digitale signatur, hvis du flytter den over på en "e-token", som du fx kan have i dit nøgleknippe. Dette er muligt på nyere computere med USB-port. En e-token kan købes hos udstederen af din digitale signatur.

4. Tag en sikkerhedskopi af din digitale signatur.
Tag en sikkerhedskopi af din digitale signatur, og opbevar den et sikkert sted.

5. Spær omgående din digitale signatur ved risiko for misbrug.
Hvis andre har fået adgang til din digitale signatur, eller hvis du har mistanke om det, skal du straks spærre den. Dette gælder også, hvis andre får kendskab til din adgangskode. Du spærrer din digitale signatur ved at kontakte det certificeringscenter, der har udstedt den. Når du bestiller din digitale signatur, modtager du en spærrekode, som du skal oplyse ved en eventuel spærring. Gem derfor denne kode, og opbevar den forsvarligt.

6. Tjek at oplysningerne i din digitale signatur er korrekte.
Tjek at oplysningerne i din digitale signatur er korrekte inden du tager den i brug. Hvis der er fejl i e-postadressen, virker din digitale signatur ikke. Hvis du får ny e-postadresse, skal du forny din digitale signatur.

Hvis du bruger din digitale signatur i e-post:

7. Hold øje med om en modtaget digital signatur er gyldig.
De fleste e-postprogrammer kontrollerer automatisk, om signaturen er gyldig. Læs evt. hjælpeteksten i dit e-postprogram. En signatur er ugyldig, hvis den er udløbet eller spærret. Spærring kan altid kontrolleres manuelt på certificeringscentrets hjemmeside, som har en spærreliste.

8. Kontroller om den digitale signatur anvendes i overensstemmelse med dens formål.
En digital signatur kan indeholde begrænsninger af, hvad den må anvendes til. Det vil stå i certifikatet, som du kan klikke frem fra e-posten. Som modtager bør du som udgangspunkt ikke stole på en digital signatur, hvis afsenderen anvender den ud over de fastsatte begrænsninger.

Hvis du bruger din digitale signatur til log-on på netsteder:

9. Vær sikker på, hvem du kommunikerer med.
Når du bruger din digitale signatur på netsteder med digitale selvbetjeningsløsning, så hold øje med, om der en lille hængelås nederst i dit browservindue. Hængelåsen symboliserer, at forbindelsen er kodet, så uvedkommende ikke kan læse med. Ved at klikke på hængelåsen, kan du få vist netstedets certifikat. Afgiv kun fortrolig information igennem din browser, når du kan se hængelåsen.

10. Luk altid din internetbrowser, når du er færdig med at bruge din digitale signatur.
Hvis du har brugt din digitale signatur som log-on på et netsted, er den "aktiv" og kan evt. bruges af andre, så længe din browser er åben. Den sikreste måde at afslutte en session på er at lukke alle åbne vinduer i din internetbrowser.

Version 1.0
December 2005

>