Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Til orientering af Udvalget for Videnskab og Teknologi fremsendes i 5 eksemplarer "It-sikkerhed overalt for alle " – Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005, samt et kort "Notat om de it-sikkerhedsmæssige ansvarsområder under andre ministerier end Videnskabsministeriet".

Med venlig hilsen

Helge Sander

Ministeriet for Videnskab, Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

It-sikkerhed overalt og for alle

Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005

1 Samfundets sårbarhed

Danmark bindes i dag sammen af et vidt forgrenet elektronisk it- og telenetværk. Vi har gennem de seneste årtier skabt os en elektronisk infrastruktur, der er blevet en lige så vigtig del af samfundet som den fysiske infrastruktur med dens veje, fly og jernbaner. Den elektroniske infrastruktur er helt fundamental, hvis vi skal indfri visionerne om at være et vidensbaseret højteknologisk samfund.

I det højteknologiske samfund skal alle – borgerne, erhvervslivet og den offentlige sektor – have uhindret og pålidelig adgang til troværdige informationer.

I et højteknologisk samfund med en veludbygget elektronisk infrastruktur bliver arbejdsprocesserne normalt både mere effektive og mere optimale. Men lige så vel som enhver anden afhængighed skaber sårbarhed, skaber afhængigheden af den elektroniske infrastruktur også sårbarhed. Det kræver en målrettet indsats at håndtere denne sårbarhed.

For at kunne træffe de nødvendige forholdsregler for at styrke it-sikkerheden er det vigtigt at foretage en risikovurdering. I risikovurderingen skal indgå en vurdering af sårbarheder og trusler, men også samfundsøkonomiske overvejelser. Det niveau af it-sikkerhed, der vælges, skal altid bygge på en afvejning af på den ene side, hvilke værdier, der står på spil og på den anden side prisen for at opnå den ønskede grad af sikkerhed.

2 It-sikkerhed i Danmark

Videnskabsministeriets arbejde indenfor it-sikkerhedsområdet tager udgangspunkt i regeringens *It- og telepolitiske handlingsplan 2003* og *Strategi for projekt digital forvaltning 2004-2006*.

Den it- og telepolitiske handlingsplan har tre mål:

- Skabe vækst i dansk erhvervsliv.
- Udvikle den offentlige sektor.
- Kvalificere danskerne til fremtidens vidensamfund.

For alle tre mål spiller it-sikkerhed en væsentlig rolle.

Den it- og telepolitiske handlingsplan opdateres med regeringens årlige it- og telepolitiske redegørelser.

Strategien for udviklingen af den digitale forvaltning i de kommende år er fastlagt i *Strategi for projekt digital forvaltning 2004-06.*

Her har regeringen sat sig en række pejlemærker for, hvad der skal nås. It-sikkerhedsområdet har medansvar for følgende pejlemærker:

- Den offentlige sektor skal levere sammenhængende ydelser med borgere og virksomheder i centrum
- Den offentlige sektor skal arbejde og kommunikere digitalt
- Digital forvaltning skal baseres på en sammenhængende og fleksibel it-infrastruktur.

Videnskabsministeriet er ikke den eneste myndighed, der beskæftiger sig med it-sikkerhed. F.eks. har Politiets Efterretningstjeneste tilsyn med systemer, der skal behandle og opbevare klassificeret materiale, der er omfattet af Statsministeriets sikkerhedscirkulære[1]. Og Datatilsynet fører tilsyn med offentlige og private organisationer og virksomheders behandling af persondata i henhold til persondataloven.

3 Overordnet mål for arbejdsprogrammet

For at nå regeringens mål på det it- og telepolitiske område er det nødvendigt, at it- og tele-anvendelsen i Danmark er baseret på velafbalancerede sikkerhedshensyn. Informationer og data skal således være

[1] Statsministeriets cirkulære nr. 204 af 7. december 2001

tilgængelige, troværdige og behandles med den nødvendige og tilstrækkelige fortrolighed.

For at nedbringe samfundets sårbarhed og for at fremme borgernes tillid til det digitale samfund og den digitale forvaltning vil Videnskabsministeriets it-sikkerhedsinitiativer opfylde en eller flere af følgende målsætninger:

- Medvirke til udvikling af en dansk it-sikkerhedskultur
- Sikre en robust it- og teleinfrastruktur
- Begrænse nuværende og fremtidige it-sikkerhedsrisici
- Minimere konsekvenser af it-sikkerhedshændelser.

3.1 Om at skabe vækst i dansk erhvervsliv

Erhvervslivet har selv en stor interesse i at styrke it-sikkerheden og dermed på den ene side undgå tab og på den anden side høste gevinsterne ved god it-sikkerhedsledelse. Erhvervslivet er selv nærmest til at løfte denne opgave.

Derfor vil Videnskabsministeriet

- være opmærksom på om erhvervslivet selv løfter opgaven med at højne virksomhedernes it-sikkerhed
- være med til at sikre en åben, effektiv og brugervenlig infrastruktur samt at tilbyde de nødvendige værktøjer for at virksomhederne kan anvende OCES digitale signaturer
- indgå i en konstruktiv dialog med erhvervslivet om samfundets it-sikkerhedsopgaver.

3.2 Om udvikling af den offentlige sektor

Hvis den digitale forvaltning skal give reelle serviceforbedringer og effektiviseringer, så kræver det, at data og it-tjenester kobles på tværs af de kendte grænser mellem myndighederne – såvel mellem myndighederne indbyrdes som mellem myndighederne og andre.

Videnskabsministeriets arbejde med it-sikkerhed skal være med til at sikre, at borgere og virksomheder trygt kan overlade alle relevante informationer til det offentlige. Det betyder, at den enkelte borger må kunne forvente, at oplysninger ikke går tabt, ikke forvanskes, og ikke videregives til uvedkommende. Hverken bevidst eller ved uheld.

Det er væsentligt, at der på tværs af myndigheder, både nationalt og internationalt, er enighed om, hvordan man skaber sikkerhed. Kun derved kan myndighederne have tillid til hinandens evne til at beskytte data og systemer. Derfor prioriteres det højt, at der etableres fælles standarder for it-sikkerhed.

Den offentlige sektor anvender i dag informationsteknologi i så stort et omfang, at sikkerhedssvigt kan være katastrofal. Det er helt afgørende, at alle offentlige myndigheder gør sig dette klart og medvirker til at undgå eller minimere svigtene. Alle myndigheder skal kunne fungere både i normale og ekstraordinære situationer. Videnskabsministeriet yder derfor løbende rådgivning om it-sikkerhed, og vurderer sikkerheden i større offentlige it-projekter.

Videnskabsministeriet foretager løbende analyser af, om nye initiativer kan højne it-sikkerheden og effektivisere it-driften.

3.3 Om at kvalificere danskerne til fremtidens vidensamfund

Det er vigtigt, at borgerne har kvalifikationerne til at håndtere it-sikkerhed både på arbejdet og i hjemmet. Og det er vigtigt, at borgerne har tillid til brugen af it og internet. Videnskabsministeriet følger derfor op på, at Danmark efterlever EU's og OECD's anbefalinger om opbygning og udvikling af en it-sikkerhedskultur. En sådan kultur bygger i høj grad på information, uddannelse og bevidsthed. Den bør supplere de teknologiske muligheder, der løbende udvikles og stilles til rådighed.

Videnskabsministeriet har it-sikkerhedsaktiviteter direkte henvendt til borgerne. Men i en række nye initiativer vil Videnskabsministeriet

- i form af pjecer og web-publikationer levere bred rådgivning om it-sikkerhed, som kan øge borgernes bevidsthed om it-sikkerhed,
- søge samarbejde med private og offentlige aktører om brede og smalle initiativer, herunder
  - *netsikker nu!* kampagnen og
  - understøtte den nationale anti-spam strategi.
- understøtte udbredelsen af digital signatur gennem en fortsat udbygning af den elektroniske infrastruktur og en målrettet offentlig information og vejledning.

4 Hovedopgaver

Digitaliseringen af den offentlige forvaltning er en af de mest omfattende og fremadrettede it-politiske aktiviteter i det danske samfund i disse år. For at en digitalisering af den offentlige forvaltning skal lykkes, skal vi kunne stole på informations- og kommunikationsmidlerne i det digitale samfund. Det stiller os overfor nogle store opgaver. De tre største opgaver i arbejdsprogrammet for 2005 er:

- Digital signatur
- Standard for it-sikkerhedsprocesser i staten
- Et tidssvarende beredskab på it- og teleområdet

4.1 Digital signatur

De fleste aktiviteter indenfor it-sikkerhed retter sig mod enten virksomheder, det offentlige eller borgerne. Men da it- og teleinfrastrukturen er så fundamental for samfundet, er der tværgående aktiviteter, som retter sig mod alle målgrupper. Således f.eks. den digitale signatur. Her koordineres arbejdet på tværs af alle tre målgrupper for at sikre den størst mulige gennemslagskraft.

I foråret 2003 blev der efter et offentligt udbud indgået aftale med TDC om frikøb af anvendelsen af digital signatur i det offentlige, udstedelsen af digital signatur til alle borgere i en periode på 4 år samt etablering af en it-sikkerhedsinfrastruktur baseret på en såkaldt "Public Key Infrastructure".

For at den digitale signatur kan virke efter hensigten – at give muligheden for fortrolig, troværdig og autentisk kommunikation – skal der opnås en kritisk masse af digitale signaturer. En forudsætning for det er, at der findes en bred vifte af offentlige tjenester, der kan anvendes med brug af digital signatur. Videnskabsministeriet vil derfor i 2005 fortsat fokusere på at udbygge infrastrukturen og at gøre det lettere for de offentlige tjenesteudbydere at anvende digital signatur.

Videnskabsministeriet vil i 2005

- Øge udbredelsen og anvendelsen af digitale signaturer i den offentlige sektor, bl.a. ved
    - at stille digitale værktøjer til rådighed, så der kan indføres digital signatur i hele den offentlige sektor og
    - yde vejledning om indførelse og anvendelse af digital signatur i den offentlige sektor,
- i samarbejde med Erhvervs og Selskabsstyrelsen øge udbredelsen og anvendelsen af digitale signaturer i den private sektor og
- udvikle "best practice" og specifikationer for implementering af den fælles-offentlige digitale signatur, f.eks. i forbindelse med at integrere kravene fra eDag2 i Elektronisk Sags og Dokument Håndteringssystemer (ESDH).

4.2 Standard for it-sikkerhedsprocesser

I januar 2004 blev det besluttet, at alle statslige myndigheder skal efterleve en fælles standard for håndtering af it-sikkerhed fra 2007. Det drejer sig mere end noget andet om at etablere det, man kunne kalde "god it-sikkerhedsledelse".

Med en implementering af standarden opnås:

- større sammenhæng, sammenlignelighed og rettidighed i vurderinger af it-sikkerhedsstrusler og –sårbarheder og beslutte relevante it-sikkerhedsforanstaltninger,
- en bedre forståelse for de risici, der knytter sig til at håndtere værdifulde og følsomme informationer og
- sikrere informationssystemer og infrastruktur.

Beslutningen fra januar 2004 følges op i Videnskabsministeriet med en række aktiviteter, der har det fælles mål at støtte den lokale it-sikkerhedsledelse.

Alle disse aktiviteter er samlet i et program, som er udarbejdet i samarbejde med Statens it-råd. KL og Amtsrådsforeningen deltager også i arbejdet. Videnskabsministeriet arbejder for, at lignende aktiviteter bliver sat i værk i kommuner og amter – af den enkle grund, at tryghed og tillid i hele den offentlige digitale forvaltning kun nås, hvis også amter og kommuner er med.

4.3 It- og teleberedskab

Et it- og teleberedskab skal sørge for, at offentlige myndigheder og andre, der arbejder indenfor beredskabsområdet, har adgang til

elektronisk kommunikation og it-anvendelse i en beredskabssituation, først og fremmest ved at sikre adgangen til offentligt udbudte it- og teletjenester.

Beredskabet skal desuden sikre en robust fælles national it- og teleinfrastruktur og dermed teleforsyning for offentlige myndigheder, erhvervslivet og den enkelte borger.

I løbet af 2004 har Videnskabsministeriet foretaget en analyse af behovet for et egentligt it- og teleberedskab. I 2005 vil Videnskabsministeriet

- fremlægge resultaterne af analysen
- følge op på analysen med anbefalinger om beredskabet
- vedligeholde det eksisterende it- og teleberedskab.

En mere detaljeret indsats kan planlægges, når analysen er fremlagt og har været igennem en efterfølgende debat og behandling.

4.4 Varslingstjeneste for staten

En varslingstjeneste for staten vil kunne give statens myndigheder en advarsel før it-systemer stopper med at fungere eller data bliver kompromitteret på grund af f.eks. virus, hackerangreb eller orme.

I 2005 foretager Videnskabsministeriet en vurdering af, hvordan behovet for en varslingstjeneste for staten bedst kan varetages.

5 Metoder

It-sikkerhed er en proces. Og derfor er det vigtigt for Videnskabsministeriet at arbejde offensivt i forhold til risici, der ligger i it-anvendelsen – og også at virke offensiv i forhold til muligheder, sårbarheder og trusler i forbindelse med nye teknologier.

Det er også vigtigt, at udviklingen af it-sikkerhed i Danmark er båret af faglighed, og at den er internationalt orienteret og åben med brede dialogfora.

5.1 Faglighed

It-problemstillinger af national karakter er ofte komplicerede. Dette gælder ikke mindst it-sikkerhedsområdet. Det er derfor meget vigtigt, at medarbejdere har den nødvendige indsigt i problemstillingerne, og at den viden, der arbejdes på grundlag af, er opdateret.

5.2 Internationalt orienteret

De mål, Videnskabsministeriet har sat for it-sikkerhedsområdet, ligger ofte i forlængelse af internationale problemstillinger. Disse skal løses internationalt. Og det er nødvendigt at fokusere det internationale samarbejde i forhold til de nationale prioriteringer.

Videnskabsministeriet deltager derfor i koordinering og udbredelse af internationale initiativer og standardiseringer indenfor it- og teleberedskab, generel it-sikkerhed samt digital signatur, og vil prioritere EU og i særdeleshed arbejdet i forhold til Det europæiske Agentur for Net- og Informationssikkerhed (ENISA) samt samarbejdet i NATO inden for civilt beredskab.

5.3 National dialog

Videnskabsministeriets mål kan kun nås, hvis arbejdet med it-sikkerhed, udpegning af indsatsområder og implementering af løsninger sker i et samspil med alle aktører, der har interesser indenfor it-sikkerhedsområdet.

Videnskabsministeriet vil i 2005 søge at styrke kontakterne yderligere til erhvervslivets repræsentanter, borgernes interesseorganisationer og andre interessenter i den offentlige sektor.

5.4 Rådet for it-sikkerhed

Rådet for it-sikkerhed vil gennem sit virke pege på de menneskelige og samfundsmæssige risici som videnssamfundet skaber gennem sin anvendelse af it og arbejde for at

- fremme en sikkerhedskultur hos borgere og virksomheder som et middel til beskyttelse af it-systemer og netværk, og
- øge bevidstheden om risici ved anvendelse af it-systemer og netværk og skabe større tillid til anvendelse af it-systemer og netværk.

Rådet for it-sikkerhed blev nedsat for en 3-årig periode januar 2003. I løbet af 2005 skal der træffes beslutning om rådets fremtid.

Ministeriet for Videnskab,
Teknologi og Udvikling

Notat om de it-sikkerhedsmæssige ansvarsområder under andre ministerier end Videnskabsministeriet

Videnskabsministeriets arbejdsprogram for it-sikkerhed 2005 beskriver bl.a. hvad Videnskabsministeriets rolle er i forhold til it-sikkerheden i Danmark.

Ministeriet for Videnskab, Teknologi og Udvikling

Denne skitse er et addendum til Videnskabsministeriets arbejdsprogram for it-sikkerhed, og har til formål at give et hurtigt overblik over andre ministeriers it-sikkerhedsmæssige ansvarsområder.

Statsministeriet

- Statsministeriet udsteder sikkerhedscirkulæret, hvor Politiets Efterretningstjeneste (PET) er udpeget som den nationale sikkerhedsmyndighed, der fører tilsyn med de offentlige it-systemer, som behandler og opbevarer NATO og EU klassificerede data. PET refererer i disse sammenhænge til statsministeriet.

Justitisministeriet

- **Datatilsynet** har tilsynspligten i forhold til persondataloven.
- **Politikredsene** efterforsker it-kriminalitet, herunder hacking og udspredelse af virus. **Rigspolitiet** har en støtteafdeling, som kan yde hjælp til den enkelte politikreds.
- **Rigspolitiet** efterforsker også anden kriminalitet hvor it indgår, såsom børneporno.
- **Politiets Efterretningstjeneste** (PET) har ansvar for national sikkerhed.

Forsvarsministeriet

- **Forsvarets Efterretningstjeneste** (FE) har ansvaret for forsvarets it-sikkerhed og for national kommunikationssikkerhed.

Finansministeriet

- Økonomistyrelsen definerer et it-sikkerhedsparadigme i forbindelse med regnskabsbekendtgørelsen og anvendelse af Navision Stat, som et sæt af anbefalinger til institutionerne.