

Antonigade 4  
DK - 1106 København

Tel. +45 33 32 05 03  
Fax +45 33 91 05 09

[www.tekno.dk](http://www.tekno.dk)  
[tekno@tekno.dk](mailto:tekno@tekno.dk)

Giro (1199) 8 51 07 68

J.nr: 03.403-032

# It-sikkerhed på tværs af grænser

Anbefalinger fra en arbejdsgruppe under Teknologirådet

## Resume af arbejdsgruppens anbefalinger

Rapporten i dens fulde ordlyd kan downloades via Teknologirådets hjemmeside [www.tekno.dk](http://www.tekno.dk).

Teknologirådet  
har til opgave at:

fremme  
teknologidebatten

vurdere teknologiens  
muligheder og  
konsekvenser

rådgive Folketinget  
og regeringen

# 1. Sårbarheder i soft- og hardware

**Problem:** Sårbarheder i hardware og i software som operativsystemer og programpakker er det alvorligste it-sikkerhedsproblem anno 2006 målt på antal hændelser og deres konsekvenser. Særligt lider små og mellemstore virksomheder, offentlige institutioner og private borgere under konsekvenserne af disse sårbarheder.

**Løsning 1:** Udvikling af en model, som sikrer, at sikkerhedsopdateringer i software bliver installeret hos brugerne straks efter et sikkerhedshul er opdaget. Almindelige brugere skal ikke acceptere disse opdateringer, mens avancerede brugere selv kan vælge at styre opdateringsprocessen. Større programopdateringer – hos nogle leverandører kaldet "service packs" – skal kun ske efter brugeraccept.

**Løsning 2:** Det skal være et EU-lovkrav, at forhandlere af elektronisk, netværksbaseret (IP-baseret) udstyr som computere, telefoner, MP3-afspillere, tyverialarmer, køleskabe m.v. leverer produkter med den nyeste sikkerhedsopdatering.

**Løsning 3:** Danmark/EU indfører en "whitelist"-ordning for soft- og hardware. Den offentlige sektor går foran og benytter kun whitelistede it-produkter.

**Løsning 4:** Certificeringsordning for Internet Service Providere (ISP'er). Alle ISP'er i EU bliver pålagt at leve op til en kodeks, der mindst svarer til det danske ISP Sikkerhedsforums Adfærdskodeks. Inden for 3-5 år bliver der stillet lovkrav om, at alle ISP'er skal ISO27001-sikkerhedscertificeres (eller tilsvarende).

# 2. Utilstrækkelig viden om it-sikkerhed

**Problem:** Utilstrækkelig viden er en væsentlig årsag til manglende sikkerhed. Den menneskelige faktor er bl.a. væsentlig i relation til "phishing", identitetstyveri og udbredelse af skadelige programmer, som kan medføre, at computeren "går ned" og at man mister harddiskens indhold af tekst, billeder, film, musik m.v – og for virksomheders vedkommende bl.a. kundedatabaser og intellektuel kapital. Manglende it-sikkerhed på grund af uvidenhed er ofte ikke alene et problem for den virksomhed eller borger, der ikke beskytter sig godt nok. Konsekvenserne af manglende sikkerhed kan sprede sig til virksomhedens kunder, samarbejdspartnere etc. – og til personer i den private brugers adresseliste – og forvolde skade og økonomiske tab her. Det er på den baggrund nødvendigt, at it-administratorer, medarbejdere og ledere prioriterer sikkerhed langt højere, end det sker i dag. Og at befolkningens generelle vidensniveau i forhold til it-sikkerhed bliver løftet betydeligt.

**Løsning 1:** Større fokus på it-sikkerhed i folkeskolen. Generelt større forankring af it-sikkerhedsaspektet i hele uddannelsesforløbet.

**Løsning 2:** Etablering af "Rådet for større it-sikkerhed" med fokus på oplysning til borgerne.

**Løsning 3:** Lovgivning mod "it-forurening".

### 3. Manglende mulighed for at skelne mellem sikre og usikre produkter og services

**Problem:** Flere og flere produkter og services indeholder en internetopkobling (Internet Protocol – IP) og det bliver på den baggrund stadig mere relevant at anbefale sikre produkter og services til forbrugerne med henblik på at højne det generelle sikkerhedsniveau. Det gælder fx i forhold til computere, mobiltelefoner, harddiskoptagere til tv, mediacentre, køleskabe og lignende i private hjem. I fremtiden vil stort set alle apparater, biler, både og fly m.v. indeholde IP-teknologi og være tilsluttet internettet. Sikkerhedsproblemerne forventes at vokse yderligere, fordi produkterne i stigende grad kommer fra hele verden og fra stadig flere producenter, hvilket vil gøre det endnu vanskeligere for forbrugere og virksomheder at gennemskue og håndtere sikkerhedsaspektet.

**Løsning:** Danmark tager initiativ til udvikling af et koncept for mærkning af internetforbundne produkter, som betyder, at privatpersoner og virksomheder får vished om sikkerhedsniveauet i det enkelte produkt. Man kan fx benytte mærkning med stjerner som i bilverdenens ”crashtest-ordning”. Mærkningsordningen skal dække hele EU og på længere sigt udbredes til det globale marked.

### 4. Manglende koordineret, grænseoverskridende politiindsats og retsforfølgelse på it-kriminalitetsområdet

**Problem:** It-kriminalitet er et vanskeligt arbejdsområde for politiet såvel i Danmark som i EU og den øvrige verden. Interpol deltager stort set ikke i bekæmpelse af it-relateret kriminalitet, og Europols rolle er relativt lille på grund af begrænsede ressourcer. Den stigende it-kriminalitet på globalt plan bliver næret af en mangelfuld politimæssig indsats. Det er problematisk, at forebyggelse og efterforskning af it-kriminalitet generelt er nedprioriteret i forhold til anden politimæssig efterforskning, at området bliver tildelt så få ressourcer, som tilfældet er, og at der derfor akut mangler personale med kompetencer på området i Danmark og internationalt.

**Løsning 1:** Strukturering af indsatsen: Anerkendelse af it-kriminalitet som et nyt politispeciale. Udnævnelse af mindst én it-kriminalitetsansvarlig i hver af de nye politikredse og etablering af en central myndighed, der kan håndtere komplekse sager om it-kriminalitet professionelt – nationalt og internationalt. Prioritering af it-kriminalitet må ikke ske på bekostning af andre politiopgaver, men skal ske på baggrund af øgede bevillinger.

**Løsning 2:** Højnelse af vidensniveauet: Politimæssig kompetenceoprustning hele vejen rundt – fra uddannelse af specialister på de enkelte it-kriminalitetsområder til kompetenceudvikling af anklagemyndighed og dommere.

**Løsning 3:** Videreudvikling af internationale samarbejdsaftaler, som skal sikre en mere effektiv håndtering af grænseoverskridende it-kriminalitet.

## 5. Mangel på sikker identifikation

**Problem:** Kommunikationssikkerhed er en forudsætning for et frit informationsflow – og for en effektiv digital forvaltning og derved en bedre offentlig service i fremtiden. Borgernes udnyttelse af den stadig mere integrerede økonomiske servicestruktur i EU – og globaliseringen i det hele taget – kan blive bremsede af mangel på en entydig identifikationsmekanisme nationalt og på tværs af EU, som bl.a. kan minimere risikoen for misbrug af personlige oplysninger. Man kan fx forestille sig, at en sådan mekanisme kan eliminere vanskeligheder i forbindelse med udveksling af patientinformationer mellem danske og udenlandske hospitaler. Det er nationalstaternes ansvar at skabe en digital identifikation, som kan beskytte borgernes personlige data imod fx identitetstyveri. Arbejdsgruppen mener, der er behov for, at alle borgere i Danmark og i hele EU bliver udstyret med en identifikationsmekanisme med meget høj sikkerhed.

**Løsning:** Danmark etablerer en langsigtet strategi om at videreudvikle den nuværende digitale signatur til et "borgerservicepas" i form af en digital identitet, som minimerer risikoen for, at den enkelte borger bliver offer for kriminelle handlinger i forbindelse med digital forvaltning, handel og kommunikation via internettet. Målet er på længere sigt, at hver borger i EU har en sådan interoperabel, digital identitet. Arbejdsgruppen mener, at man bør overveje at lade sig inspirere af det udviklingsprojekt på området, der netop nu foregår i Østrig. Det danske udviklingsarbejde skal koordineres i forhold til hele EU med henblik på opbygning af en sikker, EU-interoperabel "borgerservice-infrastruktur" med fælles kommunikationsstandarder.

## 6. Manglende fokus på it-sikkerhed i offentlige it-udbud

**Problem:** Under 5 pct. af spørgsmålene i forbindelse med offentlige it-udbud omhandler sikkerhed. Arbejdsgruppen mener ikke, der i tilstrækkelig grad bliver taget højde for it-sikkerheden, når EU og de enkelte medlemslande sender infrastrukturelle funktioner i udbud. Det er fx problematisk, at kravspecifikationer for it-sikkerhed og privacy i offentlige it-udbud er mangelfulde eller ikke-eksisterende, og at it-udbud typisk ikke indeholder en "forbundethedsanalyse", der vurderer konsekvenser ved en sikkerhedsbrist for andre områder end det, udbudet dækker.

**Løsning:** Lovgivning om, at it-sikkerhed skal være en nøgleparameter i alle offentligt udbud, hvor it indgår. Udbud skal indeholde en it-sikkerheds- og bundethedsanalyse, der vurderer konsekvenser ved en sikkerhedsbrist for andre områder end det, udbudet dækker.