It-sikkerhed på tværs af grænser

Anbefalinger fra en arbejdsgruppe under Teknologirådet

It-sikkerhed på tværs af grænser

Anbefalinger fra en arbejdsgruppe under Teknologirådet

Projektledelse i Teknologirådets sekretariat:
Bjørn Bedsted, projektleder
Jonas Egmose Mortensen, projektmedarbejder

Projektsekretær:
Eva Glejtrup

Omslag og tryk:
Vester Kopi

ISBN: 978-87-91614-32-3
ISSN 13959372
EAN: 5798000416826

Rapporten kan bestilles hos:

Teknologirådet
Antonigade 4
1106 København K
Telefon: 33 32 05 03
E-mail: tekno@tekno.dk

Rapporten og yderligere materiale kan
hentes på teknologirådets hjemmeside
www.tekno.dk/itsikkerhed2007.

Teknologirådets rapporter 2007/1

It-sikkerhed på tværs af grænser

Anbefalinger fra en arbejdsgruppe
under Teknologirådet

TEKNOLOGI-RÅDET

Indhold

1. Forord

Stadig flere samfundsfunktioner, som fx handel med varer og kommunikation mellem borgere og virksomheder og det offentlige, foregår i disse år via internettet og baserer sig dermed på globalt forbundne it-netværk. Det medfører en effektivisering, men det øger også samfundets sårbarhed over for it-sikkerhedsproblemer. Mange af disse problemer med fx it-kriminalitet og sikkerhedshuller i software kan vi, på grund af den globale forbundethed, ikke løse nationalt i Danmark. Løsningerne skal findes via samarbejde på tværs af grænser.

Teknologirådet har sammensat en arbejdsgruppe, der har fået til opgave at identificere de it-sikkerhedsproblemer, der berører Danmark mest, men samtidig ikke kan løses effektivt nationalt. Gruppen har desuden fået til opgave at komme med løsningsforslag, som det er i Danmarks interesse at arbejde for at få gennemført på regionalt og internationalt plan.

Arbejdsgruppen består af:

- Preben Andersen, chefkonsulent i Uni-C, leder af DK-CERT.
- Brian Birkvald, Security Principal & Manager i IBM's Security Group.
- Lars Neupart, adm. direktør for Neupart A/S.
- Morten Storm Petersen, adm. direktør for Signaturgruppen A/S.
- Carsten Stenstrøm, Teknologisikkerhedschef i Danmarks Radio.
- Christian Wernberg-Tougaard, Director i Unisys, medlem af ENISA's rådgivende ekspertudvalg om "Awareness Raising".

Arbejdsgruppen, der siden april 2006 har afholdt i alt otte møder, har bl.a. hentet inspiration i resultaterne fra en Teknologirådsworkshop i april 2006 med 40 danske deltagere, der bidrog til at identificere it-sikkerhedsmæssige problemer og løsningsforslag, og i en international workshop i Teknologirådet i september 2006 med udenlandske eksperter, der leverede yderligere inspiration. Rapporten er desuden blevet drøftet på en minihøring i december 2006 med deltagelse af centrale aktører på it-sikkerhedsområdet i Danmark.

Det er Teknologirådets bestyrelse, som har valgt at gennemføre dette projekt, men da det falder ind under rådets samarbejdsaftale med Videnskabsministeriet om debatskabende aktiviteter på it-sikkerhedsområdet, er det finansieret af ministeriet.

Freelancejournalist Jakob Vedelsby har skrevet rapporten i samarbejde med arbejdsgruppen, projektleder Bjørn Bedsted og projektmedarbejdere Ben Hope og Jonas Egmose Mortensen.
Rapporten kan bestilles hos Teknologirådet eller frit downloades via Teknologirådets hjemmeside, www.tekno.dk.

Teknologirådet, januar 2007

Projektleder Bjørn Bedsted

2. Resumé af rapporten

Baggrunden for projektet

Den teknologiske udvikling betyder, at flere og flere samfundsfunktioner bliver integreret med internettet. Det gælder fx kommunikation med det offentlige, bankforretninger og køb og salg af varer. Denne udvikling øger samfundets sårbarhed over for it-kriminalitet og betyder, at dårlig it-sikkerhed, som fx software med sikkerhedshuller eller manglende beskyttelse mod vira og hackere, har stadig alvorligere konsekvenser. På grund af den globale forbundethed via internettet kommer truslerne potentielt fra hele verden.

Blandt analyseinstitutter og politimyndigheder verden over er der udbredt enighed om, at problemerne med it-kriminalitet er omfattende og i vækst. Én af forklaringerne er, at det globale internet er særdeles velegnet til kriminel aktivitet. Forbryderne skjuler sig typisk bag et netværk af computere, der er placeret i mange lande, hvilket betyder, at de internetbårne kriminelle handlinger ofte er vanskelige at efterforske og opklare. Når it-kriminalitet bliver mere og mere komplekst at have med at gøre, og når kriminelle handlinger bliver sværere at gennemskue, skyldes det også, at it-forbryderne bliver dygtigere.

På trods af et stadig alvorligere trusselsbillede er problemer med it-sikkerhed mindre belyst i både Danmark og internationalt end anden kriminalitet. Mængden af videnskabelige undersøgelser og offentligt tilgængeligt statistisk materiale om it-kriminalitet er stærkt begrænset, ligesom konkrete initiativer til forebyggelse og bekæmpelse af it-kriminalitet er præget af manglende ressourcer og fokus.

For at leve op til Danmarks officielle målsætning om at være et innovativt videns- og iværksættersamfund med global gennemslagskraft, må danske borgere og virksomheder kunne kommunikere sikkert – inden for Danmarks grænser og med omverdenen. Dette er en afgørende forudsætning for, at vi kan udnytte globaliseringens potentialer – og derved en forudsætning for Danmarks velfærd i fremtiden.

Det er derfor nødvendigt, at Danmark, EU og den øvrige verden øger indsatsen væsentligt i forhold til at forebygge og bekæmpe national og grænseoverskridende it-kriminalitet. Mange af de sikkerhedsproblemer, Danmark står over for, kan vi ikke løse nationalt. De kræver internationale løsninger.

Teknologirådets arbejdsgruppe om "It-sikkerhed på tværs af grænser" har valgt at fremlægge løsningsforslag, som går væsentligt videre end det hidtil har været kutyme i Danmark på it-sikkerhedsområdet. Arbejdsgruppen mener, at tiden er inde til konkrete, målrettede skridt i form af bl.a. international lovgivning og certificerings- og mærkningsordninger.

Arbejdsgruppen mener også, at Danmark – som det højteknologiske, videnstunge og ressourcestærke samfund landet er – bør gå foran og bane vejen for, at sådanne skridt bliver taget på europæisk og internationalt plan, hvor de kan få reel effekt.

Det vil endvidere indebære en forretningsmæssig fordel for Danmark, hvis vi tager teten. Derved kan vi øge mulighederne for at opbygge en frontposition inden for it-sikkerhedsløsninger og -koncepter, som vi kan afsætte til andre lande, når de er klar til at efterfølge det danske eksempel. Vi kan i høj grad tilføre det internationale samfund værdi på dette område, pointerer arbejdsgruppen.

Seks konkrete løsningsforslag

Arbejdsgruppen har haft som mål at udvikle og præsentere internationalt orienterede løsningsforslag på de grænseoverskridende it-sikkerhedsmæssige problemområder, gruppen anser for at være blandt de vigtigste netop nu og i de kommende år. Arbejdsgruppen har udvalgt i alt seks problemområder, som er underkastet en nærmere behandling i rapporten. Som supplement hertil tilkendegiver arbejdsgruppen undervejs holdninger på en række it-sikkerhedsrelaterede områder.

Det er målsætningen, at alle angivne løsningsforslag er praktisk realiserbare. Arbejdsgruppen anbefaler, at de foreslåede løsninger bliver igangsat hurtigst muligt og simultant på de seks problemområder. Det er endvidere arbejdsgruppens intention, at løsningsforslagene skal bidrage til at forbedre den danske og internationale it-sikkerhed, der er en forudsætning for, at borgere og virksomheder kan høste de mangesidede fordele, den digitaliserede og globaliserede verden tilbyder.

Her er en oversigt over de udvalgte problemområder, rapporten behandler, og arbejdsgruppens løsningsforslag i kort form:

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 servicer

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 servicer 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 bremset 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 be-

skytte 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 ikkeeksisterende, 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 forbundethedsanalyse, der vurderer konsekvenser ved en sikkerhedsbrist for andre områder end det, udbudet dækker.

3. English summary

Background for the project

Technological development has brought about the phenomenon of an increasing number of societal functions being integrated with the Internet; including for instance, the public sector, the banking industry, and buying and selling of goods. This trend increases society's vulnerability to cyber-crime and means that poor IT-security, as often seen in the form of software flaws or lack of protection against viruses and hackers, still has serious consequences. For this reason, global interconnectedness via the Internet increases the risk of threats coming from anywhere in the world.

Among the analysis institutes and law enforcement agencies around the world, there is a clear consensus that problems associated with cyber-crime are widespread and growing. One explanation is that the global Internet is particularly well suited for criminal activity. The culprits typically hide behind networks of computers, located in numerous countries, making Internet-borne criminal action incredibly difficult to investigate and solve. The fact that cyber-crime becomes more complex and criminal action harder to detect, also points to the fact that cyber-criminals are also becoming increasingly skilled in their trade.

Though the problems grow ever greater, IT-security issues are poorly addressed in both Denmark and internationally, in respect to other forms of crime. The amount of scientific investigations and publicly available statistics regarding cyber-crime are highly limited; just as concrete initiatives to prevent and confront cyber-crime are characterized by a lack of resources and focus.

For Denmark to meet its official goal of being an innovative knowledge and entrepreneurial society, able to punch its weight at the global level, Danish citizens and companies must be able to communicate securely; both within and beyond Denmark's borders. This is an important prerequisite for taking full-advantage of globalization's potential and hence a prerequisite for Denmark's welfare in the future.

It is therefore necessary that Denmark, the EU, and the world at large, seriously increase their efforts in preventing and fighting national and transnational cyber-crime. Many of the security problems with which Denmark stands cannot be solved nationally – they require international solutions.

A working-group on "IT-security Beyond Borders", under the auspices of the Danish Board of Technology (DBT), has developed recommendations that go significantly farther than previous efforts in the arena of IT-security in Denmark have been able to. The working group holds that it is high time to take concrete and well-aimed steps in the form of, among other things, lawmaking, certification, and labeling programs.

The working group also feels that Denmark, being the technically capable, knowledge intensive, and resource-endowed nation that it is, should go forth and pave the way for such steps to be taken on European and international level, where they can have a real effect.

This will, furthermore, actuate a competitive advantage for Denmark, should it take the reins. Through such actions, Denmark can increase the opportunity to establish itself out in front in the area of security solutions and concepts, which can then be provided to other countries should they wish to follow the

Danish model. The working group points out that Denmark could contribute greatly in this area, to the benefit of the global society.

Six concrete recommendations

The working group has sought to develop and present internationally-focused recommendations for cross-border IT-security problem areas that are seen to be among the most problematic now and in the near future.

The goal is that all of the recommendations presented should be realizable in practice. The group advises that the recommended solutions will be set in motion as soon as possible, and simultaneously in the six problem areas. It is furthermore the working group's intention that the recommendations should contribute to improving Danish and international IT-security – a prerequisite to citizens and firms being able to harvest the many benefits that a digitally-connected world has to offer.

Here is an overview of the problem areas addressed in the report and a brief description of the working group's recommendations:

1. Vulnerabilities in software and hardware

Problem: Vulnerabilities in hardware and software, such as operating systems and packaged programs is were the most serious of all IT-security problems in 2006 are, as measured in the number of instances and their consequences.

The consequences of these vulnerabilities are of greater consequence for small and medium-sized enterprises (SME's), public institutions and private citizens, rather than large firms.

Solution 1: Develop a model that ensures security updates in software are installed on the users' computers directly after a security flaw is found. The process should be imperceptible for the basic user while advanced users should be given the option to steer their own update process. Large program updates, often called 'service-packs' by some providers, would however remain installable only after user acceptance.

Solution 2: There should be EU regulation that vendors of electronic, network-based (IP based) hardware such as computers, telephones, MP3-players, alarm-systems, and in the future even refrigerators, must deliver their products with the latest firmware and software updates pre-installed.

Solution 3: Denmark/the EU should create a "white-list" for software and hardware. The public sector could then set the example and drive the market by only using white-listed IT-products.

Solution 4: A certification program for Internet Service Providers (ISPs). All ISPs in the EU are obliged to follow a code that at least meets the standard set by the Danish ISP Security forum's code of conduct. Within 3-5 years, it should be made law that all ISP's are ISO 27001-certified (or meet an equivalent thereof).

2. Inadequate knowledge of IT-security

Problem: Inadequate knowledge is a significant cause of the lack of security. The human factor is, i.a. important in relation to "phishing", identity theft and the spread of harmful programs that can "crash" a computer. This can obviously cause the loss of data from the harddisk including documents, photos, films, music, etc.; and for companies, the loss of client records and intellectual capital. The lack of IT-security knowledge is rarely an isolated problem for the firms and citizens who are ill-secured. The consequences of poor security can spread to a firm's customers, partners, etc., and the people listed in private user's address list – in total, causing exponential damage and economic loss. In light of this, it is necessary that network administrators, employees and managers prioritize security much higher than they do today. And general awareness and knowledge of the population at large should be significantly raised.

Solution 1: A greater focus on IT-security in school. The security aspect should be connected with students' use of computers throughout the course of their education.

Solution 2: Establishing "The Board for Greater IT-security" focusing on citizen awareness.
Solution 3: Regulation against "Cyber-pollution".

3. The inability to differentiate between secure and insecure products and services
Problem: An ever greater number of products and services contain an element of connectivity (Internet Protocol – IP-based) and thus it is ever more relevant to offer secure products and services to users with the aim of improving the general security level. This includes computers, mobile phones, harddisk recorders in TV's, media centers, refrigerators, and similar items in a private home. In the near future, nearly all apparati, including cars, boats and planes, will contain IP technology and be connected to the net. Security problems are expected to increase further because these products will continue to be produced around the world by numerous manufacturers, making it evermore difficult for end-users and companies to comprehend and handle the security aspect.
Solution: Denmark should take the initiative to develop a concept for labeling internet-connected products, meaning that private persons and companies are given the ability to see the security level of a given product. For example, a star-rating as in the auto-industry's "crash-test" scheme, could be implemented. The labeling program should include the entire EU, and thereafter spread to the global market.

4. The lack of concerted, transnational police efforts and prosecution in the cyber-crime arena
Problem: Cyber-crime is a difficult arena for law enforcement agencies in Denmark as well as the EU and world at large. Interpol is largely absent from the fight against IT-related crimes and Europol's roll is relatively small due to limited resources. The growing amount of cyber-crime on a global plane is fraught with inadequate police efforts. It is problematic that the prevention and investigation of cyber-crime is generally prioritized so low in comparison with other police investigations, that the sector receives few resources and therefore has an acute lack of personnel with the competency to make a change in and outside of Denmark.
Solution 1: Structuring the efforts: acknowledging cyber-crime as a new law enforcement specialization. Appointing at least one unit responsible for cyber-crime in each police district, and establishing a central authority that can address complex cases concerning cyber-crime professionally – nationally and internationally. Prioritizing cyber-crime should not come at the cost of other police activities. Rather budget increases are needed to supplement the efforts.
Solution 2: Increasing the knowledge level: Law enforcement authorities must be equipped with greater competency across the board – from the education of specialists in the various sectors of cyber-crime, to increasing the knowledge of prosecutors and judges.
Solution 3: Further development of international cooperation agreements, which can ensure more efficient and effective processing of transnational cyber-crime cases.

5. Lack of secure identification
Problem: Communication security is a prerequisite for the free flow of information, efficient eGovernment, and thus better public service in the future. Citizens' usage of the increasingly integrated economic service infrastructure in the EU and around the world, can be halted by the lack of a clear identification mechanism, nationally and across the EU. This could, i.a. minimize the risk of the abuse of personal data. One could imagine a mechanism that would eliminate the difficulties connected with the exchange of patient records between Danish and foreign hospitals. It is a national responsibility to create a digital identification that can protect citizens' personal data against, i.e. identity theft. The working group concludes that all citizens in Denmark and the EU at large, should be equipped with an identification mechanism with strong security.
Solution: Denmark should establish a long-term strategy for the further development of the existing "Digital signature" into a "citizen service passport", seen as a 'digital identity, which then helps to minimize the risks involved in eGovernment, eTrade, and other forms of electronic communication. The goal is that, in the long run, all EU citizens should have an interoperable digital ID. The working group points

to a project under development in Austria, as a source of inspiration. The Danish development work should be coordinated in relation to the entire EU, with the goal of building a secure, EU-interoperable "citizen service infrastructure", using common and open communication standards.

6. The lack of focus on IT-security in public procurement

Problem: Under 5% of the criteria found in contracts for the public procurement of IT account for security. The working group finds that IT-security is not taken seriously when the EU and its member countries take bids on infrastructure and systems contracts. It is problematic that technical specifications for IT-security and privacy in the public procurement of IT products are either lacking or non-existent, and that these contracts seldom contain a "connectedness analysis", meaning an assessment of the consequences of a security breach on all of the interconnected public units, many of which are not themselves a part of the procurement agreement.

Solution: Regulation stating that IT-security must be a key parameter in all public procurement contracts, where IT is a component. Specification sheets and bids should contain both a security and connectedness analysis that assesses the consequences of a security breach for interconnected sectors.

4. Baggrund for rapporten

4.1. Danmark på den globale arena

Ifølge regeringens globaliseringsstrategi[1] skal Danmark være et førende videnssamfund, iværksættersamfund og innovativt samfund. Danmark skal være blandt de lande i verden, hvor det er bedst at bo, leve og arbejde – også om 10 og 20 år:

"Vi skal investere i Danmarks fremtid, skabe bedre muligheder for vækst og velstand og sætte nye ambitiøse mål (...) Vi skal være et land, (...) hvor vi har et globalt udsyn og spiller en aktiv rolle i verdenssamfundet. Dansk økonomi skal være mere åben og vi skal have et stærkt samspil med andre lande og kulturer. Vi skal (...) understøtte vores samspil med virksomheder, offentlige myndigheder og borgere i andre lande."

Teknologirådets arbejdsgruppe påpeger, at en væsentlig forudsætning for, at Danmark kan realisere disse mål er, at borgere og virksomheder kan kommunikere trygt og uhindret via den globaliserede verdens "digitale motorveje". Internettet med alle dets muligheder bliver et "sted", vi i de kommende år vil tilbringe stadig mere tid – både jobmæssigt, når vi kommunikerer med offentlige instanser og i fritiden i forbindelse med dialog med venner og familie og indkøb af varer og underholdning.

Hvis man ser tilbage til 1995 og fremkomsten af de første webservere, kunne ingen dengang forudse omfanget og betydningen af internettet. I 2006 er verdenssamfundet "stakåndet" over den udvikling, der har fundet sted. Hvis man på den baggrund ser fremad mod 2015, er det umuligt at indkredse udfordringerne. Det synes dog sikkert, at internettet og de digitale muligheder og risici vil fortsætte med at vokse.

For at Danmark kan udnytte det globale, digitalt baserede handelspotentiale optimalt, er det afgørende vigtigt, at digital kommunikation via internettet er sikker, at den digitale infrastrukturs troværdighed fra ende til anden er i top og at de tilknyttede it-systemer er sikret. Tilsammen vil dette betyde, at risikoen for udefrakommende misbrug bliver minimeret – og at borgere og virksomheder derved beskyttes og beskytter sig bedst muligt mod de stadig flere forbrydere, der udøver deres kriminalitet via internettet.

For at imødekomme de voksende udfordringer på dette område er det nødvendigt, at Danmark, EU og den øvrige verden øger indsatsen væsentligt i forhold til at forebygge og bekæmpe national og grænseoverskridende it-kriminalitet.

4.2. It i alting

Internet Protocol (IP) teknologi i form af intelligente småcomputere bliver i stigende grad installeret i apparater som køleskabe, tv-apparater og komfurer, og i installationer som elmålere og tyverialarmer. I fremtiden vil flere og flere apparater kunne kommunikere med andre systemer via internettet. Det kaldes pervasive computing – allestedsnærværende it.

Biler, vaskemaskiner, airconditionanlæg og frysere er nogle af de produkter, hvor pervasive computing i nær fremtid vil kunne spille en rolle for privatpersoner. For virksomheder kan det fx være ventilationsan-

[1] "Fremgang, fornyelse og tryghed. Strategi for Danmark i den globale økonomi – de vigtigste initiativer". VK-regeringen, april 2006.

læg, belysning og produktionsanlæg, som bruger internettet til at udveksle informationer – fx tænde og slukke automatisk med henblik på at reducere strømforbruget og bruge strøm, når elprisen er lavest. En vurdering lyder,[2] at der i 2010 årligt vil blive produceret 500 millioner produkter, der kan kommunikere via Internettet.

Danmark er et af de førende lande i verden, når det gælder implementering af IP-telefoni. Dette er positivt, men indebærer samtidig et sikkerhedsproblem, da mange IP-installationer er sårbare. Det er ikke IP i sig selv, der er problemet, men vi skal sikre, at ingen kan manipulere vores IP-infrastruktur med henblik på fx at bryde ind i netværk og overtage kontrollen med IP-produkter. IP-ficeringen af samfundet, hvor it indgår i stadig flere produkter og er nervetråde i det globalt forankrede digitale servicesamfund med i dag 6,4 mia. brugere "på nettet",[3] har den konsekvens, at vi – uden at tage vores forholdsregler – bliver stadig mere sårbare over for it-kriminelle. Og at sikkerhedsaspektet får stadig større betydning i samfundet.

4.3. Grænseoverskridende it-kriminalitet

It-kriminalitet er et voksende globalt problem. 60 pct. af USA's virksomheder anser it-kriminalitet for at koste dem flere penge end fysisk kriminalitet.[4] En FBI-kilde fastslår, at it-kriminalitet nu er tredjeøverst på FBI's prioritetsliste. En rapport fra 2006[5] viser, at malware såsom vira, orme og spyware i 2005 globalt kostede virksomheder 85 mia. kr. Andre kilder nævner tal, der er henholdsvis større og mindre, hvilket indikerer, at der ikke er noget samlet overblik over problemernes omfang. Men ét er samtlige analyseinstitutter og politimyndigheder tilsyneladende enige om: Problemerne med it-kriminalitet er omfattende – og de er i vækst.

Baggrunden for væksten er, at det globale internet er særdeles velegnet til kriminel aktivitet. Forbryderne skjuler sig typisk bag et netværk af computere, der videresender kommandoer til hinanden. Man kan observere, hvor et angreb kommer fra – men man ser kun det sidste led i en kæde af computere og hele kæden er ofte umulig at optrævle. Internetrelateret kriminalitet er derfor vanskelig at efterforske.

It-båren berigelseskriminalitet er i stigende omfang organiseret – og it-forbryderne har forskellige roller. Man kan fx opdele it-forbrydere i følgende hovedtyper: Programmører, hackere, organiserede bander og mellemmænd. Programmørerne udvikler værktøjer til at angribe it-systemer med. De sælger dem til hackerne, der bruger dem til at hacke sig ind på systemer, hvor de finder værdifulde oplysninger, som de sælger til organiserede bander fra den traditionelle kriminelle underverden. De bruger oplysningerne til at svindle sig til store beløb, som de via mellemmænd får vasket hvide. Der kan naturligvis være sammenfald – fx er programmøren, hackeren og den organiserede, professionelle tyv ofte én og samme person.

Danmark mærker også konsekvenserne af utilstrækkelig it-sikkerhed. Hvidvaskning af penge via internettet, organiserede indbrud på betalingsterminaler, destruktion af e-butikker og identitetstyveri ved hjælp af "phishing"[6] er blot nogle af dem. En mulig konsekvens af phishing er, at en virksomhed ikke kan eller tør sende email til deres kunder – og at kunderne mister tilliden til virksomhedens tjenester på in-

[2] Ifølge Preben Mejer, udviklingsdirektør i TDC og direktør for Innovation Lab.
[3] Ifølge ¨World Internet Usage and Population Statistics, www.internetworldstats.com/stats.htmh.
[4] Ifølge en undersøgelse foretaget af NSA, FBI og IBM, marts 2006: "US. Businesses: Cost of Cybercrime Overtakes Physical Crime". http://www-03.ibm.com/press/us/en/pressrelease/19367.wss.
[5] The Computer Economics 2005 Malware Report: The Impact of Malicious Code Attacks. http://www.computereconomics.com/article.cfm?id=1090.
[6] Begrebet "phishing" er dannet af ordene "fishing" og "phony" (falsk) og betyder at aflure personlige identiteter/adgangskoder fx via "smarte" softwareprodukter eller falske "look a like" hjemmesider.

ternettet. En undersøgelse fra USA[7] viser, at antallet af phishing-mail og økonomiske tab som følge af phishing er vokset. Fra 2004 til 2006 er antallet af voksne personer i USA, der har modtaget en eller flere phishing-mail vokset fra 57 til 109 mio. Samtidig er tabet pr. "offer" steget fra gennemsnitlig 257 til 1.244 USD. 24,4 mio. amerikanere klikkede på en phishing-mail i 2006, mens 3,5 mio. afleverede fortrolige oplysninger til phishere. "Botnet"[8] er endnu et eksempel på it-kriminalitet, som indebærer store økonomiske gevinstmuligheder, fx via afpresning af webbutikker og lignende.

Der er talrige eksempler på, at computervira har medført enorme økonomiske tab. Den hidtil dyreste virus "Love" ødelagde tilbage i 2000 værdier globalt for anslået 52 mia. kr., mens "Mydoom" lavede skader for 34 mia. kr. Et tredje eksempel er "Zotob", der i 2005 ødelagde for fem mia. kr. globalt.[9]

En international undersøgelse viser, at 24 pct. af alle danske virksomheder har været udsat for et virusangreb i 2005, mens gennemsnittet for de 15 europæiske lande i undersøgelsen er 35 pct. Udsvinget ligger mellem 23 pct. (Belgien) og 65 pct. (Ungarn). Den samme undersøgelse viser, at 35 pct. af de danske borgere har været udsat for et virusangreb – og at gennemsnittet ligeledes ligger på 35 pct. Udsvinget er her mellem 25 pct. (Cypern) og 48 pct. (Spanien).[10]

Teknologirådets arbejdsgruppe pointerer, at der, fordi internettet er verdensomspændende og it-kriminaliteten ligeså, er brug for internationale løsninger, som kan dæmme op for kriminalitetsproblemerne og sikre en så vidt mulig uhindret global handel og kommunikation. I denne sammenhæng kan Danmark fungere som igangsætter og inspirator i forhold til at påpege vigtige grænseoverskridende problemstillinger med tilhørende løsningsforslag.

4.4. Den nuværende danske indsats mod it-kriminalitet

I en redegørelse fra Rigspolitiet fra 2006[11] fremgår det, at politiet har konstateret "en stigning i såvel it-kriminalitet som anvendelse af moderne informations- og kommunikationsteknologi i forbindelse med andre former for kriminalitet" og at "udviklingen stiller politiet over for stadig større udfordringer i den kriminalitetsbekæmpende indsats."

Supplerende kan Teknologirådets arbejdsgruppe konstatere, at it-kriminalitetsområdet bliver mere og mere komplekst og vanskeligt at have med at gøre. Mængden af it-kriminalitet vokser og de kriminelle handlinger bliver stadig sværere at gennemskue, fordi it-forbryderne bliver dygtigere. På trods heraf yder dansk politi en relativt lille indsats mod it-kriminalitet. Det er endvidere arbejdsgruppens vurdering, at politiets samlede viden og indsigt på området er meget begrænset.

Det er fx et væsentligt problem, at det i dag er yderst vanskeligt for en virksomhed eller borger at anmelde en it-kriminel handling, fordi politiet generelt mangler indsigt i, hvordan de bør håndtere en sådan anmeldelse. Dette problem er særlig stort i relation til anmeldelser, der vedrører flere politikredse eller overskrider landegrænser. I disse tilfælde er det stort set umuligt at formå politiet til at modtage en anmeldelse om it-kriminalitet.

[7] Gartner Group, november 2006.
[8] Et botnet består af et netværk af ofte tusindvis af pc'er, der uden deres ejeres vidende bruges til at udsende spam, phishing mails og andre former for angreb.
[9] Ifølge http://www.computereconomics.com/.
[10] Ifølge Eurostat, februar 2006. http://epp.eurostat.cec.eu.int.
[11] "Redegørelse for udviklingen i IT-kriminalitet samt den politimæssige indsats på området".

4.5. It-sikkerhed står i skyggen

Det er meget lidt synligt i et moderne samfund som det danske og i EU-regi, at der er problemer med it-sikkerheden. Investeringer på området og konkrete initiativer og lovgivning med henblik på at forebygge it-kriminalitet er præget af manglende ressourcer og fokus.

Det er på høje tid at gøre en indsats for at synliggøre omkostningerne ved ikke at prioritere it-sikkerhed. Dette vil kunne bidrage til, at it-sikkerhed opnår større opmærksomhed og en prioritering, der står mål med de samfundsmæssige konsekvenser af manglende it-sikkerhed.

En sammenligning af it-sikkerhed og færdselssikkerhed kan være én vej til at skabe større synlighed, fremhæver arbejdsgruppen. Danmark investerer store summer i forbedringer af trafiksikkerheden, men til sammenligning meget få midler til it-sikkerhed. Manglende it-sikkerhed kan i enkelte tilfælde være livstruende (fx på sygehuse), men har først og fremmest så store og hastigt voksende økonomiske samfundsomkostninger, at det efter arbejdsgruppens opfattelse berettiger til markant større samfundsmæssig fokus på området.

På trods af et stadig alvorligere trusselsbillede, er problemer med it-sikkerhed mindre belyst i Danmark og EU som helhed end anden kriminalitet. Mængden af videnskabelige undersøgelser og offentligt tilgængeligt statistisk materiale om it-kriminalitet er stærkt begrænset. For at kunne måle effektiviteten af initiativer på de nævne sårbarhedsområder, foreslår arbejdsgruppen, at Danmark tager initiativ til at etablere international benchmarking på området.

Samtidig er det helt afgørende, at der bliver skabt et langt mere nuanceret statistisk grundlag for, at vi i Danmark – og internationalt – kan danne os et holdbart, helhedsorienteret sikkerhedsbillede som afsæt for fremtidige it-sikkerhedsinitiativer. Et styrket statistisk grundlag vil, kombineret med international benchmarking, endvidere sikre, at eventuel tvivl om niveauet for it-sikkerhed ikke står i vejen for bl.a. internetbåren samhandel via Danmark og for, at internationale virksomheder etablerer datterselskaber i Danmark.

4.6. Dialog om it-sikkerhed

For at sikre, at oplysninger og anbefalinger i denne rapport er så internationalt opdaterede som muligt, har arbejdsgruppen løbende orienteret sig om initiativer i regi af bl.a. FBI,[12] CIA[13] og EU's it-sikkerhedsorgan ENISA.[14] Arbejdsgruppen har ligeledes fulgt det it-sikkerhedsarbejde, der finder sted i den internationale CERT-organisation.[15]

Derudover har resultaterne fra to workshops i Teknologiråds-regi influeret på arbejdet. Den første blev afholdt i april 2006[16]. Resultater herfra er indgået som idémateriale og grundlag for diskussionerne i arbejdsgruppen – og har derved haft indflydelse på de løsningsforslag, som bliver præsenteret. Den anden – en international workshop – blev afholdt i september 2006. Her havde arbejdsgruppen inviteret førende it-sikkerhedseksperter[17] fra England, USA og Østrig til at diskutere løsningsmodeller for grænseoverskridende it-sikkerhedsproblemer.

[12] FBI, Information Technology, www.fbi.gov/hq/ocio/ocio_home.htm.
[13] Directorate of Science and Technology, www.cia.gov/cia/dst/home.html.
[14] The European Network and Information Security Agency. www.enisa.eu.int.
[15] Computer Emergency Response Team (CERT) har 178 team i 35 lande. Det europæiske CERT-samarbejde består af ca. 85 repræsentanter, primært universitetsforskere. CERT er verdens eneste frivillige, velfungerede it-sikkerhedsmæssige samarbejde på tværs af grænser.
[16] Læs om workshoppen her: www.tekno.dk/subpage.php3?article=1276&survey=8&language=dk.
[17] Tylor More, David Marsh, Howard Schmidt og Reinhard Posch.

Endelig er et udkast til denne rapport blevet præsenteret for en række danske it-interessenter på en minihøring i Teknologirådet den 6. december 2006. Deltagerne bidrog med værdifulde synspunkter, men kan ikke tages til indtægt for rapportens samlede indhold.[18]

4.7. Internationale og realiserbare løsningsforslag

Dette projekts hovedformål er at udvikle og præsentere internationalt orienterede løsningsforslag på de grænseoverskridende it-sikkerhedsmæssige problemer, Teknologirådets arbejdsgruppe anser for at være blandt de vigtigste anno 2006.

Arbejdsgruppens beslutning om at gå i dybden med et problem er baseret på en vurdering af dets alvor og tyngde set i et dansk og internationalt perspektiv. Samtidig er det et væsentligt kriterium, at arbejdsgruppen vurderer, at løsningsforslaget kan gøre en forskel. Endelig har arbejdsgruppen søgt at undgå problemstillinger, som andre ekspertfora p.t. er fordybet i afklaringen af.

Arbejdsgruppen pointerer, at det har været ønsket at fremlægge løsningsforslag, som går væsentligt videre end det hidtil har været kutyme i Danmark i relation til it-sikkerhed. Tiden er inde til konkrete, målrettede skridt i form af international lovgivning og internationale certificerings- og mærkningsordninger, der for alvor kan gøre en positiv forskel. Arbejdsgruppen lægger en række steder op til, at Danmark tager teten og arbejder for at der bliver taget sådanne skridt – ikke kun i Danmark, men især på europæisk og internationalt plan.

Arbejdsgruppen er opmærksom på, at initiativerne ikke må påføre danske virksomheder unødige omkostninger og derved stille dem ringere end udenlandske konkurrenter. Det er holdningen i arbejdsgruppen, at det vil være konkurrencefremmende for danske virksomheder, hvis Danmark øger forspringet på dette område og bl.a. udvikler nye sikkerhedsløsninger, vi kan eksportere til udlandet. Det gælder EU-lande, men også den øvrige verden – ikke mindst vækstøkonomierne i Indien og Kina, som huser ca. 40 pct. af verdens befolkning. Vi kan i høj grad tilføre det globale samfund værdi på dette område, pointerer arbejdsgruppen.

Arbejdsgruppen har udvalgt de vigtigste blandt en række relevante problemstillinger og har i denne proces fravalgt flere andre. De vigtigste af de problemstillinger, arbejdsgruppen har fravalgt, fremgår af appendiksafsnittet bagerst i rapporten.

Arbejdsgruppen har i rapporten valgt at behandle følgende it-sikkerhedsmæssige problemstillinger:

- Sårbarheder i soft- og hardware.
- Utilstrækkelig viden om it-sikkerhed.
- Manglende mulighed for at skelne mellem sikre og usikre produkter og services.
- Manglende koordineret, grænseoverskridende politiindsats og retsforfølgelse på it-kriminalitetsområdet.
- Mangel på sikker identifikation.
- Manglende fokus på it-sikkerhed i offentlige it-udbud.

De seks problemområder behandles så vidt muligt ensartet. Det enkelte afsnit bliver indledt med en beskrivelse af problemet, herunder arbejdsgruppens argumentation for dets alvor. For yderligere at tydelig-

[18] Deltagerne var: Kim Aarenstrup, Dansk IT. Rådet for IT- og persondatasikkerhed; Morten Klitgaard Friis, Dansk IT. Fagrådet for IT-sikkerhed; Mette Lundberg, IT-brancheforeningens udvalg for IT-sikkerhed; Henning Mortensen, IT-sikkerhedspanelet; Karsten Østnæs Rosgaard, ITEK. Udvalget for IT-sikkerhed; Knud Kokborg, Telekommunikationsindustrien i Danmark og Michael Hald, Kommunernes Landsforening.

gøre problemet, er der placeret en "case" med et eksempel fra virkeligheden ved hver problemstilling. Herpå følger arbejdsgruppens konkrete forlag til, hvordan man med fordel kan håndtere problemet og hvilke instanser i det danske og internationale samfund, der bør tage opgaven på sig.

Arbejdsgruppen anbefaler, at de foreslåede initiativer bliver igangsat hurtigst muligt og simultant på de seks problemområder, da de supplerer hinanden og til sammen kommer rundt om det samlede problemkompleks, it-sikkerhed udgør i dag. Gruppen forventer, at løsningsforslagene fra denne rapport kan bidrage væsentligt til at forbedre den danske og internationale it-sikkerhed og derved styrke mulighederne for, at danske borgere og virksomheder kan høste fordelene ved at handle og kommunikere i den digitaliserede og globaliserende verden.

5. It-sikkerhedsmæssige problemstillinger

5.1. Sårbarheder i soft- og hardware

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 stillet lovkrav om, at alle ISP'er skal ISO27001-sikkerhedscertificeres (eller tilsvarende).

Case: Orm ramte ikke-opdaterede pc'er
Den 30. april 2004 blev pc'er over hele jorden ramt af en ny trussel: Ormen "Sasser", der fik computere til at blive ustabile, samtidig med at de udsendte massive mængder af data over internettet. I Danmark blev bl.a. TV2 og If Forsikring ramt, ligesom scanningsudstyr på Herlev Amtssygehus blev sat ud af drift som følge af angrebet. Sasser ramte udelukkende computere, der ikke havde fået installeret en sikkerhedsrettelse, der fjernede en bestemt sårbarhed. Microsoft havde udsendt sikkerhedsrettelsen den 13. april 2004 – mere end to uger før angrebene startede.[19]

Problemstilling

Arbejdsgruppen vurderer, at sårbarheder i hardware og i software som operativsystemer og programpakker er det alvorligste internationale it-sikkerhedsproblem anno 2006 målt på antal hændelser og deres konsekvenser. Antallet af opdagede sårbarheder har været stærkt stigende de senere år. I hele 2005 blev der identificeret 5.990 sårbarheder, mens der i de første tre kvartaler af 2006 allerede er konstateret 5.340.[20] Forklaringen på væksten er bl.a. det voksende forbrug af software. En privat dansk bruger har gennemsnitligt 25 forskellige softwareprogrammer på sin computer. En privat virksomhed har ca. 120, mens en offentlig virksomhed har 110 forskellige programmer.

[19] "Virusorm lukkede MR-scannere på Herlev Hospital", Ingeniøren 4. maj 2005: http://ing.dk/article/20040504/IT/105070014/-1/tema-category og "What You Should Know About Sasser", Microsoft: http://www.microsoft.com/security/incident/sasser.mspx.
[20] http://www.cert.org/stats/.

I 2001 udarbejdede en EU-arbejdsgruppe et notat om sårbarheder i hardware og software.[21] Her fremgår det, at "normalt antages det stiltiende, at prismekanismen vil sørge for, at omkostningerne ved at yde sikkerhed afbalanceres over for det konkrete sikkerhedsbehov. Mange sikkerhedsproblemer er imidlertid stadig uløste, og for andre er løsningerne længe om at slå igennem på grund af visse ufuldkommenheder på markedet." Arbejdsgruppen konstaterer, at dette i vid udstrækning stadig er situationen i 2006.

Arbejdsgruppen vurderer, at det særligt er små- og mellemstore virksomheder, offentlige institutioner og private borgere, der lider under sårbarheder i soft- og hardware. Mange store virksomheder har i dag så omfattende fokus på it-sikkerhed, at de er godt rustet til at modstå truslerne fra it-kriminelle.

Der er følgende to hovedårsager til sårbarheder i software og hardware:

- Nye sårbarheder opstår og gamle bliver ved med at bestå: Sårbarheder udspringer typisk af fejl i softwareproduktets programmering, men det er ofte et uoverkommeligt projekt for leverandøren at ændre programmeringen i senere versioner af softwareproduktet. Konsekvensen er, at mens nye sårbarheder kommer til, bliver de gamle – trods "lapning" af hullerne – ved med at husere.

- Manglende opdatering: Den næstvæsentligste årsag til sårbarheder i software er, at brugerne ofte ikke opdaterer deres programmer med de nyeste faciliteter, ligesom de ofte ikke fejlretter og "lapper" på konstaterede sårbarheder, selvom leverandøren giver besked om dette og leverer rettelser.

Dertil kommer, at der har været og igen kan opstå sårbarheder i infrastrukturkomponenter. Et eksempel er "Domain Name System" (DNS), der binder internettet sammen ved at omsætte internetadresser til såkaldte Internet Protokol (IP) adresser. Hvis en sådan komponent bliver overtaget af kriminelle, der ønsker at ændre i komponentens henvisninger, kan det fx få den konsekvens, at man som bruger bliver guidet til en falsk netbank eller webshop, hvor man kan blive franarret sine adgangsoplysninger.

Forekomsten af skadelige programmer – ofte kaldet "malware"[22] – er ligeledes i vækst. I kombination med de nævnte sårbarheder i soft- og hardware, er malware grobund for øget it-kriminalitet. Fx kan it-forbrydere, ved at udnytte, at forbrugere ikke har installeret opdateringer til allerede kendte sårbarheder, samle hele netværk af inficerede computere (Botnet), som de fx kan anvende til "ude-af-drift-angreb" – også kaldet "Denial of Service" (DoS).[23] En undersøgelse fra Nordisk Ministerråd[24] viser, at 13 pct. af de danske virksomheder blev udsat for et DoS-angreb i 2005. Den samme undersøgelse viser, at 37 pct. af danske internetbrugere og 24 pct. af de danske virksomheder i 2005 var udsat for computervirus, der resulterede i tab af informationer og/eller arbejdstid.

Konsekvenserne af sårbarheder i soft- og hardware kan spænde fra at være harmløse til at have fatale konsekvenser for borgere og virksomheder. Sårbarheder kan resultere i identitetstyveri, misbrug af identiteter, datatyveri, afbrudte transaktioner og lignende, men kan også betyde krænkelse af "privacy", tab af intellektuel kapital, kundelister, persondata, håndtering af logistik og økonomiske transaktioner. For en privat bruger kan konsekvensen fx også være identitetstyveri og røveri, og at computeren bryder ned og skal genopbygges fra bunden med nyt operativsystem og software, hvilket typisk indebærer tab af data i form af tekst, billeder, indkøbte programmer m.v.

[21] "Net- og Informationssikkerheds: Forslag til en europæisk strategi" ("com2001_0298da01.pdf").
[22] Malware er en sammentrækning af de engelske ord malicious software (ondsindet programkode) og bruges som fællesbetegnelse for computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på.
[23] Et fjendtlige angreb via internettet, hvor man nedlægger en netværksservice ved at oversvømme den med ekstremt store mængder henvendelser.
[24] Nordic Information Society Statistics: http://www.norden.org/pub/uddannelse/IT/TN2005562.pdf.

Når man som forbruger indkøber en ny computer og installerer den derhjemme, er den ofte allerede på dette tidspunkt behæftet med sårbarheder, fordi den kan have stået flere måneder på forhandlerens hylde. Og fordi forhandleren – på grund af udgifterne til at holde sig ajour med de seneste softwareversioner – ikke har brugt tilstrækkelig energi på at opdatere det styresystem og den software, som er benyttet ved præinstallationen.

For yderligere at anskueliggøre situationen, sammenligner arbejdsgruppen køb af en computer med køb af en bil: Danske forbrugere ville næppe acceptere, at en bilforhandler fraskrev sig ansvaret for den solgte bil. Det ville efterlade forbrugeren uden rettigheder. Men det er faktisk situationen anno 2006, når det gælder soft- og hardwareprodukter. Man kan ikke stille forhandlere af disse til ansvar for konsekvenser for brugerne af manglende it-sikkerhed. En forbruger, der går til forhandleren og beklager sig over sårbarheder på en nyindkøbt computer, bliver typisk henvist til at gå til producenterne af de hard- og softwareprodukter, computeren består af. Det svarer til, at man som bilejer skulle henvende til sig bilfabrikken, hvis der var problemer med airbagsystemet.

Arbejdsgruppen mener, at tiden er inde til at overveje, hvorvidt der er tale om en decideret "markedsfejl", når der er sårbarheder i hard- og software, der bliver langet over disken – eftersom det kun er brugerne, der mærker konsekvenserne af sårbarhederne og ikke de producenter og forhandlere, der har mulighed for at reducere eller i bedste fald eliminere sårbarhederne.[25]

Løsningsforslag

Løsning 1

Der skal udvikles en model, som sikrer, at sikkerhedsrettelser til software bliver installeret hos brugerne straks efter et sikkerhedshul er opdaget. Sikkerhedsopdateringerne skal ske efter et koncept, er kendt fra Microsoft[26] og Apple, der begge har indført autoopdatering. Dog med den ændring, at almindelige brugere intet skal foretage sig for at få sikret deres software. Større programopdateringer skal fortsat kun ske efter brugeraccept.

Arbejdsgruppen foreslår, at der bliver formuleret en international standard på området, som er inspireret af bl.a. Microsofts løsning og som dækker alle operativsystemer og softwareproducenter på markedet. Det skal senere være et lovkrav – mindst på EU-niveau – at alle softwareproducenter benytter standarden. En sådan standard vil også gøre det nemmere for mindre produktleverandører at tilbyde opdateringer, da de ikke behøver opfinde deres egen som Microsoft og Apple. Samtidig vil det gøre det nemmere for forhandlerne at leve op til kravet i "Løsning 2" (herunder) om at levere sikkerhedsopdaterede produkter.

Løsningsfora og Danmarks rolle: Da software oftest er udviklet uden for Danmark, kræver problemet en international løsning. EU kan være løftestang for initiativer som de nævnte. Arbejdsgruppen mener, at Videnskabsministeriet bør arbejde aktivt for, at det bliver gjort lovpligtigt for softwareproducenter på det europæiske marked at følge en opdateringsstandard, der bliver udarbejdet af branchen i samarbejde med offentlige myndigheder.

Løsning 2

Det skal være et lovkrav – mindst på EU-niveau – at forhandlere af elektronisk, IP-baseret udstyr som computere, MP3-afspillere, tyverialarmer, køleskabe m.v. kun leverer produkter med den nyeste sikkerhedsopdatering.

[25] Anderson, Ross and Moore, Tyler: "Trends in Security Economics" i ENISA Quarterly, nr. 12 2005
[26] "Microsoft Update".

For at forhandlerne ikke skal opleve dette som et uoverkommeligt krav, anbefaler arbejdsgruppen, at de får en frist på tre år til at leve op til kravet. Inden for denne periode forventer arbejdsgruppen endvidere, at det vil fremstå som en klar fordel for forhandlerne at efterleve kravet, da der er en forventning om, at forbrugerne i stigende grad vil efterspørge sikre produkter. Arbejdsgruppen forudser, at levering af sikre produkter med indbygget sikkerhedsopdatering og stor brugervenlighed bliver et afgørende konkurrenceparameter for forhandlerne fremover.

Det er endvidere arbejdsgruppens forventning, at dette krav til forhandlerne vil medføre, at de til gengæld vil stille større krav til producenterne om at sikkerhedsscreene deres produkter – og at det derfor vil fremme en udvikling, som resulterer i mere sikre produkter. Dette gælder også producenter af open source software. Arbejdsgruppen erkender dog, at det bliver vanskeligt at reducere sårbarheder i den software, brugerne henter fra mange steder i verden via internettet.

Arbejdsgruppen foreslår, at brancheforeninger for it-leverandører etablerer en standard, som kan sikre, at et givet produkt er så sikkert som muligt, når forhandleren leverer det over disken. En mulig løsning kan være, at en computer eller et andet IP-baseret produkt, når forhandleren tilslutter det til internettet, automatisk etablerer forbindelse med de forskellige softwareproducenters hjemmesider og downloader de nyeste og sikreste versioner af den software, der er præinstalleret på apparatet.

Løsningsfora og Danmarks rolle: Arbejdsgruppen understreger, at lovkravet af hensyn til konkurrencesituationen skal stilles på minimum europæisk niveau. En fremgangsmåde kunne være at nedsætte et tværministerielt udvalg (med deltagelse af Videnskabsministeriet og Økonomi- og Erhvervsministeriet) med det kommissorium at arbejde for indførelse af lovkravet på EU-niveau.

Løsning 3

Arbejdsgruppen mener, at EU bør indføre en "whitelist"-ordning for sikker soft- og hardware. Ordningen skal følge internationalt anerkendte standarder og bl.a. definere en række minimumskvalitetskrav. Arbejdsgruppen mener, at en sådan whitelist-ordning vil betyde, at soft- og hardwareproducenter får større fokus på sikkerhed. Ikke mindst fordi producenterne får et økonomisk incitament til at øge sikkerheden.

Arbejdsgruppen peger på, at EU vil kunne fremme en sådan udvikling, hvis offentlige instanser i deres it-indkøb efterspørger whitelistet soft- og hardware. Arbejdsgruppen anbefaler, at EU lader sig inspirere af det såkaldte NIAP-initiativ[27], som er iværksat af USA's regering. Det langsigtede mål med NIAP er at øge forbrugernes tillid til informationssystemer og it-netværk ved bl.a. at indføre løsninger, der sikrer systematisk afprøvning af sikkerheden. NIAP fremmer sikkerhedsevaluerede it-produkter og -systemer og sætter standarder for it-sikkerhed. NIAP har den konsekvens, at hvis den it-løsning, en given virksomhed efterspørger, findes på NIAP's liste over sikker software, må virksomheden ikke indkøbe alternativer. Det har givet konkurrence mellem producenterne om at komme på denne liste. Initiativet er hastigt ved at brede sig til private virksomheder.

Arbejdsgruppen forventer, at et løft i sikkerhedsniveau i det offentlige endvidere vil have en bieffekt i form af positiv afsmitning på sikkerhedsniveauet i det private erhvervsliv.

Løsningsfora og Danmarks rolle: En mulig fremgangsmåde er at etablere en fælleseuropæisk whitelist i regi af et software "blåstemplingsorgan" – og at det er op til Videnskabsministeriet at tage initiativ til gennemførslen af dette. Det kunne være en "EU information assurance software procurement task force", der kan stille skrappere krav til sikkerhed. Organisationen skal være ubureaukratisk og uvildig – fx inspireret af neden for nævnte Communications-Electronics Security Group (CESG[28]). Kravene skal være tilpas

[27] The National Information Assurance Partnership: http://niap.bahialab.com/.
[28] CESG er "National Technical Authority for Information Assurance" for den engelske regering: www.cesg.gov.uk.

høje og godkendelsesprocessen skal til enhver tid afspejle nutidige it-sikkerhedskrav, men må ikke være markedsforvridende. Arbejdsgruppen påpeger, at små og mellemstore soft- og hardwareproducenter skal tilbydes hjælp til at få deres produkter testet, så dette ikke bliver for stor en økonomisk belastning for virksomhederne. Arbejdsgruppen foreslår, at man generelt på dette område lader sig inspirere af den internationale typegodkendelse, der i dag er gældende for bl.a. mobiltelefoner.[29]

Arbejdsgruppen ønsker en uafhængig instans, der kan sikre information assurance. Engelske CESG er som nævnt et eksempel på en tredjepartsinstans, der kan vurdere sikkerhedsniveauet – og fx verificere effektiviteten af en kryptering og om en given virksomhed på den baggrund er optimalt beskyttet mod fx industrispionage. CESG promoverer blandt andet standarderne ITSEC & Common Criteria. Flere leverandører kritiserer disse godkendelsesprocesser for at være langsomme, dyre og for ikke at give reel vished ("assurance"). Disse problemer kan undgås i en nykonstrueret løsning, hvis leverandørerne involveres i godkendelseskriterier, som det fx foregår i amerikanske ICSAlabs,[30] der drives af virksomheden Cybertrust.

Løsning 4

I dag kan enhver frit etablere sig som Internet Service Provider (ISP) i Europa – og der kommer stadig flere nye ISP'er til. Den udvikling øger behovet for internationale/fælleseuropæiske regler på området.

Arbejdsgruppen mener, man bør fastlægge et sæt internationale sikkerhedsstandarder for ISP'er – fx via en best practise såsom ISO17799 (BS7799) og en certificering såsom ISO27001 eller tilsvarende. Der findes adskillige andre certificeringsmuligheder, som kan anvendes. Arbejdsgruppen mener, man bør udvikle én fælles certificeringsmodel, som alle ISP'er skal leve op til.

Arbejdsgruppen foreslår en løsning i to tempi:

- Første skridt er, at alle ISP'er i EU bliver pålagt at leve op til en kodeks, der mindst svarer til det danske ISP Sikkerhedsforums Adfærdskodeks.[31]
- Næste skridt er, at der inden for 3-5 år bliver stillet lovkrav om, at alle ISP'er skal ISO27001-sikkerhedscertificeres (eller tilsvarende).

Løsningsfora og Danmarks rolle: Danmark bør gå foran og bringe forslag om lovkrav til ISP'er op på EU- og internationalt plan.

[29] 3GPP: http://www.3gpp.org
[30] ICSAlabs: http://www.icsalabs.com/.
[31] Se www.isp-sikkerhedsforum.dk.

5.2. Utilstrækkelig viden om it-sikkerhed

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".

Case: Succes for primitiv orm
Uvidenhed om it-sikkerhed kan resultere i, at selv meget simple trusler får stor udbredelse – det vidner ormen "Alcans" succes om. Den er et primitivt program, der spreder sig via populære fildelingsprogrammer, hvor den lægger sig som en fil med et tillokkende navn – fx navnet på et populært softwareprogram. Brugerne af fildelingsprogrammet tror, der er tale om en piratkopi af et program, de gerne vil have fat i. De henter filen og kører den – og så er deres pc inficeret med Alcan, der kan forhindre computeren i at fungere og/eller inficere den med anden malware. Hvis brugerne kørte en virustest eller i øvrigt behandlede filer fra nettet med varsomhed, ville de ikke blive ramt. Men i februar 2006 var Alcan det mest udbredte, skadelige program. I alt 250.000 pc'er fordelt over hele verden var på dette tidspunkt ramt af den primitive orm.[32]

Problemstilling

Utilstrækkelig viden har en stor del af "æren" for manglende sikkerhed – og er derved ofte årsag til phishing, identitetstyveri og at computeren "går ned" på grund af virus. Det kan resultere i tab af alt, hvad der ligger på harddisken af fx tekst, billeder, film, musik, softwareprogrammer og arbejdspladsrelateret information.

Arbejdsgruppen finder det dog urimeligt at lægge for stort et ansvar for sikkerheden over på it-brugerne. Derfor rummer denne rapport fem yderligere fokusområder ud over "Utilstrækkelig viden om it-sikkerhed" – og flere løsningsforslag retter sig mod at gøre livet lettere for brugerne. Men det er ikke muligt at beskytte brugerne i tilstrækkelig grad, og arbejdsgruppen pointerer derfor nødvendigheden af, at både 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.

Arbejdsgruppen konstaterer, at store virksomheder meget ofte har styr på sikkerheden, mens små og mellemstore virksomheder oftere har sikkerhedsproblemer. De private brugere er det helt store problem, hvilket potentielt smitter negativt af på sikkerheden på landets arbejdspladser, da mange private brugere er forbundet til it-systemerne på deres arbejdsplads via en medarbejder-pc i hjemmet.

Arbejdsgruppen mener, at det er et reelt it-sikkerhedsmæssigt problem, at brugerne ikke har tilstrækkelig viden om it-sikkerhed – og at især små og mellemstore virksomheder generelt ikke har tilstrækkelig fokus på uddannelsesområdet i relation til it-sikkerhed. Problemet rammer ikke alene den virksomhed,

[32] Microsoft, "News on Alcan, Mywife.E" fra Microsofts Anti-Malware Engineering Teams blog: http://blogs.technet.com/antimalware/archive/2006/04/03/424113.aspx.

som ikke beskytter sig godt nok. Konsekvenserne af manglende sikkerhed kan sprede sig til virksomhedens kunder, samarbejdspartnere etc. og forvolde skade og økonomiske tab her.

Sikkerhedsproblemerne er således ikke isoleret til det land, hvor virksomheden med den manglende sikkerhed ligger, men kan hurtigt sprede sig som ringe i vandet. De følgende løsningsforslag sigter derfor på at frembringe en passende it-sikkerhedskultur.

Løsningsforslag

Løsning 1

Arbejdsgruppen finder det absolut nødvendigt, at undervisning i it-sikkerhed bliver en obligatorisk del af læseplanen i folkeskolen – ikke som et decideret fag eller på bekostning af eksisterende undervisning, men som et element i form af fx et kursus et eller flere gange i skoleforløbet. Også skolefritidsordninger m.v. kan med fordel beskæftige sig med it-sikkerhed.

Arbejdsgruppen vurderer, at skolelærernes generelle kompetenceniveau på området ikke har et niveau, som er tilstrækkelig højt til, at man kan forvente, at de kan varetage et sådant kursus. Derfor vil det sandsynligvis blive nødvendigt at trække på eksterne vidensressourcer – på samme måde, som man i dag trækker på politiet til undervisning i færdselssikkerhed.

Arbejdsgruppen er bekendt med, at der bl.a. i forbindelse med "Netsikker Nu"[33] initiativet er produceret omfattende materialer til bl.a. folkeskolesegmentet. Dette kan eventuelt indgå som inspiration i forhold til de foreslåede, obligatoriske kursusforløb.

I relation til lærernes kompetenceniveau, foreslår arbejdsgruppen to initiativer: It-sikkerhedsaspektet bliver integreret i det obligatoriske pc-kørekort for lærere. Det vil øge lærernes opmærksomhed på it-sikkerhed og kan måske betyde, at de selv vil kunne varetage it-sikkerhedsundervisningen. Som et andet initiativ foreslår arbejdsgruppen, at it-sikkerhed fremover indgår som et obligatorisk ugekursus på lærerseminarerne.

Arbejdsgruppen tilføjer, at it-sikkerhed generelt bør have en større forankring i hele uddannelsessektoren. Også på universiteter og højere læreanstalter bør det være et lovkrav, at it-sikkerhed indgår i uddannelserne.

Løsningsfora og Danmarks rolle: Undervisningsministeriet bør foranledige den foreslåede udvikling i Danmark og arbejde for en tilsvarende udvikling i hele EU. Ministeriet bør iværksætte en systematisk erfaringsudvikling med andre lande.

Løsning 2

Arbejdsgruppen anbefaler, at der bliver etableret et "Rådet for større it-sikkerhed" med et selvstændigt sekretariat og autonomi til at gøre en forskel og sætte dagsordenen – bl.a. via effektiv folkeoplysning. Arbejdsgruppen mener, at et sådant råd primært skal fokusere på it-sikkerhed i forhold til borgerne. Rådet skal efter arbejdsgruppens mening bl.a. påtage sig at oplyse borgerne om mærkningsordninger i forhold til it-sikkerhed, vigtigheden af at opdatere software med sikkerhedsrettelser, anbefale software med brugervenlige sikkerhedsfunktioner m.v.

[33] www.netsikkernu.dk.

Arbejdsgruppen foreslår, at rådet modtager sin hovedbevilling fra Finansloven, men at rådet fremstår som et offentligt/privat partnerskab, hvor der også medvirker eksterne interessenter/investorer. Det er afgørende, at rådet ikke kan blive nedlagt som følge af "nye politiske vinde", men at kontinuiteten er garanteret. Det lange træk er vigtigt for at opbygge og fastholde fokus på it-sikkerhed, understreger arbejdsgruppen. Rådet kunne blive et eksempel til efterfølgelse i andre lande og bør bidrage til erfaringsudveksling på tværs af grænser.

Løsningsfora og Danmarks rolle: Politikerne opfordres til at bevilge penge på Finansloven til oprettelsen af det foreslåede råd.

Løsning 3

Arbejdsgruppen anbefaler at give virksomhederne et økonomisk incitament til at prioritere it-sikkerhed. I den sammenhæng foreslår arbejdsgruppen brug af en "forureningsanalogi", hvor virksomheden anspores til at tage initiativer, som gør, at de undgår at sprede it-forurening som følge af manglende it-sikkerhed.

Arbejdsgruppen mener, at lovgivning først er en mulighed, når befolkningen generelt er velinformeret om de sikkerhedsmæssige problemstillinger og der er opbygget en sikkerhedskultur i samfundet. Men arbejdsgruppens holdning er, at lovgivning derefter er nødvendig – og at man i den forbindelse med fordel kan trække på erfaringer fra eksisterende lovgivning i forhold til fx forurening og arbejdsmiljø. På disse områder er der først sket et gennembrud i forlængelse af lovgivning, fx i forhold til forurening, der ødelægger ozonlaget.

Miljøforurening er også grænseoverskridende og et initiativ som Kyoto-processen er international. Lovgivning på området skal indebære en mulighed for sanktioner mod virksomheder, der sjusker med it-sikkerheden – fx bøder. Disse sanktioner behøver ikke forudsætte, at der er en skadeslidt, men skal kunne tildeles, hvis virksomheden ikke lever op til lovgivningens sikkerhedskrav, mener arbejdsgruppen.

Løsningsfora og Danmarks rolle: Arbejdsgruppen anbefaler, at Justitsministeriet i samarbejde med andre relevante ministerier og EU begynder at udforske mulighederne for på sigt at holde virksomheder og individer ansvarlige for it-forurening.

5.3. Manglende mulighed for at skelne mellem sikre og usikre produkter og servicer

Løsning: Danmark udvikler et koncept for mærkning af produkter og servicer, der er forbundet med internettet – fx computere, computerprogrammer, tv, husholdningsapparater, telefoner, biler m.v. – som betyder, at privatpersoner og virksomheder får vished om sikkerhedsniveauet. Man kan fx benytte mærkning med stjerner som i bilverdenens "crashtest-ordning". Mærkningsordningen skal dække hele EU og på længere sigt det globale marked.

Case: Usikker medarbejder-pc
Regeringen gav mulighed for en medarbejder-pc-ordning med henblik på at fremme den digitale udvikling i Danmark. Diverse leverandører stillede op med hver deres pakkeløsning med pc, programmer, printer, router m.v. – fx solgte TDC en pakkeløsning med en pc, software, trådløs router og en sikkerhedspakke med antivirus, personlig firewall, spamfilter m.v. Den generelle opfattelse hos brugerne var, at de var sikkerhedsmæssigt dækket ind via denne løsning. Det viste sig imidlertid, at den trådløse router ikke var sikkerhedsmæssigt konfigureret og at brugerne derfor var totalt ubeskyttede. Dette kunne være undgået med en mærkningsordning.

Problemstilling

Det er arbejdsgruppens opfattelse, at almindelige forbrugere generelt ikke kan gennemskue de sikkerhedsrelaterede konsekvenser af at købe og bruge produkter og servicer med it-indhold. Når brugerne ikke kan se forskel på sikre og usikre produkter og servicer, vil de ofte vælge den billigste løsning – uanset at denne måske er langt mere usikker end den lidt dyrere løsning.

Problemet er særlig stort i forhold til computere. Forbrugerne kan som nævnt ikke se, hvor sikker/usikker en computers software er, når de står i købssituationen i butikken. I dag er sikkerheden i en computers "image" – det operativsystem og de programmer, computeren leveres med – ofte relativt ringe. For når brugeren ikke kan se forskel, er der intet incitament til at vælge produkter, der er sikrere end andre, og kunden vil typisk vælge den billigste (og mindst sikre) løsning. Efter købet må forbrugeren selv i gang med opdateringer og installation af sikkerhedsprogrammer. Arbejdsgruppen vurderer, at sikkerhed – hvis den er synlig for forbrugeren – i fremtiden kan blive en væsentlig konkurrenceparameter.

For andre produkter med it-indhold er sikkerhedsproblemerne endnu ikke markante. De er dog voksende i relation til bl.a. mobiltelefoni, hvor virusproblematikker er begyndt at dukke op. Lignende problemer vil sandsynligvis vise sig i forhold til bl.a. harddiskoptagere til tv, mediacentre og lignende centrale styringscomputere i private hjem.[34] I fremtiden vil stort set alle "apparater" – fra køleskabe og mikroovne til biler, både og fly – indeholde Internet Protocol (IP) teknologi og være tilsluttet internettet. Det kaldes pervasive computing – allestedsnærværende IT.[35]

[34] Se bl.a. www.detdigitalehjem.dk.
[35] Læs mere om pervasive computing i afsnitg 4.2.

Der er som nævnt mange sikkerhedsproblemer i dag – og der vil komme mange flere i fremtiden, bl.a. fordi produkterne i stigende grad kommer fra hele verden og fra mange forskellige producenter, hvilket vil gøre det stadig vanskelige for forbrugere og virksomheder at gennemskue sikkerheden.

Arbejdsgruppen konstaterer endvidere, at Danmark er et af de førende lande i verden, når det gælder implementering af IP-telefoni. Dette er positivt, men indebærer samtidig et sikkerhedsproblem, da mange IP-installationer er sårbare. Det er ikke IP i sig selv, der er problemet, men vi skal sikre, at ingen kan manipulere vores IP-infrastruktur med henblik på fx at bryde ind i netværk og overtage kontrollen med IP-produkter. Udfordringen er at sætte håndteringen af de nye usikkerheder bedre i system og fremtidssikre den teknologiske udvikling, mener arbejdsgruppen.

Løsningsforslag

Arbejdsgruppen vurderer, at der er et stort behov for at udvikle og indføre en mærkningsordning, hvormed man kan vise brugerne forskellen mellem sikkerhedsmæssigt gode og dårlige produkter. Fordelene ved en mærkningsordning vil være størst for private brugere og små og mellemstore virksomheder, der ved hjælp af ordningen får sikkerhed for, at IP-baserede produkter lever op til et bestemt sikkerhedsniveau. Store virksomheder kan også have gavn af en mærkningsordning, men for dem handler øget it-sikkerhed i endnu højere grad om at sikre kommunikationsprocesserne internt i virksomheden og med omverdenen, vurderer arbejdsgruppen.

Arbejdsgruppen pointerer, at det skal være en international mærkningsordning – i første omgang i EU-regi – da en national mærkningsordning vil blive opfattet som en teknisk handelshindring. En mærkningsordning skal udelukkende omfatte nye produkter og skal dække både hele computerpakker (med både soft- og hardware), separate softwareprodukter og øvrige produkter, der indeholder IP-teknologi. Arbejdsgruppen foreslår at indføre to mærkninger:

- Et "nysynet-mærke", som indikerer, at produktet er klar til internetbrug – og at sikkerhedsopdatering er inkluderet i en aftalt årrække.
- Et "købt som beset-mærke", som indikerer, at her skal forbrugeren selv i gang med "skruenøglen".

Tilsvarende kunne man på biblioteker, skoler, internetcafeer m.v. anvende et "Netsikker-mærke", som angiver, at her har ejeren ansvar for et veldefineret sikkerhedsniveau, som gør computeren velegnet til digital forvaltning, netbank m.v., og et "Legeplads-mærke", som angiver, at man her må regne med virus og usikkerhed.

Arbejdsgruppen fremhæver, at man desuden kan hente inspiration til den foreslåede it-sikkerhedsmærkningsordning i den eksisterende, internationale crashtest-ordning i bilindustrien, hvor biler tildeles fra 0 til 5 stjerner alt efter deres sikkerhedsniveau. Arbejdsgruppen mener, man bør definere en række sikkerhedskriterier, som det enkelte it-produkt skal leve op til. Jo flere af sikkerhedskriterierne produktet lever op til, des flere "stjerner" tildeles det.

En anden mulighed er at lade sig inspirere af den eksisterende energimærkning af hvidevarer. Det er bl.a. en erfaring herfra, at energimærkning giver industrien et incitament til at udvikle flere lavenergiprodukter. Arbejdsgruppen forudser, at en it-sikkerhedsmærkningsordning på tilsvarende vis vil give it-producenter et incitament til at udvikle sikrere produkter og gøre sikkerhed til en konkurrencemæssig fordel.

Arbejdsgruppen mener, at den uvildige instans, der skal stå for it-mærkningsordningen, også skal stå for at formulere de omtalte sikkerhedskriterier – og at man skal basere disse på et videnskabeligt grundlag. En mulighed kan være at invitere førende forskere i EU til at komme med bud på disse sikkerhedskriterier.

Løsningsfora og Danmarks rolle: Forbrugerministeriet tager initiativ til sammensætning af en arbejdsgruppe med deltagelse af it-producenter, it-eksperter, brancheorganisationer og forbrugere, der udarbejder forslag til en mærkningsordning, som kan fungere i EU. Dette bliver præsenteret for EU og kan forhåbentlig inspirere til udvikling af en EU-mærkningsordning. Herefter opfordres EU til at gå i dialog med World Trade Organization (WTO) med henblik på udvikling af en global mærkningsordning.

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

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.

Case: Falske hjemmesider gav høje telefonregninger
Omkring nytår 2005 oprettede selskaber i Panama og Hongkong over 200 danske domænenavne, der til forveksling lignede den ægte vare. Det var fx domænet "nyhedertv2.dk" (den rigtige hjemmeside har adressen "nyheder.tv2.dk"). Hvis man gik ind på det falske domæne med en sårbar computer, blev der installeret skadelig software, som fik computeren til at ringe op til dyre telefonnumre, så ejeren fik en høj telefonregning. Pengene blev indkasseret af opretteren af det falske domæne. Affæren førte aldrig til retssag og domfældelse, da de mange internationale forbindelser gjorde den vanskelig at efterforske.[36]

Problemstilling

Mens politimæssige tiltag i forhold til globale problemstillinger som børnepornografi og narkohandel er sat i system og fungerer med relativ stor effekt, er aktivitetsniveauet anno 2006 i relation til forebyggelse, efterforskning og retsforfølgelse af it-kriminalitet i Danmark, EU og den øvrige verden særdeles lavt. Udfordringen er at opnå en tilsvarende effektivitet på it-kriminalitetsområdet.

Arbejdsgruppen finder det problematisk, at der i dag bliver brugt relativt få ressourcer på at forebygge it-kriminalitet og på at fange it-forbrydere, hvorimod der bruges enorme ressourcer på at fremme it-sikkerhed ved indkøb af sikkerhedssoftware. Der bør være en bedre balance mellem forebyggelse og "helbredelse", mener arbejdsgruppen, der ligeledes finder det problematisk, at politiet ikke afsætter dedikerede ressourcer i et særskilt budget til forebyggelse og bekæmpelse af it-kriminalitet. Med den nye politikredsreform[37] er det den enkelte politimester, som skal afsætte midler ud af den samlede pulje til politikredsen til it-kriminalitet. Arbejdsgruppen frygter, at dette vil betyde en yderligere nedprioritering af it-sikkerhedsområdet.

[36] Artikler i Computerworld fra 2005, bl.a. "TV2 misbruges til svindel på nettet" af Dorte Toft, 28. januar 2005.
[37] Politikredsreformen trådte i kraft 1. januar 2007.

Arbejdsgruppen mener, at dansk politis begrænsede indsats i relation til it-kriminalitet primært kan henføres til manglende kendskab til efterforskningen i disse sager. Politiet er ikke gearet til at håndtere international it-kriminalitet og har få muligheder for at efterforske sagerne, der typisk er meget teknisk betonede og bliver gennemført ved hjælp af it-udstyr, der er placeret i ind- og udland. Og da sporene ofte er flygtige og indsamling af nye spor vanskelig eller umulig, bliver anmeldelser af it-kriminalitet nedprioriteret eller ligefrem afvist med begrundelse i ressource- eller kompetencesituationen i politikredsen. Resultatet er, at det i dag stort set er risikofrit at begå it-kriminalitet. Forbryderne bliver så godt som aldrig fanget.

Arbejdsgruppen vurderer, at det bl.a. er et problem, at man skal anmelde fx misbrug af netbanker, kreditkort og lignende handlinger – ofte iværksat af internationale it-bander – i den lokale politikreds. Her skal sagerne efterforskes parallelt med, at politiet skal håndtere cykeltyverier og indbrud. I nogle tilfælde kan man tilkalde assistance fra IT-Efterforskningscentret (NITEC) under Rigspolitiet, som dog typisk kun kan hjælpe med teknik og sjældent efterforsker selv.[38] Det betyder, at en menig politimand kan stå med en opgave, som går ud på at optrevle en hollandsk baseret nigeriansk svindlerbande, der har lænset danskeres visakort.

Det bliver løbende fremhævet, at dansk politi samarbejder med andre landes myndigheder om opklaring af it-kriminalitet. Dette stemmer dog ikke overens med, at proceduren er, at it-kriminalitet begået via udenlandske Internet Protocol (IP) numre, skal anmeldes i det land, hvor det pågældende nummer er registreret, hvilket godt kan være i Danmark, selvom nummeret er udenlandsk. Den samme tendens ses internationalt i forhold til behandling af anmeldelser, hvis "gerningsstedet" er i et andet land.

It-kriminalitet er hyppigt grænseoverskridende, hvilket nødvendiggør internationale løsninger. Men politiefterforskning på tværs af grænser vanskeliggøres bl.a. ved, at it-forbrydere ofte har held til at skjule deres identitet. Det er denne hændelse fra 2004 et eksempel på: Et ægtepar fra Korsør blev arresteret af dansk politi efter at de amerikanske myndigheder havde sporet et virusangreb mod et vekselerfirma i USA – formodentlig med det formål at pengeafpresse firmaet – til deres computer. Det viste sig, at ægteparrets computer på grund af manglende sikkerhed var overtaget og blev "fjernstyret" af ukendte gerningsmænd via internettet.

It-kriminalitet har vist sig at være et vanskeligt arbejdsområde for politiet i Danmark, 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 politiindsats, mener arbejdsgruppen, der finder det særdeles problematisk, at forebyggelse og efterforskning af it-kriminalitet generelt er nedprioriteret i forhold til anden politimæssig efterforskning, og at området bliver tildelt så få ressourcer som tilfældet er – og at der derfor er akut mangel på personale med kompetencer på området både herhjemme og internationalt.

Det er ikke mindst problematisk, at virksomheder og borgere ikke kan anmelde it-kriminalitet til kompetente myndigheder – og at dommere generelt ikke har tilstrækkelig viden på området til at dømme i it-sager. Arbejdsgruppen mener, at den relativt lave prioritering af it-kriminalitet først og fremmest skyldes manglende politisk forståelse af it-kriminalitetens natur – at it ikke er begrænset til en bestemt fysisk lokalitet, men åbner virtuelle adgange til kriminalitet.

Arbejdsgruppen mener grundlæggende, det er nødvendigt, at politikerne i Danmark, EU og den øvrige verden erkender problemets omfang og grænseoverskridende karakter. Den konkrete operationalisering

[38] Hovedparten af NITEC's ressourcer anvendes til såkaldt "bevissikring" af indholdet på beslaglagte computere, mens der bruges relativt få ressourcer på at gøre en målrettet indsats i forhold til opfølgning på og efterforskning af anmeldelser af it-kriminalitet af dansk eller udenlandsk oprindelse.

af indsatsen mod it-kriminalitet kan herefter tage ved lære af de strategier og metoder, politiet anvender med henblik på at opdage og eliminere børnepornografi på nettet.

Arbejdsgruppen pointerer, at den øgede politimæssige indsats på it-kriminalitetsområdet, der anbefales i det følgende, ikke må ske på bekostning af politiets håndtering af anden kriminalitet. I betragtning af, at it-kriminalitet er et relativt nyt og hurtigt voksende problem, bør politiet modtage yderligere ressourcer til dette område.

Løsningsforslag

Løsning 1

Arbejdsgruppen foreslår, at man i hver af de nye store politikredse udnævner mindst én person med indsigt i området, så virksomheder og borgerne har den fundamentale retssikkerhed, at de kan få hjælp, hvis de bliver udsat for it-kriminalitet. Samtidig etableres en central myndighed på området på linie med "Statsadvokaturen for Særlig Økonomisk Kriminalitet"[39] – og it-kriminalitetsområdet bliver anerkendt som et politispeciale, der kræver en særlig og central indsats.

Det er afgørende, at denne centrale myndighed kan arbejde på tværs af politikredsgrænserne uden skelen til jurisdiktioner. Ved at samle indsatsen ét sted, vil man endvidere opnå større erfaringsoprustning i forhold til håndtering af dette komplekse kriminalitetsområde. Samtidig bliver det nemmere at etablere samarbejde på tværs af landegrænser. En central myndighed skal i et vist omfang samarbejde med politikredsene i Danmark. Ikke mindst skal myndigheden være rådgivende for de nye større politikredse i mindre og efterhånden rutinemæssige sager om it-kriminalitet.

Tanken er, at den centrale enhed tager sig af den komplekse it-kriminalitet, mens de lokale it-eksperter i politikredsene håndterer de mere dagligdags problemstillinger – og i øvrigt fungerer som bindeled mellem politikredsene og den centrale it-enhed. En styrket national indsats skal ledsages af krav om en øget international, koordineret indsats via Europol og muligvis Interpol.

Arbejdsgruppen forslår, at politiet fremover også prioriterer en fremgangsmåde i forhold til mindre it-kriminelle forseelser, som resulterer i hurtig sagsbehandling og domfældelse. Arbejdsgruppen mener, man bør lade sig inspirere af behandlingen af fx det at køre for hurtigt i trafikken. Her registrerer politiet en ulovlig handling og kan på baggrund af gældende love og regler hurtigt udstede en bøde – uden typisk at interessere sig yderligere for den pågældende lovovertræder. En sådan strategi i forhold til mindre it-kriminelle forseelser kan sikre, at der kommer flere sager "over disken", og at der endvidere kommer større politimæssig fokus på it-kriminalitet, hvilket vil have en præventiv effekt.

Arbejdsgruppen fremhæver samtidig nødvendigheden af, at Europol ansætter specialister, der kan koordinere indsatsen mellem medlemslandene og den øvrige verden i forhold til den globale, grænseoverskridende it-kriminalitet.

Arbejdsgruppen foreslår endvidere, at der bliver etableret et samarbejde mellem de centrale politimæssige myndigheder og de lokale CERT-enheder og ISP'er. Man bør også etablere en uafhængig CERT-enhed i hvert land, som koordinerer sikkerhedshændelser i landet.

Løsningsfora og Danmarks rolle: De foreslåede nationale initiativer bliver igangsat af Justitsministeriet i Danmark, der bør gå foran med krav om en markant opprioritering af efterforskning af it-kriminalitet.

[39] Også kaldet "Bagmandspolitiet".

Herefter agerer Danmark inspirationskilde for EU. Det er arbejdsgruppens holdning, at hvert land i EU bør etablere en central, national enhed, der koordinerer indsatsen mod it-kriminalitet i landet og i forhold til udlandet. Da megen it-kriminalitet er grænseoverskridende, skal enheden samarbejde med de tilsvarende enheder i de øvrige EU-lande. Koordination af samarbejdet – i EU og mellem EU og den øvrige verden – kan ske via det europæiske politisamarbejde Europol. Gruppen opfordrer desuden Justitsministeriet til at arbejde for en markant forøgelse af Europols og Interpols indsats i forhold til it-kriminalitet.

Løsning 2

Arbejdsgruppen mener, at alle lande bør uddanne specialister i politiet på diverse it-kriminalitetsområder (hacking, phishing osv.), så den nødvendige kompetence til internationalt samarbejde om bekæmpelse af it-kriminalitet er til stede. Politiet skal også trænes i kriminalteknisk analyse af computere.

Arbejdsgruppen er opmærksom på, at et sådant initiativ sandsynligvis vil medføre, at politiet bliver en rekrutteringsbase for it-sikkerhedsfolk til det omgivende samfund, fordi behovet for disse kompetencer er særdeles omfattende. Det er derfor en forudsætning, at it-sikkerhedseksperter inden for politiet bliver tilbudt konkurrencedygtige ansættelsesforhold.

Arbejdsgruppen fremhæver, at politiet via en intensiveret kriminalpræventiv indsats skal bidrage til at styrke it-sikkerheden i offentlige og private virksomheder i Danmark – og at der derfor er behov for en styrkelse af det kriminalpræventive arbejde.

Samtidig finder arbejdsgruppen det problematisk, at anklagemyndighedens vidensniveau generelt er lavt på it-kriminalitetsområdet. Derfor skal man ruste anklagemyndigheden i det enkelte land kompetencemæssigt til at behandle it-kriminalitet, herunder at omsætte indholdet i de kriminelle forhold til noget, som dommerinstitutionen forstår, kan forholde sig til og dømme ud fra.

Løsningsfora og Danmarks rolle: Arbejdsgruppen vurderer, at Europol har ansvar for at koordinere en fælleseuropæisk indsats i relation til at løfte kompetenceniveauet hos anklagemyndighed og dommere. Arbejdsgruppen anbefaler, at Justitsministeriet i Danmark fremfører problemet over for Europol. Det anbefales endvidere, at Justitsministeriet tager initiativ til at løfte politiets videns- og kompetenceniveau markant.

Løsning 3

Der eksisterer flere aftaler om politimæssigt samarbejde om efterforskning af it-kriminalitet på tværs af grænser både internationalt og i EU. Arbejdsgruppen vurderer, at disse – især de internationale - ikke fungerer efter hensigten. På trods af eksisterende samarbejdsaftaler er det svært at få udenlandsk politi til at afsætte ressourcer til samarbejde om efterforskning i konkrete sager. Der er derfor behov for at revitalisere det internationale samarbejde. Ét af mange redskaber i denne sammenhæng kunne være at etablere en ekstra sikker, international hjemmeside, hvor nationale enheder kan placere og se hinandens data. Man kunne i første omgang etablere en sådan hjemmeside på EU-niveau, men der er ingen tvivl om, at et bredere, internationalt samarbejde er nødvendigt.

Et andet konkret forslag til grænseoverskridende samarbejde er, at enhver it-bruger opfordres til at melde det til sin ISP, når vedkommende bliver ramt af en ulovlig hændelse – fx et virusangreb. Dette skal kunne ske anonymt. ISP'erne skal opfordres til efterfølgende at lukke ned for det IP-nummer, hvorfra angrebet udspringer – og sprede viden om dette IP-nummer og angrebet til de øvrige ISP-leverandører via et nationalt/internationalt ISP Sikkerhedsforum i stil med det danske.[40]

[40] Se www.isp-sikkerhedsforum.dk.

Løsningsfora og Danmarks rolle: Justitsministeriet opfordres til at undersøge, hvorfor de eksisterende samarbejdsaftaler ikke fungerer efter hensigten. Det næste skridt kan være at udbygge EU's agentur for it-sikkerhed (ENISA), som kan stå for håndhævelsen af internationale samarbejdsinitiativer, koordinere samarbejdet, samle erfaringer og komme med nye tiltag på området. Agenturet kan med fordel suppleres med et tilsvarende organ i FN-regi – og Justitsministeriet opfordres til at undersøge mulighederne for dette. Ministeriet opfordres endvidere til at arbejde for at få G8 til at sætte det internationale samarbejde om it-kriminalitet på dagsordenen.

5.5. Mangel på sikker identifikation

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.

Case: En forudsætning for arbejdskraftens frie bevægelighed
Med indførelse af arbejdskraftens frie bevægelighed i EU er der opstået et behov for, at virksomheder og borgere fra andre lande i en kortere periode kan bo og fungere på linie med en nationalstats borgere – fx i forhold til landets digitale løsninger til forvaltning og sundhed. Et interoperabelt, elektronisk identitetssystem er grundlag for adgangen til de nødvendige løsninger, men også løftestang for indhentning af fuldmagter og automatiseret udveksling af nødvendige data mellem myndigheder på tværs af landegrænser.

Problemstilling

Borgernes udnyttelse af den stadig mere integrerede økonomiske servicestruktur – kombineret med muligheden for at arbejde i andre EU-lande m.v. – kan blive bremset af mangel på en entydig, sikker og multifunktionel identifikationsmekanisme, der kan fungere både nationalt og på tværs af EU's grænser til handel og kommunikation med offentlige instanser m.v. En sådan identifikationsmekanisme vil – udover at gøre livet lettere for de enkelte brugere – også sikre dem væsentligt mod kriminalitet og misbrug af personlige oplysninger.

Kommunikationssikkerhed er en forudsætning for informationsstrømmens frie flow – og for en effektiv digital forvaltning og derved en bedre offentlig service i fremtiden. Det er nationalstaternes ansvar og behov at skabe en digital borgeridentifikation, som kan beskytte borgernes personlige data mod fx identitetstyveri, men det er et fælles EU-anliggende at sikre, at denne identifikation er anvendelig på tværs af EU.

Arbejdsgruppen mener, der er behov for, at alle borgere i Danmark – og i hele EU – bliver udstyret med en interoperabel identifikationsmekanisme med meget høj sikkerhed. Man kunne kalde det for "2. generation af CPR" – et område, hvor Danmark altid har været foregangsland.

Løsningsforslag

Arbejdsgruppen mener, at vi i Danmark skal tage initiativ til udvikling af et dansk borgerservicepas i form af en "digital identitet", som kan fungere på tværs af grænser i EU, og som minimerer risikoen for, at den enkelte borger bliver offer for kriminelle handlinger og misbrug af personlige data i forbindelse med

handel og kommunikation via internettet. Arbejdsgruppen mener ikke nødvendigvis, at hele EU skal have præcis den samme tekniske løsning for digital identitet, men pointerer vigtigheden af, at de nationale løsninger er koblet sammen i et fælles, interoperabelt EU-system. Dette har mange fordele – fx vil en dansker, der bliver indlagt på et hospital i et andet EU-land, hurtigt kunne identificeres som EU-borger og potentielt blive behandlet sikrere, fordi de udenlandske læger – i en fremtid, hvor dette er muligt – kan tilgå danskerens elektroniske patientjournal via borgerservicepasset (den digitale identitet).

Arbejdsgruppen fremhæver, at arbejdet bør bygge videre på de danske initiativer i relation til digital signatur. Samtidig kan man overveje at lade sig inspirere af det udviklingsarbejde på området, der netop nu foregår i Østrig. Her arbejder man – som en del af EU's program "i2010"[41] – på at gøre landets it-arkitektur interoperabel med andre EU-landes it-arkitektur. I Østrig mener man heller ikke, at en EU-løsning for digital identitet nødvendigvis skal bygge på ét fælles kort, men nærmere på en informationsstruktur, man kan få adgang til ved hjælp af flere forskellige "carriers" såsom mobiltelefoner, bankkort, sygesikringskort m.v. – og på flere forskellige sikkerhedsniveauer alt efter den konkrete aktivitet. Hver nation kan vælge sin egen carrier/løsning, men skal så levere den bagvedliggende informationsstruktur, der skal leve op til nogle fælles standarder, herunder sikkerhedsstandarder, der gør den interoperabel med informationsstrukturerne i de øvrige lande.

Arbejdsgruppen pointerer, at begrebet "privacy" er centralt i relation til borgerservicepas. Privacy handler grundlæggende om retten til at være alene uden at være overvåget af andre, og retten til at bestemme, hvad man vil offentliggøre om sig selv og under hvilke omstændigheder. Men man kan definere privacy på flere måder. I den digitale verden taler man ofte både om sikkerhed, beskyttelse af personfølsomme data og om privacy som et bredere begreb relateret til den personlige integritet og selvbestemmelse. Privacy kan således handle om at give brugerne rettigheder til fx at få oplyst, hvor deres personlige data er registreret, og til at slette og ændre i de personlige data. Og det kan handle om at give brugerne kontrol over deres data, så de bestemmer, hvem der kan tilgå dem, til hvilket formål og hvornår de må kædes sammen. Arbejdsgruppen mener, at man skal designe borgerservicepasset på en sådan måde, at privacy er maksimalt beskyttet.

Arbejdsgruppen understreger, at der allerede findes en infrastruktur i form af digital signatur via internettet, som man kan anvende til formålet – og at der først og fremmest er behov for at sikre, at processerne bagved er interoperable og sikre. Det er nødvendigt at afklare de fælleseuropæiske forudsætninger for bl.a. at kunne autentificere hinandens borgere i forhold til hinandens systemer og derigennem skabe den nødvendige interoperabilitet.

Løsningsfora og Danmarks rolle: Arbejdsgruppen understreger, at der er behov for politisk opbakning til etableringen af et borgerservicepas/en digital identitet i Danmark. Kravspecifikationerne bør være politisk bestemte og udviklet af et bredt udvalg af centrale aktører på området, eventuelt med forankring i Videnskabsministeriet. Udviklingen af den konkrete løsning bør bl.a. basere sig på de tanker og erfaringer, man har gjort sig i Danmark om digital signatur. Det danske arbejde på området skal – sammen med østrigske og eventuelt andre initiativer i EU – koordineres med henblik på opbygning af en sikker, interoperabel "borgerservice-infrastruktur" i EU med fælles kommunikationsstandarder. Arbejdsgruppen pointerer, at der også bør deltage almindelige borgere i arbejdet med at udvikle borgerservicepasset med henblik på at gøre den færdige løsning så brugervenlig som muligt. Videnskabsministeriet bør samtidig arbejde på EU-plan for opbygningen af den nødvendige interoperabilitet.

[41] "i2010 – A European Information Society for Growth and Employment". http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm.

5.6. Manglende fokus på it-sikkerhed i offentlige it-udbud

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

Case: Røntgensystem afbrudt af ormeangreb
Vejle Amt var i august 2006 udsat for et massivt ormeangreb, som betød, at de sygehuse, der benyttede sig at det fælles amtsnet også blev angrebet. Ormeangrebet medførte, at man ikke kunne tilgå hinandens systemer, herunder et røntgensystem, som blev benyttet af alle sygehuse i amtet. Dette system var utilgængeligt i flere dage, hvilket bl.a. havde den konsekvens, at lægerne ikke kunne sammenligne aktuelle røntgenbillede med historiske billeder i røntgensystems database.

Problemstilling

Det danske samfund rummer en række vitale områder – bl.a. it/tele, energisektoren og transportsektoren[42] - der skal holdes i drift under alle forhold. Fælles for dem er, at de afhænger af en underliggende it-infrastruktur, der er en vigtig del af den såkaldte "kritiske nationale infrastruktur". Mange samfundsfunktioner, der hører under de nævnte områder, har traditionelt været ejet og finansieret af det offentlige – og beskyttelse af infrastrukturen har været en integreret del af den såkaldte totalforsvarsplanlægning. Efter den kolde krigs ophør har samfundet i vid udstrækning privatiseret de offentlige tjenester og omkostningerne forbundet med tjenesterne er blevet reduceret. I denne proces har samfundet givet afkald på det tidligere særdeles høje robusthedsniveau.

Samtidig indfører den offentlige sektor – i takt med den voksende digitalisering af samfundet – nye elektroniske sags- og dokumenthåndteringssystemer, som skal gøre det lettere at håndtere sager og dokumenter i elektronisk form – både i den enkelte enhed og på tværs af institutioner, forvaltninger og myndigheder. Ifølge arbejdsgruppen sker denne udvikling uden at man samtidig har maksimal fokus på sikkerhed.

Når en offentlig virksomhed har behov for at få løst en opgave – fx udvikling af et nyt it-system – og opgaven overstiger et vist beløb, skal den sendes i udbud i EU. Det indebærer, at leverandører fra hele EU kan byde på opgaven. I forbindelse med en sådan udbudsforretning skal de potentielle leverandører svare på en lang række spørgsmål. Det er arbejdsgruppens erfaring, at 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 et væsentligt problem, at kravspecifikationer for it-sikkerhed, it-forbundethed og privacy i diverse offentlige udbud er mangelfulde eller ikke-eksisterende, mener arbejdsgruppen.

[42] Disse tre områder udpeges som indsatsområder i rapporten "Et robust og sikkert samfund", juni 2005. www.forsvaret.dk.

Et typisk it-udbud i dag indeholder fx sjældent en "forbundethedsanalyse", som vurderer konsekvenser ved en sikkerhedsbrist for andre områder end det, udbudet dækker – og det er et problem, påpeger arbejdsgruppen. Sygehusfællesskabet i en region er et eksempel på, hvordan en sikkerhedsbrist kan forplante sig gennem forbundne it-systemer. Her deles man om infrastruktur og databaser, som bl.a. indeholder røntgenbilleder. Disse data er kritiske for borgernes helbred og skal kunne tilgås døgnet rundt af samtlige læger i regionen.

Et andet eksempel er manglende mobiltelefondækning i en katastrofesituation. Det kan få fatale konsekvenser, hvis kommunikationen mellem myndighederne og redningsmandskabet svigter. Endvidere kan et nedbrud i elforsyningen have meget omfattende konsekvenser – fx for sygehuse, brandstationer m.v., hvor der anvendes Internet Protokol (IP) styrede kortlæsere. Man kan ikke anvende disse, hvis internettet er gået ned på grund af strømsvigt. I virksomheder, der anvender sådanne kortlæsere på dørene, vil man ved et strømsvigt ikke kunne komme ud og ind – med mindre der er etableret en nødstrømforsyning.

Løsningsforslag

For at højne sikkerhedsniveauet hos de offentlige myndigheder i EU – og dermed også løfte niveauet i det øvrige samfund – anbefaler arbejdsgruppen, at der ved lovgivning indføres krav om, at it-sikkerhed skal være en nøgleparameter i alle offentligt udbud, hvor it indgår – og at en it-sikkerheds- og forbundethedsanalyse skal være en del af udbudet. Det betyder, at udbudet skal indeholde en analyse af de mulige konsekvenser af en sikkerhedsbrist og især fokusere på, hvordan en sådan brist kan påvirke andre sektorer og forplante sig gennem forbundne it-systemer. Hvor det er relevant, skal vurderingen også tage højde for statens beredskabsbehov. Alle risici skal være kortlagt og gennemtænkt – og der skal foreligge planer for, hvordan it-brugerne skal reagere i de forskellige scenarier.

Arbejdsgruppen mener, at sikkerhedsstandarden DS484, der i dag er et krav i forhold til statslige og regionale it-løsninger og forventes at blive det i forhold til løsninger til kommunerne i løbet af 2007, er mangelfuld på privacy området. Der er behov for at etablere et centralt organ – fx en Digital Sikkerhedstaskforce – som har ansvar for at etablere et nyt regelsæt for it-sikkerhed i den offentlige sektor ved udbud, der berører privacy og andre kritiske samfundsinteresser. Det er oplagt at gennemføre dette i forbindelse med Kvalitetsreformen af den offentlige sektor. Dette centrale organ kunne også få ansvar for at gennemføre de omtalte forbundethedsanalyser med henblik på at sikre den it-mæssige sammenhæng i de forskellige samfundsområder – fx sundhedsområdet – og på tværs af områderne. Man kan med fordel trække på erfaringer fra beredskabsområdet.

Danmark kan gå forrest på dette område, men da større offentlige udbud er underlagt EU-regler, er det, for at undgå konkurrenceforvridning, nødvendigt at indarbejde kravene om sikkerheds- og forbundethedsanalyser i EU's udbudskrav..

Løsningsfora og Danmarks rolle: Der nedsættes på politisk initiativ en Digital Sikkerhedstaskforce (fx i regi af Finansministeriet), der får til opgave at arbejde på EU-plan for fastsættelse af de anbefalede udbudskrav (fx via ENISA) – og på national plan at fastsætte de samme krav for mindre offentlige indkøb, der ikke sendes i udbud i EU.

6. Kilder og links

Danske kilder og links

Computerworld (avis). Artikler fra 2005, bl.a. "TV2 misbruges til svindel på nettet" af Dorte Toft, 28. januar 2005. http://www.computerworld.dk/.

Dansk IT: http://dansk-it.dk/.

Det Danske Computer Emergency Response Team (under Uni-C): www.cert.dk.

Det Digitale Hjem. www.detdigitalehjem.dk.

Forsvaret, juni 2005: "Et robust og sikkert samfund", juni 2005. www.forsvaret.dk.

Ingeniøren (avis): Artiklen "Virusorm lukkede MR-scannere på Herlev Hospital", 4. maj 2005 http://ing.dk/article/20040504/IT/105070014/-1/tema-category.

ISP Sikkerhedsforum. www.isp-sikkerhedsforum.dk.

IT-Branchen: http://itb.dk/.

ITEK – Branchefællesskabet for IT, Tele, Elektronik og Kommunikationsvirksomheder (Under Dansk Industri): www.itek.dk.

IT-Sikkerhedspanelet: http://www.si.dk/wimpdoc.asp?page=tema&objno=191315248.

IT- og Telestyrelsen: www.itst.dk.

Netsikkerkampagnen. www.netsikkernu.dk.

Rigspolitiet: "Redegørelse for udviklingen i IT-kriminalitet samt den politimæssige indsats på området".

Teknologirådet, "It-infrastrukturens sårbarhed", rapport, maj 2004, http://www.tekno.dk/subpage.php3?article=868&toppic=kategori7&language=dk.

Teknologirådet. "RFID – muligheder og risici", rapport, juni 2006, http://www.tekno.dk/subpage.php3?article=1212&toppic=kategori7&language=dk.

Teknologirådet. "Idékatalog med rådata fra workshop om it-sikkerhed", http://www.tekno.dk/subpage.php3?article=1276&toppic=kategori7&language=dk.

VK-regeringen, april 2006: "Fremgang, fornyelse og tryghed. Strategi for Danmark i den globale økonomi – de vigtigste initiativer".

Internationale kilder og links

Anderson, Ross: Why Information Security is Hard – An Economic Perspective (artikel). http://www.acsac.org/2001/papers/110.pdf.

Center for Internet Security. Et nonprofit organ, der bl.a. tildeler licenser i forhold til it-sikkerhed. www.cisecurity.org/index.html.

CERT: http://www.cert.org/stats/.

CIA, Directorate of Science and Technology: www.cia.gov/cia/dst/home.html.

Computer Economics: http://www.computereconomics.com/.

ENISA, The European Network and Information Security Agency. www.enisa.eu.int.

Europarådet: "International convention on cybercrime". 28 lande har skrevet under på konventionen og 14 har ratificeret den, herunder Danmark. Konventionen er åben for lande uden for EU. USA har skrevet under, men ikke ratificeret: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

European Security Research Programme (ESPR): http://ec.europa.eu/enterprise/security/index_en.htm.

Europol. Europol finansieres gennem bidrag fra medlemsstaterne. Bidragene beregnes i forhold til deres BNI. Budget for 2006: 63,4 mio. EUR. Der er 590 ansatte i Europol, heraf 90 forbindelsesofficerer, der repræsenterer forskellige retshåndhævende myndigheder (politi, toldvæsen, gendarmeri, indvandringsmyndigheder m.v.). http://www.europol.eu.int/.

Eurostat, februar 2006. http://epp.eurostat.cec.eu.int.

EU, "Net- og Informationssikkerheds: Forslag til en europæisk strategi" ("com2001_0298da01.pdf").

EU, "A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment". EU-kommissionen, COM(2006) 251. http://ec.europa.eu/information_society/doc/com2006251.pdf.

EU, "Communication on creating a safer information society by improving the security of information infrastructure and combating computer-related crime" (EU, 2001): http://europa.eu.int/ISPO/eif/InternetPoliciesSIte/CrimeCommEN.html.

EU, "Critical Infrastructure Protection in the fight against terrorism" (EU, 2004): http://europa.eu.int/eur-lex/LexUriServ/site/en/com/2004/com2004_0702en01.pdf.

EU. Information Society Technologies (et it-sikkerhedsrelateret arbejdsprogram under EU): http://cordis.europa.eu/ist.

EU. "Forum on Cybercrime", som samler bl.a. politiinstanser, ISP'er, forbrugergrupper, databeskyttelsesenheder m.v. med det formål at skabe gensidig forståelse og samarbejde på EU-niveau – og bl.a. skabe awareness om risici ved it-kriminalitet og sprede viden om best practises om it-sikkerhed, afdække anti-kriminalitetsværktøjer og udvikle "early warning" systemer og mekanismer: http://ec.europa.eu/justice_home/news/information_dossiers/forum_crimen/index_en-htm.

EU. ESRAB - European Security Research Advisory Board: http://europa.eu/eur-lex/lex/LexUriServ/LexUriServ.do?uri=OJ:C:2005:180:0002:0002:EN:PDF.

FBI, Information Technology: www.fbi.gov/hq/ocio/ocio_home.htm.

FIRST – Forum of Incident Response and Security Teams: www.first.org. FIRST har bidraget til at udvikle CVSS – Common Vulnerability System – som er et ratingsystem, der kan opdage sårbarheder i software og foreslå en prioriteret response: www.first.org/cvss.

G8 High Tech Crime Subgroup. Gruppen har bl.a. til opgave at støtte G8-landenes muligheder for at forebygge, efterforske og retsforfølge ulovligheder, der involverer computere, netværk og nye teknologier. Se bl.a.: http://www.usdoj.gov/criminal/cybercrime/intl.html.

i2010 – A European Information Society for Growth and Employment": http://ec.europa.eu/information_society/eeurope/i2010/index_en.htm.

ICANN – Internet Corporation for Assigned Names and Numbers: www.icann.org/.

"Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors": http://www.cert.org/archive/pdf/insidercross051105.pdf.

Interpol http://www.interpol.int/.

IRG – Independent Regulators Group: European National Telecommunications Regulatory Authorities: http://irgis.anacom.pt/site/en/irg.asp.

ISPA: http://www.ispa.org.uk/.

ITU: International Telecommunications Union (under FN): http://www.itu.int/home/index.html.
ITU – Cyber security Portal: http://www.itu.int/cybersecurity/index.html.

Microsoft (information om ormen "Sasser"): "What You Should Know About Sasser". http://www.microsoft.com/security/incident/sasser.mspx.

Microsoft Security Intelligence Report: http://www.microsoft.com/downloads/details.aspx?FamilyId=1C443104-5B3F-4C3A-868E-36A553FE2A02&displaylang=en.

Nordic Information Society Statistics. http://www.norden.org/pub/uddannelse/IT/TN2005562.pdf.

NWCCC – National White Collar Crime Center. Centeret arbejder for at oprette et landsdækkende støttesystem for myndigheder, der beskæftiger sig med forebyggelse, efterforskning og retsforfølgelse af økonomisk og hightech kriminalitet i USA. Det er en nonprofit-organisation, som er finansieret af den amerikanske kongres. Medlemmerne er forskellige retslige myndigheder, statslige lovgivningsenheder, og stats- og stedlige anklagemyndigheder: http://www.ic3.gov/.

OECD – Internet Security: www.oecd.org/sti/security-privacy.

Schneier, Bruce: www.schneier.com.

The Computer Economics 2005 Malware Report: The Impact of Malicious Code Attacks. http://www.computereconomics.com/article.cfm?id=1090.

The National Information Assurance Partnership: http://niap.bahialab.com/.

"US Businesses: Cost of Cybercrime Overtakes Physical Crime": http://www-03.ibm.com/press/us/en/pressrelease/19367.wss.

U.S. Department of Justice: "International Aspects of Cybercrime": http://www.usdoj.gov/criminal/cybercrime/intl.html#Vc.

World Internet Usage and Population Statistics: www.internetworldstats.com/stats.htmh.

WSIS - World Summit for Information Society – FN initiative: www.itu.int/wsis/.

7. Appendiks. Øvrige it-sikkerhedsproblemer og deres håndtering

Her følger en liste over de vigtigste af de øvrige it-sikkerhedsmæssige problemstillinger, arbejdsgruppen har drøftet og derefter valgt ikke at gå i dybden med. Fravalgene skyldes ikke, at der er tale om uvigtige problemstillinger. Arbejdsgruppen har lagt vægt på i rapportens hovedtekst at identificere og prioritere de områder, der med størst fordel kan bidrage til udviklingen af den internationale it-sikkerhed. I enkelte tilfælde skyldes fravalg endvidere, at en given problemstilling allerede er ved at blive håndteret på fornuftig vis.

1. Mangelfuld formidling af viden om sikkerhedsbrister

Problem: Producenter af hardware og software har ingen forpligtelser eller aftaler om at videreformidle eller frigive oplysninger om eventuelle it-sikkerhedsbrister. Dette vanskeliggør mulighederne for at begrænse skader af it-relateret kriminalitet.
Løsning: EU's it-sikkerhedsgruppe, ENISA, har udviklet løsningsmodeller og arbejder på etablering af et organ for indrapportering og videreformidling af sikkerhedsbrister. Se ENISA's hjemmeside – www.enisa.eu.int/.

2. Manglende viden om borgernes opfattelse af it-sikkerhed

Problem: Større viden på området er et nødvendigt grundlag for at kunne sikre, at borgerne får større fokus på it-sikkerhed.
Løsning: En analyse af, hvordan borgerne opfatter trusselsbilledet, vil være et godt udgangspunkt for en indsats og udvikling af mere pædagogiske sikkerhedssystemer. Borgerne bør inddrages i en debat om, hvem der skal holdes ansvarlig for hvilke dele af it-sikkerheden.

3. Nye teknologier skaber nye trusler

Problem: Nye teknologier skaber altid nye trusler. Nogle it-relaterede trusler mod borgere og virksomheder i de kommende år vil kunne henføres til udbredelse af ny teknologi, som brugerne ikke er vant til at anvende, og hvor man ikke er bevidst om misbrugsmulighederne. Et eksempel herpå er "messageing", der i dag ikke bare er et ungdomsfænomen, men også et effektivt forretningsværktøj med betydning for virksomheders vækst og indtjening. Virksomheder er ad den vej blevet udsat for uventede spamangreb, fordi de ikke var bevidste om, at dette var en risiko.
Et fremtidseksempel omhandler Radio Frequency Identification (RFID), der er en teknologi indlejret i en computerchip, der kan aflevere et produkt-id, som entydigt identificerer et produkt. Da dette kan ske på afstand og for mange varer samtidig, spås teknologien en massiv tilstedeværelse i fremtidens produkter. Problemet er, at teknologien potentielt kan blive misbrugt af kriminelle til at overvåge borgere og virksomheder. Samtidig kan man fjerndestruere RFDI og dermed omgå systemet. Fremtidens butikstyve kan fx have en "RFID-zapper", som de anvender til at "slukke for" dyre varer, som de gemmer blandt de mange andre, der skal skannes, så de dyre ikke bliver opdaget.
Løsning: Udvikling af standarder for "best practise". Derudover skal det være et krav om, at der bliver skabt bedre sammenhæng mellem forskning og anvendelse – at samfundet prioriterer, at forskningsproblemstillinger bliver formidlet til dem, der udvikler og anvender teknologierne, for at samfundet proak-

tivt kan beskytte sig mod de trusler, som bliver identificeret. Det er derfor afgørende, at vi internationalt deltager i fora omkring nye teknologier og deres anvendelse.

4. Globaliseringen skaber behov for globale sikkerhedsstandarder

Problem: Den danske standard for statens håndtering af it-sikkerhed og god it-sikkerhedsskik, DS484, er ukendt uden for Danmark. DS484 er en effektiv og sammenhængende standard. Problemet er, at den ikke korresponderer med sikkerhedsstandarder uden for Danmark.
Løsning: Danmark skal fuldt ud acceptere og implementere anerkendte internationale standarder og ikke selv opfinde den dybe tallerken. DS484 udskiftes med ISO-standarden ISO27001. Det bør være et krav, at standarder på it-sikkerhedsområdet altid er åbne og internationale. Overgangen kan eventuelt ske ved at følge en modnings- og udfasningsstrategi, som betyder, at nationale standarder bliver erstattet med passende internationale standarder, når disse er til rådighed.

5. Mangelfuld viden om it-sikkerhed i andre lande

Problem: Der er meget begrænset viden om, hvordan andre lande håndterer it-sikkerhedsmæssige udfordringer. Det betyder, at vi fx ikke ved, hvor sikker/usikker en betalingsgateway i et givet land er. Et hovedproblem er, at man i alle lande prøver at opfinde den dybe tallerken i stedet for at trække på hinandens viden, kompetencer og erfaringer. Der er næppe tvivl om, at et lands it-sikkerhedsmæssige stade i fremtiden bliver lige så afgørende for, om man ønsker at placerer sin virksomhed der, som fx spørgsmålet om, hvorvidt der er adgang til en veluddannet arbejdsstyrke. Det skyldes, at det i fremtidens digitale servicesamfund er nødvendigt at have tilgang til digitale servicer og tjenester for at sikre, at man kan arbejde og levere sine produkter og servicer. It-sikkerhedsfaktorer, som et land vil blive målt på, er bl.a. følgende: Er der en troværdig og altid tilgængelig infrastruktur? Bliver der gjort op med it-kriminelle – bliver anmeldelser taget alvorligt? Er der risiko for at blive privacy-angrebet? Hvad gør myndighederne for at begrænse udbredelsen af spam og vira?
Løsning: Benchmarking af it-sikkerhed på tværs af EU og eventuelt globalt. Som virksomhed, der overvejer at etablere sig i et land, skal man kunne købe viden om landets it-sikkerhedsniveau. Dette er forsøgt etableret af flere globale markedsaktører i bl.a. revisionsbranchen. Det kan være en mulighed at etablere et europæisk it-sikkerhedsagentur, som er ansvarlig for jævnlig benchmarking af forskellige landes it-sikkerhed. Formålet er at skabe øget bevidsthed på it-sikkerhedsområdet og øget konkurrence om it-sikkerhed, men også at opsamle viden på baggrund af fælles mål for it-sikkerhed. Udenrigsministeriet har etableret en arbejdsgruppe, som skal tiltrække udenlandske virksomheder ved at benchmarke Danmarks sikkerhed i forhold til sikkerheden i andre lande. Se www.invest.indk.com.

6. Internet Governance – hvem skal kontrollere nettet?

Problem: Internet Governance handler om, hvem der kontrollerer internettet. The Internet Corporation of Assigned Names and Numbers (ICANN) er den nonprofitorganisation, der håndterer systemet med internetadresser. Nogle mener, at internettet er kontrolleret af kommercielle interesser i stedet for at være en global ressource, som alle har lige adgang til at gøre brug af. Andre frygter, at ønsker om at reformere den bestående "Internet Governance-situation" er udtryk for et maskeret mål fra visse regeringers side, om at kontrollere indhold på nettet og sætte grænser for ytringsfriheden.
Løsning: Arbejdsgruppen er uafklaret. For inspiration se bl.a. www.icann.org. Danmark er involveret i arbejdet under FN om Internet Governance.

7. DS484 er for krævende for små og mellemstore virksomheder

Problem: Små og mellemstore virksomheder tager ofte ikke stilling til alle sikkerhedsproblemer i virksomheden – typisk kun punktsikkerhed. Der er behov for it-sikkerhedsstandarder, som er umiddelbart tilgængelige for SMV'er.
Løsning: Udvikling af en international "light" sikkerhedsstandard til SMV'er.

8. It-professionelle ved ikke nok om it-sikkerhed

Problem: Systemudviklere og andre it-professionelle er generelt utilstrækkeligt uddannede inden for it-sikkerhed. Problemet er stort og der er behov for at øge vidensniveauet. Konsekvensen af den begrænsede viden er bl.a., at it-sikkerhed ofte bliver behandlet som punktsikkerhed og ikke som "end-to-end" sikkerhed. Der mangler en bred forståelse af problemet og det samspil og de udfordringer, it-sikkerhed indebærer i forhold til en helhedsløsning.
Løsning: Man skal stille krav til certificering og forståelse af problemløsning på tværs – ikke kun om punktsikkerhed. Man bør indføre uddannelser og certificering af personer, der arbejder med it-sikkerhed, så man bliver "autoriseret it-sikkerhedsekspert". Det bliver dog vanskeligt at udvikle it-sikkerhedscertificering, som er relevant for alle it-professionelle. Der kan også indføres en autorisation af virksomheder, der sælger sikkerhedsløsninger. Man bør uarbejde en branchekodeks og et brancheklagenævn. Ansvaret for at implementere it-certificeringer kan fx placeres under EU-organerne ENISA, ISC2 eller ISACA. ENISA skal samtidig udbygge samarbejdet med resten af verden.

9. Den interne trussel – når ansatte saboterer

Problem: En betydelig del af alle sikkerhedshændelser i en virksomhed – tilsigtede eller utilsigtede – kan tilskrives ansatte eller partnere. Fx blev en systemadministrator hos en amerikansk virksomhed i våbenindustrien vred over, at han fik en mindre rolle at spille i virksomheden. Han placerede alle firmaets programmer til styring af produktionen på en enkelt server. Derefter truede han en kollega til at udlevere alle sikkerhedskopier af programmerne. Systemadministratoren blev fyret. Nogen tid senere slettede et program, han havde efterladt, indholdet på serveren med produktionsprogrammerne. Det kostede firmaet over 10 mio. dollars at genoprette de tabte programmer og data.[43]
Løsning: Arbejdsgruppen er uafklaret.

10. IP version 6 er ikke indført i EU

Problem: Internet Protocol Version 6 er taget i brug i Asien og USA, men ikke i EU. Protokollen vil eliminere flere – om ikke voldsomt alvorlige – sikkerhedsproblemer, hvis den også bliver taget i brug i EU.
Løsning: IPv6 er dog langt fra hele løsningen, da denne også har sikkerhedsmæssige problemer – man kan fx manipulere QOS-feltet og lave DoS-angreb. Der er behov for krav om væsentligt højere sikkerhed i komponenter, der benyttes til IP-telefoner. Man skal kunne gøre et producentansvar gældende med fokus på et IP-produkts sikkerhedsmæssige konsekvenser. Læs bl.a. mere på: http://www.ipv6.org/. En arbejdsgruppe under it- og telestyrelsen arbejder på en analyse af IPv6 som oplæg til en dansk strategi for overgangen til IPv6.

[43] "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors", http://www.cert.org/archive/pdf/insidercross051105.pdf.

Teknologirådets udgivelser 2006

Teknologirådets rapporter:

"Perspektiver ved indførelse af gratis offentlig transport". Teknologirådets rapport 2006/16.

"Morgendagens transportbrændstoffer". Danske perspektiver. Teknologirådets katalog 2006/15.

"Internationalisering af uddannelse". Redigeret udskrift og resumé af høring i Landstingssalen den 30. august 2006. Teknologirådets rapport 2006/14.

"Tilsætningsstoffer i tobaksvarer". Redigeret udskrift og resumé af høring i Landstingssalen den 26. april 2006. Teknologirådets rapport 2006/13.

"Regulering af miljø- og sundhedsaspekter ved nanoteknologiske produkter og processer". Vurderinger og anbefalinger fra en arbejdsgruppe under Teknologirådet, juni 2006. Teknologirådets rapport 2006/12.

"Sundhedsydelser med IT – Pervasive Healthcare i den danske sundhedssektor". Vurderinger og anbefalinger fra en arbejdsgruppe under Teknologirådet. Teknologirådets rapport 2006/11.

"Høring om terrorbekæmpelse". Resumé, skriftlige oplæg og redigeret udskrift af høring i Landstingssalen, onsdag den 10. maj 2006. Teknologirådets rapport 2006/10.

"Velfærd fremover – en udfordring". Resumé og redigeret udskrift af konference på Christiansborg den 22. marts 2006. Teknologirådets rapport 2006/9.

"Lille Land hvad nu?". - Information og debat om Danmarks situation i lyset af globaliseringen. Teknologirådets rapport 2006/8.

"Københavns Cityring". Høring for Borgerrepræsentationen i København den 30. marts 2006. Teknologirådets rapport 2006/7.

"Grøn transport – kan vi, og vil vi?". Resume og redigeret udskrift af høring i Folketinget den 5. april 2006. Teknologirådets rapport 2006/6.

"Høring om Miljøteknologi". Resumé og redigeret udskrift af høring i Landstingssalen på Christiansborg den 21, februar 2006. Teknologirådets rapport 2006/5.

"RFID fra produkt til forbrug. - muligheder og risici ved RFID-teknologi i værdikæden" Teknologirådets rapport 2006/4.

"Hvordan skal vi bruge den nye viden om menneskets hjerne?". Europæiske borgere i dialog om hjerneforskning. Teknologirådets rapport 2006/3.

”Dansk energiforbrug i fremtiden”. Resumé og redigeret udskrift af høring i Folketinget den 25. januar 2006. Teknologirådets rapport 2006/2.

”Dansk energiproduktion i fremtiden”. Resumé og redigeret udskrift af høring i Folketinget den 17. november 2005. Teknologirådets rapport 2006/1.

Nyhedsbrevet ”Fra rådet til tinget”:

Nr.232 11/06: Gratis offentlig transport
Nr.231 11/06: Ønskes: En ny privacy-politik
Nr.230 10/06: Uddannelse til globalt marked
Nr.229 06/06: Bedre sundhed hvis færre røg
Nr.228 06/06: Bliver man syg af NANO?
Nr.227 06/06: Danmarks energifremtid

TeknologiDebat Fokus:

TD4/2006: Teknologivurdering i EU
TD3/2006: Fremtidens energikilde
TD2/2006: Patient i fremtidens it-sundhedsvæsen
TD1/2006: Årsberetning 2005

Alle Teknologirådets udgivelser kan læses og hentes gratis fra Rådets hjemmeside www.tekno.dk

Gratis nyhedstjenester:

- Abonner på Teknologirådets elektroniske nyhedsbrev TeknoNyt, der orienterer om hvad der sker i Teknologirådet og i teknologiens verden. Send en mail til teknonyt@tekno.dk
- Abonner på Teknologirådets nyhedsbrev til Folketinget ”Fra rådet til tinget” ved at sende en mail til rtt@tekno.dk