
Brugernes it-sikkerhed

Analyse af interviewmøde med
private brugere samt anbefalinger
fra en arbejdsgruppe sammensat
af Teknologirådet

Brugernes it-sikkerhed

Analyse af interviewmøde med private brugere
samt anbefalinger fra en arbejdsgruppe
sammensat af Teknologirådet

Projektledelse i Teknologirådets sekretariat:
Bjørn Bedsted

Projektmedarbejder:
Julie Refsgaard Lawaetz

Projektsekretær:
Eva Glejtrup

Omslag:
Communikanten.dk

Tryk:
Vester Kopi

Tekst:
Teknologirådet

Oplag: 340
ISBN: 978-87-91614-40-8

Rapporten kan bestilles hos:

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

Denne rapport er hentet på Teknologirådets hjemmeside:
www.tekno.dk

Teknologirådets rapporter 2008/1

Indhold

1. FORORD	4
2. RESUMÉ	5
3. EXECUTIVE SUMMARY	7
4. INTRODUKTION.....	9
4.1 Metode	10
4.2 Rapportens indhold.....	11
5. LØSNINGSFORSLAG	12
5.1 Digital identitet	12
5.2 Automatiske sikkerhedsopdateringer	14
5.3 Pc-syn	15
5.4 Tvungen mailfiltrering samt installation af firewall og virusfilter	16
5.5 Sikkerhedsmærkning af it-produkter.....	17
5.6 Blokering af adgang til skadelige hjemmesider.....	18
5.7 Online lagring af data.....	18
6. ANALYSE	20
6.1 Generelt om deltagernes forhold og indstilling til it-sikkerhed.....	20
6.2 Digital identitet	22
6.3 Automatiske sikkerhedsopdateringer	24
6.4 Pc-syn	27
6.5 Tvungen mailfiltrering samt installation af firewall og virusfilter	29
6.6 Sikkerhedsmærkning af it-produkter.....	31
6.7 Blokering af skadelige hjemmesider.....	32
6.8 Online lagring af data.....	34
7. ANBEFALINGER FRA GRUPPEN	36
8. ORDLISTE	40
9. TEKNOLOGIRÅDETS UDGIVELSER 2006-2007	43

1. Forord

It-sikkerheden er en stadigt voksende udfordring for private brugere. På arbejdspladsen tages der professionelt hånd om sikkerheden, men i hjemmet er brugerne overladt til sig selv og til it-kyndige venner og familiemedlemmers velvillighed. Undersøgelser viser, at mange brugere har svært ved at håndtere opgaven og andre undersøgelser tyder på, at mange gerne ville være den foruden.

Dårlig eller manglende it-sikkerhed kan foruden at være til gene for den enkelte bruger også udgøre en trussel for det øvrige net, hvor en usikker computer kan bruges som mellemlid ved berigelseskriminalitet og angreb på andres computere, hjemmesider mm. Teknologirådet har derfor sammensat en arbejdsgruppe, som har haft til opgave at udvikle løsningsforslag med tiltag, som kan lette private brugeres håndtering af it-sikkerhed og dermed hæve det generelle it-sikkerhedsniveau.

Sådanne tiltag kan dog være kontroversielle, og selv om mange brugere gerne vil blive fri for besværet med selv at stå for sikkerheden, er det uvist, om brugerne vil betale den pris, det kan koste, fx i form af afgivelse af kontrollen med deres computer til andre. Løsningsforslagene er derfor blevet præsenteret for en gruppe almindelige brugere på et interviewmøde, hvor deltagerne har fået mulighed for at drøfte de dilemmaer, som flere af løsningsforslagene rummer. På baggrund af dette har arbejdsgruppen udarbejdet deres endelige anbefalinger til, hvordan de næste skridt kan tages for at hjælpe private brugere med at håndtere it-sikkerheden.

Medlemmerne af arbejdsgruppen er:

- Susanne Karstoft, Juridisk Institut, Aarhus Universitet
- Per Tejs Knudsen, cBrain
- Nicholai Kramer Pfeiffer, Cybercity
- Birgitte Mikkelsen, Finansrådets it-sikkerhedsgruppe
- Jakob Illeborg Pagter, Alexandra Instituttet
- Steffen Stripp, Dansk Metal

Ivan Damgård og Christian Wernberg-Tougaard har læst og kommenteret rapporten forud for udgivelsen.

Det er Teknologirådets bestyrelse, der 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.

Rapporten er skrevet af Teknologirådet i samarbejde med arbejdsgruppen, som har udformet løsningsforslagene og de endelige anbefalinger. Rapporten kan bestilles hos Teknologirådet eller frit downloades fra rådets hjemmeside www.tekno.dk.

Teknologirådet, april 2008

Projektleder Bjørn Bedsted

Projektmedarbejder Julie Refsgaard Lawaetz

2. Resumé

Samfundets stigende afhængighed af netbaseret handel, administration og service forudsætter en sikker og velfungerende it-infrastruktur. Dermed er en høj it-sikkerhed, både offentligt og privat, en væsentlig faktor for samfundets fremtidige udvikling.

Trusselsbilledet ændrer sig løbende, men det er i dag i høj grad op til den enkelte bruger at have it-sikkerheden i orden. Manglende viden om tekniske sikkerhedsløsninger samt u hensigtsmæssig adfærd fra brugerens side udgør en sikkerhedsrisiko ikke alene for brugeren selv i form af bl.a. virus eller hacking med systemnedbrud, identitetstyveri etc. som følge; også andre brugere og det øvrige samfund kan rammes af manglende it-sikkerhed hos private brugere. En usikker computer kan eksempelvis bruges som mellemlid ved berigelseskriminalitet, angreb på andres computere, hjemmesider mm.

Det er i alles, såvel brugerens som samfundets, interesse at højne brugernes it-sikkerhedsniveau og Teknologirådet ønsker med denne rapport at skabe debat om it-sikkerhed set fra brugernes perspektiv samt bidrage til den fremtidige udformning af holdbare it-sikkerhedsløsninger ved at pege på løsninger, der matcher brugernes ønsker, evner og holdninger.

En arbejdsgruppe, sammensat af Teknologirådet, har udarbejdet løsningsforslag, som har til formål at lette den enkelte brugers håndtering af egen it-sikkerhed og dermed øge det generelle it-sikkerhedsniveau. Sådanne forslag er dog ikke uden omkostninger for den enkelte bruger, og forslagene indeholder derfor kontroversielle tiltag i form af fx nedsat kontrol med egen computer og adgang til internettet.

I hvilken retning og hvor langt almindelige it-brugere ønsker at gå for at højne deres egen it-sikkerhed blev undersøgt på et interviewmøde i november 2007. Her udtrykte 23 almindelige it-brugere bosat i Odense deres generelle holdning til it-sikkerhed samt til de konkrete løsningsforslag først gennem besvarelse af et spørgeskema, dernæst i gruppediskussioner. Der var på interviewmødet et udtrykt ønske om at få hjælp til at håndtere sikkerheden og det er gruppens indtryk, at borgerne overvejende accepterede de indgreb, som løsningsforslagene indebærer, selvom alle selvfølgelig ikke gjorde. Blandt andet på baggrund af brugernes holdninger, har arbejdsgruppen formuleret deres anbefalinger.

Anbefalinger

Arbejdsgruppen mener, at håndteringen af it-sikkerhed i dag i for høj grad er overladt til den enkelte bruger. Den nuværende situation er hverken rimelig eller hensigtsmæssig i forhold til behovet for at opretholde et samfundsmæssigt ønskværdigt sikkerhedsniveau. Gruppen anbefaler derfor, at de lovgivende og udøvende myndigheder fremover tænker (mere) i modeller, der letter de private brugeres håndtering af it-sikkerhed ved at flytte en del af opgaven tættere på de aktører, der har en reel mulighed for at højne sikkerheden. Konkrete bud på sådanne sikkerhedshøjnende initiativer er at finde blandt de løsningsforslag, som arbejdsgruppen har udviklet.

Arbejdsgruppen anbefaler,

- at der indføres en digital identitet, der muliggør sikker identifikation. Identiteten skal udelukkende rumme oplysninger, der identificerer brugeren, og skal være påkrævet når brugeren ønsker at benytte offentlige services på nettet, hvor identifikation forlanges. Identiteten skal også kunne benyttes til private services, som fx netbank, men en sådan sammenblanding af adgangen til private og offentlige services forudsætter en væsentlig oplysningsindsats, såfremt den ikke skal møde modstand blandt brugerne.
- at sikkerhedsopdateringer af software automatiseres i så vid udstrækning, det er muligt.
- at der arbejdes med at udvikle og etablere et offentligt pc-syn af brugernes sikkerhedsniveau med krav, som de skal leve op til, såfremt de ønsker at anvende offentlige services på internettet. Det offentlige bør ved indførslen af sådan et pc-syn tilbyde vejledning i, hvordan man lever op til de krav, således at pc-synet opleves som en hjælp af de private brugere.
- at danske mailudbydere tilbyder mailfiltrering, der som standard er aktiveret. I modsætning til nu, hvor brugerne i nogle situationer selv skal slå den til.
- at indføre sikkerhedsmærkningsordning af it-produkter, som skal tage højde for den hurtige udvikling inden for it.
- at det undersøges nærmere, hvorledes direkte skadelige hjemmesider, der fungerer som en aktiv del af it-kriminaliteten, kan sortlistes og blokeres.
- at der gøres en større indsats for at orientere private brugere om de fordele og ulemper, der er forbundet med at lagre private data på nettet hos kommercielle serviceudbydere. Det anbefales også, at offentlige myndigheder kaster et kritisk blik på de rettigheder, der omfatter disse data.

3. Executive summary

Society's increasing dependency on net-based trade, administration and service presupposes a secure and well-functioning IT-infrastructure. A high level of IT-security in both private homes and society in general therefore plays a significant role for the future development of the society.

Even though the character of the security threats is continuously changing, the handling of IT-security in private homes is today largely up to the individual user. The lack of knowledge of technical security solutions combined with undesirable user behaviour represents a security threat not only towards the individual user e.g. in the shape of virus or hacking which might lead to system breakdown, identity theft etc. Other users and the remaining society may be harmed as well by a single user's lack of IT-security. For instance, an insecure computer may be used as an intermediary facilitating enrichment crimes, attacks on other computers, homepages and so on.

It is therefore in everybody's best interest, the individual users' as well as society's, to raise the level of IT-security among the private users. With this report The Danish Board of Technology therefore wishes to encourage a debate about IT-security seen from the users' perspective and to contribute to the future development of durable IT-security solutions by pointing out those, which match the wishes, abilities and opinions of the private users.

A working group appointed by the Danish Board of Technology has proposed some solutions aimed at easing private users' handling of their IT-security and thereby increasing the overall level of IT-security. However, such solutions are not without consequences for the individual user, and the solutions therefore involve controversial initiatives such as restricting the users' control over their own computers and access to the Internet.

At an Interview Meeting in November 2007 it was investigated in what direction and how far ordinary IT-users are willing to go in order to increase their IT-security. 23 ordinary IT-users, all residents of the Danish city Odense, expressed their general opinion on IT-security and on the concrete solutions proposed. Their opinions were examined by first having them to answer individual questionnaires and secondly involving them in group deliberations.

The users generally expressed a strong wish for help to handle IT-security at the interview meeting and it is the working group's impression that the citizens predominantly accepted the consequences outlined in the proposed solutions, even though not everybody did. The working group has formulated their recommendations based on, among other things, the opinions of the users.

Recommendations

The working group finds that the degree, to which the handling of IT-security today is left with the individual user, is too high. The present situation is neither fair nor reasonable considering the need to maintain a societal desirable security level. The working group therefore recommends that legislative and the executive authorities promote models, which facilitates the private users' handling of IT-security by moving a part of the task closer to actors with a real possibility to raise the level of security. Concrete proposals to such security increasing initiatives can be found among the proposed solutions prepared by the working group.

The working group recommends

- to introduce a digital identity enabling secure identification online. The identity is meant solely to contain information identifying the user and will be mandatory, should the user wish to utilise public services online, where identification is required. The identity may also be used in connection with private services, e.g. online banking. However, such an intermixture of the access to private and public services presupposes an extensive information effort, if resistance among the users is to be avoided.
- to automate security software updates to the largest possible extent.
- to make an effort in developing and implementing a public pc-inspection of the security level of private users' computers with standards the computer must meet if users wish to make use of public services online via the computer. When introducing such a pc-inspection, public authorities must offer guidance in how to meet the demands so that private users experience the pc-inspection as helpful.
- that the Danish mail providers offer mail filtration activated by default, contrary to present conditions, where the users in some situations must switch the filter on themselves.
- to introduce a security labelling of IT-products taking into account the rapid development of IT.
- to closely investigate the possibility of blacklisting and blocking web pages with an obvious criminal intent and damaging effect on users' internet security.
- to put greater efforts into informing private users about pros and cons regarding online storage of private data facilitated by commercial service providers. It is also recommended that public authorities critically examine the rights and access to these data.

4. Introduktion

It-sikkerheden er en stadigt voksende udfordring for private brugere. Trusselsbilledet ændrer sig løbende og bidrager til forvirring og usikkerhed i de private hjem. U hensigtsmæssig adfærd og manglende viden om tekniske sikkerhedsløsninger, firewalls, virusfiltre, sikkerhedsopdateringer mm., udgør en risiko for den generelle sikkerhed på nettet.

Manglende it-sikkerhed kan give gener for brugeren selv. Virus, phishing og hacking kan eksempelvis føre til kompromittering af personlige oplysninger, identitetstyveri, systemnedbrud og økonomisk tab. Men også for andre kan dårlig eller utilstrækkelig it-sikkerhed medføre gener. En usikker computer kan f.eks. bruges som mellemed ved berigelseskriminalitet og angreb på andres computere, hjemmesider mm. Har brugeren eksempelvis hjemmearbejdsplads, kan uhensigtsmæssig adfærd i hjemmet også give problemer på arbejdspladsen og føre til kompromittering af andres personlige oplysninger, systemnedbrud, tyveri af intellektuelle rettigheder og fortrolige forretningsdata og deraf afledt økonomisk tab for arbejdspladsen.

Ansvar for håndtering af private brugeres it-sikkerhed ligger naturligt nok som udgangspunkt hos brugerene selv, men også softwareproducenter, internetudbydere og staten har et ansvar for at gøre sikkerheden lettere at håndtere for brugerne. Spørgsmålet er, hvilken fordeling af ansvaret, der er mest hensigtsmæssig og rimelig.

En undersøgelse af danskernes generelle it-kundskaber foretaget af Teknologisk Institut i 2007 konstaterer, at næsten 40% af den danske befolkning enten helt mangler IKT-færdigheder eller kun har dem i ringe grad¹. I en anden undersøgelse fra It- og telestyrelsen af den danske befolknings holdning til it-sikkerhed påpeges det, at forståelsen af it-sikkerhed er forholdsvis lav, og at der bør tages højde for dette, når fremtidens sikkerhedsløsninger skal tilrettelægges². En fokusgruppeundersøgelse fra 2002 af borgernes generelle viden, holdninger og adfærd i forhold til it-sikkerhed blotlægger den udbredte indstilling blandt deltagerne, at sikkerhed ikke er noget, man ønsker at tænke for meget på³. Det er svært at holde sig opdateret og vide, hvordan man bør agere, og sikkerheden skal helst bare være i orden, uden at man selv skal gøre noget. Er den ikke det, viser undersøgelsen, reagerer folk typisk med bekymring og afholder sig fra at udnytte visse muligheder på nettet.

En målrettet indsats for at højne brugernes bevidsthed (såkaldt "awareness raising") er naturligvis nødvendig, men med de ovenfor nævnte undersøgelser in mente er det rimeligt at antage, at en sådan indsats ikke kan stå alene. Der er for mange, der ikke forstår sig på it-sikkerhed, og om end denne gruppe reduceres med tiden, vil den altid være tilstede. Der synes derfor at være et behov for at omfordele noget af ansvaret for sikkerhedshåndteringen gennem eksempelvis regulering, koordinering og automatisering af indsatsen.

En rapport fra 2007 om "Personal Internet Security" fra The House of Lords i Storbritannien anlægger samme synsvinkel og konkluderer overordnet, at det hverken er rimeligt eller hensigtsmæssigt at

¹ "Borgernes IKT-færdigheder i Danmark" 2007, udarbejdet af Teknologisk Institut

² "Undersøgelse af den danske befolknings holdning til it-sikkerhed" 2006, udarbejdet af Parkegaard og Kristensen Sikkerhed.

³ "IT-sikkerhed. Analyse af borgernes viden, holdninger og adfærd" 2002, udarbejdet af PLS Rambøll

overlade ansvaret for håndteringen af it-sikkerhed til private brugere i en situation, hvor den teknologiske udvikling går stadig hurtigere, og flere og flere kriminelle opererer på internettet⁴.

Teknologirådet har på denne baggrund ønsket at sætte fokus på private brugeres it-sikkerhed ved at identificere tiltag, der kan omfordele noget af ansvaret for håndteringen af it-sikkerhed, for dermed at hæve det generelle sikkerhedsniveau. Der findes imidlertid ingen undersøgelser af, hvor langt private brugere er villige til at gå i forhold til at overdrage håndteringen af it-sikkerheden til andre, og det har været et mål for dette projekt at bidrage med viden om dette.

En arbejdsgruppe, sammensat af Teknologirådet, har fået til opgave at udarbejde et idékatalog med løsningsforslag, der er realistisk gennemførlige, men indeholder kontroversielle tiltag, som kan stille de private brugere, der skal tage stilling til dem, i et dilemma. Dette skyldes, at med forslag, der højner sikkerheden, følger ofte en pris, der skal betales, i form af fx nedsat kontrol med brugerens egen computer og adgang til internettet.

Løsningsforslagene er blevet præsenteret for og vurderet af private brugere på et interviewmøde. På baggrund af såvel egen overbevisning som brugernes holdninger til løsningsforslagene, har arbejdsgruppen udarbejdet sine anbefalinger.

Arbejdsgruppen består af følgende medlemmer:

- Susanne Karstoft, Juridisk Institut, Aarhus Universitet
- Per Tejs Knudsen, cBrain
- Nikolai Kramer Pfeiffer, Cybercity
- Birgitte Mikkelsen, Finansrådets it-sikkerhedsgruppe
- Jakob Illeborg Pagter, Alexandra Institutet
- Steffen Stripp, Dansk Metal

Projektet er finansieret af Videnskabsministeriet og fokuserer, efter aftale med It- og telestyrelsen, hovedsageligt på it-tekniske problemstillinger og sikkerhedsløsninger. Flere sikkerhedsmæssige problemstillinger af privacy-karakter er derfor bevidst udeladt. Det gør dog ikke løsningsforslagene mindre væsentlige, og det er gruppens vurdering, at der er behov for en bred debat om privacy, fx i forbindelse med elektroniske patientjournaler, registre og samtykkeerklæringer.

4.1 Metode

Udarbejdelsen af løsningsforslagene er foretaget af medlemmerne af arbejdsgruppen på grundlag af eksisterende viden på området. At de er udviklet af arbejdsgruppen er dog ikke ensbetydende med, at arbejdsgruppen synes, at forslagene alle bør gennemføres. Opgaven har i første omgang været at formulere nogle forslag, som brugerne selv kunne tage stilling til. Først i deres anbefalinger tager gruppen samlet stilling til, hvad de selv mener om løsningsforslagene.

Løsningsforslagene er blevet præsenteret for en gruppe private it-brugere på et interviewmøde i Odense den 27. november 2007. Det er Teknologirådet, der har stået for afholdelsen samt for analysen af resultaterne.

Interviewmøde er en metode til at foretage holdningsundersøgelser blandt en gruppe på omkring 25 borgere. Metoden bygger på en kombination af gruppeinterviews og spørgeskema. Gruppeinter-

⁴ "Personal Internet Security" 2007, published by the Authority of House of Lords

viewene skaber liv i debatten og sikrer, at deltagerne får mulighed for at inddrage aspekter, som ikke kan rummes i spørgeskemaet. Til gengæld sikrer spørgeskemaet, at alle deltagerne høres, og at der skabes sammenlignelige data på væsentlige områder.

De 23 borgere, der mødte op i Odense, havde forud for interviewmødet fået tilsendt de af arbejdsgruppen udarbejdede løsningsforslag. Interviewmødet varede tre timer og blev indledt med en introduktion til emnet, hvorpå spørgeskemaer blev uddelt. Deltagerne havde en lille time til at besvare spørgeskemaerne. Herefter blev deltagerne inddelt i mindre grupper og interviewet omkring deres holdninger til de præsenterede løsningsforslag. Gruppeinterviewene varede lidt over en time.

Udvælgelsen af deltagerne er foregået i flere skridt. Først udsendtes 2000 invitationer til borgere bosat i Odense Kommune ved hjælp af et tilfældigt udtræk fra CPR-registeret. Heraf meldte omkring 70 borgere positivt tilbage, og blandt disse udvalgte 30 borgere til at deltage i interviewmødet. Gruppen af deltagere er sammensat på en måde, der korresponderer nogenlunde med den befolkningsmæssige fordeling i Danmark på køn, alder, uddannelse og beskæftigelse.

4.2 Rapportens indhold

Først præsenteres løsningsforslagene i den form, hvori de blev præsenteret for deltagerne forud for interviewmødet. Hvert forslag rummer både en teknisk beskrivelse og en præsentation af mulige fordele og ulemper, som arbejdsgruppen har ønsket, at deltagerne på interviewmødet skulle forholde sig til.

Derefter følger en analyse af resultaterne fra interviewmødet. Denne er hovedsagelig af kvalitativ karakter, idet den bygger på diskussionerne mellem deltagerne på interviewmødet, men analysen rummer også kvantitative data fra besvarelserne af spørgeskemaet, som deltagerne udfyldte på mødet.

Endelig præsenteres arbejdsgruppens anbefalinger, som alle relaterer sig til såvel resultaterne fra interviewmødet som til medlemmernes fælles overbevisning.

En ordliste med forklaringer på it-termer kan ses bagerst i rapporten. Desuden kan spørgeskemaet med tilhørende svartabeller downloades fra projekthjemmesiden på www.tekno.dk. Udskrifter af gruppeinterviewene kan rekvireres i rå form hos Teknologirådet.

5. Løsningsforslag

I dette afsnit følger løsningsforslagene udarbejdet af arbejdsgruppen i den form, de blev præsenteret i for deltagerne, forud for interviewmødet. Dog er introduktionen til løsningsforslagene udeladt. Rækkefølgen af forslagene er ikke prioriteret, og forslagene sigter på forskellige problemer af sikkerhedsmæssig karakter. Nogle af forslagene overlapper hinanden forstået på den måde, at de opstiller forskellige løsninger på de samme problemer. Det betyder, at indføres et løsningsforslag, vil det muligvis være overflødigt at indføre et andet. Endelig er et par af løsningsforslagene trinopdelt forstået på den måde, at først er grundideen med forslaget beskrevet, og derefter følger forskellige udvidelser af forslaget.

Med løsningsforslagene udsendtes til borgerne også en ordliste, hvori en række centrale begreber, fx virus og internetudbydere, er samlet med en kort forklarende tekst. Ordene, der indgår i ordlisten er markeret med en stjerne *, første gang de optræder i løsningsforslagene. Denne ordliste er at finde i bagerst i rapporten.

5.1 Digital identitet

Meget af den kontakt med offentlige myndigheder og private firmaer, som før i tiden indbefattede personlig eller skriftlig henvendelse, foregår i dag over internettet. Du kan melde din flytning, skifte læge, rette din selvangivelse, købe varer og udføre utallige andre ærinder bare ved at klikke lidt rundt på nettet. Når du benytter services på nettet, udveksles personfølsomme data. Falder disse data i de forkerte hænder, kan de misbruges til fx at stjæle dine penge eller din identitet, dvs. at kriminelle får mulighed for at udgive sig for at være dig på nettet, og nysgerrige personer kan få ting at vide om dig, som du ikke ønsker, at andre skal kende til.

Når du bevæger dig rundt på nettet, har du en interesse i, at andre ikke kan udgive sig for at være dig, og at uvedkommende ikke har adgang til de personlige informationer, du sender og modtager. Det er nødvendigt, at du kan identificere dig, og at din identifikation* er så sikker som muligt. Disse behov kan opfyldes med en digital identitet⁵.

Hvad er en digital identitet?

Den digitale identitet, der foreslås her, består af id-data og en adgangskode. Forslaget indebærer, at den digitale identitet skal benyttes, når du vil identificere dig på nettet, fx i forbindelse med netbank eller når du skal kommunikere med det offentlige over nettet. Id-dataene indeholder information om, hvem du er, fx cpr-nummer, men ikke yderligere personlige informationer, altså ingen lægejournaler eller lignende. Dine id-data kan opbevares på et usb-stick* eller på en chip, som fx kan sidde i et plastikkort, ligesom dit dankort, eller i en mobiltelefon, ligesom dit simkort gør det. Formen af din digitale identitet, altså hvor dine id-data er gemt, betyder ikke så meget. Det afgørende er, at identiteten er transportabel og består af to dele: En kode, som skal huskes udenad, og et hardware* element, hvor dine id-data er lagret, fx en chip på et kort. Koden vil være længere end den firecifrede pinkode og består af både tal og bogstaver. Ekspert på området siger, at sådan en digital identitet vil beskytte dine personlige oplysninger bedre end den digitale signatur*, som nogle danskere allerede har fået tilsendt og installeret på deres computere. I modsætning til den nuværende digitale signatur

⁵ Arbejdsgruppen har valgt at bruge betegnelsen "digital identitet", for at kunne tænke frit og ikke lade sit løsningsforslag være bundet af at skulle forholde sig til den digitale signatur. Det skal imidlertid understreges, at elementerne i det forslag, gruppen her præsenterer, godt kan indarbejdes i en ny udgave af den digitale signatur.

er den digitale identitet, som foreslås her, ikke installeret på computeren, men tilsluttet via hardware elementet. Dette gør den digitale identitet sværere for uvedkommende at misbruge sammenlignet med den nuværende digitale signatur.

I de følgende afsnit beskrives to forskellige måder, hvorpå den digitale identitet kan anvendes. Første trin omhandler den digitale identitet i forbindelse med kommunikation med det offentlige. På andet trin udvides den digitale identitet til også at omfatte adgang til netbank og andre situationer, hvor identifikation er nødvendig.

Offentlig digital identitet

Forestil dig, at du og alle andre borgere får tildelt en digital identitet, som beskrevet ovenfor. Den digitale identitet skal *altid* anvendes, når du ønsker at benytte dig af offentlige services på nettet, fx melde din flytning, skifte læge, rette din selvangivelse osv. Identiteten er mobil, og du kan derfor udføre dine ærinder med det offentlige via en hvilken som helst computer med internetforbindelse, fx en computer på et bibliotek. Og du kan bruge den samme kode, når du skal udveksle personlige oplysninger med kommunen, skattevæsenet osv. Hvis du ikke ønsker at benytte den digitale identitet, har du ikke mulighed for at interagere med det offentlige via internettet.

Gennemføres dette forslag, bliver det sværere for kriminelle at misbruge din digitale identitet, medmindre de har både din adgangskode og dine id-data. Hvis dine id-data (som kan opbevares på fx en chip eller et usb-stick) bliver væk eller stjålet, har du mulighed for at spærre din digitale identitet, ligesom fx dit dankort, og få en ny. Du kan også få en ny adgangskode, hvis du har glemte den gamle.

Fordele og ulemper

Indføres den digitale identitet, er det slut med at huske på mange forskellige koder til forskellige offentlige services på nettet. Med én kode og én lagringsenhed for dine id-data, fx et usb-stick eller en chip i et plastikkort eller en mobiltelefon, får du en mere sikker digital signatur og identifikation, som du kan tage med dig overalt. Det bliver sværere at stjæle din digitale identitet, fordi både id-data og kode er nødvendige for at anvende identiteten. Den digitale identitet hjælper dig til at opnå en bedre beskyttelse af dine personlige oplysninger, men hvad siger du til at blive påtvunget sådan en sikkerhed?

Indføres den digitale identitet, skal du anvende den, hvis du fuldt ud vil kunne udnytte det offentlige serviceudbud. Borgere, som ikke har så nemt ved at bruge it, vil dermed ikke få samme muligheder for at benytte offentlige services lige så nemt og bekvemt som borgere, der har nemt ved det. Sådan er det allerede nu, hvor de, der ikke har en computer, eller har svært ved at bruge den på internettet, må benytte sig af telefonen eller personligt fremmøde. Flere og flere services vil i fremtiden blive tilgængelige på nettet – og det offentliges åbningstider for personlig kontakt vil måske skrumpes. Er det rimeligt, at alle offentlige services ikke er lige tilgængelige for enhver? Der er altså argumenter både for og imod indførslen af en digital identitet. Hvilke synes du vejer tungest?

Fælles digital identitet til offentlige og private services

Ud over offentlige services på nettet, kan den digitale identitet i princippet udvides til at omfatte alle situationer, hvor du skal identificere dig over for private virksomheder, hvad enten du færdes på nettet eller i den fysiske verden. Hidtil har bankerne fx haft deres eget sikkerhedssystem til netbank parallelt med den offentlige digitale signatur. I forbindelse med fornyelse af den nuværende offentlige digitale signatur er det måske en god ide at udarbejde den digitale identitet i samarbejde med bankerne?

Du vil også kunne anvende din digitale identitet, når du køber varer over nettet. Dermed kan det blive mere sikkert for dig at handle på nettet, når du, frem for blot at indtaste fx dankortoplysninger, også bruger din digitale identitet til at identificere dig som ejeren af dankortet. Den digitale identitet kan også anvendes uden for nettet som medlemskort til foreninger, fitnessklubber m.v., til adgang til diskoteker, køb af spiritus eller i andre forbindelser med aldersbetinget adgangsbegrænsning.

Fordele og ulemper

Fordelen ved at samle alle kort i ét med den digitale identitet er, at du kun behøver huske én kode samtidig med, at selve identifikationen kan blive sikrere for dig. Men hvis uheldet er ude, og din lagringsenhed med id-data havner i de forkerte hænder, er du til gengæld mere udsat for misbrug, idet din digitale identitet kan misbruges i mange flere sammenhænge. Måske foretrækker du alligevel at have flere forskellige digitale identiteter, selvom en samlende identitet ville være nemmere? Og måske foretrækker du også at adskille offentlig og privat adgangskontrol?

5.2 Automatiske sikkerhedsopdateringer

En sikkerhedsopdatering* er en opdatering* til et styresystem*, fx Windows, eller et program*, fx Internet Explorer. Opdateringen retter op på fejl og mangler i styresystemer eller programmer, der ellers kan gøre det let for hackere at bryde ind i din computer via internettet. Det er derfor en fordel, at så mange brugere som muligt er opdaterede, da en computer med manglende sikkerhedsopdateringer er lettere at bryde ind i og kan misbruges som mellemlid i it-kriminalitet. Hvis dine programmer ikke er opdaterede, kan det altså give problemer for både dig selv og for andre brugere på nettet.

Nogle brugere vil gerne selv tage stilling til, hvorvidt de vil tage imod en bestemt opdatering eller ej, fordi de har tiltro til, at de selv kan håndtere sikkerheden. Andre brugere takker nej til opdateringer, fordi de ikke kan overskue dem. Derudover har nogle måske installeret software* uden licens, piratkopier, og takker nej af frygt for, hvordan en evt. opdatering vil påvirke deres ulovligt installerede software. Dette er ofte ubegrundet; en opdatering fungerer som regel også til piratkopier.

Ikke alle opdateringer er fejlfrie

Selvom langt hovedparten af opdateringer fungerer fejlfrit, kan nogle opdateringer medføre problemer. Dels kan der være fejl i selve opdateringen; dels kan opdateringen udløse problemer med fejlfulde programmer, der indtil opdateringens installering har kørt upåklageligt trods deres fejl; og endelig kan der opstå problemer ved samspillet mellem den installerede opdatering og andre programmer, selvom både opdateringen og de andre programmer i sig selv er fejlfri.

Så sent som i sommeren 2006 medførte en fejlupdate til Windows, at cd-rommer solgt i tusindvis med programmer som Den Store Danske Encyklopædi og div. ordbøger ikke var i stand til at køre. Løsningen var enten at afinstallere den skyldige fejlupdate eller at installere en specialupdate. Det er også kendt fra computerspilmiljøet, at visse opdateringer får programmer til at køre dårligere end uden opdateringerne. Opdateringer kan altså medføre irriterende fejl, men heldigvis er der langt imellem, at det sker.

Tvungne sikkerhedsopdateringer

Forestil dig, at sikkerhedsopdateringer skal ske tvungent og automatisk. Så snart der udsendes en ny sikkerhedsopdatering, vil din computer downloade* og installere den, uden først at bede om din accept. Du får ikke mulighed for at melde opdateringen fra. Sikkerhedsopdateringerne skal dog komme særskilt, således at du stadig kan takke nej til normale programopdateringer, der ikke har

betydning for din computers sikkerhed. En normal programopdatering kunne fx være en opdatering til tekstbehandlingsprogrammet Word, således at programmet kan håndtere flere filformater.

Fordele og ulemper

Med automatiske sikkerhedsopdateringer er du og alle andre opdaterede, og dermed mindskes risikoen for virus*angreb mv. samt it-kriminelles muligheder for at misbruge computere. Opdateringerne hjælper dig således med at gøre din computer og din færden på nettet mere sikker og mindsker samtidig risikoen for, at du spreder virus og lignende til andre – og de til dig. Men sikkerhedsopdateringerne er tvungne, og du mister derfor lidt kontrol over din computer. I tilfælde af en fejlfuld opdatering har du ikke længere mulighed for at annullere den enkelte opdatering. Og du har ikke mulighed for at bestemme, med hvilken opdatering dine programmer skal køre.

Er det rimeligt at tage retten til selvbestemmelse fra den del af brugerne, der gerne selv vil tage stilling til sikkerhedsopdateringerne? Og vil du acceptere det besvær, opdateringerne kan give en sjælden gang imellem til gengæld for at højne din egen og andres sikkerhed?

5.3 Pc-syn

Offentligt pc-syn

Som beskrevet i forslaget ovenfor er din egen sikkerhed på nettet afhængig af andre netbrugeres sikkerhed. Jo flere syge børn, der er i vuggestuen, desto større risiko er der for, at dit eget barn også bliver smittet. Foruden din fordel ved selv at have en sikkerhedsopdateret computer, er det altså en fordel for dig, at andre netbrugere også har det.

I dag er den direkte grund til at have en sikkerhedsopdateret computer bedre at kunne beskytte den mod truslerne på nettet, fx virusangreb. Men at tage sig sammen til at få styr på it-sikkerheden kan være svært for brugere, der ikke har oplevet problemer. Tænk, hvis det offentlige ville hjælpe og tilskynde dig og andre brugere til at have sikkerheden i orden?

Adgangskontrol til alle offentlige hjemmesider

Dette løsningsforslag går på, at det offentlige skal påtage sig et større ansvar for at højne it-sikkerheden. Først ved at hjælpe private brugere, altså dig, til at installere sikkerhedssoftware og herefter ved vedvarende at kontrollere, om sikkerhedssoftwaret og andet software på din computer er opdateret. Måden, hvorpå det skal gøres, er at kontrollere adgangen til *alle* offentlige hjemmesider, dvs. alt lige fra dit lokale biblioteks hjemmeside til skat.dk. Kontrollen sker ikke for at beskytte offentlige hjemmesider, men for at beskytte brugerne. Det offentlige kan godt på anden vis håndtere sikkerheden på sine egne hjemmesider, men ved jævnligt at kontrollere it-sikkerheden på brugernes computere bidrager det offentlige på denne måde til, at din og andre brugeres færden på hele nettet bliver mere sikker.

For at få adgang til en hvilken som helst offentlig hjemmeside skal du have en elektronisk attest på, at din computer opfylder en række sikkerhedskriterier. Kriterierne kunne være, at der skal være installeret og opdateret sikkerhedssoftware på din computer, fx antivirusprogram, firewall*, anti-spyware*, samt at computerens styresystem og en række softwareprogrammer (fx Word) skal være opdateret. Kriterierne fastsættes af en offentlig instans, fx IT- og Telestyrelsen.

Den elektroniske attest kan indhentes på en særlig hjemmeside, som du også har adgang til, før du har attesten. Her påbydes du en computerscanning efter ovenstående kriterier. Scanningen kan sammenlignes med syningen af en bil. For at bilen har tilladelse til at køre i trafikken, skal den opfylde en række sikkerhedskrav. Tilsvarende skal din computer opfylde en række sikkerhedskrav, før

du får attesten. Selve computerscanningen tager kun fem minutter og kan ske om natten eller i baggrunden, mens du arbejder med noget andet.

Attesten er tidsbegrænset og gældende en måneds tid, hvorefter din computer atter skal scannes, hvis du ønsker adgang til en hvilken som helst offentlig hjemmeside. Resten af internettet, og selvfølgelig hjemmesiden, hvor attesten nedhentes, er stadig tilgængeligt for dig, uanset om du har attesten eller ej. Opfylder din computer ikke kriterierne ved computerscanningen, får du ikke attesten. Du henvises herefter til en hjemmeside, der indeholder informationer, telefonnummer til en hotline og links til fx gratis antivirusprogrammer, så du hjælpes til at få en sikrere computer.

Pointen ved forslaget er, at du, ligesom alle andre brugere, motiveres til at holde din computer sikkerhedsopdateret, da du ellers ikke vil kunne få attesten og dermed nægtes adgang til offentlige hjemmesider. Og måske er det meget godt jævnlige at blive mindet om at holde computeren sikkerhedsopdateret? Det er allerede en del af mange private virksomheders sikkerhedspolitik at scanne computere. Så hvorfor ikke også gøre det til en del af din og andre private brugeres?

Fordele og ulemper

Du får regelmæssigt kontrolleret om din computer har sikkerheden i orden, og hvis der er problemer, kan du få hjælp til at løse dem. Selve scanningen kan dog være tidskrævende og irriterende, og du har ingen mulighed for at vælge den fra, hvis du vil have adgang til offentlige hjemmesider. Alt andet lige bliver det mere besværligt at få adgang til offentlige hjemmesider, fordi det nu kræves af dig, at du har styr på dine sikkerhedsopdateringer og opdaterer din attest jævnlige. Det er måske store krav at stille til brugere, der i forvejen har svært ved it-sikkerhed. Eller også er det en god måde at hjælpe dem på vej? I hvert fald vil forslaget også have den væsentlige effekt, at din færden på resten af nettet bliver mere sikker. Og hvis din nabo tvinges til at være sikkerhedsopdateret, er risikoen, for at du rammes af et virusangreb, mindre.

Er det rimeligt at opstille minimumskrav, om på hvilket niveau din it-sikkerhed skal være, før du tillades adgang til offentlige hjemmesider? Eller skal det offentlige blande sig uden om din sikkerhed på nettet?

Pc-syn også krævet til netbank

Det er også i bankernes interesse, at det generelle sikkerhedsniveau hæves. Derfor kunne bankerne have en interesse i at stille de samme krav som ovenfor til, at din pc skal være synet og scannet (enten af det offentlige eller af en anden instans), før du får adgang til netbanken. Det er nemlig dem, der skal dække hovedparten af tabet, hvis du bliver frarøvet penge via netbanken. Synes du, det er rimeligt, hvis bankerne stiller krav til, at din computer er nyligt synet, før du kan få adgang til netbanken?

5.4 Tvungen mailfiltrering samt installation af firewall og virusfilter

En internetudbyder* er en virksomhed, der giver dig adgang til internettet, fx TDC eller Cybercity. Internetudbydere spiller en central rolle i kontrollen med netværkstrafikken og har derfor flere muligheder for at højne sikkerheden på nettet. I det følgende beskriver vi to forskellige.

Tvungen mailfiltrering

De fleste internetudbydere tilbyder i dag deres kunder at scanne mails og filtrere dem fra, der indeholder virus. De frasorterede mails ryger direkte ind i en særlig karantæne-mappe, hvorfra det stadig, hos de fleste udbydere, er muligt for dig som bruger at læse dem. Der er dog fortsat mange brugere,

som takker nej til at få deres mails scannet og filtreret. Og på den måde får meget virus lov til at snige sig ind i indbakken og sprede sig til andre computere.

For at dæmme op for den mængde virus, der flourer via mailudveksling, ville en løsning være, at scanning og filtrering af mails ikke sker frivilligt, men automatisk. Dette løsningsforslag indebærer, at du ikke kan have en mailadresse hos din internetudbyder, uden at dine mails bliver scannet og en del af dem frasorteret. De frasorterede mails ryger i karantænemappen, som du kun kan få adgang til ved at logge på en særlig hjemmeside hos din internetudbyder. Du kan altså stadig læse de frasorterede mails, men det bliver mere besværligt for dig at gøre det.

Fordele og ulemper

Når mails gennem internetudbydernes mailservere scannes og virusbefængte mails frasorteres, vil en større del af den mængde virus, der spredes via mail, blive fanget. Risikoen for at modtage og selv sprede virus via mail mindskes, men du mister også kontrollen over, hvilke mails du modtager i din indbakke.

Mailfiltrering som standardindstilling

I stedet for at gøre ordningen tvungen kan mailfiltrering være en standardindstilling, når kunder anvender internetudbydernes mailservices. I dag skal kunderne selv aktivt tilvælge mailfiltrering. Ved at gøre filtrering til standardindstilling vil en større del af brugerne få scannet deres mail. Valgfriheden er bevaret, idet du og andre brugere har mulighed for at fravælge filtreringen. I forhold til forslaget ovenfor, hvor filtreringen sker tvungent, er den samlede forbedring af sikkerheden mindre ved dette forslag, idet nogle vil fravælge filteret og potentielt kunne sprede virus til andre.

Tvungen installation af firewall og virusfilter

I dag blander internetudbyderne sig ikke i deres kunders it-sikkerhed. At lade internetudbyderne scanne al internettrafik for virus og malware* ville blive usandsynligt dyrt og nedsætte hastigheden på nettet væsentligt. Det smarteste sted at filtrere trafikken er teknisk set på den enkelte brugers computer. Dette forslag indebærer derfor, at internetudbyderne skal stille krav til alle deres kunder om, at de skal have installeret firewall og virusfilter* på deres computer, før de overhovedet får lov til at komme på nettet. Forslaget overlader det til den enkelte bruger at sørge for installationen, men internetudbyderne skal tilbyde vejledning om programtyper og installation til deres kunder.

Fordele og ulemper

Har du ikke installeret et virusfilter og en firewall, nægtes du adgang til nettet. Er det et rimeligt krav at stille? Programmerne kan koste penge (nogle kan fås gratis på nettet) og besvær, men til gengæld vil du selv sprede mindre malware til andre – og de til dig.

5.5 Sikkerhedsmærkning af it-produkter

Der kan være stor forskel på sikkerhedsniveauet på forskellige it-produkter, men som forbruger – og ofte også forhandler – kan det være svært at se forskel. Typisk vælger mange derfor produkterne ud fra prisen, uden at tænke over sikkerheden.

Et forslag, der kan modvirke denne tendens, er at indføre en mærkningsordning for it-produkter ligesom smiley-ordningen for restaurationshygiejne. Ordningen skal gælde både for software i almindelighed og software integreret med hardware. Fx skal hardware som usb-sticks og computere mærkes, selvom det i princippet er softwaret på usb-sticket eller computeren, der bedømmes, og ikke selve hardwaret.

Ordningen skal gøre det nemmere for dig at vælge sikre produkter. Produkternes brugervenlighed mht. opsætning af sikkerhedskonfigurationer skal også indgå som en del af vurderingen. Sikkerheden skal med andre ord være let at få op at køre, når produktet tages i brug. Formålet er at give øget konkurrence producenterne imellem ved at gøre sikkerhed til en konkurrenceparameter.

Fordele og ulemper

Med en mærkningsordning får virksomhederne incitament til at sætte fokus på sikre og brugervenlige produkter. Samtidig bliver det nemmere for dig som kunde at vælge mellem forskellige produkter. Mærkningsordningen medfører dog udgifter for producenterne, idet de skal betale for at få sikkerhedsgodkendt deres produkter. Som kunde er det i sidste ende dig, der kommer til at betale denne merudgift. Er du villig til at betale ekstra for visheden om, at den vare, du vælger, har it-sikkerheden i orden?

5.6 Blokering af adgang til skadelige hjemmesider

Der findes på internettet en del skadelige hjemmesider. Her tænker vi især på to forskellige grupper af skadelige hjemmesider. Den første gruppe indbefatter hjemmesider, hvor du enten udsættes for eller har adgang til skadelig software såsom virus og andet malware. Måske startes en virus-download uden din accept, ligeså snart du kommer ind på siden, eller også lokkes du uvidende til at downloade den. Ved at have opdateret sikkerhedssoftware og opdaterede programmer kan du reducere din sårbarhed over for disse typer af skadelige hjemmesider. Den anden gruppe indeholder phishing* hjemmesider, dvs. falske hjemmesider, hvor du lokkes til at opgive personlige oplysninger, fx taste dit netbank-login, som siden hen misbruges. Her hjælper kun din sunde fornuft.

Du kan til dels gardere dig mod skadelige sider ved at holde din computer sikkerhedsopdateret eller bruge din sunde fornuft. Men forestil dig, at skadelige hjemmesider bliver sortlistet og blokeret, så du slet ikke har adgang til dem.

Sortlistningen af skadelige hjemmesider skal ifølge dette forlag udføres af et internationalt eller nationalt overvågningscenter. Her fastsætter en bredt sammensat gruppe af teknikere, jurister mfl. kriterier for sortlistningen. Du kan også som privat bruger indberette sider, du synes, ser mistænkelige eller skadelige ud. Overvågningscenteret kan efter en vurdering af siden påbyde internetudbydere at blokere for den anmeldte hjemmeside. Når en skadelig side er blokeret, kan du ikke længere få adgang til den via nettet.

Fordele og ulemper

Ved at blokere for skadelige hjemmesider bliver nettet sikrere at færdes på. Til gengæld har du ikke selv kontrol over, hvilke hjemmesider du har adgang til. Andre vurderer, hvorvidt en side er farlig for dig, og dette vil muligvis indbefatte nogle fejlvurderinger, således at ufarlige hjemmesider sortlistes. Er en side blokeret, kan sidens ejer anke blokeringen og få åbnet siden igen. Behandlingstiden for ankesagen kan dog være lang og dermed medføre omkostninger for både sidens ejer og brugere. Hvor går grænsen mellem beskyttelse af private brugere og censur? Og hvem skal vurdere, om en side er skadelig eller ej?

5.7 Online lagring af data

Dette er ikke et egentligt løsningsforslag, men en beskrivelse af en udvikling, som vi vil bede dig om at vægte fordele og ulemper ved.

Stadigt flere it-brugere opbevarer data på nettet ved brug af online*, kommercielle udbydere. Og måske gør du det også selv uden egentlig at tænke videre over det? Der er mange forskellige måder, hvorpå du kan opbevare data på nettet. Hvis du bruger webmail*, en mailservice*, der er tilgængelig på nettet, fx Gmail* og Hotmail*, kan du eksempelvis gemme personlige filer ved at sende en mail til dig selv og vedhæfte filerne. Filerne ligger i så fald som vedhæftninger til mails i din indbakke, der er gemt hos udbyderen af webmailen. En anden udbredt måde at opbevare data online* på er at uploade* dokumenter, billeder eller andre filer i sociale netværk på nettet. Et socialt netværk på internettet er en hjemmeside, hvor du kan kommunikere og udveksle filer med dine venner, fx Facebook eller MySpace. Der findes også en lang række online programmer, som gratis tilbyder dig opbevaring og deling af data. Eksempelvis udbyder Google et billedprogram Picasa, hvor du kan uploade billeder og dele dem med dine venner.

Når først dine data ligger opbevaret på nettet, hvad enten det er i din mailindbakke eller på hjemmesider, fx sociale netværk, behøver du ikke længere bekymre dig om at tage en sikkerhedskopi af dem. Hvis din computer går ned, ligger dine data jo stadig gemt hos udbyderne af disse services, og du kan få adgang til dine data over nettet. Fælles for udbyderne er, at de som oftest stiller deres services gratis til rådighed for dig ved hjælp af reklamefinansiering.

Der er delte meninger om denne kommercielt drevne udvikling. Selvom du er mere sikker på ikke at miste dine data, hvis de er gemt online i stedet for på din egen computer, er der en større risiko for, at andre får mulighed for at se dem. De kommercielle udbydere har fx en interesse i at dele dine personlige oplysninger med reklamebureauer, som vil målrette deres reklamer mest muligt. Et eksempel herpå er webmailudbyderen Gmail. Enhver mail, du modtager, scannes automatisk med det formål, at de reklamebannere, der vises, når du åbner mailen, passer til indholdet af mailen.

Fordele og ulemper

Når dine data er lagret online, er du bedre sikret mod datatab som følge af computernedbrud eller virus. Dine data ligger nemlig "trygt" gemt på servere i et professionelt it-miljø hos en kommerciel udbyder. Til gengæld kan du ikke helt vide dig sikker på, at dine private data forbliver private. For i princippet har den kommercielle udbyder adgang til at se dine data og måske videregive dem til en tredjepart med kommercielle interesser for øje.

Hvad vægter tungest hos dig? At dine data bevares sikkert hos en kommerciel udbyder, eller at dine private data forbliver private?

6. Analyse

I denne del af rapporten præsenteres resultaterne fra interviewmødet, hvor deltagerne har forholdt sig til løsningsforslagene i den forrige del af rapporten. Først følger et afsnit om deltagerne generelle forhold og indstilling til it-sikkerhed. Dernæst analyseres de syv løsningsforslag et ad gangen. Hvert afsnit indledes kort med en præsentation af de væsentligste resultater fra spørgeskemabesvarelserne⁶. Herefter inddrages materialet fra gruppeinterviewene, hvorpå analysen hovedsagelig er fundet, og deltagerne argumenter for og imod de enkelte løsningsforslag præsenteres. Som oftest er kun få deltagere i deres argumentation entydigt for eller imod de respektive løsningsforslag. Således kan den samme deltager eksempelvis fremføre argumenter både for og imod et givent forslag. Det skal bemærkes, at citater fra gruppeinterviewene er medtaget for at eksemplificere borgernes holdninger, og at analysegrundlaget således er større end det fremlagte.

6.1 Generelt om deltagerne forhold og indstilling til it-sikkerhed

Fælles for deltagerne er, at de alle bruger internettet privat, og at langt hovedparten af deltagerne (20 ud af 22) i spørgeskemabesvarelserne angiver at være forholdsvis bekymrede for sikkerheden ved færden på nettet. Men herefter hører enigheden op, og deltagerne kan overordnet set opdeles i to nogenlunde lige store grupper.

Den ene gruppe føler sig generelt tryk ved brug af internettet og udtrykker ikke den store bekymring under interviewene:

"Du skal ikke være så bange for al det der it. Brug det dog."

Nogle af disse deltagere ser sig i stand til at håndtere egen it-sikkerhed og mener, at langt de fleste problemer kan undgås ved kritisk stillingtagen samt omtanke ved færden på nettet:

"Generelt når vi snakker sikkerhed på nettet, så synes jeg, at meget af det omhandler ganske almindelig sund fornuft i den måde, man gebærder sig på."

Den anden gruppe har svært ved at overskue it-sikkerheden og føler afmagt:

"Jeg synes, det med it-sikkerheden er frygteligt uoverskueligt for almindelige mennesker, og jeg har ikke tiltro til noget som helst."

Godt halvdelen (13 ud af 22) af deltagerne tilkendegiver i spørgeskemaet, at der er muligheder på nettet, de ikke benytter sig af, da de er nervøse for sikkerheden. Blandt andet kan downloading af ukendte filer, installation af ukendte programmer, opgivelse af kortoplysninger eller mail, internethandel og ikke-dansksprogede sider afholde deltagerne fra at udnytte nettets mange muligheder.

Som oftest er denne gruppe afhængig af hjælp til it-sikkerhed udefra. Enten fordi de ikke magter at håndtere it-sikkerheden:

⁶ En samlet oversigt over alle resultater fra spørgeskemabesvarelserne kan hentes på www.tekno.dk.

"Men når jeg sidder derhjemme helt privat med mit eget gardin og min egen potteplante, så har den [computeren] bare at være sød ved mig. Og det er den ikke altid. Så bliver jeg hys, og så bliver jeg ked af det. Fordi jeg forstår det ikke, og jeg ved ikke, hvad jeg har gjort. ... og jeg bliver ærgerlig over, at mine evner ikke rækker til mere."

Eller også fordi det bare er nemmere at lægge ansvaret over på andre i husstanden:

"Jeg har bare ladet min mand stå for alt det der med sikkerheden på computeren. Det er egentlig ikke fordi, jeg ikke har forstand på det. ... Altså på en eller anden måde er det bare nemmere at lægge ansvaret fra sig. Det er jo lidt dumt, for på den måde mister man jo også hurtigt overblikket over, hvad der sker af nye ting."

Typisk klarer deltagerne i denne gruppe sig ved hjælp fra familie og bekendte. Foreligger denne mulighed ikke, betaler de for professionel hjælp.

Under gruppeinterviewene fylder personlige beretninger om problemer med it-sikkerhed meget. Blandt deltagerne hersker udbredt frustration over egen manglende evne til at håndtere sikkerheden og en mere generel forundring over de problemer, manglende it-sikkerhed kan medføre. Knyttet til disse beretninger udtrykkes ofte et ønske om, at nogle burde indrette it-systemerne mere hensigtsmæssigt og brugervenligt, og at det bør være nemmere at få hjælp, når problemer opstår.

I stand til at håndtere it-sikkerhed på egen hånd?

At deltagerne kan opdeles i to grupper, der henholdsvis ser sig selv i stand eller ude af stand til at håndtere egen it-sikkerhed, ses også i spørgeskemabesvarelserne. Her angiver 10 ud af 22 deltagere at de, til dels, kan håndtere it-sikkerhed på egen hånd, mens de resterende 12 deltagere ikke føler, at deres evner rækker. Inddeles disse svar efter køn, fremgår det, at de mandlige deltagere i langt højere grad føler sig i stand til at håndtere egen it-sikkerhed end de kvindelige deltagere; henholdsvis 7 ud af 11 mandlige deltagere mod 3 ud af 11 kvindelige deltagere. Foretages tilsvarende inddeling efter alder, ses kun en svag tendens i retning af, at en større del blandt de 20-44-årige føler sig i stand til at håndtere egen it-sikkerhed, end den ældre aldersklasse gør det; henholdsvis 5 ud af 9 deltagere blandt de 20-44-årige mod 5 ud af 13 deltagere blandt de 45-70-årige. En inddeling efter uddannelse afslører ingen klare tendenser.

Hvor skal ansvaret for den enkelte brugers it-sikkerhed placeres?

Om den enkelte deltager selv ser sig i stand til at håndtere sin egen it-sikkerhed, spiller ikke overraskende ind på deltagerens opfattelse af, hvor ansvaret for it-sikkerhed skal placeres. Besvarelserne indikerer, at størstedelen af deltagerne mener, at den enkelte bruger er ansvarlig for it-sikkerheden på egen computer. De fem deltagere, der ikke tilslutter sig denne holdning, ser sig alle selv ude af stand til at håndtere egen it-sikkerhed.

Selvom deltagerne først og fremmest placerer ansvaret for it-sikkerhed hos den enkelte bruger, er mange af dem, under stillingtagen til de konkrete løsningsforslag, mere villige til at fralægge sig en del af ansvaret end deres principielle indstilling indikerer. Tendensen i gruppeinterviewene er, at de fralægger sig ansvaret til fordel for en forøgelse af sikkerheden, selvom dette medfører både mindre selvbestemmelse og øget kontrol ovenfra. Deltagerne har generel stor forståelse af de dilemmaer, som løsningsforslagene stiller dem overfor. En deltager udtrykker det således:

"Principielt er jeg imod sådan et overvågningssamfund. Men på den anden side, som jeg siger, det er svært som almindelig bruger at overskue alle de der ting, hvor man fak-

tisk skal have ekspertviden for at være sikker på at få lukket alle hullerne. Øh, så hvad skal man vælge?”

6.2 Digital identitet

Offentlig digital identitet

Af spørgeskemabesvarelsene fremgår det, at størstedelen af deltagerne går ind for indførslen af den digitale identitet til offentlige services (17 ud af 21 deltagere). Dog fastholder omkring halvdelen, at it-svage borgere, der ikke er vant til at bruge it-teknologi af forskellige årsager, ikke skal hæftes mere af den teknologiske udvikling, end de allerede er.

Argumenter for

Under gruppeinterviewene angiver deltagerne to klare argumenter for indførslen af den digitale identitet: væsentligst er øget sikkerhed, dernæst følger øget bekvemmelighed ved kun at skulle benytte én adgangskontrol til offentlige services. Deltagerne accepterer præmissen om, at forslaget medfører højere sikkerhed, som givet i løsningsforslagene, men giver også udtryk for, at de ikke selv kan vurdere det. Dog hæfter flere deltagere sig ved den eksterne hardwaredel af den digitale identitet som højnende for sikkerheden. At hardwaredelen af den digitale identitet således ikke konstant ligger lagret på computeren, men kan 'holdes i hånden' og sluttes til eller fra computeren efter behov øger, ifølge deltagerne, sikkerhed, hvilket en deltager udtrykker her:

”Man har den der usb eller chip, man stikker i computeren; det synes jeg højner ens egen personlige tryghed.”

Argumentet om øget bekvemmelighed ved kun at skulle benytte én adgangskontrol til offentlige services bundes i betragtningen om, at kun én kode er nødvendig for at få adgang til alle offentlige online services, i modsætning til i dag, hvor brugeren ofte skal anvende flere forskellige koder, når offentlige online services benyttes.

Argumenter imod

Som eneste argument mod indførslen af den offentlige digitale identitet nævner deltagerne under gruppeinterviewene konsekvensen af at miste den digitale identitet. Herved afskæres brugeren midlertidigt fra at kommunikere med det offentlige over nettet, og ydermere foreligger risikoen for misbrug af personlige oplysninger.

Problematikken omkring it-svage borgere

It-svage borgeres begrænsede muligheder for at benytte den digitale identitet ligger deltagerne meget på sinde og fylder således betydeligt i debatten om den digitale identitet. Imidlertid vægtes hensynet til de it-svage borgere ikke særlig højt som modargument til indførslen af den digitale identitet. Som en deltager klart udtrykker det:

”Man kan jo ikke bremse udviklingen, fordi der sidder en masse mennesker og ikke kan finde ud af det.”

Derimod er deltagerne overvejende enige i, at der skal gøres en indsats for at hjælpe borgere, der ikke har nemt ved it. It-svage borgere skal kunne henvende sig et sted for at få hjælp til at anvende den digitale identitet, samtidig med at offentlige instanser fortsat skal være tilgængelige for personlig henvendelse for alle borgere, der ønsker at benytte sig af det. En deltager forklarer det sådan:

"I det øjeblik man gør flere ting statsstyret, kontrolleret, så ligger der også et ansvar på vores stat om at sørge for, at de svageste i samfundet også har mulighed for det."

Der er en overvejende forventning blandt deltagerne om, at den ældre, ofte it-uvante, generation vil blive erstattet af den yngre, mere it-vante generation, hvilket formodes at føre til en reduktion af gruppen af it-svage borgere. Dernæst påpeger en del af deltagerne, at indførslen af den digitale identitet muligvis vil blive fulgt af en tilvænningsperiode, hvor behovet for støtte og vejledning vil være stort hos især gruppen af it-svage borgere. Efterhånden som borgerne tager identiteten til sig, ventes gruppen af it-svage borgere yderligere at mindskes. En deltager sammenligner indførslen af den digitale identitet med indførslen af selvangivelser:

"Der er sådan en parallel til det, at da der skulle skrives selvangivelser for mange år siden, der var jeg da også rundt ved familie og så videre og skrev deres selvangivelser. Det er jo samme metode. I en overgangsfase. Det er et spørgsmål om tid, så alle være der."

Overordnet er deltagerne således enige om, at den digitale identitet skal indføres på trods af risikoen for at hægte de it-svage borgere af; dog med det forbehold, at det offentlige skal yde en særlig indsats i en overgangsperiode for også at få så mange som muligt med. Tilsvarende resultat er også at finde i spørgeskemabesvareelserne, hvor hovedparten af deltagerne (18 ud af 23 deltagere) tilkendegiver, at selvom visse grupper ikke er i stand til at anvende den digitale identitet, bør identiteten indføres til gavn for dem, der godt kan bruge den.

Fælles digital identitet til offentlige og private services

Ud fra besvareelserne i spørgeskemaet er det ikke muligt entydigt at konstatere, hvorvidt deltagerne generelt er for eller imod udvidelsen af den digitale identitet til også at omfatte private services. I gruppeinterviewene hersker derimod overvejende enighed om, at offentlig og privat adgangskontrol skal adskilles.

Argumenter for

Som eneste fordel for en fælles digital identitet anvendelig til både offentlige og private services fremhæver nogle af deltagerne under gruppeinterviewene bekvemmeligheden ved kun at skulle huske på én kode og benytte én identitet.

Argumenter imod

To overordnede argumenter fremføres af deltagerne under gruppeinterviewene mod udvidelsen af den digitale identitet til også at omfatte private services. Først peger deltagerne på omfanget af den skade, der kan opstå i tilfælde af, at den digitale identitet mistes. Dernæst udtrykker deltagerne bekymring for samt forvirring omkring, hvorvidt deres færden på internettet registreres, samt om deres fortrolige oplysninger kan misbruges.

Skaden, der følger af en mistet og muligvis misbrugt digital identitet, er, ifølge deltagerne, mere omfangsrig, desto bredere anvendelsesområde den digitale identitet har. Dette beror på betragtningen om, at jo flere anvendelsesmuligheder den digitale identitet omfatter, desto flere muligheder afskæres brugeren midlertidigt fra, og desto flere risici foreligger for misbrug af identiteten i tilfælde af, at identiteten mistes. En deltager påpeger tilfældet, hvor kriminelle, efter at have hacket sig ind i en bank og tilranet sig brugerens digitale identitet, udover at misbruge identiteten i forbindelse med bankrøveri, også får adgang alle andre steder, hvor den digitale identitet kan anvendes:

"Man kunne jo forestille sig, at nogen kunne hacke sig ind fx i banken, og så kunne de jo faktisk komme videre, så har man jo ens identitet, og så er der åbent hele spektret rundt."

Det andet modargument bunder i deltagernes mistro til, at deres personlige data forbliver fortrolige, hvis offentlig og privat adgangskontrol sammenblandes. De frygter, at deres færden på internettet registreres, samt at oplysningerne er tilgængelige for uvedkommende og dermed kan misbruges. Deltagerne udtrykker deres frygt for, at jo flere services den digitale identitet giver adgang til, desto flere udbydere af private services vil potentielt få adgang til den enkelte brugers personlige oplysninger. En deltager udtrykker sin frygt for, hvad der følger af en sammenblanding af offentlig og privat adgangskontrol:

"Så føler jeg, at så har alle adgang til alle ens oplysninger i større omfang."

Der er blandt deltagerne således større skepsis over for private serviceudbydere end det offentlige. Deltagerne skelner mellem det offentlige, der skal tilbyde en service, og private virksomheder, som lever af at sælge et produkt, hvilket en deltager udtrykker her:

"Bankerne går ind og tilbyder et produkt – det er en forretning."

Størstedelen af deltagerne er herved bekymrede for en sammenblanding af offentlig og privat adgangskontrol og har ikke ubetinget tiltro til, at deres personlige oplysninger behandles fortroligt.

Delkonklusion

Deltagerne er overvejende positive over for forslaget om den digitale identitet anvendt i offentlig regi. Øget sikkerhed er det vigtigste argument for, dernæst følger bekvemmeligheden ved kun at skulle anvende én kode og én identifikation over for det offentlige på nettet. Deltagerne er bevidste om, at løsningen muligvis vil medføre teknologisk marginalisering og påpeger, at det offentlige skal leve op til sit ansvar for at tage hånd om it-svage borgere.

Deltagerne er generelt imod, at den digitale identitet også skal kunne anvendes til private services. Modstanden beror mestendels på en opfattelse blandt deltagerne af, at sammenblanding af offentlig og privat adgangskontrol medfører en betydelig risiko for misbrug af personlige oplysninger, men også på et mere principielt synspunkt om, at offentlig og privat adgangskontrol bør være adskilt.

6.3 Automatiske sikkerhedsopdateringer

Af spørgeskemabesvareelserne fremgår det, at et lille flertal af deltagerne (12 ud af 22 deltagere) går ind for forslaget om tvungne automatiske sikkerhedsopdateringer, knap en tredjedel af deltagerne (7 ud af 22 deltagere) er imod, og den resterende del ved ikke. I gruppeinterviewene synes deltagerne dog at være mere ligeligt splittede.

Argumenter for

Deltagerne fremhæver i gruppeinterviewene to overordnede argumenter for indførslen af automatiske sikkerhedsopdateringer: øget sikkerhed og hjælp til at håndtere egen it-sikkerhed.

Den øgede sikkerhed ses af deltagerne som resultatet af, at alle brugere tvinges til at installere sikkerhedsopdateringer. En deltager forklarer, at tvungne opdateringer er en god løsning, idet mange ikke opdaterer selv:

"Det er ok, fordi der er så mange, der ikke gør det [opdaterer]."

At forslaget letter den enkelte brugers håndtering af egen it-sikkerhed fremhæves som en fordel af flere af de deltagere, der er positivt stemt over for forslaget. Denne gruppe deltagere ser sig ikke selv i stand til at overskue eller tage stilling til de enkelte sikkerhedsopdateringer og vil derfor gerne fralægge sig en del af ansvaret for egen it-sikkerhed. De ser forslaget som en hjælp, hvilket en deltager forklarer her:

"Jeg vil gerne spares for lidt sved på panden med de der ting, fordi det bliver jeg virkelig nervøs over. Selvfølgelig ikke mindre efter at jeg blev bestjålet for næsten toethalvttusinde, hvor jeg ikke gjorde noget."

Af de deltagere, der er positivt stemt over for forslaget, har flere visse forbehold overfor forslaget. Eksempelvis påpeger nogle af deltagerne det tids- og ressourcekrævende i at hente og installere sikkerhedsopdateringer. Dette er i tråd med spørgeskemabesvarelsene, hvor et par deltagere begrundet afvisning af installation af sikkerhedsopdateringer med mangel på tid. Under gruppeinterviewene foreslår flere deltagere, at det i en vis udstrækning skal være muligt for brugeren selv at bestemme tidspunktet for, hvornår opdateringerne hentes ned og installeres. En deltager udtrykker det således:

"Og når jeg siger, jeg vil vælge, så er det fordi at de tidspunkter, hvor de vil opdatere de programmer der, de vil lave en opdatering, det er ikke altid, det lige passer mig."

Andre deltagere støtter ligeledes op om forslaget, men understreger at fejlfulde opdateringer kan være omkostningsfulde, idet den enkelte bruger ikke længere selv kan annullere dem. En deltager ser her fralæggelsen af ansvar som en fordel, men påpeger problematikken med fejlfyldte opdateringer:

"Jeg synes også, det er fint nok, hvis det bare bliver proppet ned i min computer, så jeg ikke selv skal spekulere så meget på det. Det er sådan set i princippet fint nok, men når det så går hen og kolliderer med andre programmer, hvem er det så lige, man ringer til? ... Så hvis man laver sådan noget, der er tvunget, så skal der være meget support til, så tror jeg, det bliver dyrt."

Argumenter imod

Under gruppeinterviewene ser deltagerne de tungest vejende argumenter mod indførslen af tvungne sikkerhedsopdateringer som fratagelsen af selvbestemmelse over egen computer samt risikoen for, at en fejlfuld opdatering påvirker styresystemet eller andre programmer negativt.

Retten til selvbestemmelse og bevarelsen af den personlige frihed nævnes af flere deltagere som grundlaget for deres modstand mod tvungne automatiske sikkerhedsopdateringer. Ifølge denne gruppe deltagere bør kontrollen med den enkelte computer udelukkende placeres hos ejeren, hvilket en deltager udtrykker således:

"Og så går jeg også ind for min personlige frihed. Den, synes jeg, bliver begrænset, hvis nogen har direkte adgang til, hvad der sker på min computer. Så det er jeg da stærkt imod."

Frygten for, at en opdatering indeholder en fejl, vejer tungt hos en stor del af deltagerne. Denne gruppe deltagere er meget bevidste om den tilstedeværende risiko for, at en opdatering indeholder

fejl, som sætter funktioner i styresystem eller andre programmer ude af kraft, og vil derfor fastholde rettigheden til at takke nej til eller annullere en fejlfyldt opdatering. En deltager spørger retorisk:

"Hvorfor skulle jeg så tage en opdatering ned, hvis det går ud over et andet program?"

I hvor høj grad det er den principielle fratagelse af selvbestemmelse og ansvar eller blot den konkrete risiko for fejlupdateringer, der ligger til grund for deltageres modstand mod tvungne automatiske sikkerhedsopdateringer, står ikke klart, om end argumentet om den konkrete risiko for fejlupdateringer fylder mest i debatten.

Nogle deltagere synes at kunne tilslutte sig forslaget om tvungne, automatiske sikkerhedsopdateringer, såfremt de kan vide sig sikre på, at opdateringerne ikke indeholder fejl. En deltager udtrykker det således:

"Hvis man var helt sikker på, at det [sikkerhedsopdateringerne] ikke karambolerer med noget, så tror jeg ikke, der var nogen, der havde noget imod det."

Et par andre deltagere ytrer under gruppeinterviewene ønske om selv at foretage valget om, hvorvidt de vil acceptere sikkerhedsopdateringer eller ej, men føler sig ikke tilstrækkelig rustet til at foretage det. Lignende tendens gør sig gældende i spørgeskemabesvareelserne, hvor knap en tredjedel af deltagerne angiver, at de til tider afviser en sikkerhedsopdatering, fordi de har svært ved at vurdere, om det er en sikkerhedsopdatering eller en skadelig fil. En deltager forklarer:

"Så som du også siger, skal man have valget. Problemet er så, synes jeg, at man nogle gange får det valg, og man ved egentlig ikke, hvad man vælger fra eller til, fordi man ved ikke nok om det, hvad der ligger bag."

Automatiske sikkerhedsopdateringer som standardindstilling

Et kompromis mellem tilhængere og modstandere af forslaget synes at tegne sig i en af interview-grupperne. De er samlet set enige om, at brugerne er forskellige, hvad angår deres viden om it-sikkerhed og evne til selv at varetage it-sikkerheden. En deltager konstaterer eksempelvis:

"Min far er it-konsulent, så han må have nogenlunde styr på det... Min mor har ingen anelse om, hvad hun sidder og laver."

Deltagerne i denne gruppe tilslutter sig derfor, at det skal være muligt for brugere selv at vælge, om de vil tage ansvaret for egen sikkerhed og holde deres computer opdateret, eller om de vil fralægge sig ansvaret – og selvbestemmelsen – og køre med tvungne opdateringer. En deltager udtrykker det simpelt:

"Det skal være et tilvalg."

En anden deltager skitserer ideen:

"Så kunne det også være noget, man valgte: 'Vil du selv stå for sikkerheden og opdateringer, eller vil du have os til at gøre det?'"

Delkonklusion

Deltagerne er forholdsvis splittede, hvad angår forslaget om tvungne, automatiske sikkerhedsopdateringer. En del vil gerne fratages ansvaret for på egen hånd at holde deres computer sikkerhedsop-

dateret, hvorimod en stor gruppe deltagere værner kraftigt om deres personlige frihed og retten til at sige nej til en muligvis fejlfuld opdatering. Dog synes et acceptabelt kompromis i en af interview-grupperne at være en løsning, hvor brugeren frit kan vælge selv at stå for at downloade og installere sikkerhedsopdateringer eller overlade det til andre og dermed lade opdateringerne ske automatisk.

6.4 Pc-syn

Offentligt pc-syn

I spørgeskemaet tilslutter omkring halvdelen af deltagerne (11 ud af 23 deltagere) sig forslaget om bestået pc-syn som adgangsgivende til offentlige hjemmesider. Den resterende halvdel kan opdeles ligeligt i tvivlere og modstandere af forslaget. Nogenlunde samme fordeling er at finde i gruppeinterviewene.

Argumenter for

Deltagerne, der går ind for forslaget om offentlig pc-syn, fremfører som argument under interview-mødet, at pc-synet øger den enkelte brugers it-sikkerhed på to måder. Dels øges den enkelte brugers egen sikkerhed direkte, da pc-synet motiverer, tilskønner og hjælper den enkelte bruger til at holde sin egen computer sikkerhedsopdateret. Et par deltagere udtrykker det således:

"Det er en god ting ... Fordi så bliver man forpligtet."

"For ens egen skyld vil det måske nok være en fordel. Så jeg kan kun tilslutte mig, at man får den [computeren] tjekket en gang imellem."

Dels øges den enkelte brugers egen sikkerhed indirekte, da pc-synet forpligter andre brugere til at holde deres computere sikkerhedsopdateret. Dette begrænser risikoen for, at den enkelte bruger modtager virus og lignende fra de øvrige brugere. En deltager sammenligner pc-synet med kørekortet, som alle borgere påkræves at erhverve sig, således at de er i stand til at færdes sikkert i trafikken uden at være til fare for sig selv eller medtrafikanter.

"Vi sætter jo ikke spørgsmålstegn ved, at vi som mennesker skal have kørekort. Der er jo også krav til at få kørekort. Men i princippet er der jo ikke forskel. ... Der er nogle, der heller ikke må køre bil. Hvis du har et dårligt syn, og hvis du er over 80, så må du heller ikke køre bil."

Opbakningen til forslaget om pc-syn synes for de fleste deltageres vedkommende at være forudsat af, at det offentlige skal stille hjælp og støtte til rådighed for it-svage borgere:

"Hvis et samfund ønsker at stille de krav, så må man også gå ind og være garant for, at der er stillet hjælp til de mennesker, der ikke kan finde ud af det."

Flere deltagere er dog under gruppeinterviewene kun betinget positive over for forslaget, hvilket de forklarer som resultat af manglende viden om den konkrete udførsel af pc-synet. Spørgsmål som, hvor ofte synet skal udføres, hvor ressourcekrævende selve scanningen er, samt hvilke kriterier der kræves opfyldt førend computeren godkendes, synes at være af afgørende betydning for deltagernes stillingtagen. Et par deltagere forklarer her:

"Nu har jeg ikke særlig stor tålmodighed, når det gælder computere, det skal bare fungere og køre, og det er mit værktøj, også jeg skal bruge det, så det er netop – hvor lang

tid tager det, og hvor mange ressourcer kræver det? Det er det, der er det vigtige for mig."

"Det kommer an på hvilke kriterier, der ligger til grund for, om den [computeren] er god nok eller ikke er god nok."

Argumenter imod

Deltagerne, der er modstandere af offentlig pc-syn, anfører under gruppeinterviewene tre argumenter imod forslaget: besvær, begrænset valgfrihed af sikkerhedsprogrammer samt generelt uønsket offentlig indblanding i den enkeltes private computer.

Først og fremmest anser en stor del, af de overfor forslaget negativt stemte deltagere, pc-synet som anledning til besvær. En deltager forklarer sig:

"Jeg tror, det vil være sådan: 'Nej, nu er der allerede gået en måned igen, og vi skal have gjort det der, og jeg orker det ikke, og hvor er det besværligt.'"

En del af disse deltagere frygter endvidere, at pc-synet frem for at hjælpe it-svage borgere til en bedre it-sikkerhed, vil afskære disse brugere yderligere fra at anvende offentlige services online, idet de it-svage borgere ikke vil være i stand til at udføre pc-synet. To af deltagerne udtrykker det således:

"Jeg tror ikke, de [it-svage borgere] bliver hjulpet. De opgiver."

"Så taber man nogle brugere på gulvet."

En gruppe af deltagerne påpeger begrænset valgfrihed af sikkerhedsprogrammer som en mulig følge af implementeringen af pc-synet. Det er konsekvensen af, at godkendelse af brugerens pc forudsætter, at der er installeret godkendte sikkerhedsprogrammer. Brugeren vil således blive tvunget til at vælge sine sikkerhedsprogrammer blandt de på listen godkendte, hvilket en deltager udtrykker sådan:

"Så tvinger de [det offentlige] jo sådan set én til visse produkter."

En deltager er bekymret for, hvordan gratisprogrammer vil figurere på en sådan liste:

"De, som udbyder et gratisprogram, de vil jo ikke betale for at få deres godkendt, som sådan, fordi de forærer det jo i princippet bare væk."

Et fåtal af deltagerne synes desuden at have den indstilling, at computeren tilhører den enkelte brugers privatsfære, og at det offentlige derfor ikke skal blande sig i, hvilke sikkerhedssoftware og -opdateringer den enkelte bruger har installeret.

Under gruppeinterviewene hersker blandt nogle deltagere en bekymring for, at personlige data scannes ved pc-synet. Efter forklaring fra de øvrige deltagere, om at forslaget går på scanning af sikkerhedssoftware og -opdateringer, fortager bekymringen sig.

Pc-syn også krævet til netbank

I spørgeskemabesvarelsene gør samme holdningsfordeling sig gældende for pc-syn krævet til netbank som for offentlig pc-syn. Omtrent halvdelen af deltagerne (11 ud af 23 deltagere) er for pc-syn

til netbank, en fjerdedel ved ikke og en fjerdedel er imod. Dokumentationen i interviewmaterialet er meget lille, da forslaget kun behandles i én af de fire interviewgrupper.

Argumenter for

Som argument for pc-syn krævet til netbank fremfører et par deltagere, at det er rimeligt at bankerne stiller krav til deres kunder om at sikkerhedsopdatere deres computere, eftersom det er bankerne, der skal dække tab ved tyveri. En deltager forklarer:

"Det [at banken gerne må stille krav], synes jeg, er helt okay. Fordi det lige præcis er dem [bankerne], der har erstatningsforpligtelsen."

Ligesom under diskussionen af det offentlige pc-syn påpeger et par deltagere, at de it-svage borgere ikke skal afskæres muligheden for personlig henvendelse i banken i tilfælde af problemer med pc-synet. En deltager udtrykker det således:

"Nu sagde du selv, borgerservicen skulle opretholdes. Bankskranken skal også opretholdes."

Argumenter imod

Argumenter mod forslaget har ikke været til diskussion i interviewgrupperne, men det virker rimeligt at antage, at deltagerne har de samme principielle indvendinger mod pc-syn krævet til netbank, som de har til offentligt pc-syn. Således er det principielle modargument, at det offentlige ikke skal blande sig i, hvilke sikkerhedssoftware og -opdateringer den enkelte bruger har installeret, da computeren tilhører den enkelte brugers privatsfære.

Delkonklusion

Godt halvdelen af deltagerne er positivt indstillet over for forslaget om pc-synet til offentlige hjemmesider såvel som til netbank. Af argumenter for forslaget fremhæves først og fremmest øget sikkerhed samt for bankernes vedkommende retten til at kræve en vis sikkerhedsstandard af deres kunder. Deltagerne lægger vægt på det offentliges forpligtelse til at yde støtte til it-svage borgere. Af modargumenter er det væsentligste besværet med selve udførelsen af pc-synet, dernæst begrænset valgfrihed af sikkerhedsprogrammer og endelig ret til selvbestemmelse over egen computer. Manglende viden om den konkrete udførelse af pc-synet, herunder scanningstid, -frekvens, -ressourcebeslaglægning osv., bevirker forbehold overfor egentlig stillingtagen til forslaget hos en række deltagere.

6.5 Tvungen mailfiltrering samt installation af firewall og virusfilter

Tvungen mailfiltrering

Godt halvdelen af deltagerne (13 ud af 22 deltagere) tilslutter sig forslaget om tvungen mailfiltrering i spørgeskemabesvarelsenerne. Lidt flere (15 ud af 23 deltagere) tilslutter sig forslaget om blot at indføre mailfiltrering som en standardindstilling, der kan fravælges af den enkelte bruger. I gruppeinterviewene går størstedelen af deltagerne ind for tvungen mailfiltrering.

Argumenter for

Hovedparten af deltagerne tilslutter sig i gruppeinterviewene forslaget om tvungen mailfiltrering med argumentet om, at sikkerheden øges, når virus frasorteres. En deltager medgiver:

"Hvis det er for at skanne virus, så er det i orden."

Størstedelen af de over for forslaget positivt stemte deltagere fastholder dog, at muligheden for at få adgang til de frasorterede mails fortsat skal være til stede, hvilket er i tråd med formuleringen af løsningsforslaget. En deltager udtrykker således:

"Jeg ville ikke have noget problem med, at det blev sorteret fra, hvis man selv havde muligheden for at gå ind og se de mails et eller andet sted. De skal være tilgængelige på en eller anden måde."

Nogle deltagere vil, som spørgeskemabesvareelserne også indikerer, gerne blot have mailfiltreringen slået til som standardindstilling.

"At den sådan fra standardopsætning er slået til. Jeg tror måske, det er den bedste måde at gøre det på."

I en af interviewgrupperne ser nogle deltagerne det som en fordel, at forslaget flytter ansvar fra den enkelte bruger til internetudbyderne. En deltager har den klare holdning, at her hører ansvaret hjemme:

"Jeg synes, det er internetudbyderens ansvar, at vi er sikre på nettet, helt sikkert. Og det er ikke andres."

Argumenter imod

Under gruppeinterviewene er et fåtal af deltagere imod forslaget. Denne gruppe deltagere er imod indblanding udefra og vil gerne selv varetage egen sikkerhed. Dette udtrykker de bl.a. således:

"Jeg er imod alt, der indeholder ordet tvang."

"Det skal være muligt for mig at klikke den tvang fra."

"Tvungen mailfiltrering, den er jeg ikke så meget for ... igen er du tilbage til almindelig sund fornuft, kender du ikke afsenderen, så slet den."

Tvungen installation af firewall og virusfilter

I spørgeskemaet tilslutter flertallet af deltagerne (14 ud af 22 deltagere) sig forslaget om, at internetudbyderne skal kræve sikkerhedssoftware installeret hos deres kunder. I gruppeinterviewene drøftes forslaget kun i meget begrænset omfang.

Der fremføres ingen argumenter for eller imod forslaget under gruppeinterviewene, men et par deltagere udtrykker bekymring for opretholdelsen af deres mulighed for selv at vælge deres sikkerhedssoftware. En deltager formulerer det således

"Hvem bestemmer så, hvilke programmer det skal være? Hvis min mailudbyder, nu har jeg ikke nogle af dem der, kom og sagde til mig, at jeg skulle have noget bestemt, jamen så ville jeg sige, at de måtte give mig det. Jeg vil ikke betale for det. Fordi jeg mener grundlæggende, at med sådan nogle ting kan jeg godt beskytte mig selv."

Det ligger desuden mange af deltagerne på sinde, at listen over godkendt sikkerhedssoftware skal udvælges af en uvildig instans, gerne det offentlige. En deltager siger:

"Det offentlige skal gå ud og stikke nogle overordnede regler af for at strukturere udbyderne. Man skal jo tænke på, at Cybercity og TDC er også forretninger."

Delkonklusion

Flertallet af deltagerne tilslutter sig forslaget om tvungen mailfiltrering, da de mener, det øger sikkerheden samtidig med, at muligheden for at læse de frasorterede mails bevares. Deltagerne, der er modstandere af forslaget, vil gerne opretholde den enkelte brugers ret til selv at vælge, i hvilket omfang og med hvilken sikkerhedssoftware vedkommende ønsker at beskytte sin computer, og fastholder, at ansvaret for it-sikkerheden ligger hos den enkelte bruger.

Det er ikke muligt entydigt at klarlægge deltageres holdninger til tvungent sikkerhedssoftware. Dog ligger det mange af deltagerne på sinde, at sikkerhedssoftwaret skal godkendes af en uvildig instans.

6.6 Sikkerhedsmærkning af it-produkter

I spørgeskemabesvarelserne angiver langt hovedparten af deltagerne (20 ud af 23 deltagere), at de synes, det er en god ide at lave en sikkerhedsmærkningsordning for it-produkter. Under gruppeinterviewene er deltagerne ligeledes overvejende for forslaget, om end en del skepsis udtrykkes, og mange argumenter mod fremføres.

Argumenter for

Under gruppeinterviewene fremfører deltagerne øget sikkerhed som argumentet for indførelsen af forslaget. Flere deltagere (10 ud af 23 deltagere) tilkendegiver i spørgeskemabesvarelserne, at de har svært ved på egen hånd at vurdere sikkerheden af et givet it-produkt, og at en sikkerhedsmærkning derfor vil hjælpe dem med at vælge det sikrere alternativ. To deltagere udtrykker her:

"Jeg ville sige, at det ville være lettere. Der er flere produkter, end vi kender."

"Det [mærkningsordningen] ville jeg nok gå ind og bruge, for jeg har ikke spor forstand på noget af det."

Deltagerne, der går ind for forslaget, er bevidste om, at en mærkningsordning vil resultere i dyrere produkter og er villige til at betale merprisen for bedre at kunne vælge et sikrere it-produkt. I spørgeskemabesvarelserne angiver langt hovedparten af deltagerne (19 ud af 23 deltagere), at de er villige til at betale ekstra for, at et it-produkt, som en computer, er sikkerhedsmærket.

Dernæst tilslutter deltagerne sig, at mærkningsordningen skal ske på baggrund af vurderinger fra en uvildig ekspertgruppe. En deltager udtrykker her:

"Man kunne vel godt forestille sig noget uvildigt, ligesom dansk standard."

"Du skal have et eksperthold, der simpelthen sidder og laver de bedømmelser ... Hvis det er den almindelige forbruger, så melder jeg pas."

Argumenter imod

Under gruppeinterviewene fremfører enkelte deltagere som argument imod mærkningsordningen, at de ikke vil betale merprisen for, at et it-produkt er sikkerhedsmærket, da tilsvarende information

om it-produkters kvalitet og sikkerhedsstandard er at finde frit tilgængeligt i form af brugerafstemninger på internettet eller i anmeldelser i computermagasiner. En deltager forklarer:

"Jeg vil ikke betale for det [sikkerhedsmærkningen], for der er så mange internetbrugere, der går ind og stemmer på de her produkter, man køber i dag. Så kan man simpelthen vælge den, der har den højeste rating. Der er ingen grund til, at der er en myndighed, der går ind og tager ansvar for det. I hvert fald ikke sådan, at jeg er tvunget til at betale ekstra for nogen produkter, jeg kunne have fået billigere under alle omstændigheder."

Dernæst ytrer andre deltagere mistillid til, hvorvidt det i det hele taget er muligt at sikkerhedsmærke it-produkter. Nogle deltagere mener, at såvel udviklingen af it-produkter som af skadeligt software går for stærkt til, at en kategorisering vil være tilstrækkeligt opdateret:

"Udviklingen går så hurtigt. Det er meget svært hele tiden at være med."

Andre deltagere mener, at det ikke er muligt at sikkerhedsmærke et it-produkt alene, da dets sikkerhedsniveau vil afhænge af samspillet med styresystem og andre softwareprogrammer, hvilket varierer fra computer til computer:

"Med Nordic Antivirus, det er sådan 50/50. På nogle computere virker det helt vildt godt, og på andre virker det ikke ... Det er derfor, jeg ikke tror, den der mærkning ville virke så godt, fordi det er jo, hvordan man kombinerer det [it-produktet med computerens styresystem og øvrige software]."

Sidst har et par deltagere svært ved overhovedet at forstå, hvorledes der kan være forskel på sikkerheden af de forskellige produkter, og dermed, hvordan mærkningsordningen er mulig.

"Jeg har svært ved at se, hvordan man kan lave det sikrere. Altså hvad er det, vi skal sikre?"

Delkonklusion

Deltagerne er meget positivt stemte over for sikkerhedsmærkning af it-produkter. Som argument for forslaget nævnes, at mærkningsordningen vil føre til valg af sikrere it-produkter og dermed øget sikkerhed, hvilket tilhængerne af forslaget gerne betaler merprisen for. Modsat vil enkelte deltagere ikke betale ekstra for en, for dem, overflødig sikkerhedsmærkning, idet de selv mener sig i stand til at skaffe sig gratis information om sikkerhedsstandard fx afstemninger på nettet. Sidst udtrykker en gruppe af deltagerne skepsis overfor, hvorvidt en troværdig sikkerhedsmærkning af it-produkter i det hele taget er mulig.

6.7 Blokering af skadelige hjemmesider

Langt størstedelen af deltagerne (20 ud af 22 deltagere) tilslutter sig i spørgeskemabesvarelserne forslaget om sortlistning og blokering af skadelige hjemmesider.

Argumenter for

Argumentet for at sortliste og blokere en hjemmeside er ifølge deltagerne i gruppeinterviewene at øge sikkerheden. En deltager udtrykker det sådan:

*"Hvis der er en hjemmeside, der foranlediger, at der kan komme trojanske heste og spo-
leorm eller hvad hulan det nu hedder [latter]. Så er det der, at hammeren skal falde."*

Til at foretage sortlistningen peger deltagerne på et slags "it-politi" eller en offentligt forankret eks-
pertgruppe. Et par af deltagere udtrykker det således:

*"Et panel... Altså det skal være nogen, som har rimelig forstand på det."
"Man skal lade det offentlige komme på banen."*

Argumenter imod

Enkelte deltagere er modstandere af forslaget, da de ser sortlistning og blokering af hjemmesider
som censur og dermed et indgreb i den personlige frihed. En deltager udtrykker sin bekymring såle-
des:

*"Jeg er bekymret for den censur og den kontrol, der ligger i det. Hvilken myndighed
skulle være i stand til at vurdere det [hvilke sider jeg er interesseret i] på mine vegne,
som almindelig forbruger?"*

Desuden mener et par af deltagere, at det er umulig i praksis at holde nettet fuldstændig frit for ska-
delige hjemmesider. En deltager skitserer kort:

"Hvis du lukker én side, så kommer der dagen efter tusind nye."

Hvor går grænsen mellem beskyttelse og censur?

I spørgeskemaet tager deltagerne stilling til, i hvilke tilfælde de mener, at en hjemmeside bør sortli-
stes og blokeres. Her tilslutter et flertal af deltagere (15 ud af 22 deltagere) sig fuldstændigt den mest
omfangsrige blokering, som omfatter hjemmesider, der indeholder information om fremstilling af
malware. Endnu flere deltagere tilslutter sig de mindre omfattende forslag om henholdsvis at bloke-
re hjemmesider, hvorfra malware kan downloades (18 ud af 22 deltagere) samt hjemmesider, hvor
brugeren automatisk udsættes for angreb med malware (20 ud af 22 deltagere). En deltager tilken-
degiver:

*"De eksempler, der er beskrevet, hvor det er opskrifter på, hvordan man laver orme og
så videre - de skal bare væk. De skal slet ikke være tilgængelige. Selvfølgelig skal de ikke
det."*

Denne censurering af information stiller en mindre gruppe deltagere sig skeptiske overfor:

*"Det er et indgreb i den personlige frihed, at der er nogen, der tager et sådan valg på
min vegne. Der er da heller ikke nogen, der skal beslutte, hvad for nogle bøger jeg vil
ned at låne på biblioteket."*

Delkonklusion

Langt hovedparten af deltagerne går ind for forslaget om sortlistning og blokering af skadelige
hjemmesider med det ene argument, at det medfører øget sikkerhed. Enkelte deltagere er imod for-
slaget, idet de opfatter sortlistning og blokering af hjemmesider som censur, samt tvivler på, hvor-
vidt blokeringen har nogen effekt.

6.8 Online lagring af data

Over halvdelen af deltagerne (14 ud af 23 deltagere) angiver, at de er bekymrede for den udvikling, at personlige data i stigende grad opbevares på nettet af private virksomheder. Under gruppeinterviewene synes nogenlunde samme holdningsfordeling at gøre sig gældende.

Deltagerne er skeptiske over for udviklingen grundet en bekymring for, om de data, der opbevares på nettet, er tilgængelige for uvedkommende. I spørgeskemaet angiver 15 ud af 23 deltagere, at de er bekymrede for den overvågning, der måske kunne finde sted, når data sendes eller gemmes via online services. En deltager udtrykker sin skepsis:

"Det kunne være en dejlig ting for ens billeder, men jeg tør ikke bruge det, fordi så kan de komme andre steder hen, og andre kan have adgang til dem."

Der hersker blandt et par deltagere ydermere bekymring om, hvorvidt rettigheden over egne data mistes, når disse opbevares af kommercielle tjenester på nettet. Som eksempel nævnes det sociale netværk Facebook.com, hvor brugerne, i det øjeblik de opretter en profil, giver Facebook rettighed til at bruge de billeder og data, som brugerne eventuelt opbevarer der. En deltager fortæller:

"Facebook skriver direkte, at de har rettighederne til at bruge billederne til noget andet, hvis de har lyst til det... Og det står med meget småt."

Bekymringen afholder flere af deltagerne fra at opbevare fx billeder på nettet. Andre forholder sig mere positivt, men dog selektivt til mulighederne:

"Man ved jo, at hvis man lægger noget ud på nettet, så har man ikke fuld kontrol over det, så kan man jo bare sortere i de data, der bliver lagt ud."

Efterledes denne forholdsregel, ser deltagerne ikke de store problemer i at anvende kommercielle services til opbevarelse af data på nettet. En deltager siger:

"Hvis der er nogen, der har lyst til at se på min fine have, så skal de være velkomne."

En mindre gruppe deltagere fremfører desuden to fordele ved opbevarelse af data på nettet. Dels reduceres risikoen for at miste data, når disse ligger på nettet frem for at være gemt på egen computer, som en deltager pointerer her:

"Det er bare et spørgsmål om at uploade det til et eller andet sted, og så ved man, de er der."

Dernæst fremhæves fordelene i at opbevare data på nettet, som deltagerne ønsker at dele med bekendte. En deltager forklarer:

"Vi er begyndt at lægge ud på nettet, så kan svigerfar og svigermor følge med i hvordan det går, og så kan vi smide alle de der ting derop, og så kan de gå derind og kigge, det føler vi os sådan rimelig sikre ved."

Delkonklusion

Et lille flertal af deltagerne ser overvejende udviklingen med opbevarelse af personlige data på nettet som bekymrende. Bekymringen afholder nogle fra at opbevare billeder på nettet, mens størstedelen af deltagerne er positivt stemt over for de muligheder, det giver. Især fremhæves den fordel, at risikoen for at miste data reduceres. Deltagerne er dog bekymrede for, om deres personlige data forbliver fortrolige og tager derfor deres forholdsregler, hvis de anvender kommercielle tjenester til opbevaring af data på nettet.

7. anbefalinger fra gruppen

Arbejdsgruppen mener, at håndteringen af it-sikkerhed i dag i for høj grad er overladt til den enkelte bruger. Den nuværende situation er hverken rimelig eller hensigtsmæssig i forhold til behovet for at opretholde et samfundsmæssigt ønskværdigt sikkerhedsniveau. Gruppen anbefaler derfor, at de lovgivende og udøvende myndigheder fremover tænker (mere) i modeller, der letter de private brugeres håndtering af it-sikkerhed ved at flytte en del af opgaven tættere på de aktører, der har en reel mulighed for at højne sikkerheden.

Gruppen har udarbejdet nogle idéer til, hvordan dette kan lade sig gøre, idet det har været ønsket at teste, hvor langt brugerne er villige til at gå for at blive hjulpet med sikkerheden. De beskrevne løsningsforslag indebærer derfor nogle indgreb over for de private brugere, som er højnende for såvel den enkelte brugers som det generelle sikkerhedsniveau. Men som også er mere indgribende end nuværende foranstaltninger, idet de indebærer øget kontrol med og begrænsning af brugernes udfoldelsesmuligheder på nettet. Indgrebenes karakter varierer mellem at stille kontante krav til brugere og en egentlig overdragelse af ansvaret for visse sikkerhedsopgaver til andre aktører.

Der var på interviewmødet et udtrykt ønske om at få hjælp til at håndtere sikkerheden, og det er gruppens indtryk, at brugerne overvejende accepterede de indgreb, som løsningsforslagene indebærer, selvom alle selvfølgelig ikke gjorde. I det følgende tager arbejdsgruppen endelig stilling til de løsningsforslag, de selv har udviklet, og giver deres anbefalinger til, hvordan man – bl.a. set i lyset af brugernes reaktion – bør forholde sig til dem fremover.

Digital identitet

Arbejdsgruppen anbefaler indførsel af en digital identitet til anvendelse for såvel offentlige som private services på internettet⁷. Den digitale identitet skal være hardwarebaseret eller på anden vis give en tilsvarende sikkerhed.

Fordelen ved indførsel af en digital identitet er for borgerne, at der kan ske tilstrækkelig sikker identifikation af de enkelte brugere, dvs. sikring af autenticitet. Sikkerheden i identifikation af brugerne er afgørende for, hvilke ydelser og tjenester, der fremover vil blive tilbudt på nettet. Jo sikrere identifikation af brugerne, desto mindre er risikoen for, at følsomme personoplysninger mv. falder i de forkerte hænder. Herved kan udbuddet øges af tjenester, som f.eks. involverer helbredsoplysninger, oplysninger om økonomiske forhold mv., dvs. at den enkelte brugers adgang til og indsigt i, hvilke oplysninger der er lagret om den pågældende, kan forbedres. Arbejdsgruppen vurderer, at mobiliteten og brugervenligheden i det hele taget har væsentlig indflydelse på, i hvilket omfang borgerne vil benytte den digitale identitet.

Den digitale identitet skal udelukkende rumme oplysninger, der identificerer brugeren, og ikke yderligere personlige oplysninger som fx lægejournaler, hvor et betalingsmiddel har været brugt og til hvad osv. Sørger man for udelukkende at etablere identiteten som en fremgangsmåde, der skal sikre, at brugeren er den, hun giver sig ud for at være, deler arbejdsgruppen ikke brugernes bekymring for, om den foreslåede løsning kunne give private virksomheder mulighed for at hente personlige oplysninger om deres kunder hos offentlige myndigheder og vice versa. Det er imidlertid nødvendigt at

⁷ Arbejdsgruppen har valgt at bruge betegnelsen "digital identitet", for at kunne tænke frit og ikke lade sit løsningsforslag være bundet af at skulle forholde sig til den digitale signatur. Det skal imidlertid understreges, at elementerne i det forslag, gruppen her præsenterer, godt kan indarbejdes i en ny udgave af den digitale signatur.

tage brugernes generelle modstand mod at bruge den digitale identitet til både offentlige og private services seriøst. Denne modstand peger på behovet for en betydelig oplysningsindsats, såfremt en fremtidig digital identitet skal benyttes til både private og offentlige services, hvilket gruppen anser som en ønskværdig udvikling.

For yderligere at komme truslen om registrering af færden på nettet til livs, er det også vigtigt, at brugerne til stadighed har alternative muligheder for identifikation til tjenester, hvor der ikke er behov for den stærke identifikation som den digitale identitet giver. Det kan fx dreje sig om mindre kritiske tjenester eller anonym kommunikation med offentlige, hvor det åbenlyst er uhensigtsmæssigt med en stærk identifikation.

Arbejdsgruppen anbefaler, at anvendelsen af digital identitet skal være tvunget for borgere, som ønsker at benytte offentlige services på nettet, hvor identifikation i dag er påkrævet. Det forhold, at it-svage borgere ikke kan bruge en digital identitet, bør ikke stoppe den teknologiske udvikling. Arbejdsgruppen har ikke taget stilling til, hvilke tilbud der bør stilles til rådighed for denne gruppe af borgere.

Automatiske sikkerhedsopdateringer

Arbejdsgruppen anbefaler, i tråd med over halvdelen af brugernes ønske, at automatiske sikkerhedsopdateringer fremmes på forskellig vis, fx ved at programproducenter opsætter programmer, således at brugeren aktivt skal fravælge opdateringer. Arbejdsgruppen er opmærksom på, at der kan være en række udfordringer i forhold til at få programleverandørerne til at indrette deres produkter på en sådan måde, navnlig fordi der i vid udstrækning er tale om internationale virksomheder. Dette forslag skal derfor ses i sammenhæng med forslagene om pc-syn og sikkerhedsmærkning, hvilke indebærer, at brugerne tilskyndes til og vejledes i etablering af automatiske sikkerhedsopdateringer.

Tvunget pc-syn

Arbejdsgruppen anbefaler, i overensstemmelse med halvdelen af brugernes ønske, at der arbejdes med at udvikle og etablere et pc-syn, som på sigt kan blive en forudsætning for at anvende offentlige services på internettet. Pc-synet skal kontrollere brugernes sikkerhedsniveau og nægte dem adgang til offentlige services, såfremt det er for lavt. Forslaget kan gennemføres alene under medvirken af offentlige myndigheder og vurderes at kunne give et stort løft af sikkerheden.

Der er imidlertid en række udfordringer, der skal håndteres. Disse udfordringer vil primært være af praktisk og teknisk karakter, fx hyppighed og tidspunkt for gennemførelse af pc-syn, så det ikke holder private brugere fra at anvende offentlige services på internettet. Arbejdsgruppen anbefaler derfor, at ordningen starter som et frivilligt tilbud, som brugerne bliver mødt med på visse offentlige hjemmesider. Dette giver mulighed for at indhente de nødvendige erfaringer. Dertil kommer, at pc-synet af nogle af brugerne på interviewmødet blev opfattet som et indgreb i den personlige frihed og indblanding i privatlivets fred, da der ligger billeder og andre data af privat karakter på de computere, der skal synes. Det er derfor vigtigt, at et fremtidigt pc-syn konstrueres således, at det ikke giver adgang til personlige data, men udelukkende scanner for huller i softwareprogrammer, malware o. lign.

Gruppen vurderer, på baggrund af brugernes kommentarer på interviewmødet, at såfremt de praktiske problemer løses tilfredsstillende (fx at pc-synet ikke tager for lang tid), vil danske brugere være endnu mere positivt stemt overfor indførslen af pc-synet som et egentligt krav for overhovedet at benytte offentlige services. Denne accept, vurderer gruppen, vil dog i høj grad også være afhængig af, at det offentlige kæder pc-synet sammen med en effektiv vejledning af brugerne i, hvordan de opfyl-

der sikkerhedskravene. Det offentlige skal stille hjælp til rådighed for de brugere, de stiller skærpede sikkerhedskrav til, således at forslaget opfattes som en hjælp af brugerne.

Tvungen mailfiltrering

Arbejdsgruppen anbefaler, i overensstemmelse med de fleste brugeres ønsker, at danske mailudbydere indfører mailfiltrering, der som standard er aktiveret. I modsætning til nu, hvor brugerne i nogle situationer selv skal slå den til.

Sikkerhedsmærkning

Arbejdsgruppen vurderer, at en troværdig og velfungerende sikkerhedsmærkningsordning af it-produkter vil kunne højne det generelle sikkerhedsniveau og anbefaler derfor, at den indføres. Gruppen begrundes bl.a. sin anbefaling med, at en stor del af brugerne på interviewmødet bakkede op om forslaget og var villige til at betale ekstra for sådan en mærkning, hvis det kan hjælpe dem til at vælge sikrere produkter.

Dog deler arbejdsgruppen nogle af brugernes bekymringer om, hvordan en sådan ordning skulle fungere i praksis. Denne skepsis går eksempelvis på hvilke produkter, der skal mærkes og på hvorledes mærkningen af meget dynamiske produkter, som fx software, der kræver regelmæssige sikkerhedsopdatering, skal ske. En troværdig mærkningsordning skal tage højde for, at udviklingen inden for it går hurtigt, men gruppen mener også, at dette er muligt fx ved kun at give software, der tilbyder automatiske sikkerhedsopdateringer af høj kvalitet og med tilstrækkelig høj frekvens, en høj score.

Blokering af skadelige hjemmesider

Arbejdsgruppen anbefaler, at muligheden for at blokere adgangen til skadelige hjemmesider undersøges nærmere. Det kan naturligvis kun komme på tale at blokere en hjemmeside, hvis den pågældende side utvivlsomt fungerer som en aktiv del af it-kriminaliteten, eksempelvis phishing-sites og sider, hvorfra man uforskyldt downloader malware.

Arbejdsgruppen er opmærksom på, at såfremt en blokering i praksis skal vanskeliggøre de it-kriminelles aktiviteter, er det nødvendigt med en hurtig beslutningsproces. Arbejdsgruppen er dog også opmærksom på, at en sådan hastig behandling vil indebære risici for fejl, og at der er en række ytringsfriheds- og retssikkerhedsmæssige problemer knyttet til eventuelle blokeringer. Der er således fortsat behov for en række overvejelser i relation til en mulig fremgangsmåde ved behandling af eventuelle blokeringer af hjemmesider. Det er derfor ikke på nuværende tidspunkt muligt for gruppen at komme med en entydig anbefaling på dette punkt. Arbejdsgruppen har ikke forholdt sig til, hvem der eventuelt vil skulle vurdere, om en hjemmeside skal blokeres eller ej, men det synes dog oplagt, at det i givet fald bør ske i et organ, der er bemyndiget hertil, således at det ikke vil være den enkelte internetudbyder, der skal træffe beslutning og bære ansvaret herfor.

Brugerne på interviewmødet udviste meget lav tolerance over for alle typer af skadelige sider, og der var størst støtte til at lukke sider med et åbenlyst skadeligt indhold, såsom sider, hvorfra der automatisk downloades malware, når man går ind på dem. Gruppen hæfter sig imidlertid ved, at over halvdelen af deltagerne også tilslutter sig blokering af hjemmesider, der blot indeholder viden om konstruktion af malware. Som nævnt ovenfor har arbejdsgruppen kun forholdt sig til blokering af hjemmesider, der utvivlsomt aktivt udgør et sikkerhedsmæssigt problem for brugerne af de pågældende hjemmesider. Arbejdsgruppen finder ikke, at hjemmesider, der blot indeholder ren information, er skadelige i en sådan grad, at blokering af dem kan komme på tale, og sådanne hjemmesider er ikke omfattet af anbefalingen.

Online lagring af data

Arbejdsgruppen forudser en udvikling, hvor brugerne i stigende grad vil benytte sig af online services til lagring af personlige data. Der er væsentlige fordele for brugerne forbundet ved dette, der som dataene oftest vil være bedre beskyttet mod systemnedbrud og medfølgende tab af eksempelvis ferie billeder. Modsat giver online lagring af data andre større mulighed for at få adgang til folks personlige data. Denne mulighed bekymrer flere af deltagerne på interviewmødet, mens andre håndterer det ved kun at lagre data på nettet, som andre gerne må se. Det er arbejdsgruppens vurdering, at der mangler klarhed blandt brugerne omkring graden af fortroligheden af og rettighederne til de data, der lagres på nettet. Især rettighederne giver anledning til bekymring og gruppen anbefaler, at der gøres en indsats for at oplyse brugerne om dette. Det anbefales også, at offentlige myndigheder kaster et kritisk blik på de rettigheder, der omfatter data lagret på tredjepartsservere.

8. Ordliste

Ordforklaringer på en række centrale begreber.

Anti-spyware software

Sikkerhedssoftware som beskytter mod spyware, se spyware.

Anti-virus software

Sikkerhedssoftware som beskytter mod virus og andet malware, se virus, se malware.

Digital signatur

Digital underskrift bestående af en fil samt en kode. Filen gemmes på computeren. Den digitale signatur kan anvendes på nettet til at underskrive digitale dokumenter og identificere brugerens identitet. *Fx kan selvangivelsen rettes via nettet ved brug af den digitale signatur.*

Downloade

At overføre en eller flere filer fra en server eller en anden fjern maskine via et net til den lokale computer. Modsat uploade. *Fx at downloade en sikkerhedsopdatering eller en musikfil fra internettet.*

Firewall

Et program fungerende som et beskyttende filter. Firewall'en kontrollerer dataudvekslingen mellem to computere via fx internettet, og beskytter din computer mod malware, se malware.

Freeware

Gratis software. *Fx Open Office.*

Gmail

En webmail udbudt af søgemaskinen Google, se mailservice.

Hardware

Fysiske komponenter som anvendes inden for it. *Fx tastatur, skærm, harddisk, grafik-kort og lignende.*

Hotmail

En webmail udbudt af Microsoft, se mailservice.

Identifikation

Legitimation. På nettet er det ofte nødvendigt at kunne forevise troværdig identifikation, fx i forbindelse med netbank. *Fx digital signatur.*

Identitetstyveri

Tyveri hvor personlige oplysninger/din identitet stjæles, således at tyven har mulighed for at udgive sig for at være dig på internettet. Eksempelvis kan en tyv misbruge dine dankortoplysninger til at handle over nettet.

Internetudbyder

En internetudbyder er en virksomhed, der giver dig adgang til internettet, *fx TDC eller Cybercity.*

IP-adresse

Forkortelse for Internet-Protokol-adresse. Nummer på netværksenheder, som anvendes, når disse kommunikerer med hinanden i et netværk. Fx har computerservere og netværksprintere alle en IP-adresse.

ISP

Forkortelse for Internet Service Provider. En ISP er en udbyder af internet, se internetudbyder.

It

Forkortelse for informationsteknologi.

Keylogger

Program, som uden brugerens kendskab, gemmer brugerens tasteanslag, således at uvedkommende kan få kendskab til brugerens adgangskoder, osv.

Kryptering

Omskrive data til en kode, som kun afsender og modtager kan læse.

Malware

Sammentrækning af ordene malicious software (ondsindet programkode). Fællesbetegnelse for programmer, der udfører skadelige eller uønskede handlinger på den computer, hvorpå de kører. *Fx virus, orm, trojansk hest, keylogger.*

Mailservice

En mailservice er en tjeneste, der giver dig mulighed for at sende mails. *Fx Gmail eller Hotmail.*

Online

Online kan oversættes med 'på nettet'. En online service er en service, der er tilgængelig på nettet. *Fx han købte tøj online.*

Opdatering

En opdatering til et program er et lille stykke software, der forbedrer eller reparerer programmet. Har opdateringen til formål at forbedre sikkerheden kaldes den en sikkerhedsopdatering, se sikkerhedsopdatering.

Operativsystem

Se styresystem.

Orm

Skadeligt program, som reproducerer sig selv for at sende kopier til andre computere og på den måde belaster netværket. Ormen er ikke afhængig af at være vedhæftet et eksisterende program og kan således sprede sig selv.

Phishing

Svindel, hvor it-kriminelle narrede internetbrugere til at opgive fx kreditkort- eller netbankoplysninger. Det foregår oftest ved, at brugeren modtager en troværdigt udseende mail, fx lignende bankens, som lokker brugeren til at tilbagesende personlige informationer eller indtaste dem på en falsk hjemmeside.

Program

Se software.

Protokol

Regelsæt vedrørende kommunikationen mellem computere.

RAM

Forkortelse for Random Access Memory. RAM er arbejdshukommelsen i en computer. Styresystemkomponenter, programmer og anden data, der bliver brugt meget, gemmes her, så det hurtigt kan hentes frem. Det er meget hurtigere at læse fra og skrive til RAM end en harddisk.

Signeret mail

En signeret mail er en underskrevet mail. Underskriften består i et certifikat, som identificerer afsenderen.

Sikkerhedsopdatering

En sikkerhedsopdatering er en opdatering til et styresystem, fx Windows, eller et program, fx Internet Explorer. Opdateringen retter op på fejl og mangler i styresystemer eller programmer, der ellers kan gøre det let for hackere at bryde ind i din computer via internettet.

Software

Software er programkode, en række instruktioner, der får computeren til at udføre handlinger for at løse en given opgave. *Fx tekstbehandlingsprogrammer, regneark mfl.*

Spam

Spam er uønsket mail, ofte i form af reklamer, der har til formål at lokke modtageren til at købe produkter eller services over nettet.

Spamfilter

Program der filtrerer mail for spam og virus, således at brugeren undgår disse.

Spyware

Et program som installeres på en computer uden brugerens viden eller accept, hvorefter uvedkommende har mulighed for at følge

med i, hvad der sker på computeren eller misbruge den. Spyware kan fx overvåge og sende personlige informationer ud eller selvstændigt installere software på computeren.

Styresystem

Også kaldet operativsystem. Styresystemet er den grundlæggende software i en computer, hvorfra alle andre programmer samt hardware styres. *Fx Windows og Linux.*

Trojansk hest

Program, der installerer skadelig software under dække af at foretage sig noget andet. En trojansk hest kan i modsætning til ormen ikke sprede sig selv.

Uplode

At uploade er at overføre en eller flere filer via et net fra den lokale computer til en server eller en anden, fjern computer. Modsat downloade. *Fx at uploade billeder til en hjemmeside.*

Usb-nøgle/usb-stick

Transportabelt hardware, der kan tilsluttes computeren og hvorpå data kan lagres.

Virus

Skadeligt program, der spreder sig ved at inficere andre programmer. Skaderne kan være ødelagte filer, videregivelse af adgangskoder osv. En virus skal være vedhæftet et program (eller en mail), og kan ud fra den oprindelige definition ikke sprede sig selv. Betegnelsen 'virus' anvendes i dag dog også som et synonym for malware, se malware.

Virusfilter

Program, der filtrerer mail for virus og lignende, således at brugeren undgår at modtage disse.

Webmail

En, som oftest gratis mailservice, der er tilgængeligt på nettet. Fra en webmail kan du sende og modtage mails fra hvilken som

helst computer med internetadgang. *Fx Gmail og Hotmail.*

9. Teknologirådets udgivelser 2006-2007

Teknologirådets rapporter:

"Prioritering i sundhedssystemet"

Teknologirådets rapport 2007/5

"Lægeordineret heroin"

Teknologirådets rapport 2007/4

"Biodiversitet 2010"

-hvordan når vi målene?

Teknologirådets rapport 2007/3

"Det fremtidige danske energisystem"

Teknologiscenarier.

Teknologirådets rapport 2007/2.

"Energibehov med potentiale

-danske aktører i spil"

Idékatalog om innovationsbehov på energiområdet.

Teknologirådets rapport marts/2007.

"It-sikkerhed på tværs af grænser".

Anbefalinger fra en arbejdsgruppe under Teknologirådet.

Teknologirådets rapport 2007/1.

"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.

"Sundhedsydelse 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.

Nyhedsbrevet "Fra rådet til tinget":

Nr.248 01/08: Danmarks nye katastrofeberedskab under lub

Nr.247 01/08: Nej til Big Brother mod terror

Nr.246 12/07: Grundlag for prioriteringer skal frem i lyset

Nr.245 10/07: Energi for fremtiden

Nr.244 09/07: Åben og aktive innovationsprocesser er nødvendige

Nr.243 06/07: Lægeordineret heroin nu

TeknologiDebat Fokus:

TD1/2008: Årsberetning 2008

TD4/2007: Halmhuse er blevet til tybehuse

TD3/2007: Trafik i lange baner

TD2/2007: Varme hænder og kolde chips

TD1/2007: Årsberetning 2006

TD4/2006: Teknologivurdering i EU

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

Teknologirådet

Antonigade 4
1106 København K

Telefon 33 32 05 03
Telefax 33 91 05 09

tekno@tekno.dk
www.tekno.dk

Giro 8 51 07 68

Teknologirådet har til opgave at:

fremme
teknologidebatten

vurderer teknologiens
muligheder og konsekvenser

rådgive folketinget
og regeringen