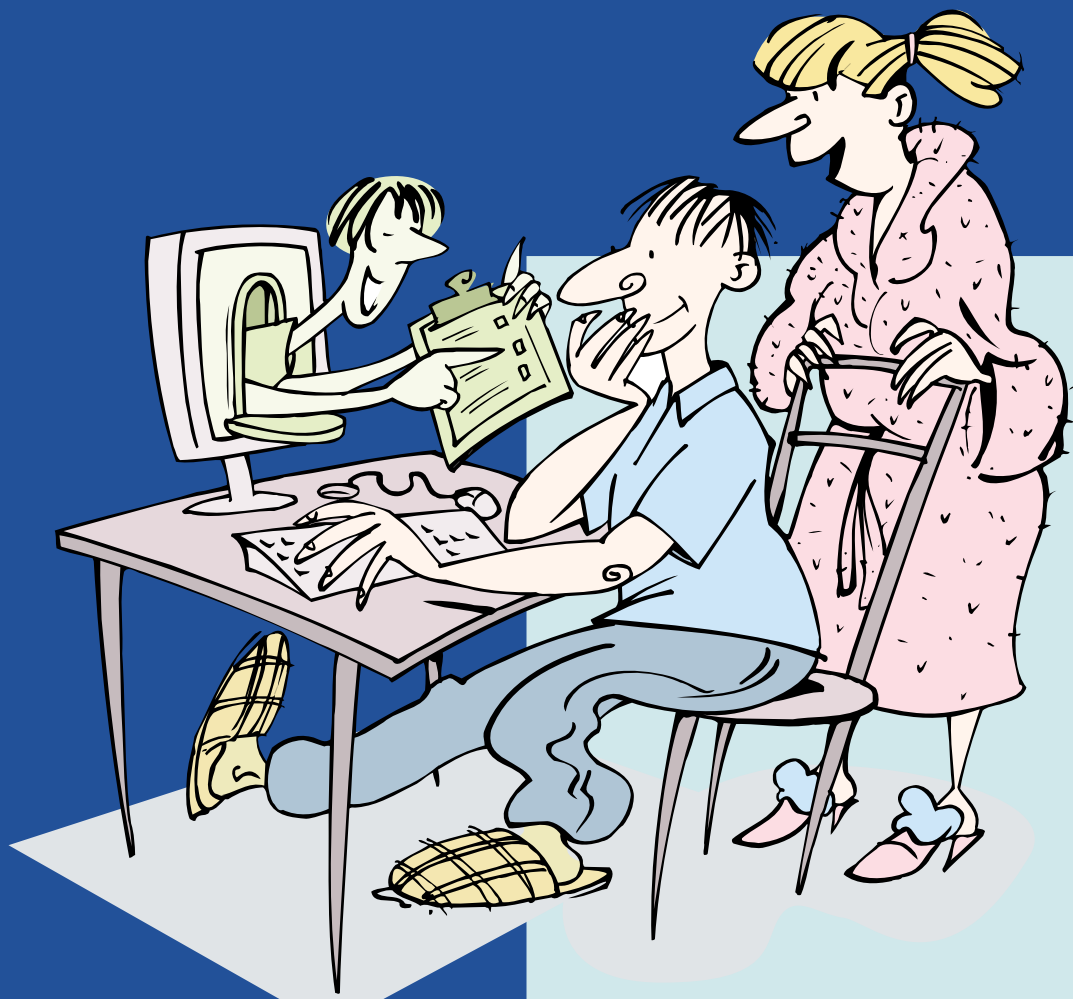
IT-Sikkerhedsrådet

Privatliv på internet

praktiske råd



Privatliv på internet

- en redegørelse med praktiske råd for den private internet-bruger

Ministeriet for Videnskab, Teknologi og Udvikling
April 2002

Privatliv på Internet
– en redegørelse med praktiske råd for den private internet-bruger

Publikationen kan købes ved
henvendelse til:
IT- og Telestyrelsen, Danmark.dk
Tlf. 1881
E-post sp@itst.dk
www.netboghandel.dk
Pris ved løssalg 50,- kroner inkl. moms

Publikationen kan også hentes
Ministeriet for Videnskab,
Teknologi og Udviklings hjemmeside
www.videnskabsministeriet.dk
ISBN (Internet): 87-91258-02-2

Udgivet af:
IT-Sikkerhedsrådet
c/o Ministeriet for Videnskab,
Teknologi og Udvikling
Bredgade 43
1260 København K
Tlf. 3392 9700
Fax 3332 3501
E-post fsk@fsk.dk

Tryk: K. Larsen & Søn A/S
Oplag: 2.000
ISBN: 87-91258-01-4

Forsideillustration:
Lars Refn

INDHOLD

FORORD

Internettet har opnået en sådan udbredelse, at mange private brugere i dag er vænnet til at bruge nettet til indkøb, bankforretninger, indberetning til det offentlige og så videre. Denne udvikling er sket til trods for, at vi i medierne ofte må læse og høre mange skrækhistorier om aflytning, brug af personlige oplysninger og svindel med kreditkort.

At den skepsis, der har været mod at benytte nettet til forpligtende handlinger, er ved at forsvinde, kan for eksempel aflæses i brugen af internetbaserede banksystemer, som gennem de seneste år har opnået meget stor udbredelse. Men hvilke muligheder har myndigheder, virksomheder, herunder teleselskaber og andre egentlig for at se brugerne over skulderen? I hvilken grad kan vi forvente privatlivets fred opretholdt når vi bruger internettet? Kan myndigheder eller andre spore al aktivitet på internet? Hvilke oplysninger er frit tilgængelige? Og hvad kan man som forbruger selv gøre?

Med denne redegørelse vil IT-Sikkerhedsrådet forsøge at beskrive de tekniske og juridiske svar, der findes på disse spørgsmål om beskyttelsen af forbrugerens privatliv på internettet. Dele af redegørelsen stammer fra den redegørelse med titlen „Privatliv på internet“, som IT-Sikkerhedsrådet udsendte i juni 1998, og som i dag i vidt omfang må anses for at være forældet. Men både omfang, formål og ikke mindst det tekniske indhold af den nuværende redegørelse er anderledes.

Redegørelsen indledes i afsnit 1 med en beskrivelse af det historiske og tekniske grundlag for internet, som vi kender det i dag. Derpå følger i afsnit 2 en nærmere redegørelse for, hvilke risici der er for at blive kigget

over skulderen, når man anvender nettet - enten ved at nogen trænger ind og uberettiget læser kommunikation eller ved at oplysninger, tilsigtet eller ubevidst, lagres som „elektroniske spor“. Herpå følger i afsnit 3 en oversigt over nogle af de juridiske regler der beskytter privatlivet på nettet. Afsnit 4 og 5 indeholder en praktisk vejledning henvendt direkte til brugeren i, hvad man kan gøre, hvis man vil sikre sit privatliv på internet.

København i april 2002

Mads Bryde Andersen
Professor, dr.jur.
Formand for IT-Sikkerhedsrådet

1 INTRODUKTION TIL INTERNET

Hvad er internet?

Internettet er et globalt netværk, der forbinder tusindvis af datanet og lokalnet og flere millioner computere, dataservere og pc'er i en verdensomspændende infrastruktur. Kommunikationen sker via teleforbindelser og computere, som udgør henholdsvis forbindelseslinjer og knudepunkter på internet. Knudepunkterne er henholdsvis routere og servere. En router er en computer, der blot modtager og afsender pakker af data mellem forskellige transmissionsmedier uden at gøre noget ved indholdet af pakkerne. En server er en computer, der lagrer programmer og data, og hvori data skabes, bearbejdes, ændres eller forædles på anden vis.

Internettet ejes ikke af en bestemt organisation eller virksomhed, men er så at sige en fælles infrastruktur bestående af datanet og IT-ressourcer. Den samlende kraft er TCP/IP protokollerne, som er blevet til igennem internettets cirka 30 årige udviklingshistorie. Disse protokoller (og det første net der baseredes på dem), blev skabt i 1969 som et forsknings-projekt under det amerikanske forsvarsministerium (Department of Defence, DoD). DoD trak sig i 1983 helt ud af internet-samarbejdet for i stedet at opbygge det lukkede MilNet. Internettet blev herefter videreført af uddannelsesinstitutionerne under en stigende kommerciel deltagelse. Selvom disse beslutninger umiddelbart kun berørte den amerikanske del af internet, har de haft betydning for resten af verden, eftersom det var her internettets grundlæggende arkitektur blev skabt.

I 1991 besluttede The National Science Foundation, der står bag de amerikanske forskningsbevillinger til internet, at fjerne tidligere restriktioner om brug af nettet til kommercielle formål. Samtidig hermed etableredes foreningen Commercial Internet eXchange association (CIX) under deltagelse af virksomhederne General Atomics (CERFnet), Performance Systems International, Inc. (PSInet) og UUnet

technologies, Inc. (AlterNet). Disse virksomheder, der senere er suppleret med flere andre, indgik efterfølgende i et samarbejde, der havde til formål at sikre den fornødne kapacitet ved internet.

De mest benyttede internet-tjenester i dag er

– World Wide Web.
– Elektronisk post (e-post).
– Chat og nyhedsgrupper.

Ud over disse er der en lang række andre tjenester, som benyttes i større eller mindre grad, blandt andet filtransport (FTP) til hentning af filer fra (ofte frit tilgængelige) arkiver. De nævnte tjenester er imidlertid mest relevante for problemstillingen om privatlivsbeskyttelse på internet.

At internet-kommunikation adskiller sig fra så megen anden kommunikation i det moderne samfund skyldes som nævnt anvendelsen af de såkaldte TCP/IP kommunikationsprotokoller, som anvendes af de ressourcer og personer, som bruges og kan nås via nettet. Protokollerne fungerer således, at meddelelser, der overføres via nettet, vil blive splittet op i mindre „informations-bidder" - såkaldte pakker - der i princippet sendes af sted hver for sig. Teknikken kan sammenlignes med, at et brev forvandles til bunker af postkort, der ikke nødvendigvis følger samme vej fra afsender til modtager. Pakkerne er nummererede, og skulle en eller flere af pakkerne gå tabt undervejs, beder den modtagende computer afsender-computeren om at sende de manglende pakker igen. Når samtlige pakker er nået frem til deres bestemmelsessted, stykkes de sammen til det oprindelige brev. For en nærmere gennemgang af disse protokoller henvises til side 16.

Internet-udbydere

De fysiske netværksforbindelser på nettet ejes og drives oftest af teleselskaber. De logiske netværksforbindelser og routere ejes og drives oftest af internet-udbydere. Begrebet „internet-udbyder" (omtales ofte ISP =

Internet Service Provider) dækker over et virvar af „operatører", der spænder fra internationale koncerner, teleselskaber, offentlige institutioner, konsortier og universiteter og ned til mindre IT-virksomheder og små web-bureauer, der er vært for web-information fra „lejere", eller som reklamerer for egne produkter og tjenester.

En virksomhed, organisation eller privat bruger tilslutter sig internettet ved at erhverve et opkoblings-abonnement hos en internet-leverandør. Opkobling til internet-leverandøren, og dermed til det globale internet, sker via en teleforbindelse, som for eksempel kan være enten en opkalds-forbindelse (almindelig telefoni, ISDN eller ADSL), en fast teleforbindelse eller tilslutning til et datanet via satellit, radiokædeforbindelse eller lignende Betaling for brugen af internettet sker typisk alene ved betaling af dels teleomkostningen for denne (lokale) forbindelse til internet-leverandøren og dels abonnementsafgiften til internet-leverandøren for adgangs- og brugsretten til internettet via denne forbindelse.

Infrastrukturen i det globale internet hviler på de tusindvis af transmissions-forbindelser med videre, som internet-udbyderne - bilateralt eller multilateralt - har etableret imellem sig for at opnå gode nationale og internationale forbindelser i internet. Der er ingen central koordinering eller styring af, hvem der etablerer forbindelser med hvem, og der er heller ikke en entydig fysisk kerne i infrastrukturen. Forbindelserne etableres på initiativ af og betales af de involverede parter. De sikkerheds-problemer, der muligvis kan siges at ligge i denne „anarkistiske" opbygning af internettet (og som for eksempel kan få betydning i en beredskabssituation) er ikke omfattet af denne redegørelse.

Når der i denne redegørelse tales om „internet-udbydere", for eksempel i forbindelse med spørgsmålet om disses mulighed for at overvåge brugerens e-post-korrespondance, sigter dette begreb altså ikke alene på virksomheder, der sælger internet-abonnementer til enkeltpersoner med videre, men også på de virksomheder, der selv er tilsluttet internettet med en e-post-server, hvortil og -fra medarbejdere kan kommunikere på internet. At begrebet „internet-leverandør" dermed omfatter meget andet end virksomheder, der markedsfører internet-adgang overfor deres kunder,

har stor retspolitisk betydning. Det er vanskeligt at indføre regler (for eksempel om sikkerhed), der skal være gældende for alle „internet-leverandører", når man har at gøre med en så ubestemt kreds af aktører.

Af samme grund er markedet for internet-udbydere ganske uhomogent. Der findes ingen særlige branchestandarder, der forpligter internet-udbyderne til at overholde bestemte niveauer for sikkerhed, adgang, service og lignende, og det opfattes generelt som en styrke ved internet, at denne del af teleområdet ikke er genstand for den tætte lovregulering, der kendes fra andre dele af området. Flere lande har dog indført visse regler for logning af datatrafik med videre. I Danmark er internet-udbyderne således omfattet af telelovgivningen. Af samme grund kan det formentlig lægges til grund, at sikkerheden hos de enkelte internet-udbydere på globalt plan er meget svingende og svært gennemskuelig for den enkelte bruger.

IP-adresser og domænenavne

På internettet adresseres alle enhederne (computere og routere med videre) med globalt entydige net-adresser - såkaldte IP-adresser (IP = Internet Protocol). Administration af IP-adresser er en af de (få) opgaver, som koordineres centralt af en internet-organisation (ICANN).

Det oprindelige koncept for IP-adresser var, at alle maskiner, der er forbundet til internet, skulle have en unik adresse - det vil sige en unik IP-adresse, som altid er tilknyttet samme maskine. Under internettets udvikling er der imidlertid dels blevet knaphed på IP-adresser (et 4*8-bits adresserum), dels er der opstået behov for en mere dynamisk opfattelse og brug af IP-adresser. Dette har ført til, at dynamisk tildeling af IP-adresser samt brug af såkaldte „private IP-adresser" i interne virksomheds-net i dag er udbredt, for eksempel via en firewall med adressekonverterings-faciliteter.

I praksis betyder den dynamiske brug af IP-adresser, at pc'erne hos private internet-brugere og hos medarbejderne i de virksomheder, der

har valgt dynamisk IP-adressering, skifter IP-adresse (indenfor en pulje af IP-adresser) hver gang, de benyttes. Når for eksempel en privat internet-bruger kobler sin maskine op til en internet-leverandør via telefonnettet, får maskinen typisk tildelt en midlertidig IP-adresse ud fra en pulje af IP-adresser, som leverandøren har rådighed over. Brugerens maskine beholder denne IP-adresse, sålænge forbindelsen holdes, og ved næste opkobling får maskinen sandsynligvis tildelt en anden IP-adresse.

I modsætning til den dynamiske brug af IP-adresser, kan der tildeles permanente IP-adresser til brugernes pc'er. Pc'erne vil dermed (såfremt der ikke foretages adresse-mapning i en router eller firewall ud mod internet) være mulige at identificere og genkende på internet. For private brugere, som har opkaldsforbindelse til internet, er det hos enkelte internet-udbydere muligt at få reserveret en permanent IP-adresse tilhørende denne bruger. Med en permanent (unik) IP-adresse kan den enkelte maskine endvidere tildeles et domænenavn (for eksempel „pc1.firma.dk").

Domænenavne er brugervenlige navne, som knyttes til IP-adresser i den såkaldte DNS-tjeneste (Domain Name System). For eksempel er domænenavnet www.vtu.dk knyttet til IP-adressen 195.215.15.250, som er tildelt web-serveren for Ministeriet for Videnskab, Teknologi og Udvikling. I praksis kan flere domænenavne dele samme IP-adresse, ligesom flere IP-adresser kan lede til samme domænenavn.

„The Internet Corporation for Assigned Names and Numbers" (ICANN, www.icann.org) har i dag ansvar for tildeling af domænenavne og IP-adresser på øverste niveau (for eksempel .com, .net og landespecifikke domæner, som .dk). ICANN blev dannet i oktober 1998, og har overtaget de funktioner, der indtil da blev varetaget af IANA (Internet Assigned Numbers Authority). ICANN er i juridisk forstand en privat virksomhed, der fungerer i henhold til en aftale med det amerikanske handelsministerium (Department of Commerce).

Hvor beslutning om oprettelse af nye top-domæner ligger i ICANN, beror selve administrationen af andenordens domænerne (som for eksempel domænenavnet firma.dk) hos eksterne organisationer. I Danmark vare-

tages administrationen af „.dk“-domænet således af Dansk Internet Forum (DIFO), der er en privat forening stiftet af en række leverandør- og bruger-organisationer med berøring til den danske del af internet.

Driften af DNS-systemet er i dag blevet en fundamental forudsætning for, at internet kan fungere. Hvis ikke DNS-systemet kan oversætte et domænenavn til en IP-adresse, vil kommunikation i praksis være umulig. Derfor er det vigtigt, at de virksomheder, der er ansvarlige for tildeling af domænenavne på topniveau (for eksempel .dk og .com) er underlagt visse sikkerhedskrav. IT-Sikkerhedsrådet har givet anbefalinger herom i sin redegørelse fra 2001 om internet-sårbarhed.

Routere

Routeren kan betragtes som tilkørselsvejen til internet. Når brugeren fra sin arbejdsplads har sendt en e-postmeddelelse, vil denne meddelelse blive grebet af en router, der sørger for at sende meddelelsen videre ud på internet. Routeren vælger transmissionsvejen for hver pakke, der skal videresendes. Hver router på vejen vælger kun den næste forbindelse, som pakken skal sendes til, hvilket sker på grundlag af en tabel over grupper af IP-adresser - en såkaldt routningstabel. For hver gruppe viser tabellen, hvilke forbindelser, der vil bringe pakken nærmere sit mål. Hvis der findes flere mulige forbindelser kan valget mellem disse eventuelt ske på grundlag af den øjeblikkelige belastning på linjerne. Visse metoder til belastningsudjævning kan også betyde, at en router forsøger at fordele pakker til samme modtager over flere forbindelser.

Routernes tabeller over forbindelser ændres automatisk, når en router tages ud (går i stykker), eller når der sættes en ny router ind et eller andet sted eller sker andre ændringer. Oplysninger om ændringer udveksles fra router til router. Denne dynamiske og selvkonfigurerende infrastruktur er væsentlig for „kernen“ eller hele den centrale del af internet.

Når infrastrukturen virker perfekt, kommer alle pakker ad den mest effektive vej. Det er i øjeblikket op til net-operatørerne, om den mest

effektive rute er den hurtigste eller den billigste, men i fremtiden vil effektiviteten også afhænge af den pris, brugeren betaler.

Hvor „kernen" i internettet er de ovenfor nævnte selvkonfigurerende routere og forbindelserne imellem dem, kan „skallen" siges at udgøres af de forbindelser, som benyttes til brugernes tilkobling, og den eller de første router(e), som pakkerne passerer på vej ind i internet. Routerne i nærheden af „skallen" er ofte manuelt konfigureret til at vide, hvilke forbindelser brugerne sidder på, og hvilke der fører til „kernen". Det drejer sig typisk om routere hos brugerens internetudbyder, og for små udbyderes vedkommende tillige om routere hos den leverandør, der leverer for eksempel international forbindelse.

Dette betyder, at man ikke kan forudsige, hvilken vej en pakke vil følge i „kernen", fordi meddelelsen kan komme frem ad vidt forskellige ruter, alt afhængigt af, hvilke forbindelser der måtte være tilgængelige på transmissionstidspunktet. Oprindelig tilvejebragte man denne egenskab for at gøre de tilsluttede computere mindre følsomme for militære angreb. I dag er egenskaben en væsentlig grund til internettets dybest set kaotiske opbygning, hvor nye net kobles på i en uendelig maskenet-struktur. Den funktion, man hermed opnår, kan beskrives som kommunikation uden central styring. Blandt andet af denne grund er det i dag vanskeligt for internet-udbydere at garantere en oppetid eller en mindste tilgængelig båndbredde på tværs af internet. Derfor kan det være nødvendigt at foretage en nøje risikoanalyse, hvis man overvejer at basere en sikkerheds-kritisk applikation på nettet. IT-Sikkerhedsrådet har givet nærmere anbefalinger om denne afvejning i sin redegørelse fra 2001 om internet-sårbarhed.

Det gælder dog som hovedregel, at trafik mellem en netleverandørs egne kunder ikke vil forlade leverandørens eget net eller system. Det er også i leverandørernes interesse at befordre kommunikation over de billigste linjer, og derfor vil der typisk etableres bilaterale forbindelser sådan, at kommunikation mellem brugere fra samme land ikke behøver at komme udenfor landet, med mindre der opstår fejl.

Muligheden for at sikre internet-kommunikation mod aflytning med videre er derfor størst, når der kommunikeres mellem danske internet-leverandører, idet aflytningsmuligheden her står og falder med sikkerheden hos den enkelte internet-leverandør (heri indbefattet virksomheder med videre, der fungerer som „internet-udbydere" overfor medarbejdere og andre, gennem faste opkoblinger til internet). Om man kommunikerer sikkert på nettet vil derfor altid være et spørgsmål om sikkerheden hos „det svageste led" blandt andet hos den part, med hvem man kommunikerer.

TCP/IP protokollerne

Som nævnt ovenfor er TCP/IP-protokollerne kendetegnende for den kommunikation, der sker via internet. TCP/IP protokolsuiten understøttes af alle betydende IT-leverandører og er i dag en dominerende standard for kommunikation mellem udstyr fra forskellige leverandører.

Begrebet „TCP/IP" dækker i daglig tale over en hel suite af protokoller, som benyttes i internetsammenhæng. Dels findes et antal basisprotokoller, blandt andet selve IP (Internet Protocol) og TCP (Transmission Control Protocol), som skal understøttes af alle computere, som benytter TCP/IP protokolsuiten - og dermed af alle computere på internet. Men herudover findes et stort antal anvendelsesspecifikke protokoller samt protokoller for, hvordan TCP/IP benyttes over forskellige transmissionsmedier. Eksempler på anvendelsesspecifikke protokoller (se om anvendelser i afsnittet nedenfor) i TCP/IP protokolsuiten er World Wide Web protokollen HTTP (Hyper Text Transfer Protocol), e-post protokollen SMTP (Simple Mail Transfer Protocol) og NetNews protokollen NNTP (Network News Transfer Protocol).

Ved tilslutningen af computere til internettet er det blandt andet vigtigt at tage stilling til, hvilke TCP/IP anvendelsesprotokoller, der skal benyttes, og det kan være en fordel rent sikkerhedsmæssigt, at de protokoller, som ikke skal benyttes, fjernes fra ens udstyr. For eksempel vil det ofte indebære en sikkerhedsrisiko, hvis en computer på internettet understøtter muligheden for filadgang udefra gennem filtransportprotokollen (FTP).

Tilsvarende indebærer sikkerhedsopsætning af en firewall, at der spærres for bestemte protokol-typer, som man ikke ønsker at understøtte (udefra og/eller indefra).

Brugernes anvendelse af internet

Hovedparten af den information, der overføres via internet, sker fra og til brugere, der betjener sig af udstyr, de selv kobler til nettet. Brugeren er ofte selv den mest kritiske person, når det gælder internet-sikkerhed. En kæde er ikke stærkere end dens svageste led, og for en stor del af de sikkerhedsproblemer, der har betydning i det praktiske liv, er brugeren selv det svageste led.

Et væsentligt sikkerhedsproblem i den forbindelse er brugerens omgang med sit password, altså den kode, der i de fleste e-postsystemer skal afgives for at få adgang til brugerens postadresse, og som dermed giver mulighed for at sende og modtage post, læse lagret post og så videre. Vælger brugeren et password, der er let at gætte (for eksempel sit eget eller et familiemedlems navn, fødselsdag eller lignende) stiller brugeren dermed ikke blot sin e-post-„identitet" til rådighed for hackere eller andre, der måtte forsøge at skaffe sig rådighed over brugerens system; lagret e-postkorrespondance bliver tilmed tilgængeligt for sådanne hackere. IT-Sikkerhedsrådet har givet nærmere vejledning om valg og omgang med password i sin vejledning fra 2000: „Adgangskontrol til en hjemmeside".

Behovet for at anvende sikre passwords vil altid bero på risikoen for at lide retstab med videre i forbindelse med en sådan uautoriseret overtagelse af brugerens system. Når sikkerhedsniveauet vælges, må det imidlertid tages i betragtning, at der er gode muligheder for at „gætte" passwords ved hjælp af dertil indrettede programværktøjer. Jo længere ens password er, og jo mere det adskiller sig fra ord og navne, der forekommer i leksika og ordbøger, desto bedre er man sikret mod sådanne angreb. Styrken af password kan for eksempel øges ved at anvende specialtegn, som kolon, komma og parenteser.

Brugerens udstyr og internet-software

Internet-brugeren har normalt adgang til internet-tjenesterne fra en pc men kan også betjene sig af for eksempel mobiltelefon og enheder tilkoblet TV. Anvendelsen af en pc- eller TV-skærm kan i sig selv give grundlag for aflytning, hvad enten skærmen anvendes til internet-kommunikation eller til andet brug. Ved hjælp af særligt udstyr kan man således fra mange meters afstand „aflæse" de magnetfelter, som skærmen udsender og dermed få kendskab til, hvad der står på skærmen. Da disse problemer ikke er særegne for internet-kommunikation, behandles de ikke yderligere i det følgende.

Selve adgangen til internettet kan enten være etableret direkte fra brugerens udstyr (opkaldsforbindelse for pc'er og opkalds- eller fast forbindelse for servere) eller ske via for eksempel en virksomheds lokalnet, som er forbundet til internettet via en internet-leverandør. I sidstnævnte tilfælde vil der i dag ofte være en såkaldt „firewall" mellem virksomhedens interne IT-system og internettet for at beskytte mod udefra kommende angreb, for eksempel hacker-angreb.

Operativsystemerne i pc'erne indeholder de grundlæggende kommunikationsfaciliteter (TCP/IP protokollerne med videre) for at skabe kommunikationsmulighed med internet. Dertil kommer programmer for de tjenester, som brugeren benytter, for eksempel web, e-post, filtransport (FTP), nyhedsgrupper (NetNews), chat og mange andre.

Til de mest almindelige operativsystemer fra Microsoft og Apple Computer (Macintosh) medfølger programmer til web og e-post, hvorved mange brugeres behov for internet-programmer er dækket. Dertil kan brugeren få behov for en række tillægsprogrammer til for eksempel FTP, nyheds-grupper og chat. De mindre programmer kan ofte findes i gratisversioner på internettet.

Desværre har der til mange internet-programmer historisk været knyttet en række sikkerhedsmæssige problemer („huller"). Sådanne huller er typisk hurtigt blevet rettet af de pågældende leverandører, der selvsagt

ikke kan leve med sådanne produktvanskeligheder. Markedet kan for så vidt siges selv at rumme mekanismer, der sikrer en løbende sikkerhedsmæssig finjustering af disse produkter. Alligevel må det siges at være kritisk, at mange af de mest udbredte programsuiter til internetkommnikation erfaringsmæssigt har vist sig at være usikre. Ingen vil kunne garantere selv de mest forkromede browser-produkter mod uventede svagheder, og disse sikkerhedsspørgsmål bør derfor give anledning til en løbende og konstant interesse. Det kan i den forbindelse fremhæves, at den større integration mellem programmerne kan medføre en øget risiko for sikkerhedshuller.

2 HVILKE ELEKTRONISKE SPOR EFTERLADER MAN PÅ NETTET?

2.1 Problemstillingen

Enhver der bruger internet efterlader sig et vist spor afhængigt af om brugeren anvender et e-postprogram, søger rundt på nettet via internet-browser eller benytter chat-programmer.

Al data på internet sendes mellem entydige internet-adresser - såkaldte IP-adresser (ikke at forveksle med e-postadresser). Typisk har virksomheder, offentlige institutioner og myndigheder en fast IP-adresse, hvilket er nødvendigt når man er permanent koblet på internettet, hvorimod private som oftest kun har midlertidige IP-adresser, der automatisk tildeles opkaldsenheden når der skabes forbindelse til internettet (et stigende antal private forbrugere har forbindelser, der permanent er på internettet og derfor ofte er tildelt en fast IP-adresse). Brugen af IP-adresser er registreret hos teleselskaberne, men giver ingen information om hvem, der har sendt data fra/til en given IP-adresse. Oplysningerne gemmes hos teleselskaberne til brug for eventuel efterforskning af kriminalitet og kan kun udleveres til politiet mod forevisning af en dommerkendelse.

Et eksempel: En borger har fra sin hjemme-pc via modem koblet sig på internettet. Opkaldsenheden (computeren) er nu tildelt en midlertidig IP-adresse, hvilket teleselskabet har registreret. Via borgerens (eventuelt automatiske) login kan teleselskabet se hvilket internet-abonnement, der er i brug, men ikke hvilken person, der benytter computeren.

Ved „elektroniske spor“ forstås oplysninger om, hvilken information den enkelte bruger har sendt, modtaget eller efterspurgt med videre samt hvornår og hvordan. Sådanne oplysninger om brugen af tjenester og om indholdet af kommunikation på internettet kan teoretisk set tænkes opsamlet på enhver maskine, informationen passerer forbi, og dette kan give anledning til bekymring med hensyn til beskyttelsen af privatlivets fred.

Spørgsmålet om anonymitet og elektroniske spor hører nøje sammen. Er man anonym, gør det ikke noget, at man efterlader sig elektroniske spor, eftersom den færden, der hermed lægges frem, ikke kan henføres til en selv. Har man derimod aktivt givet sig til kende, for eksempel ved brug af et betalingskort, spiller det en rolle, hvad der sker med de spor, man efterlader sig.

2.2 Web-tjenester

Når brugeren med sin browser kobler sig op til en web-server, efterlades der i længere tid information på serveren om brugerens færden og i visse tilfælde også hans identitet på nettet. Der kan være flere årsager til, at denne information samles. For det første kan det være nyttigt for eksempel i forbindelse med elektronisk markedsføring at vide, hvilke web-sider der er kraftigt efterspurgt. Denne information kan for eksempel bruges til at tage beslutning om, hvilke produkter eller lignende der skal satses på. Angribes maskinen af en hacker, der søger uautoriseret adgang eller har til hensigt at blokere tjenesten, kan opsamling af detaljerede oplysninger for det andet være den eneste metode til at spore angriberen.

De opsamlede oplysninger omfatter typisk tidspunktet, IP-adressen på den maskine forespørgslen kommer fra, eventuelt brugernavnet for den konto, der benyttes, navnet på det dokument forespørgslen handler om og resultatet af opkoblingen (i form af en fejlkode, hvis forespørgslen afslås, eller størrelsen på det udleverede dokument, hvis forespørgslen er efterkommet). Indholdet af dokumentet opsamles ikke, men da det jo typisk ligger på samme maskine, kan der umiddelbart hentes en kopi.

Afhængig af brugerens situation vil IP-adressen med større eller mindre præcision kunne bruges af en web-tjenesteudbyder til at identificere selve brugeren. Hvis brugeren således benytter en pc med en permanent, unik IP-adresse (og denne ikke mappes til en anden IP-adresse i en firewall), kan brugeren (det vil sige brugerens maskine) identificeres entydigt ud fra IP-adressen. I nogle tilfælde vil der endvidere være knyttet et domæne-

navn til en sådan IP-adresse, hvorved navnet på brugerens maskine direkte kan slås op i DNS-systemet (domænenavns-tjenesten).

Hvis brugerens maskine derimod tildeles en dynamisk IP-adresse, for eksempel som ved internet-adgang via telefonopkald fra private, vil det kun være muligt for web-tjenesteudbyderen at spore, hvilken internet-leverandør brugeren har benyttet, men ikke hvilken specifik maskine eller bruger der er tale om. Hvis internet-leverandøren har mulighed for at logge de telefonnumre, som opkaldene kommer fra (baseret på A-nummeroverførsel), er det også muligt for denne at spore den enkelte bruger. Internetleverandøren har typisk også mulighed for at identificere brugerens login (brugernavn) - gennem en analyse af logfiler - og dermed de identitetsoplysninger, brugeren har afgivet ved abonnementets oprettelse.

I virksomheder, hvor der benyttes dynamisk IP-adressering, eller hvor der sker adresse-konvertering i en firewall, vil det kun være muligt for Web-tjenesteudbyderen at spore, hvilken virksomhed brugeren kommer fra. Systemadministratoren i virksomheden har imidlertid mulighed for at identificere den specifikke maskine, jævnfør afsnit 2.7 side 32 om virksomhedens firewall.

Der overføres endvidere allerede ved den første kontakt mellem brugerens browser og web-serveren en række tekniske informationer om brugerens browser-software (version og type), hvilke filtyper der accepteres med videre. De web-steder, der besøges, har mulighed for at aflæse visse informationer fra brugerens pc. Informationerne benyttes til blandt andet statistik og til at optimere visningen af siderne.

Information om, hvilke oplysninger ens browser uopfordret oplyser web-servere om, kan fås på web-siden „Forbrugersikkerhed“ (www.forbrugersikkerhed.dk), hvor der er en såkaldt „Sportester“.

Internet-browsere, som Microsoft Internet Explorer, Netscape Navigator, Opera og andre opbygger en historik over besøgte sider og deres indhold, hvilket givet mulighed for at bladre frem og tilbage mellem tidligere besøgte sider uden nødvendigvis at skulle genskabe hele siden hver gang.

Det er ikke umiddelbart muligt for et tilfældigt web-sted at se en liste over samtlige andre web-steder brugeren har besøgt. Derimod kan web-stedet registrere adressen på den side, der sidst er besøgt.

Med mindre brugeren selv taster oplysninger ind på siden kan web-stedet ikke se identiteten på den person, der besøger siden.

Cookies

En „cookie" er en lille mængde data (tekst-baseret og i en størrelsesorden typisk op til nogle tusind bytes), som en server kan bede brugerens browser om at gemme (på brugerens maskine). Disse data vil derefter blive sendt hver gang brugeren henter et nyt dokument fra den samme server.

Formålet med at sende en cookie er at fastholde en tilstand eller viden i brugerens interaktion med serveren, for eksempel for at kunne gennemføre et „login-forløb" eller kunne udbyde personligt tilpassede web-sider. For eksempel kan serveren give brugeren mulighed for at vælge, hvilket sprog serveren skal præsentere siderne på eller opbygge en „indkøbskurv" med varer, der senere kan bestilles i en samlet transaktion. Hvis serveren bruger cookies til formålet vil disse data kunne overleve, at brugerens forbindelse bryder ned og senere retableres inden for en vis tidsgrænse, for eksempel 30 minutter. Der kan knyttes en levetid til hver cookie - et sprog vælges typisk permanent, mens en indkøbsliste måske er irrelevant efter en dag.

Hvis en server ikke anvender cookies er IP-adressen den eneste oplysning, som en server automatisk kan benytte til at identificere den specifikke bruger, og det er en meget upålidelig metode. Dels kan en brugers IP-adresse være midlertidig (dynamisk tildelt), dels kan der være mange brugere, der deler den samme IP-adresse, fordi de henter web-sider gennem firewalls eller proxy-servere, der udadtil lader flere brugere fremstå som én.

Netop det, at brugeren bliver genkendelig overfor serveren, kan give anledning til bekymring med hensyn til anonymitet. Nyere udgaver af de populære browsere har derfor indstillinger til at advare brugeren om cookies eller permanent helt at nægte modtagelsen af cookies, og det er også muligt at slette cookies efter hver opkobling til nettet. Brugeren vil imidlertid afskære sig fra adgang til en række informationstjenester ved permanent at spærre for cookies, og brugen af advarsler (i form af en advarsel i en pop-up boks, som browseren viser ved forekomsten af en cookie) vil hurtigt irritere brugeren så meget, at advarslerne slås fra igen.

En server kan ikke få fat i en brugers cookies til andre servere eller overhovedet registrere, at de findes (med forbehold for fejl i browseren). Serveren kan heller ikke bruge cookies til at finde ud af for eksempel brugerens e-post-adresse (medmindre brugeren selv oplyser denne) eller hvilke andre sider, brugeren har besøgt.

En cookie er derfor ikke uden videre person-henførbar. Hertil kræves, at brugeren selv har afgivet oplysning om sin identitet, eller at oplysningen om, hvem der kommunikerede fra den dynamisk tildelte IP-adresse fremskaffes på anden vis (for eksempel ved dommerkendelse). Er der derimod tale om, at brugeren afgiver sin identitet, når han besøger en web-side, rummer cookie-teknologien en misbrugsmulighed for den websideudbyder, som vil anvende oplysningerne til at frembringe og udnytte brugsprofiler af den besøgende.

HTTP-henvisninger

HTTP-protokollen, der bruges til transport af web-sider, har en speciel egenskab: Når en bruger følger en henvisning på en web-side, vil „navnet" (URL'en) på den henvisende side blive sendt med, når browseren beder om den nye side. Dette sker hovedsagelig for at gøre det muligt for en web-administrator at finde og rette ukorrekte henvisninger, men det kan også give uvedkommende mulighed for opsamling af oplysninger om en brugers aktiviteter på nettet.

En særlig problemstilling i denne forbindelse knytter sig til anvendelsen af formularer med indtastningsmulighed på web-sider. Formularer findes for eksempel i mange søgetjenester, hvor brugeren taster søgeord ind i særlige felter. Af tekniske årsager sker det ofte, at de oplysninger, der er tastet ind i formularen, vil stå anført i navnet på den web-side, man får som svar på sin søgning. Dette er i sig selv ikke et problem, men hvis svarsiden indeholder links til andre web-servere, for eksempel i form af reklamer, vil navnet på svarsiden blive sendt til disse andre servere. Og da svarsiden som før nævnt indeholder oplysninger om, hvad brugeren har søgt efter, kan disse servere - som altså eksempelvis kan tilhøre reklamebureauer - aflæse brugerens søgeoplysninger og gentage søgningen eller eventuelt opbygge en profil for brugerens anvendelse af web-sider.

Det er teknisk muligt for administratoren af en web-server (for eksempel en søgetjeneste) at undgå at afsløre oplysninger i formularer og lignende for annoncører, men det er ikke muligt at sløre serverens navn. Det er tillige teknisk muligt at programmere browseren til at undlade at videresende navnene på henvisende sider eller at give brugeren kontrol over, hvorvidt det skal ske, men sådanne faciliteter findes ikke i dag i browserne.

2.3 Søgemaskiner og katalog-tjenester

En af de helt nødvendige tjenester på internettet er de såkaldte „søgemaskiner“, der er effektive søgeværktøjer og katalog-tjenester, som kan hjælpe brugerne til at finde den information eller de personer, de søger.

Søgemaskinerne kan benyttes til at finde frem til web-sider eller indlæg i nyhedsgrupper ud fra angivne nøgleord. Flere af de populære søgemaskiner fungerer ved løbende at indsamle information fra samtlige web-sider og fra samtlige nyhedsgrupper på internet. Det er derfor muligt at indtaste en persons navn, for eksempel „Peter Hansen“ og derved - i løbet af få sekunder - at få henvisninger til de web-sider eller de indlæg i nyhedsgrupper, som indeholder teksten „Peter Hansen“ - eventuelt kombineret med andre søgekriterier og -ord.

Der findes også flere former for katalog-tjenester (directories) på internet, blandt andet kataloger over e-postadresser hvor det er muligt at søge bestemte personer frem. Nogle af disse kataloger fungerer ved tilmelding, men andre kataloger søger selv e-postadresser frem fra web-sider og fra indlæg i nyhedsgrupper. I Danmark er TDCs e-postkatalog blevet et centralt opslagsværk for søgning af e-postadresser (www.epost.dk). Effekten af disse meget kraftige søgeværktøjer og kataloger er, at når man først har udsendt information på internet, så vil denne information meget nemt kunne søges frem og forbindes med ens person af alle internet-brugere. Mange brugere er næppe klar over, at deres indlæg i nyhedsgrupper og eventuelt omtale på web-sider med videre kan søges frem så nemt, som det er tilfældet.

2.4 Elektronisk post

Når en e-postmeddelelse sendes fra afsender til modtager, mellemlagres meddelelsen under overførslen midlertidigt (på disk) på en e-postserver hos afsenderen og hos modtageren, inden den „afleveres“ i en fil, for eksempel på en pc hos modtageren, når denne læser meddelelsen. Eventuelt kan der ske en yderligere mellemlagring, for eksempel hvis den modtagende organisation benytter en ekstern leverandørs e-post-server som generel modtage-maskine for e-post, eller hvis der har været et midlertidigt nedbrud i en af serverne eller i kommunikations-forbindelserne.

Mellemstationerne hører i reglen til - i form af e-postservere - i afsenders eller modtagers organisation eller hos en af deres internet-udbydere (blandt andet for privat-brugere). Disse mellemstationer er ikke routere, men maskiner af samme type som web-servere. En person med de rette adgangsprivilegier til mellemstationen kan læse det midlertidigt lagrede brev eller tage en kopi.

Typisk vil selve brevet kun ligge i kort tid på en mellemstation. Det bliver slettet, så snart det er afleveret til den næste server. Derimod vil mellem-stationen opsamle og gemme oplysninger om både afsender, modtager

og brevets størrelse. Er der problemer med at sende brevet videre, kan det dog blive liggende i længere tid på en mellemstation, hvor hverken afsender eller modtager har kontrol over det. Et ikke-afleveret brev ligger dog sjældent i ubegrænset tid på en sådan mellemstation. Efter nogle dage (typisk mellem 1 og 14 dage) bliver brevet slettet, og en besked herom bliver normalt sendt til afsenderen (eventuelt indeholdende den originale meddelelse).

Når brevet er modtaget, det vil sige lagret i en fil der hører til modtager-adressen, vil det på et tidspunkt blive læst af modtageren, når denne kobler op til eller logger ind på maskinen. Herefter kan brevet overføres til brugerens pc eller private diskområde.

Det er brugerens postprogram og opsætning, der afgør om dette sker. Det er dog ikke usædvanligt, at brugere lader alle deres breve ligge i denne fil, indtil de eventuelt bliver slettet. Det er sådanne ikke-slettede breve, som en systemadministrator eller en anden person med de rette systemprivilegier nemmest kan overvåge.

Enhver e-post bærer, udover selve indholdet, på information om afsender og modtagers IP-adresse, samt hvilke enheder e-posten eventuelt har passeret undervejs på internettet. Typisk vil e-posten være lagret både hos afsender og modtager. Under transport fra afsender til modtager vil indholdet af e-posten (brevteksten) normalt ikke blive lagret andre steder.

Som følge af den internationale terroraktivitet i efteråret 2001 har flere lande fremsat eller gennemført lovforslag, der indebærer øget registrering og opbevaring af de oplysninger, der efterlades ved (blandt andet) internet-kommunikation. Herhjemme er dette sket ved den antiterror-pakke, som justitsministeren fremsatte i december 2001. I andre lande er overvågningen langt mere intens end foreslået her. Hvis en e-post fra en dansk borger således passerer en server i et sådant land kan det betyde, at en kopi af meddelelsen bliver gemt på den pågældende server. Flere udbydere af gratis e-postadresser, som for eksempel Hotmail, er for eksempel amerikanske og er derfor omfattet af de mere vidtgående amerikanske krav om logning.

I lighed med al anden trafik på internettet er transportvejen for epost ikke på forhånd givet. Det er derfor vanskeligt målrettet at finde spor af e-post fra enkeltpersoner med mindre der er adgang til afsender eller modtagers udstyr.

E-post via browser

På internettet findes adskillige tjenester hvor man frit kan oprette en e-postadresse. Benyttes en sådan tjeneste vil ens epost af hensyn til tilgængeligheden være lagret hos udbyderen, og al adgang ske gennem en internet browser.

E-post via browser kan med fordel benyttes når der er behov for at få adgang til e-post fra fremmede computere i internetcaféer, på biblioteket, fra hoteller eller lignende. Ved brug af internet-browsere efterlades der en omfattende historik på den maskine, der benyttes, hvilket kan betyde, at de e-postbreve, der læses via browseren efterlades på maskinen efter brug. Om muligt bør man forsøge, at slette de midlertidige filer, der er genereret af browseren, og lukke browser-programmet ned. Det vil betyde, at de midlertidige filer med eventuelle private oplysninger ikke er umiddelbart tilgængelige på maskinen.

E-post via post-program

Benyttes et post-program fra en stationær maskine (for eksempel en hjemme-pc) vil e-posten typisk (om end det er valgfrit) blive slettet hos udbyderen når posten hentes af brugeren. Der vil under disse omstændigheder således ikke blive efterladt særlige spor hos udbyderen.

2.5 Nyhedsgrupper

Nyhedsgrupper fungerer som en slags fælles opslagstavler eller diskussions-fora for internet. Systemet er delt op i mange tusinde emneområder, der

kaldes nyhedsgrupper; indlæg i diskussionerne kaldes nyhedsindlæg eller blot „indlæg“. Indlæggene i nyhedsgrupperne kopieres mellem dedikerede servere („news-servere“) placeret hos internet-udbyderne, så leverandørens kunder kan hente og læse de seneste ugers indlæg i nyhedsgrupperne herfra. Hvis en bruger ønsker at læse en bestemt nyhedsgruppe, som ikke umiddelbart ligger på den server, han eller hun henter nyhedsindlæg fra, kan brugeren bede serverens ejer (via administratoren) om at skaffe gruppen hjem. Alternativt kan brugeren finde en anden server, der både har den ønskede gruppe og vil tillade adgang fra brugerens maskine. En almindelig kommerciel server har i dag typisk 35-40.000 nyhedsgrupper, men antallet af eksisterende grupper er langt højere. Det vil dog næppe være muligt at finde samtlige grupper, da nogle af dem kun forekommer på en eller to servere.

Da nyhedsindlæg findes i utallige kopier rundt om i verden, er der ikke nogen centralt placeret logfil, hvor man kan se, hvem der har læst et bestemt indlæg. Derimod kan den enkelte server gemme oplysninger om læsning af indlæg, men det er typisk kun antallet af læste indlæg fra hver gruppe, der gemmes. Oplysningerne herom kan dog også være følsomme, for eksempel hvis det drejer sig om en gruppe med særlige politiske eller religiøse synspunkter. En bruger har også mulighed for at variere valget af server ved læsning, således at det er svært at finde den server, der har oplysningerne. Dette er i modsætning til elektronisk post, hvor det er en bestemt server, der modtager al post til en given post-adresse.

2.6 Chat-programmer

Ved hjælp af chat-systemer kan flere brugere „tale“ sammen ved at skrive direkte til hinanden i en slags nedskreven tale. Brugerne kommer via særlige programmer (der normalt skal anskaffes særskilt) i kontakt med en central server, der indeholder en tabel over de personer der er koblet på systemet i øjeblikket. Når en bruger er koblet på systemet, vil den centrale server straks registrere dette og andre personer på serveren vil få besked om dette og kunne kommunikere i skrift til den nye bruger.

De fleste chat-servere har adgang til de samme informationer som web-steder, det vil sige hvilken type computer man bruger, hvilken version af internet-browser og operativsystem der anvendes med mere. Hvis der benyttes et særskilt program til såkaldt Internet Relay Chat (IRC) vil serveren også have adgang til de andre oplysninger, der er indtastet i programmet, for eksempel brugerens navn. Det afhænger af serveren, hvilke informationer de andre brugere har adgang til. Visse chat-steder gemmer en log af al samtale på chat-stedet, og kan overgive denne logfil til politiet i forbindelse med efterforskning af kriminel aktivitet.

2.7 Maskinernes lagring af spor

Brugerens pc

På den pc, som benyttes af brugeren, vil browseren lagre både filer og andre oplysninger fra den seneste tids brug af internet. Både private brugere i hjemmet og medarbejdere i virksomheder vil derfor efterlade information om deres „surfing" på nettet på den benyttede pc (normalt lokalt på harddisken på brugerens pc).

For det første lagres en „URL-historik" - en log som kan fortælle, hvilke web-adresser brugeren har besøgt i den seneste tid. I MS Internet Explorer gemmes indtastede web-adresser (URL'er) eksempelvis i en pull-down menu under browserens indtastningsfelt for web-adresser, og besøgte web-adresser logges både i en menu og i browserens interne URL-historik, som benyttes til at vise allerede besøgte web-adresser med en anden farve end ikke-besøgte adresser. Det vil således være muligt for en anden person, som får adgang til pc'en, at se hvilke web-adresser der har været besøgt. Det er kun muligt i enkelte browser-versioner (de nyeste) at slette denne form for log og historik.

For det andet vil browseren - af hensyn til optimering og hurtigere svar-tider når samme web-sider besøges flere gange - cache (det vil sige lagre lokalt til genbrug) både HTML-filer og andre fil-typer, som hentes hjem, for eksempel gif- og jpeg-billeder, i et lokalt cache-lager. Indholdet af

dette cache-lager kan uden videre ses (i filer på harddisken) af andre brugere, som får adgang til pc'en. Indholdet i cache-lageret bliver først slettet, efterhånden som browseren cacher nye filer under brugerens brug af internet. Størrelsen af cache-lager kan sættes af brugeren selv, og det er muligt for brugeren at slette indholdet af cache-lageret, men de fleste brugere er næppe klar over disse muligheder.

Cache-lageret giver ikke anledning til særlige problemer, så længe det findes på brugerens egen pc. Derimod kan der som nævnt opstå problemer, når brugeren betjener sig af udstyr, der findes på offentligt tilgængelige steder, for eksempel i internet-caféer, biblioteker eller undervisnings-institutioner. I disse tilfælde beror muligheden for at opretholde anonymitet udelukkende på driftsstedets sikring af det pågældende udstyr.

Sidst skal det nævnes, at brugerens fil med internet book-marks - altså de data, brugeren selv har ønsket at lagre for senere at kunne finde frem til besøgte web-sider - naturligvis også kan ses af andre brugere, som får adgang til pc'en.

Der ligger derfor i dag meget både åbenlys og mere skjult information om en brugers internet-brug på den pc, som benyttes.

Virksomhedens firewall

De fleste virksomheder, som har adgang til internet i dag, har installeret firewall på deres forbindelse til internettet for at beskytte virksomhedens interne IT-miljø overfor hackere med videre. En medarbejder i en virksomhed, som har adgang til internettet og benytter det i det daglige arbejde, foretager derfor sine informationssøgninger på internettet gennem virksomhedens firewall.

Da det er en af de væsentlige sikkerhedsmæssige faciliteter i en firewall, at den løbende optager en fuldstændig log over samtlige transaktioner, der foretages (både indgående og udgående), vil alle medarbejdernes transaktioner på internettet også logges i virksomhedens firewall. Med

brug af de statistik- og opfølgningsværktøjer, som følger med firewall'en, er det derfor muligt for system-administratoren at se præcis, for eksempel hvilke web-sider den enkelte medarbejder har besøgt og hvor mange gange og så videre. En sådan logning kan give anledning til problemer af både juridisk og samarbejdsmæssig art. Herom henvises til IT-Sikkerhedsrådets vejledning „Brug af e-post og internet på arbejdspladsen" (januar 2002).

En sådan sporing kan blive lidt vanskeligere, hvis der benyttes dynamisk IP-tildeling i virksomheden, men den er stadig mulig og overkommelig med brug af de rigtige værktøjer. Mange medarbejdere er i dag næppe klar over, at en så intens overvågning af deres færden på internettet er mulig. Denne form for informationsindsamling om medarbejdernes udførelse af arbejdet med videre er sammenlignelig med at føre log over, hvilke telefonsamtaler de enkelte medarbejdere fører - blot mere detaljeret, idet for eksempel information om læste filer (filnavne) også kan spores, hvis det ønskes.

Routere

Som tidligere nævnt er routeren den computer, der videresender pakker på internet. Alle data, der sendes via internet, passerer på vejen fra afsender- til modtager-system et antal routere og et antal transmissionsforbindelser, som kan være af forskellig art (lokalnet eller telelinjer med videre) og drives af forskellige organisationer.

De eksisterende programmer til dedikerede routere indeholder ikke faciliteter til aflytning af dataindholdet i pakker. Nogle modeller er konstrueret således, at der føres en meget kortlivet statistik over, hvilke par (afsender og modtager) af IP-adresser der bruger en forbindelse, men oplysningerne kan ikke aflæses. Desuden er lager-kapaciteten (det vil sige RAM) på maskinen meget begrænset, og der er ingen disk til opsamling. Dataindholdet af alle videresendte pakker bliver lagret kortvarigt i routerens RAM, indtil det bliver overskrevet af andre pakker eller oplysninger.

For at ændre en routers funktionalitet vil det kræve, at man har eller opnår adgang til routerens privilegerede kommandoer. En router indeholder ikke programmer af generel art og kan normalt ikke udføre programmer, der er beregnet til at udnytte fejl i styresystemer.

3 ER MAN SIKRET PRIVATLIV PÅ INTERNET?

3.1 Det grundlæggende problem

Umiddelbart kan det synes selvmodsigende at tale om privatliv på et verdensomspændende kommunikationsnet, hvis store styrke netop er, at det nedbryder alle kendte grænser og giver let adgang til mere information end noget andet hidtil kendt medium. Men ligesom vi normalt forventer, at de telefonsamtaler, vi fører over afstande, ikke er tilgængelige for tredjeparter, har vi alle behov for - og måske også krav på - at kunne fastholde en privatsfære, når vi færdes på nettet.

At der er en sådan forventning, understøttes af lovgivningen. Dansk lovgivning beskytter på forskellige måder den interesse, det enkelte menneske kan have i ikke at få sine data behandlet, herunder ved registrering af personoplysninger. Nogle af disse regler har generel karakter, medens andre alene gælder for bestemte typer af personregistrering, eller inden for bestemte sektorer:

3.2 Straffeloven

I straffelovens kapitel 27 om „Freds- og ærekrænkelser" findes flere regler, der hver på deres måde beskytter privatlivets fred.

Ifølge straffelovens § 263 straffes således den, der bryder eller unddrager nogen et brev, telegram eller anden lukket meddelelse eller optegnelse eller gør sig bekendt med indholdet. Denne bestemmelse kan for eksempel bringes til anvendelse, hvis gerningsmanden retsstridigt gør sig bekendt med indholdet af en elektronisk postmeddelelse. Særlige grænsetilfælde opstår her i forbindelse med den tilegnelse af elektronisk post, der kan finde sted i ansættelsesforhold. Se hertil IT-Sikkerhedsrådets vejledning „Brug af e-post og internet på arbejdspladsen" (januar 2002).

Herudover giver straffelovens § 263, stk. 2, hjemmel til at straffe den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et anlæg til elektronisk databehandling. Denne bestemmelse, der ofte omtales som „hacker-paragraffen", kan anvendes såvel ved målrettet indtrængen i IT-systemer, som ved ulovlig aflytning (snifning med videre) af den kommunikation, der sker via hjemmesider.

I begge tilfælde er strafferammen bøde eller fængsel indtil 6 måneder. Begås de nævnte forhold med fortsæt til at skaffe sig eller gøre sig bekendt med oplysninger om en virksomheds erhvervshemmeligheder eller under andre særlige skærpende omstændigheder, kan straffen stige til fængsel i indtil 4 år.

Straffeloven indeholder ligeledes en „hæleri-paragraf", hvorefter tilsvarende straf som den nævnte kan pålægges den, der uden at have medvirket til gerningen skaffer sig eller uberettiget udnytter oplysninger, som er fremgået ved overtrædelsen. Denne regel har sammenhæng med den generelle regel om beskyttelse af privatlivets fred i straffelovens § 264d. Efter denne bestemmelse kan man straffes med bøde eller fængsel i op til 6 måneder, hvis man „uberettiget videregiver meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan unddrages offentligheden".

Foruden straffelovens regler om privatlivets fred kan det være relevant i denne sammenhæng at omtale nogle andre straffebestemmelser, som undertiden vil blive realiseret, når gerningsmanden uberettiget har skaffet sig adgang til et IT-system. Således straffer straffelovens § 279a den, „som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling". Bestemmelsen hører til i straffelovens kapitel om berigelsesforbrydelser. Den forudsætter således, at der sker en uberettiget „formueforskydning".

3.3 Persondataloven

En meget bred beskyttelse af individets privatliv er sikret gennem lov om behandling af personoplysninger (i daglig tale kaldet persondataloven), som er gennemført i dansk ret 1. juli 2000 på grundlag af et EU-direktiv fra 1995.

Loven bygger på et almindeligt princip om, at enhver form for „behandling" af personoplysninger som udgangspunkt skal have hjemmel i loven, jævnfør nærmere dennes § 6. En sådan hjemmel findes for eksempel, når den registrerede har meddelt samtykke til persondatabehandlingen - enten udtrykkeligt eller i kraft af aftale - eller hvis det følger af en særlig retlig forpligtelse eller særlig lovhjemmel, at behandlingen kan finde sted. Endvidere kan behandling finde sted, hvis den er nødvendig for at den dataansvarlige kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse. Når en behandling efter disse regler er tilladt, skal den i øvrigt finde sted efter nogle generelle principper om god databehandlingsskik med videre. Navnlig må behandling ikke gå videre end nødvendigt, og der skal løbende ske ajourføring af oplysninger.

Loven giver desuden den registrerede en række rettigheder blandt andet til at få indsigt i, hvilke oplysninger der behandles om denne. Ligeledes har den registrerede ret til at gøre indsigelse mod en behandling, og herunder også ret til at gøre indsigelse mod en videregivelse af oplysninger.

Datatilsynet, der administrerer loven, har udsendt en række retningslinier og vejledninger, der kan hentes og læses på tilsynets hjemmeside - www.datatilsynet.dk

3.4 Teleområdet

De generelle regler i persondataloven suppleres på teleområdet med de regler om sikring af personoplysninger, der findes i kapitel 5 i bekendtgørelse nr. 1169 af 15. december 2000 om udbud af telenet og teletjenester. Ifølge § 28 heri skal udbydere af offentlige telenet og teletjenester

give kunderne mulighed for at blokere for A-nummer-overførelser, ligesom den kaldte slutbruger gratis skal kunne afvise ankommende opkald, som har blokeret for visningen af A-nummeret. Herudover fastslår bekendtgørelsens § 30, at udbydere af offentlige telenet og teletjenester skal sikre, at trafikdata vedrørende slutbrugere slettes eller anonymiseres efter samtalens afslutning, medmindre der er givet særlig hjemmel for at gøre undtagelse fra denne regel. En sådan undtagelse er for eksempel gjort i relation til behandling og opbevaring af data med henblik på debiteringsformål. Udbydere af offentlige teletjenester er i øvrigt underlagt en forpligtelse til med henblik på sikring af netsikkerheden at træffe passende tekniske og organisationsmæssige foranstaltninger for at beskytte de udbudte tjenester, jævnfør § 31.

3.5 Betalingsmidler

Ifølge § 13 i lov om visse betalingsmidler finder persondataloven anvendelse på sådanne midler med visse modifikationer. Udstederen skal for det første sikre, at brugerens CPR-nummer ikke kan aflæses fysisk eller elektronisk af andre end udstederen. Dernæst må oplysninger om, hvor brugeren har anvendt betalingsmidlet - og hvad han har købt - i mangel af særlig hjemmel kun behandles til visse driftsmæssige formål eller i retshåndhævelsesøjemed. Dog har udstederen også mulighed for at behandle oplysninger om, hvor brugeren har anvendt betalingsmidlet, i rådgivningsøjemed og med sigte på systemtilpasninger.

Betalingsmiddelloven hed tidligere lov om betalingskort. Det nye navn er blandt andet valgt for at præcisere, at loven også gælder for betalingsmidler, der ikke har fysisk karakter, for eksempel fordi de iværksættes ved brug af en kode.

Loven indeholder særlige regler om retsforholdet i tilfælde, hvor et betalingsmiddel - eller den hertil hørende kode - er anvendt uberettiget af en tredjepart. Lovens princip er her, at udstederen af et betalingsmiddel hæfter for et sådant misbrug, medmindre brugeren har handlet uforsvarligt. Brugeren hæfter dog med et beløb på indtil kroner 1.200,

hvis betalingsmidlet uberettiget har været anvendt med korrekt kode. Yderligere hæftelse kan opstå, såfremt den personlige kode uberettiget har været anvendt, hvis brugeren har undladt at underrette udsteder om, at koden er kommet andre til kendskab eller har oplyst den hemmelige kode til den, der efterfølgende uberettiget udnytter den. Som bruger er det derfor vigtigt at holde koden hemmelig og personlig og at give besked straks efter, at der måtte være opstået mistanke om uberettiget anvendelse.

Yderligere oplysninger om sikkerhed ved brug af elektronisk betalingsmidler kan findes på hjemmesiden www.forbrugersikkerhed.dk

3.6 Praktiske perspektiver

De citerede regler viser, at man som udgangspunkt har ret til at kommunikere uden at uvedkommende kan læse med. På internettet medfører dette først og fremmest, at brugere bør have adgang til at kunne sende e-post med sikkerhed for, at der ikke uberettiget bliver læst over skulderen. Dette udgangspunkt kan efter omstændighederne modificeres, hvis kommunikationen sker via en arbejdsplads. Problemstillingerne er nærmere behandlet i IT-Sikkerhedsrådets vejledning „Brug af e-post og internet på arbejdspladsen“ (januar 2002).

Dernæst har man - i et vist omfang - ret til at færdes anonymt på internet. Det bør som udgangspunkt være muligt for brugeren at „surfe“ mellem web-sider, uden at enkelte web-tjenesteudbydere eller andre aktører kan samle oplysninger om denne færden. Eksempelvis bør kommercielle virksomheder ikke have mulighed for at samle oplysninger om enkeltindividers personlige præferencer med henblik på at benytte oplysningerne i markedsføringsøjemed, medmindre den pågældende har givet samtykke hertil.

Retten til at færdes anonymt må generelt opvejes mod ønsket om i et retssamfund at have rimelige muligheder for at efterforske kriminalitet uden at vi af den grund ender i det totale registrerings- og overvågningssamfund.

3.7 Offentlige databaser

Den enkelte kan ikke modsætte sig, at oplysninger om ham eller hende er tilgængelige på nettet, selv om man ikke selv har givet samtykke til, at oplysningerne optræder. En lang række oplysninger, der tidligere kun var tilgængelige ved direkte henvendelse til en offentlig myndighed eller institution er nu tilgængelige på internettet i overensstemmelse med ønsket om at skabe større åbenhed i forvaltningen.

Denne åbenhed gælder selvsagt kun information, der ikke allerede i lovens forstand er karakteriseret som personlig eller personfølsom. Flere myndigheder giver dog også adgang for privatpersoners til egne personlige oplysninger, hvor den mest kendte formentlig er Told•Skat. Adgang til sådanne oplysninger sker typisk via et personligt kodeord og/eller ved anvendelse af certifikater.

Udbuddet af frit tilgængelig information fra myndigheder med videre bliver større og har i enkelte tilfælde givet anledning til overvejelser om den øgede offentlighed har været i alles interesse. Blandt disse eksempler kan nævnes vurderingsfortegnelsen over ejendomme i hovedparten af de danske kommuner, hvor overvejelserne har gået på rimeligheden i, at alle fik let adgang til indsigt i den del af privatøkonomien, der vedrører ens bolig.

Som eksempler på sådanne offentlige personrelaterede informationsdatabaser på internettet kan nævnes følgende:

– Oplysningen: www.dehvidesider.dk
  Telefonoplysningen fra en række af de største teleselskaber. Søg på telefonnummer, navn eller vejnavne. Her findes også oplysninger om virksomheder (De Gule Sider), fax- og mobilnumre. Disse giver desuden mulighed for masseopslag, det vil sige for eksempel søgninger på alle personer på en vej, alle ved navn Jens Hansen og så videre.

– E-postkataloger: www.epost.dk
  Her findes en liste over mere end 1 million e-postadresser i Danmark. Listen over e-postadresser er dog langtfra komplet. Der findes et lignende e-postkatalog på; joes.jubii.dk

– Vurderingsfortegnelsen: vurdering.netborger.dk
  Vurderingsfortegnelsen indeholder oplysninger om ejendoms-vurderinger i Danmark, hvor der kan søges på adresser.

– NetTidende: www.nettidende.dk
  NetTidende er udviklet af Statens Information og indeholder meddelelser som har retsvirkninger for borgere, virksomheder og myndigheder. Offentlige meddelelser i Statstidende, Tingbladet og udbudsavisen er samlet her, og giver blandt andet mulighed for at søge efter pantebreve i fast ejendom, både og biler. (via Tingbladet). Oplysninger om blandt andet gældssaneringer, tvangsauktioner og konkursboer findes via Statstidende.

– Geodata: www.geobroadcast.dk
  På siden kan man blandt andet via digitale kort, se den gennemsnitlige husstandsindkomst på en vej i Danmark, og en oversigt over affaldsdepoter. Oplysningerne stammer fra Danmarks Statistik.

– Kommunedata: www.netborger.dk
  Her findes oplysninger om danske kommuners økonomi, beskatning, serviceniveau, arbejdsløshed med videre.

Åbne postlister:
Flere amter, kommuner og ministerier har indført åbne postlister, der er tilgængelige på internet. På denne måde kan enhver se hvilken post den pågældende myndighed modtager i form af registrering af afsender og en overskrift.

4 HVAD KAN DU SELV GØRE?

Du kan finde en mængde gode råd og henvisninger i IT-Sikkerhedsrådets vejledning „Sikkerhed ved e-post og internet - hacking og virus“, som er tilgængelig på IT-Sikkerhedsrådets hjemmeside www.it-sikkerhedsraadet.dk

4.1 Kryptering

At kryptere information vil sige at forvanske informationen styret af en nøgle, så ingen andre end de, der har en korrekt nøgle, kan læse informationen. Hvis uvedkommende får adgang til dokumenter og filer på en maskine, vil krypteringen hindre, at de kan læses.

E-post kan også krypteres og medvirke til at sikre, at kun rette modtager kan afkode meddelelsen.

Fælles for al anvendelse af kryptering er, at det ofte er beskyttelsen af hemmelige nøgler og kodeord, der er afgørende for totalsikkerheden i krypteringen.

4.2 Kodeord

Beskyttelse mod uvedkommendes adgang til personlige oplysninger sker ofte under anvendelse af kodeord (eller password). Kodeord bør være personlige og ikke deles med andre. Et kodeord bør være svært nok til at ingen andre kan gætte det, men nemt nok til at du kan huske det.

Følgende regler bør overholdes, hvor man selv kan vælge kodeord:

– Kodeordet må ikke skrives ned.
– Kodeord må ikke udleveres til andre.

– Kodeord bør bestå af en blanding af tal, bogstaver og specialtegn.
– Kodeord bør være på mindst 6 tegn.

Alt efter hvor vigtig kodeordet er, bør det skiftes mindst hver 3-9 måned.

IT-Sikkerhedsrådet har i publikationen „Adgangskontrol til en hjemmeside" behandlet spørgsmålet om kodeord nærmere. Her kan der findes gode råd om valg af kodeord og alternative beskyttelsesmekanismer. Publikationen kan læses og hentes på IT-Sikkerhedsrådets hjemmeside; www.it-sikkerhedsraadet.dk

4.3 Beskyt hjemme-pc'en

I lighed med virksomheders IT-systemer er privates hjemme-pc'er i stigende grad blevet mål for hacker- og virus-angreb. Får uvedkommende adgang til hjemme-pc er der særlig risiko for at private dokumenter og informationer (for eksempel kodeord) kommer andre til kendskab. Derfor bør hjemme-pc'en beskyttes mod sådanne angreb, for eksempel under anvendelse af antivirus-programmer, ved opdatering af programmer og ved at benytte den sikkerhed, der er indbygget i browsere og e-postprogrammer.

Uvedkommendes adgang til hjemme-pc'en lettes, jo oftere den er koblet på internettet. Brugere med hurtige internet-forbindelser, ADSL eller kabelmodem bør være særligt opmærksomme, idet de oftere er koblet på internettet i længere tid ad gangen, hvorved pc'en bliver mere synlig på internettet. Enkelte teleselskaber tildeler hjemme-pc'er en fast IP-adresse på internettet, hvorved adgangen yderligere lettes.

De enkelte led i beskyttelse af den private hjemme-pc er nærmere beskrevet i IT-Sikkerhedsrådets publikation „Sikkerhed ved e-post og internet", der kan læses og hentes på IT-Sikkerhedsrådets hjemmeside; www.it-sikkerhedsraadet.dk

5. BØR MAN AFGIVE PERSONLIGE OPLYSNINGER?

Generelt bør man være forsigtig med at afgive personlige oplysninger på web-steder. Personlige oplysninger, så som navn, adresse, e-postadresse, telefonnumre og kreditkortnumre, afkræves ofte i forbindelse med udbudte varer eller tjenester på web-steder.

5.1 Modtagerens identitet

Er det nødvendigt at afgive personlige oplysninger via en hjemmeside bør man først og fremmest sikre sig, at modtageren er den rette. Det er desværre ofte vanskeligt for den almindelige bruger at afgøre, hvem der er modtager af eventuelle indtastede oplysninger. Ofte er web-sider delt i forskellige områder, der stammer fra mere end et firma. For eksempel er mange internet-reklamer i form af bannere leveret direkte til hjemmesiden via tredjeparter.

For dels at imødekomme dette behov, dels for at sikre transporten af data over internettet mod aflytning er der i alle nyere browsere indbygget en sikkerhedsfunktion. Når denne er aktiveret vil der i bunden af browser-vinduet typisk være placeret en lille hængelås, som vist i eksemplet her fra Microsofts Internet Explorer.

Er hængelåsen låst, som i eksemplet, er siden krypteret under transport. Andre browsere bruger ikoner, hvor hængelåsen er åben hvis siden ikke var krypteret under transport.

Klikker man på låsen kan man se hvilken organisation eller virksomhed serveren er registreret til og på den måde afgøre modtagers identitet.

5.2 Hvilke oplysninger skal man være forsigtige med

Ønsker man at gøre brug af tjenester på internettet kan det være nødvendigt at afgive personlige oplysninger, som et led i levering af tjenesten eller varen. Det være sig navn og adresse i forbindelse med forsendelser, (kredit-)kortnumre ved handel, epostadresser og i visse tilfælde cpr-numre.

Er det nødvendigt at indtaste personlige oplysninger bør man være opmærksom på kun at afgive de oplysninger, der er nødvendige for effektueringen af den vare eller tjenesteydelse, der ønskes. Der kan være behov for afgivelse af navn og adresse, men ikke nødvendigvis e-postadressen.

Kun i særlige tilfælde, for eksempel i forbindelse med kontakt til offentlige myndigheder, pengeinstitut med videre, kan der være behov for at afgive cpr-nummer.

Anvendelse af e-post er en let og billig måde for virksomheder til at udsende informationer om produkter, varer, nyheder med videre. Ved uforsigtighed kan man derfor let blive mål for en stor mængde e-post fra virksomheder og organisationer, og man bør derfor nøje overveje, hvorvidt det er nødvendigt at oplyse sin e-postadresse.

5.3 Kan man være sikker på, at oplysninger behandles korrekt hos modtager?

Inden de personlige oplysninger indtastes på web-stedet bør man se efter om virksomheden/organisationen har offentliggjort en politik om behandling af personlige oplysninger.

Det kan være vanskeligt for udenforstående at overbevise sig om, at virksomheden bag et web-sted behandler oplysningerne korrekt og ikke udleverer disse til tredjemand. Er man i tvivl kan man søge støtte i en række mærkater, der udstedes af organisationer og virksomheder. Findes disse ikke eller er man kommet i tvivl bør man overveje alternative web-steder.

I Danmark findes en række segl og mærkater, der ses på web-steder. Vi skal her kort referere nogle udvalgte segl.

E-mærket er et dansk mærke, der er udviklet af en række store danske organisationer, herunder Dansk Industri, Dansk Handel og Service og Forbrugerrådet. Mærket er rettet mod web-steder med e-handel, og opnås ved at søge E-handelsfonden. Ved ansøgning skal virksomheden oplyse om en række forhold, der skal opfylde E-handelsfondens kriterier. De dækker blandt andet fortrydelsesret, reklamation og fortrolighedspolitik.
Se mere på: www.e-handelsfonden.dk

Verisign Secure Site, er et certifikat, der alene bekræfter identiteten af den virksomhed, der står bag web-stedet. Certifikatet giver ingen vished for web-stedets behandling af de oplysninger, der indsamles.

Adskillige andre firmaer udbyder lignende certifikater. I Danmark blandt andet TDC TeleDanmark, KommuneData og EuroTrust.
Se mere på: www.verisign.com

TRUSTe, EU Safe Harbor, er en europæisk version af et amerikansk segl, der kan udstedes på baggrund af en ansøgning, hvor virksomheden bag web-stedet skal erklære, at den lever op til TRUSTe's kriterier om beskyttelse og behandling af personlige oplysninger. TRUSTe forbeholder sig ret til at underlægge virksomheden ekstern kontrol. Tilsvarende findes et amerikansk TRUSTe segl. Se mere på: www.truste.org

WebTrust, er et amerikansk udviklet segl, der udstedes af særligt uddannede revisorer, efter et sæt internationale kriterier. Virksomheder der har et sådant segl er underlagt en halvårlig kontrol for eksempel vedrørende behandling af personoplysninger (consumer protection). Se mere på: www.webtrust.org

Virksomheder, organisationer og offentlige myndigheder, der opbevarer og behandler personlige oplysninger, skal desuden overholde persondataloven, der sætter de juridiske rammer for behandling af personoplysninger.

6 NYTTIGE SIDER PÅ INTERNETTET

IT-Sikkerhedsrådet:	www.it-sikkerhedsraadet.dk	IT-Sikkerhedsrådets hjemmeside under Ministeriet for Videnskab, Teknologi og Udvikling.
Forbrugerrådet:	www.forbrugerraadet.dk	Forbrugerrådets hjemmeside
Forbrugersikkerhed:	www.forbrugersikkerhed.dk	Forbrugerrådet og FDIH's hjemmeside til internetforbrugeren. Gode råd om sikkerhed i forbindelse med e-handel og færden på internettet generelt
Retsinformation:	www.retsinfo.dk	Database over danske love, nuværende som gældende
Datatilsynet:	www.datatilsynet.dk	Datatilsynets hjemmeside. Datatilsynet fører tilsyn med enhver behandling, der er omfattet af lov om behandling af personoplysninger,
Netfornuft:	www.netfornuft.dk	Gode råd om færden på internettet. Oprettet og vedligeholdt af Forbrugerinformation (www.fi.dk)

6.1 Bilag 1: Sikkerhedsstandarder på internet

Traditionelt opdeles en beskrivelse af sikkerheden i fire temaer. For det første tales om sikkerheden for fortrolighed - det vil sige at data ikke kan læses af uvedkommende. Umiddelbart sendes meddelelser afsted som åbne postkort, og fortrolighed ved kommunikation over internettet opnås alene ved anvendelsen af krypteringsteknikker til at kode meddelelsen, således at den er uforståelig for alle andre end den ønskede modtager-(gruppe).

For det andet taler man om sikkerheden for, at data ikke ændres undervejs af uvedkommende i et forsøg på bedrageri, hærværk eller måske chikane. Sikkerheden for integriteten af en meddelelse kan derfor også have betydning for sikring af privatlivets fred. Integriteten kan blandt andet sikres ved kryptering samt ved anvendelse af matematiske teknikker, der uddrager og sammenligner „fingeraftryk" af meddelelser.

Det tredje tema er sikkerheden for, at den, der står som afsender på meddelelsen, er rette vedkommende. Sikkerheden for ægtheden kan blandt andet opnås ved hjælp af brug af krypteringsteknikker, herunder ved anvendelse af troværdige tredjeparter.

I nær tilknytning til spørgsmålet om ægthed er problemet om uafviselighed. Uafviselighed er todelt. Den første del betyder populært sagt, at modtageren af en meddelelse kan være sikker på, at afsenderen ikke senere nægter at have sendt et bestemt dokument (en analogi til et underskrevet dokument). Den anden del betyder derimod, at afsender kan være sikker på, at modtager ikke senere nægter at have modtaget dokumentet (en analogi til en papirkvittering).

I det følgende beskrives en række standarder på internet, og der gives en opregning af, hvilke af de beskrevne sikkerhedstemaer der tilgodeses med de forskellige standarder.

SSL - Secure Sockets Layer

SSL er en protokol, som oprindeligt blev udviklet af Netscape, men som nu understøttes af hovedparten af de kommercielle browsere.

SSL tilbyder pålidelig kommunikation mellem en „server“ og en „klient“ (eksempelvis brugerens browser).

SSL baseres på, at serveren har et certifikat, som dels udnyttes til at udveksle symmetriske krypteringsnøgler mellem serveren og klienten, således at der kan skabes fortrolighed og integritet i kommunikationen, dels giver sikkerhed for serverens ægthed. Udstyres browseren med brugerens certifikat, gives også sikkerhed for brugerens ægthed (identitet), når denne kobler sig op til browseren.

Der er ikke i SSL direkte mulighed for at knytte en digital signatur til kommunikationen. Uafviselighed er dermed ikke sikret.

PGP – Pretty Good Privacy

„Pretty Good Privacy“ eller PGP er ikke blot en protokol, men også en softwareimplementering af protokollen, der er gratis tilgængelig til privat anvendelse. PGP er skabt til sikker e-post, men kan også bruges til kryptering af andre filtyper, og programmet tilbyder alle de ovenfor nævnte aspekter af sikkerhed.

PGP baserer sig på anvendelsen af asymmetriske nøgler eller public key-kryptering. Det har hidtil ikke i tilknytning til PGP været muligt at benytte certifikater til certificering af ejerens identitet. Dette er imidlertid nu understøttet således, at produktet integrerer direkte med diverse nøglecentre. Historisk har PGP ellers været baseret på, at brugerne gensidigt certificerer hinandens identitet og troværdighed.

PGP-programmet, der findes i en gratis version og en kommerciel version, kan blandt andet hentes fra http://www.pgp.dk, hvor der også er opbygget en database over offentlige nøgler.

Standarden for udveksling af e-post via PGP hedder PGP/MIME.

S/MIME

„Secure MIME“ er en internet-standard for sikkerhed i elektronisk post, der benytter sig af e-post standarden MIME (Multi-purpose Internet Mail Extensions), der anvendes til hovedparten af al elektronisk post, der sendes via internet.

S/MIME baseres på public key kryptering og sikrer alle de ovenfor nævnte aspekter af sikkerhed. S/MIME er designet til at anvende certifikater udstedt af troværdige tredjeparter.

S/MIME er godkendt som en internet-standard og er implementeret i diverse e-post klienter fra blandt andet Microsoft og IBM (Lotus Notes).

IP-sec

IP-sec er en standard for sikring af internettet trafik, som tilbyder sikring af fortrolighed og integritet. IP-sec kan implementeres i den nuværende IP-protokol version 4 og vil indgå som standard i den nye version 6.

IP-sec fungerer på netværksniveau og kan dermed på een gang skabe sikkerhed for flere internet-anvendelser - e-post, www-trafik med videre.

IP-sec vil typisk blive implementeret i netværksudstyr (routere) og anvendt til at skabe virtuelle private netværk (VPN) over internet, for eksempel mellem en fjernarbejdsplads og en virksomheds netværk eller mellem to lokalnetværk på forskellige fysiske lokationer.

IP-sec baseres til dels på asymmetrisk kryptering.

Privatliv på internet

Redegørelse med praktiske råd for den private internet-bruger

Internettet har opnået en sådan udbredelse, at mange private brugere i dag er vænnet til at bruge nettet til indkøb, bankforretninger, indberetning til det offentlige og så videre. Denne udvikling er sket til trods for, at vi i medierne ofte må læse og høre mange skræk-historier om aflytning, brug af personlige oplysninger og svindel med kreditkort.

Med denne redegørelse giver IT-Sikkerhedsrådet en beskrivelse af de tekniske og juridiske svar, der findes på spørgsmål om beskyttelsen af forbrugerens privatliv på internettet.

Umiddelbart kan det synes selvmodsigende at tale om privatliv på et verdensomspændende kommunikationsnet, hvis store styrke netop er, at det nedbryder alle kendte grænser og giver let adgang til mere information end noget andet hidtil kendt medium. Men ligesom vi normalt forventer, at de telefonsamtaler, vi fører over afstande, ikke er tilgængelige for tredjeparter, har vi alle behov for - og måske også krav på - at kunne fastholde en privatsfære, når vi færdes på nettet.

Ministeriet for Videnskab, Teknologi og Udvikling