

# **Privacy fremmende teknologier**

**- en introduktion til at beskytte privatlivets fred på din computer**

## Indholdsfortegnelse

Baggrund

Trusselsbilledet

Tillid

Scenarier for beskyttelse

Beskyttelse af lagret information og funktionalitet

Beskyttelse af transmission

Beskyttelse af trafikinformationen

Beskyttelse af databaser

Opsummering

## Baggrund

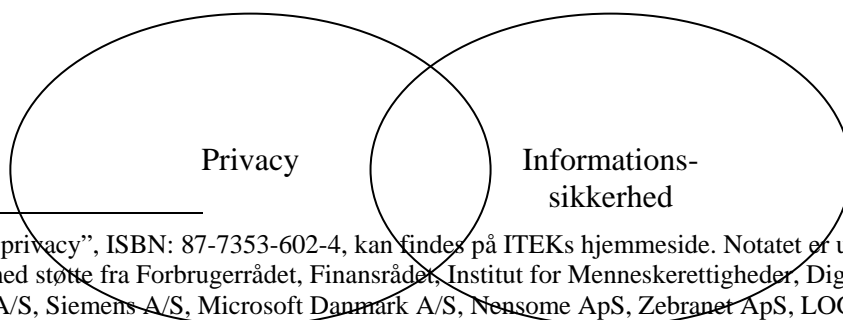
Beskyttelse af elektronisk lagrede informationer hos borgere og i mindre virksomheder har gennem de senere år haft stor fokus i ITEK og Dansk Industris arbejde med informationssikkerhed. Arbejdet har været fokuseret på at beskytte computeren mod fejl, medarbejdernes handlinger og angreb fra personer med ondsindede hensigter eller programmer med skadelig virkning. De mindre virksomheders computernetværk eller enkelte computere kan i mange sammenhænge sidestilles med private brugeres situation og en del af arbejdet har derfor også kunnet bruges af private.

Et element indenfor emnet informationssikkerhed handler om beskyttelse af privatlivets fred - også kaldet privacy. Den nærmere afgrænsning af dette emne er gennemgået i notatet ”Principper for privacy”<sup>1</sup>. Privacy er et bredt begreb, der kan handle om så forskellige ting som behandling af personlig information, beskyttelse af sin fysiske krop, retten til at kommunikere privat og grænsedragningen mellem det private miljø og andre miljøer.

I denne vejledning vil vi udelukkende beskæftige os med den delmængde af privacy, der vedrører beskyttelsen af personhenførbare informationer og retten til at kommunikere privat ved anvendelsen af computere. Der er altså kun tale om beskyttelse af private personreleterede oplysninger og ikke f.eks. firmaoplysninger, ejendomsoplysninger eller andre fortrolige oplysninger, som det normalt er en god ide at beskytte.

Privat kommunikation skal forstås som dels den kommunikation man foretager sig som privat person og dels den kommunikation man foretager sig som virksomhed. Computere skal forstås meget bredt. Der er computere i mange ting men de fleste af de gode råd, der gennemgås i denne vejledning, er tænkt i forhold til personlige computere (PC’er) koblet på internettet. En del af rådene kan dog også overføres til andre computere.

Vi kan præcisere det område vejledningen beskæftiger sig med ved det område, hvor de to cirkler overlapper, i nedenstående figur:



<sup>1</sup> ”Principper for privacy”, ISBN: 87-7353-602-4, kan findes på ITEKs hjemmeside. Notatet er udarbejdet af ITEK og Dansk Industri med støtte fra Forbrugerrådet, Finansrådet, Institut for Menneskerettigheder, Digital Rights, AIM Danmark, TDC A/S, Siemens A/S, Microsoft Danmark A/S, Newsome ApS, Zebranet ApS, LOGISYS A/S, Parkegaard og Kristensen Sikkerhed ApS, RFIDsec ApS og CSIS ApS.

Forskellen mellem de to cirkler kan illustreres ved et par eksempler.

1. Når man taler om informationssikkerhed handler det om at beskytte informationer uanset om disse er private eller ej. En virksomhed vil f.eks. beskytte regnskabsdata og holde dem private. Vi er dermed i det overlappende felt i figuren.
2. Visse informationer ønsker man imidlertid at beskytte uden at de skal holdes private. Det kan f.eks. være informationer som man gerne vil beskytte mod ændring, men som man gerne vil stille til offentlighedens rådighed. Hermed er vi til højre i figuren.
3. Endelig er der måske informationer man ikke ønsker andre skal kende til - ikke fordi man frygter for sin sikkerhed eller for et misbrug af informationen, men ganske enkelt fordi man føler at det er noget man kun ønsker at dele med bestemte mennesker. Vilårlig aflytning af telefoni kan f.eks. betyde at nogle man kender kommer til at høre noget, man egentlig helst bare ville holde mellem sig selv og en anden bestemt part. Vi er dermed til venstre i figuren.

I det overlappende felt tager man ansvar for balancerne, dvs. man sikrer hensynet til alle involverede ved at designe med forebyggelse og bæredygtighed selv når det går galt.

Vejledningen har til formål at skitsere, hvordan man ved hjælp af forskellige teknologier og den rette adfærd kan sikre, at oplysninger, som er personhenførbare, og som man gerne vil bevare fortroligt, ikke opsnappes af uvedkommende, når de lagres, behandles og kommunikerer elektronisk.

Denne vejledning er udarbejdet af ITEK og Dansk Industri i samarbejde med IT-sikkerhedspanelet under ministeriet for Videnskab, Teknologi og Udvikling, Finansrådet, Institut for Menneskerettigheder, Digital Rights, Forsvarets Forskningstjeneste, AIM Danmark, TDC A/S, Siemens A/S, Microsoft Danmark A/S, Nensome ApS, Zebranet ApS, IBM Danmark A/S, LOGISYS A/S, Parkegaard og Kristensen Sikkerhed ApS, RFIDsec ApS, Unispeed A/S og CSIS A/S og med tilslutning fra Forbrugerrådet.

### **Trusselsbilledet**

En række interessenter kan med de rette værktøjer tiltvinge sig adgang til en computer og/eller den kommunikation, der flyder fra denne, hvis computeren og dens kommunikation ikke er tilstrækkeligt sikret eller hvis computeren betjenes uhensigtsmæssigt af brugeren.

Eksempler på hvad der sker af kommunikation og overvågning, som kunne true brugerens privacy omfatter bl.a.:

- **Personer med ondsindede formål.** Eksempler omfatter personer som forsøger at snige programmer ind på computeren med det formål at bruge computeren til at sende spam eller bruge den til at angribe andre. Personer der via phishing forsøger at stjæle brugerens elektroniske identitet og således at give sig ud for ham i forhold til f.eks. netbank. Personer som forsøger at få adgang til og opsnappe fortrolige informationer om f.eks. forretningshemmeligheder eller personhenførbare oplysninger.
- **Skadelige programmer.** Der flourer på internettet en del programmer, som hele tiden forsøger at finde computere med sårbarheder på. Disse computere kan angribes af de skadelige programmer og sikre at en person et sted i verden får kontrol over computeren.

- **Almindeligt anvendte programmer.** En række af de programmer man bruger til daglig opdateres løbende for at skabe ny funktionalitet eller for at udbedre dårlig programmering, der kunne føre til sårbarheder på computeren. Disse programmer kontakter typisk producenten af sig selv eller fordi brugeren har bedt dem om at gøre det for at blive opdateret. Visse programmer kontakter også producenten med andre formål for øje. Og det kan være hensigtsmæssigt at sætte sig ind i hvilken kommunikation, der foregår mellem det lokalt installerede program og producenten.
- **Internetudbydere.** Internetudbydere skal kunne udskrive regninger for det forbrug, som kunden har. Det er derfor nødvendigt at internetudbydere gemmer visse oplysninger om brugernes færden på nettet til regningsformål.
- **Interaktive services.** En række services via nettet vil ved brug kræve at brugere afgiver en række informationer om sig selv. Der ligger ikke altid fra udbyderen af servicen en kritisk vurdering bag hvilke information, der reelt er behov for yde den pågældende service. Desuden findes der også falske serviceudbydere, som ikke reelt udbyder en service, men som blot har lavet sin hjemmeside for at lokke informationer fra brugerne – f.eks. kreditkortnummer.
- **Myndighederne.** I Danmark kræver myndighederne at internetudbydere og visse serviceudbydere gemmer en masse oplysninger om brugernes adfærd på nettet. Oplysningerne skal stilles til rådighed for myndighederne hvis de kan sandsynliggøre behovet for det gennem en dommerkendelse. Formålet er at kunne analysere disse data med henblik på at dæmme op for mulighederne for terrorangreb og andre forhold, der kan skade det danske samfund. Tilsvarende gemmer myndighederne i andre lande oplysninger om den trafik, der går gennem landet. Reglerne for anvendelse af sådanne data varierer fra land til land og man kan derfor som bruger ikke gennemskue hvilke oplysninger der gemmes om ens adfærd rundt omkring og hvad disse oplysninger bruges til.
- **Virksomheder,** som bevidst eller uforvarende opbevarer, behandler og udveksler private oplysninger om deres kunder, medarbejdere og andre personer, som de har kontakt med, uden at iagttage de lovmæssige og etiske krav til informationsbehandlingen.

Ovenstående er ikke en fuldstændig liste over de interessenter som truer borgernes privacy. Men gennem disse eksempler kan vi få et billede af, hvem der er der har interesse i at krænke privacy og dermed få et billede af, hvem det er nødvendigt at sætte ind overfor.

## Tillid

I nær tilknytning til disse interessenter er det vigtigt at vælge en strategi for, hvordan man vil beskytte sig. Beskyttelsen bør afhænge af, hvem man i en given situation mener, man kan have tillid til. Det bør være op til den enkelte person at vurdere dette og selv kunne styre, hvem man skal have tillid til og eventuelt over tid revidere sit syn på, hvem der har fortjent ens tillid.

Man kan selvfølgelig vælge de to ekstremer: enten altid at beskytte sig mod alt<sup>2</sup> eller aldrig at beskytte sig. Men det kan også være relevant at vurdere fra gang til gang om hvem man i denne situation vil beskytte sig imod.

I mange sammenhænge kan man fx vælge at have tillid til sin internetudbyder, bank og myndighederne, men ikke er sikker på om man kan have tillid til en konkret tjenesteudbyder på

---

<sup>2</sup> Det skal bemærkes at der teoretisk findes systemer, som giver brugeren kontrol over hvordan han i enhver situation og til enhver tid gennem pseudonymer kan vælge at styre den kontakt han har med sine omgivelser baseret på hans vurdering af hvilke tillid han kan have til dem. Disse systemer er imidlertid desværre endnu en teoretisk mulighed og vil derfor ikke være genstand for yderligere gennemgang i denne vejledning.

nettet. I andre sammenhænge kan man måske vælge at have tillid til tjenesteudbydere alene, men samtidig ønske at de øvrige parter er uvidende om transaktionen. Og siden der ikke i praksis findes én let måde til at styre dette kompleks af hvem man har tillid til kan det at praktiske årsager være relevant at prioritere sine indsatsområder.

Endelig kan selve den beskyttelse man vælger måske give anledning til ekstra opmærksomhed hos dem, som man egentlig ville beskytte sig imod. Man bør derfor som led i sin strategi overveje tre forhold:

1. Hvilken risiko vil jeg beskytte mig imod?
2. Hvilken tillid har jeg til de produkter/services jeg benytter?
3. Hvilken mistæneliggørelse risikerer jeg ved at benytte beskyttelsen?

### **Scenarier for beskyttelse**

På baggrund af de muligheder de forskellige interessenter har for at få adgang til informationer på en PC eller kommunikation via nettet kan vi beskrive forskellige scenarier hvor beskyttelse er nødvendigt.

#### *Beskyttelse af lagret information og funktionalitet*

For det første er det vigtigt at beskytte de informationer der ligger lagret på computeren og desuden beskytte den funktionalitet computeren i sig selv har således at den ikke anvendes til ondsindede formål. Dette gøres ved at forhindre adgang til computeren for uvedkommende, og at slette informationerne effektivt, hvis computeren overlades til andre, fx ved reparation eller kassation.

#### *Beskyttelse af transmission*

For det andet er det vigtigt at beskytte den information som transmitteres fra computeren til en modtager ude i verden mod at blive opsnappet. Det kunne f.eks. være en mail som afsendes eller en fil som uploades. Her tænker vi alene på indholdet af informationen og den vigtigste metode hertil er kryptering.

#### *Beskyttelse af trafikinformation*

For det tredje er det i nogen sammenhænge vigtigt at undgå, at nogen kan se, hvem man er, og hvem man kommunikerer med (trafikinformation). Den grundlæggende ide er her, at man kan ønske at købe en tjenester, hvor man gerne vil være anonym overfor den man køber tjenesten af, at banken ikke kan se, hvad det er for en tjeneste, man køber, samt at internetudbyderen og myndighederne ikke kan se, hvem man køber tjenester af. Dette kan opnås ved at opnå en vis kontrol med den vej, som brugerens kommunikation rejser gennem nettet.

### **Beskyttelse af lagret information og funktionalitet**

Lagret informations og computerens funktionalitet beskyttes bedst ved at forhindre at uvedkommende får adgang til computeren. Dette er et helt centralt element i disciplinen informationssikkerhed og det er absolut lettere sagt end gjort.

- **Firewall.** Det første vigtige element i at beskytte sin computer mod uvedkommende er at installere et program, som kontrollerer og overvåger hvem der kobler sig op til computeren. Et sådant program kaldes en firewall. Firewallen fås enten som et program eller som en boks, som man sætter mellem sin internetudbyder og den computer man vil beskytte. Gennem firewallen kan man beslutte hvilke adgangsveje der skal være åbne ude fra nettet og ind til computeren –

de såkaldte porte. Mange programmer vil gerne kommunikere gennem netop deres egen port og når man installere et program vil programmet derfor bede om at firewallen åbner for denne port. Når brugeren installere programmet vil firewallen derfor typisk spørge brugeren om man ønsker at åbne denne port. Her er det så at brugeren skal vurdere om der skal gives tilladelse til det eller om porten skal lukkes således at programmet ikke kan køre via nettet, men kun lokalt på computeren. Firewallen laver typisk en liste (log) over forsøg på at komme i kontakt med computeren.

*Anbefaling: Der bør installeres en firewall og mængden af programmer, der skal have lov til at gå på nettet bør begrænses mest muligt.*

*Værktøj:*

- **Opdatering.** Det sker ret hyppigt at der opdages måder at bruge et program på, som det ikke var tiltænkt, da programmet blev lavet – altså en slags programmeringsfejl. Der er dels tale om fejl, der påvirker programmets almindelige funktion, dels om fejl, som gør programmet sårbart overfor angreb udefra. Disse programmeringsfejl opdages ofte i tide og producenten laver så en opdatering til programmet, som man kan installere for at gøre fejlen god igen. Hvis programmet har fået lov af firewallen til at gå på nettet, kan de programmer der er installeret på computeren ofte selv spørge udbyderen om der findes opdateringer.

*Anbefaling: Styresystemet, browseren og sikkerhedspakken bør have adgang til at opdatere sig selv via nettet.*

*Værktøj:*

- **Detektion af forsøg på indtrængning.** Der findes programmer, som har lært at genkende de mønstre der optræder på en computer, når der er nogen der forsøger at trænge ind på den. Disse programmer kaldes intrusion detection programmer. Der findes også programmer, der kan stoppe for et sådant forsøg på indtrængning og disse kaldes intrusion prevention programmer.

*Anbefaling: Det bør overvejes at anskaffe sig programmer til intrusion detection og intrusion prevention.*

*Værktøj:*

- **Sikkerhedspakke.** Virus, orme, spam og spyware er programmer eller mails, som kan bruges til at skaffe en uvedkommende person adgang til computeren og dermed krænke privacy. For at beskytte sig mod den slags skadelige programmer bør der altid være installeret en sikkerhedspakke, som fjerner den slags ting fra den kommunikation, der er med computeren enten via nettet eller via lagermedier. Pakken koster typisk penge og man skal anskue denne årlige omkostning på samme måde som serviceeftersynet på sin bil – den kører ikke hvis den ikke løbende holdes ved lige. Tilsvarende fungerer computeren ikke hvis den ikke løbende beskyttes. Pakken kan måske også bruges til kryptering af harddisken for det tilfælde at uheldet alligevel skulle have været ude.

*Anbefaling: Der bør installeres en sikkerhedspakke på computeren. Pakken bør som minimum kunne bekæmpe virus, orme, spyware og spam. Pakken bør desuden indeholde en firewall og kan tillige indeholde en overvågning af om der sker uhensigtsmæssige aktiviteter på computeren.*

*Værktøj:*

- **Handlinger.** At tage sig i agt og tænke sig om er altid den bedste beskyttelse af privacy. Det betyder at man ikke skal installere vilkårlige programmer, når en tilfældig hjemmeside opfordrer til det. Man skal overveje om de sammenhænge, hvor man afgiver personhenførbare oplysninger, er tilstrækkeligt tillidsvækkende. Man bør undlade at navigere rundt på hjemmesider med tvivlsomt indhold. Hvis man bliver bedt om at identificere sig kan man f.eks. bruge "Test" som navn og oprette en ny mailadresse til det konkrete formål. På den måde undgår man at afgive personhenførbare information.

*Anbefaling: Man skal udvise fornuft i sin færden på nettet præcis som man gør det i den virkelige verden.*

*Værktøj:*

- **Sikring af data.** At forebygge mod konsekvenserne af sikkerhedsbrud for eksterne parter risici i egne databaser er både til glæde for de eksterne parter og egen troværdighed og sikkerhed. Det betyder, at man skal tage udgangspunkt i worst case og sikre, at man så vidt muligt designer systemer, som ikke f.eks. indeholder identificerende oplysninger og genbrugelige nøgler, som kan blive tilgængelige for en angriber. Gjort rigtigt kan man forebygge mod hele klasser af sikkerhedsproblemer og gøre sikkerhed til en win-win, hvor selv et alvorligt sikkerhedsbrud blot betyder, at man skal hente en backup og fortsætte uanfægtet, fordi en angriber ikke har lært noget, som kan misbruges overfor eksterne parter.

*Anbefaling: Man skal designe systemer med det udgangspunkt de kan fejle og tage de bedst mulige forbehold herfor.*

*Værktøj: Privatlivsfremmende teknologier, selektiv kryptering, blinded certifikates, mixnets, digital cash, asymmetriske nøgler, kontekst specifikke nøgler etc.*

### **Beskyttelse af transmission**

Når man færdes på nettet bliver det indhold man kommunikerer pakket ned i små pakker, der flyder mellem afsender og modtager. Der vil ved en sådan kommunikation altid være trafik i begge retninger. Undervejs passerer pakkerne mange forskellige interessenter, og alle mellemliggende parter, der ekspederer pakkerne, vil have mulighed for at læse deres indhold. Disse interessenter er typisk ligeglade med hvilket indhold, der er i pakker, der transmitteres. Men i visse tilfælde vil de interessere sig for kommunikationen.

Myndighederne vil måske interessere sig for kommunikationen, hvis man uvidende kommunikerer med en person, der er mistænkt for en alvorlig forbrydelse. Myndighederne har dermed et incitament til at overvåge en given brugers kommunikation for at fastslå, om man er involveret i den mulige forbrydelse. Der kan også sidde personer, der har ondsindede hensigter, som gerne vil opsnappe en given brugers kommunikation for at give sig ud for at være vedkommende og måske få adgang til betalingskortnumre m.v.

Indholdet i en kommunikation kan beskyttes på flere måder:

- **Kryptering.** Kryptering af kommunikation vil typisk være den bedste måde at beskytte sig på. Kryptering foregår ved, at man kører den tekst og de mediefiler man vil kommunikere gennem et krypteringsprogram. Meddelelsen bliver herved ulæselig med mindre man har en given nøgle til at dekryptere den. Har man tillid til en tredjepart kan man overlade dekrypteringsnøglen til denne interessent og give modtageren af meddelelsen adgang til at anvende nøglen. Dette sker i mange sammenhænge f.eks. ved anvendelse af digital signaturs krypteringsfunktion, hvor TDC A/S er den der opbevarer nøglerne. Har man ikke tillid til en tredjepart må man på anden vis kommunikere nøglen til dekryptering til den part, som skal læse den krypterede meddelelse. Ved anvendelse af kryptering er krypteringens styrke afgørende for hvor sikker man kan være på at en krypteret meddelelse, der opsnappes af uvedkommende, ikke kan dekrypteres. Den uvedkommende part som opsnapper meddelelsen kan nemlig forsøge at se om han kan gætte krypteringsnøglen. Med de gode automatiserede værktøjer man har til dette formål i dag kan det være ret let at dekryptere en krypteret meddelelse, hvis krypteringen ikke er tilstrækkelig stærk. Styrken afhænger af den såkaldte nøglelængde den valgte krypteringsalgoritme.

*Anbefaling: Det anbefales at kryptere meddelelser, som man vil være sikker på andre ikke læser indholdet af. Til krypteringen bør anvendes en tilstrækkelig stærk krypteringsform. Som*

*minimum bør nøglelængden være 128 bit og kryteringsalgoritmen bør være en af følgende typer: triple-DES, AES eller RC4.*

*Værktøj:*

- **Lukkede netværk.** Hvis man kommunikerer meget med den samme part igen og igen kan det være relevant at anvende et lukket netværk, mellem de to parter. Dette kan ske ved simpelthen at trække et kabel mellem de to parter (hvad der ofte er praktisk umuligt og urealistisk dyrt) eller ved at anvende et virtuelt, privat netværk (VPN), dvs en logisk vej gennem internettet, som er lukket af for uvedkommende i den periode kommunikationen står på. Anvendelsen af lukkede netværk er kun relevant for virksomheder og virksomhedens internetudbydere kan hjælpe med oplysninger om hvordan man i praksis kan etablere det. Et lukket netværk er typisk beskyttet med kryptering af indholdet, evt suppleret med en række konfigurationsmæssige parametre i nettet. Virksomheden bør stille krav til sin internetudbydere om detaljeret specifikation af beskyttelsen.

*Anbefaling: Virksomheden skal overveje at anvende lukkede netværk i de situationer, hvor der igen og igen kommunikeres med den samme interessent.*

*Værktøj:*

### **Beskyttelse af trafikinformation**

Når man kommunikerer via nettet pakkes informationerne som nævnt ned i små pakker, der sendes begge veje under en kommunikation. I pakkerne findes indholdet af den meddelelse der kommunikeres. Men hertil kommer en række tal, som sikrer at pakkerne kan finde vej fra afsender til modtager og tilbage igen. Disse numre vil vi kalde trafikinformation. De antager forskellige former afhængigt af hvordan pakken ser ud. Typisk er der imidlertid tre numre, som kan bruges til at afsløre, hvem der kommunikerer. Det er adressen på modtageren (IP-adresse), adressen på afsenderen (IP-adresse) og adressen på den computer der sendes fra (netkort-adresse). Disse informationer kan vi med en fællesbetegnelse kalde header-informationer. Vi vil ikke i denne vejledning gennemgå hvordan denne kommunikation fungerer i praksis og hvordan de omtalte adresser anvendes. For en gennemgang af dette henviser vi til ITEK og Dansk Industris vejledning: "Elektronisk infrastruktur – virksomhedens IT-sikre placering", som kan downloades fra ITEKs hjemmeside. Her vil vi blot slå fast at de personer, der kan læse disse adresser også med stor sandsynlighed kan finde frem til hvilken person, der står bag. Hvis du vil beskytte din privacy er det derfor nødvendigt at beskytte disse adresser.

Det er relativt vanskeligt at skjule disse informationer for alle parter idet f.eks. brugerens internetudbydere jo skal have adgang til at se hvor en forsendelse kommer fra og hvor den skal hen. Ellers kan internetudbyderen ikke levere pakken. Derfor findes der kun løsninger, som delvist kan dæmme op for dette problem. Den ene type løsninger drejer sig om at kryptere de dele af oplysningerne, som ikke er strengt nødvendige for at pakken kan leveres. Den anden type løsning drejer sig om delvist at kontrollere pakkens vej gennem nettet og dermed sløre, hvem der er de reelt kommunikerende parter.

- **Kryptering af headerinformationer.** Når en pakke sendes indeholder den som nævnt afsenderens og modtagerens IP-adresser og afsenderens netkort-adresse. Netkort-adressen ligger imidlertid i en pakke inden i den pakke, som er påført de to IP-adresser. En pakke der sendes på nettet er således i virkeligheden en pakke med kinesiske æsker, hvor der er pakker indeni pakker. Kun den alleryderste pakke kan man ikke kryptere, hvis informationerne skal frem. Man kan få programmer, som krypterer indholdet af alle de pakker, der ligger indeni den yderste pakke. Dermed kan man skjule sin netkort-adresse. Dette kan være relevant, hvis man

sidder på en computer på indersiden af et netværk, hvor der er mange netkort-adresser – f.eks. i en boligforening eller i en virksomhed.

*Anbefaling: Det skal overvejes om man vil anvende kryptering på pakkeniveau, således at header-informationerne er krypteret.*

*Værktøj:*

- **Anonymisering og åbne proxy-servere.** En proxy er en computer, som er stillet op med det formål dels at sløre informationer om de computere der står bag den og dels med det formål at aflaste kommunikationslinierne ved at lagre hyppigt hentede hjemmesider lokalt. Hvis man anvender en computer, der står bag en proxy-server vil det være proxy-serverens IP-adresser, der står som afsender af informationerne og dermed afslører man ikke sin egen IP-adresse. Denne form for privacy er dog ikke total idet proxy-servere som regel er ejet af enten internetudbyderen eller det netværk man selv er placeret på. Generelt kan man sige at privacy altid må gradbøjes og enhver grad af privacy er afhængig af tillid (til produktet, leverandøren, serviceudbyderen, osv.).

Imidlertid kan funktionaliteten anvendes til at sløre sin information. På nettet findes nemlig såkaldte anonymiseringsservices, som man kobler op til og som så står som afsender-IP-adressen overfor den man kommunikerer med. Hos internetudbyderen ser det således alene ud som om man kommunikerer med den såkaldte anonymiseringsservice. Og hos modtageren ser det ud som om det er anonymiseringsservicen, der spørger efter informationerne. Hvis der skal etableres et link mellem de to kommunikationer kræver det adgang til anonymiseringsservicen. Her vil evnen til at sløre pakkernes vej gennem nettet altså bero på den tillid man har til anonymiseringsservicen og de myndigheder der eventuelt på legalt grundlag måtte kunne kontrollere den.

En stærkere anonymisering kan opnås ved at anvende kæder af åbne proxy-servere der er placeret på nettet af forskellige organisationer. Ofte vil sådanne servere være placeret i lande, hvor myndighedernes kontrol er begrænset. Desuden kan man på intet rimeligt grundlagt fastslå hvilken tillid man kan have til de pågældende servere og organisationerne bagved.

*Anbefaling: Det skal overvejes om man vil anvende en anonymiseringsservice for at sløre hvem man kommunikerer med. Herunder skal det overvejes hvilken tillid man med rimelighed kan have til denne.*

*Værktøj:*

- **Åbne trådløse netværk.** Mange steder står der åbne og ubeskyttede trådløse netværk, som er offentligt tilgængelige. Vi vil helt sikkert se en vækst i antallet af disse services. Hvis man anvender et sådant netværk kan hvem som helst koble sig på uden at identificere sig med afsender-IP-adresse direkte fordi det vil være netværkets IP-adresse, der står som afsender. Hvis man anvender et sådant netværk i kombination med kryptering af header informationer kan man være relativt sikker på at man ikke kan spores.

Det skal bemærkes at åbne trådløse netværk kan være ulovlige at anvende, hvis de ikke er opsat som en service, men i stedet er åbne som følge af en sikkerhedsbrist.

*Anbefaling: Der skal overvejes om at man anvende åbne trådløse netværk for at sløre hvem man kommunikerer med.*

*Værktøj:*

- **TORnetværket.** TORnetværket er et netværk af computere, som man kan dirigere sin trafik igennem. Pakkerne tager så i stedet for den hurtigste vej gennem internettet, som angives af internetudbydernes routere, en bestemt vej gennem et netværk af private computere. Fordelen ved dette er, at det bliver nærmest umuligt for alle parter at se, hvem der reelt kommunikerer. Internetudbydere kan se at man kommunikerer med en computer i TORnetværket. Men hvad der sker inden i netværket kan ingen se. Man kan således få sin pakke frem til den tiltænkte

modtager på den anden side af netværket uden at nogen kan spore hvem de to parter er. Når det er umuligt for de computere som pakken passerer igennem på TORnetværket at læse indholdet skyldes det at pakkerne krypteres. Desuden vil pakken ikke hele tiden tage den samme vej gennem TORnetværket, som det ofte reelt sker når pakker rejser via internetudbydere. Dermed kan ingen enkelt computer opsamle alle de pakker der hører sammen. Man kan derfor have rimelig tiltro til TORnetværket. Imidlertid er TORnetværket ingen vidunderløsning. Der findes eksempler på at man kan opspore, hvem der kommunikerer hvis browseren tillader anvendelse af forskellige former for plugins. Det er derfor relevant at have to browsere - en man bruger til almindelig surfen og en man bruger til sikker surfen, hvor det meste af funktionaliteten er skrællet af.

*Anbefaling: Det skal overvejes at anvende TORnetværket til at sløre, hvem man kommunikerer med.*

*Værktøj:*

Det skal bemærkes at de metoder, som er beskrevet i dette afsnit er af tvivlsom karakter. De anvendes ofte af hackere og andre personer med ondsindede hensigter, som jo også har et stærkt incitament til at skjule, hvem de er. Der er således et dilemma mellem at anvende disse metoder til et godt formål, beskyttelse af privacy, og et ondt formål, angreb på andre. Man skal derfor ved anvendelsen af disse metoder overveje om man mistænkeliggør sig selv overfor den man ønsker at beskytte sig imod.

Netop fordi metoderne kan anvendes af personer med ondsindede formål vil der være visse services, der forsøger at detektere kommunikation via disse metoder med henblik på at blokere for dem. Man kan derfor ikke være sikker på at få sin egen legitime kommunikation igennem på denne måde.

## **Opsummering**

Vi har nedenfor opsummeret de muligheder man har for at forbedre sin privacy gennem anvendelse af en række forskellige værktøjer:

### **Beskyttelse af lagret information og funktionalitet**

- Der bør installeres en firewall og mængden af programmer, der skal have lov til at gå på nettet bør begrænses mest muligt.
- Styresystemet, browseren og sikkerhedspakken bør have adgang til at opdatere sig selv via nettet.
- Det bør overvejes at anskaffe sig programmer til intrusion detection og intrusion prevention.
- Der bør installeres en sikkerhedspakke på computeren. Pakken bør som minimum kunne bekæmpe virus, orme, spyware og spam. Pakken bør desuden indeholde en firewall og kan tillige indeholde en overvågning af om der sker uhensigtsmæssige aktiviteter på computeren.
- Man skal udvise fornuft i sin færden på nettet præcis som man gør det i den virkelige verden.
- Man bør designe ud fra at systemsikkerhed kan og vil fejle – og forebygge konsekvenser heraf

### **Beskyttelse af transmission**

- Det anbefales at kryptere meddelelser, som man vil være sikker på andre ikke læser indholdet af. Til krypteringen bør anvendes en tilstrækkelig stærk krypteringsform. Som minimum bør nøglelængden være 128 bit og kryteringsalgoritmen bør være en af følgende typer: triple-DES, AES eller RC4.
- Virksomheden skal overveje at anvende lukkede netværk i de situationer, hvor der igen og igen kommunikerer med den samme interessent.

### **Beskyttelse af trafikinformationen**

- Det skal overvejes om man vil anvende kryptering på pakkeniveau, således at header-informationerne er krypteret.
- Det skal overvejes om man vil anvende en anonymiseringservice for at sløre hvem man kommunikerer med. Herunder skal det overvejes hvilken tillid man med rimelighed kan have til denne.
- Der skal overvejes om at man anvende åbne trådløse netværk for at sløre hvem man kommunikerer med.
- Det skal overvejes at anvende Tor-netværket til at sløre hvem man kommunikerer med.