

Anbefalinger vedr. privacy

IT-sikkerhedspanelet under Ministeriet for Videnskab, Teknologi og Udvikling har i løbet af de seneste møder drøftet nødvendigheden af at forbedre borgere og virksomheders privacy i forbindelse med forskellige teknologier/domæner - herunder f.eks. systemer til digital forvaltning, RFID og sundhedssektoren. Overvejelserne har resulteret i dette katalog over anbefalinger til tiltag.

Informationssamfundet er grundlæggende baseret på, at brugerne kan have tillid til anvendelse af it-systemer. Dette gælder uanset om systemerne er offentlige eller private, nye eller gamle, er placeret i ind- eller udland, fysiske eller elektroniske, osv. Tillid til systemerne er baseret på mange ting - f.eks. at de er tilgængelige, når brugerne ønsker det, og at de ikke laver fejl. Men tillid er i høj grad også baseret på retten til privacy.

Den ultimative privacy kan brugerne have i det tilfælde, hvor de er anonyme. I dette scenario vil brugeren ikke skulle afgive oplysninger, der kan identificere ham. Dette er imidlertid i mange sammenhænge hverken praktisk eller rimeligt i forhold til et tradeoff med behovet for, at kunne identificere en person i forbindelse med f.eks. kriminalitet.

Et andet scenario kunne være muligheden for at brugeren kan oprette pseudonymer og dermed have kontrol over hvem, der skal have adgang til hvilken information og hvor længe, uden at brugeren er identificeret. I tilfælde af særlige behov - f.eks. ved kriminalitet - kan man så hæve pseudonymet og identificere brugeren. Men typisk vil de parter, brugeren kommunikerer med, ikke kunne identificere ham. Denne type systemer er ikke særligt udbredte.

I virkelighedens verden afgiver brugeren typisk personhenførbare data, når han kommunikerer med en anden part. Dette sker f.eks. ved afgivelse af CPR-nummer, IP-adresse eller betalingskortinformationer. I dette scenario identificeres brugeren ikke nødvendigvis fuldstændigt ved afgivelse af informationerne, men brugeren kan meget let identificeres, hvis man får adgang til blot et par af denne type informationer. Da dette scenario er det mest udbredte, har Panelet valgt at forholde sig til dette.

Blandt de vigtigste ting for tilliden til systemerne er, at de informationer, brugerne afgiver, er i overensstemmelse med deres forventninger til brugen af de pågældende informationer. Brugere vil således gerne undgå tab af deres personlige integritet eller med andre ord have privacy.

En lang række faktorer spiller en rolle for at sikre denne privacy. Visse forhold er allerede på plads: F.eks. har vi en lovgivning, som vedrører behandlingen af personlysninger, mange virksomheder og organisationer laver privacy-politikker, og en række teknologier kan bruges til at beskytte digital privacy. Flere initiativer er imidlertid nødvendige, og sikkerhedspanelet har derfor lavet dette katalog over anbefalinger til nye tiltag.

For det første er det vigtigt, at brugerne orienteres om, hvilke oplysninger, der indsamles om dem hvornår, af hvem og med hvilket formål. Det er også vigtigt, at brugerne får redskaber, der sætter dem i stand til at beskytte sig selv og foretage vurderinger af, hvilken beskyttelse - om nogen - de vurderer, der er nødvendigt. Det første indsatsområde vedrører derfor brugernes awareness.

For det andet er det vigtigt, at der sker en fortsat udvikling på teknologiske privacymuligheder således, at de forskellige aktører har mulighed for at beskytte brugernes privacy og således, at brugerne kan fravælge løsninger, som de ikke finder betryggende.

For det tredje må love og regler være på plads således, at de beskytter brugernes privacy under hensyntagen til modsatrettede hensyn som f.eks. terrorisme og anden form for kriminalitet.

Endelig for det fjerde er det nødvendigt at tilvejebringe ny viden på området, således at de tre første prioriteter til stadighed passer ind i et moderne samfund.

De fire forhold kan forbedres ved at følge nedenstående forslag til nye initiativer.

A. Awareness

Jurisdiktion og regelfortolkning

Det er uklart for virksomhederne og borgerne, hvilke regler der gælder, når man via internettet besøger servere i udlandet. Visse regler er slået fast i "Lov om behandling af personoplysninger". Det er dog stadig uklart, hvilke regler der gælder i f.eks. det tilfælde, hvor det amerikanske justitsministerium har udbedt sig oplysninger om søgninger fra Google, Yahoo og Microsoft. Der er derfor behov for afklaring af og oplysning om:

- hvornår man er beskyttet af de danske regler, når man afgiver oplysninger ved brug af nettet - og herunder internationale søgemaskiner
- hvornår man har ret til at få adgang til egne data i de tilfælde, hvor der ikke er blevet spurgt efter samtykke eller andet
- hvilken lovgivning vi som borgere kan forventes at være underlagt af lovgivning, når nettet anvendes
- hvor og efter hvilke regler en eventuel retssag skal føres (værneting).

Logning af data

Mens man surfer på nettet logger forskellige interessenter informationer om ens computer og anvendelsen af denne. Der bør udarbejdes en vejledning, som tydeligt præciserer overfor borgere og virksomheder hvilken logning af data der finder sted i henhold til "Logningsbekendtgørelsen". Desuden bør private udbydere af kommunikationsforbindelser redegøre for hvilke data, der i øvrigt systematisk (for alle kunder) opsamles om kunderne. Endelig bør der udarbejdes en vejledning i, hvordan borgere og virksomheder kan kommunikere via mail og internet med sikkerhed for, at deres trafik ikke overvåges af parter, som brugeren ikke har tillid til.

Privacyportal

Der er behov for at borgere og virksomheder har en samlet portal, hvor de kan finde informationer om privacy. Der skal kunne findes oplysninger om teknologier, lovgivning, vejledninger, demonstration af løsninger, muligheder for at spærre sin elektroniske identitet og helt overordnet de fleste af de initiativer, som er foreslået i dette idekatalog over privacy.

Identitetstyveri

Der skal ved udstedelse af personligt henførbare akkreditiver (f.eks. Digital Signatur) oplyses om, hvor man skal henvende sig, hvis man har mistanke om, at hele eller dele af akkreditivet er kompromitteret. Der bør desuden laves en portal, som indeholder oplysninger om, hvordan man kan få spærret sin digitale identifikation (se også forslaget om privacyportal).

Demonstrationsprojekt

Det foreslås, at der tilvejebringes en hjemmeside, som demonstrerer hvordan et udvalg af privacy enhancing technologies virker, med og uden identifikation af brugeren o.a. Hjemmesiden skal ses som en privacy-pendant, til den tidligere hjemmeside, som demonstrerede hvordan elektroniske betalinger finder sted, og som var tilvejebragt af "e-kredsen" under Ministeriet for Videnskab, Teknologi og Udvikling.

B. Udvikling og udbredelse af Privacy Enhancing Technologies

Skabelon for arkitektur til privacyløsninger

I tråd med de standardiseringstiltag der ligger for digital forvaltning i almindelighed (SOA, FESD og OIOXML) bør der laves en skabelon for den offentlige arkitektur til privacyløsninger.

I skabelonen skal f.eks. fastlægges principper, processer og forretningsgange for, hvordan bestemmerne for videregivelse af personhenførbare data, som bestemt i "Lov om behandling af personoplysninger", "Lov om offentlighed i forvaltningen" og "Forvaltningsloven", bedst kan efterleves i offentlige it-systemer. Herunder i særdeleshed at borgerne har mulighed for at bevare kontrol med egne data, godkende videregivelse til trustede parter i enhver kontekst og ændre deres privacypræferencer kontinuerligt afhængig af kontekst.

I skabelonen bør f.eks. også anvises, hvorledes data ikke udleveres til andre end den, der har behov for og hjemmel til disse data i deres myndighedsudøvelse.

Specifikt for sundhedssektoren bør det anvises, hvorledes Sundhedsstyrelsens vejledning nr. 118 af 13/10 2003 tænkes overholdt. I vejledningens afsnit 7 er det anført, at systemerne skal være indrettet sådan, at det kun er netop det sundhedspersonale, der behandler patienten, der får adgang til journalen.

Den pågældende skabelon bør også indgå i arkitekturarbejdsgruppen under IT- og Telestyrelsen.

C. Lovgivning og regler

Offentlige kunders efterspørgsel efter Privacy Enhancing Technologies

"Lov om behandling af personoplysninger", "Lov om offentlighed i forvaltningen" og "Forvaltningsloven" angives ofte som standardformulering for etablering af sikkerhed og privacy hvorved privacy reelt ikke bliver en del af vurderingskriterierne på løsningen. Der bør derfor tilvejebringes en guide / et hjælpeværktøj til offentlige kunder, så de kan få hjælp til at præcisere, hvilke kontekstafhængige krav, der er aktuelle i forhold til privacy.

Tilsvarende bør der laves et udkast til bilag til standardkontrakten (K01 og K02), som specificerer, hvad offentlige kunder mener med formuleringen om overholdelse af "Lov om behandling af personoplysninger", "Lov om offentlighed i forvaltningen" og "Forvaltningsloven". Dette skal dels sikre, at de tilbud, som afgives, er sammenlignelige på anvendelse af privacyforanstaltninger, og dels sikre at tilbud, som er stærke på privacy, men som også er dyrere, bliver vægtet i forhold til den bedre privacy.

Kodeks for minimal dataindsamling

Der er behov for at skabe incitament til at undlade at indsamle flere data end nødvendigt for et givent formål - herunder at der ikke opfordres til afgivelse af frivillige data, som ikke er strengt nødvendige. Dette skal sikres gennem udarbejdelse og efterlevelse af en kodeks, som præciserer og konkretiserer ordlyden om begrænset dataindsamling i Lov om behandling af personoplysninger. Det bør således klart oplyses, hvad der er formålet med hver enkelt indsamlet information.

Revision af Privacy principper

OECD vil efter sigende revidere sine privacy anbefalinger fra 1980. Det anbefales, at Danmark involverer sig aktivt i denne proces og at IT-sikkerhedspanelet under Ministeriet for Videnskab, Teknologi og Udvikling høres løbende i processen og eventuelt udpeges til at deltage i en dansk forhandlingsdelegation.

ENISA

Det Europæiske agentur for Netværks- og Informationssikkerhed bør sætte privacy på dagsordenen. Under overskriften 2.1 i ENISAs arbejdsprogram for 2007 hedder "Awareness raising and building confidence". Imidlertid berører afsnittet ikke "confidence". Der bør derfor fra dansk side fremføres at ENISA bør tage et initiativ på dette område. Dette kunne omfatte:

- indsamling af best practises om generel privacy, ISP privacy (inklusive logning), RFID-privacy og biometric privacy
- Studere og udvikle en generel trust model
- arbejde for at fremme privacy principperne fra OECD og Europarådet
- evt. arbejde for at fremme crossborder samarbejde om privacy

Præcisering af Lov om behandling af personoplysninger

Artikel 17, stk. 1 i Persondatadirektivet (direktiv 95/46/EC) er ikke implementeret ordret i den danske lov.

I artiklen hedder det at:

" Medlemsstaterne fastsætter bestemmelser om, at den registeransvarlige skal iværksætte de fornødne tekniske og organisatoriske foranstaltninger til at beskytte personoplysninger... Disse foranstaltninger skal under hensyn til det aktuelle tekniske niveau og de omkostninger, som er forbundet med deres iværksættelse, tilvejebringe et tilstrækkeligt sikkerhedsniveau i forhold til de risici, som behandlingen indebærer, og arten af de oplysninger, som skal beskyttes".

Formuleringen i kursiv er ikke medtaget i den danske lovtæst, men er nævnt i bemærkningerne til persondataloven § 41, stk. 3, som implementerer art. 17, stk. 1. Fraværet af denne formulering i den danske lovtæst betyder, at det ved udvikling og implementering af it-systemer ofte overses, at personoplysninger SKAL sikres på en teknologisk aktuel måde. Hermed opfylder it-systemerne ikke kravene i persondataloven og persondatadirektivet.

Tilgængelige privacypolitikker

Virksomheder, institutioner og organisationer, der har hjemmesider, bør have formuleret en privacypolitik og bør have et tilgængeligt privacystatement. For offentlige aktører bør dette indgå i Ministeriet for Videnskab, Teknologi og Udviklings test: "Bedst på nettet". For private aktører bør det knyttes op på anvendelsen af e-handelsmærket. Ministeriet for Videnskab, Teknologi og Udvikling samt e-handelsfonden bør vurdere, om det offentlige privacystatement er i overensstemmelse med de faktiske forhold.

Privacypolitik og -statement kan f.eks. genereres af OECD's privacy-policy-generator.

Offentligt / privat samarbejde

Der skal etableres et fora mellem det offentlige og det private, som kan sikre, at den fornødne holistiske tilgang til hvordan privacy kan håndteres både teknologisk, samfundsmæssigt, økonomisk, etc. i forhold til de løsninger som påtænkes.

D. Forskning

Privacy forvirring

Hvad det præcist er, der forstås med privacy, og hvordan man systematisk kan arbejde med privacy, er ingen steder præcist afklaret. Der er derfor behov for forskning i, om der kan etableres en klassifikation indenfor privacy, som er afhængig af data, risici, processer, systemer, scenarier og transaktioner.

Undersøgelse af privacy behov

Det er ligeledes nødvendigt at få et klart billede af borgernes opfattelse af privacy - herunder hvilken opfattelse de har af privacy, om de er klar over hvor eksponeret de er, hvornår de er villige til at være eksponeret for at få en service, og hvor meget deres privacy er værd i forskellige sammenhænge. Der er derfor behov for et forskningsprojekt, som kortlægger borgernes opfattelse af og behov for privacy.

Tradeoff mellem brugervenlighed og privacy

Mange teknologier findes ikke i en version, der tager hensyn til privacy. Det kan i sådanne tilfælde være nødvendigt at anvende supplerende teknologier, som giver den fornødne privacybeskyttelse (f.eks. en krypteringspakke til et mailprogram). Hvor der findes teknologier, som kan give privacybeskyttelse, anvendes de ikke altid i de kontekster, hvor det kunne være formålstjenligt. Borgere stilles derfor ofte over for det falske valg mellem at anvende en teknologi uden privacy eller helt at undlade at anvende teknologien.

Hvordan teknologierne anvender privacy bør være åbent og transparent for brugeren. Der bør derfor iværksættes et forskningsprojekt, som ud fra de særlige kompetencer i brugervenlighed, som vi har i Danmark, vurderer hvordan denne transparens kan sikres.