ITEK

12. august 2014

Folketinget
Att.: Birgitte Toft-Petersen
Christiansborg
1240 København K

Danish ICT and Electronics Federation

Vedr. høring over beretning nr. 3

DI har modtaget "Høring over beretning nr. 3" om bedre beskyttelse af personfølsomme oplysninger og effektivt tilsyn. DI takker for muligheden for at afgive bemærkninger og har i den anledning nedenstående kommentarer.

Overordnet er det af stor betydning at sikre en bedre beskyttelse af personoplysninger. Gentagne sager med tab af personoplysningers fortrolighed bidrager til at underminere tilliden til digitaliseringen. Dette har konsekvenser for såvel den offentlige som den private sektor. DI noterer sig derfor med tilfredshed, at Folketingets Kultur- og Retsudvalg har sat fokus på området.

Bredt fokus på sikkerhed
DI bakker op om, at arbejdet ikke begrænses til at kortlægge sikkerheden ved betalingskort. De tab af personoplysninger, der er sket gennem de seneste år, omfatter mange andre områder – f.eks. hacking mod kørekortregisteret, SSIs fejlagtige udlevering af sundhedsoplysninger, mange sager med fejlagtig offentliggørelse af personoplysninger i kommuner og på uddannelsesinstitutioner samt udtræk af personoplysninger fra tingbog.dk og fra bibliotekerne. Der er derfor behov for at se på, hvordan man grundlæggende kan forbedre sikkerheden ved behandling af personoplysninger i hele den offentlige sektor.

Moderne metoder og teknologier
En række moderne metoder og teknologier lover særdeles godt for at beskytte personoplysninger.

Der er for det første tale om analyse af om en given teknologisk løsning beskytter personoplysningerne godt og om oplysningerne behandling i overensstemmelse med lovens krav om formål, dataminimering, m.v. Dette kaldes en Privacy Impact Assessment (PIA). Der bør udarbejdes en skabelon for PIA, og denne bør gøres obligatorisk at anvende ved alle større offentlige it-projekter. Skabelonen bør tage udgangspunkt i, om det overhovedet er nødvendigt at identificere borgeren for at behandle vedkommendes personoplysninger, og i givet fald hvornår i behandlingsprocessen identifikation er nødvendig. Dette vil i nogle sammenhænge give

H. C. Andersens Boulevard 18
1787 København V
Danmark

(+45) 3377 3377
itek@di.dk
itek.di.dk

CVR: 16 07 75 93

en bedre beskyttelse af personoplysninger, end man kan opnå ved at anvende den skabelon for PIA, som Digitaliseringsstyrelsen har udarbejdet

For det andet bør god sikkerhed designes ind i it-løsningerne fra starten. Der bør opstilles en række helt overordnede designprincipper, som skal være grundlaget for behandling af personoplysninger. Dette kaldes Privacy by Design.

For det tredje bør der indarbejdes nye såkaldt privatlivsfremmende teknologier i de offentlige it-løsninger. Disse teknologier spænder over en bred vifte af muligheder og inkluderer i den ene ende af spektret anonymisering og pseudonymisering og i den anden ende logning og rollebaseret adgangskontrol. Der bør allerede når en løsning designes stilles krav om, at disse teknologier anvendes.

En god proces for sikker omgang med personoplysninger er derfor som følger: Man laver en analyse af, hvordan et it-system under udarbejdelse påvirker privatlivet, hvis/når der skal behandles personoplysninger. På baggrund af analysen vælges et sikkert design baseret på en gruppe af teknologier, som i særlig grad understøtter privatlivets fred. Der er behov for at disse metoder og teknologier i langt højere grad end i dag tages i anvendelse, og dette skal sikres politisk.

Persondataforordning
Lovgivning på området er en central forudsætning for at sikre en god beskyttelse af personoplysninger. Der er behov for at modernisere lovgivningen på området, som EU Kommissionen med forslaget til ny persondataforordning, har lagt op til. Der er behov for, at Danmark er langt mere imødekommende overfor EU Kommissionens forslag til persondataforordning, end det er tilfældet i dag.

For det første er det vigtigt, at forslaget bæres igennem som en forordning, der harmoniserer reglerne i Europa. Det nuværende direktiv er implementeret på 28 forskellige måder i de forskellige lande. Det betyder, at borgerne ikke kan forvente ens behandling af deres personoplysninger i Europa, og at virksomhederne skal implementere beskyttelse af personoplysninger på en ny måde, for hvert land de driver virksomhed i. De forskellige nationale implementeringer betyder også, at de europæiske nationalstater står svagere overfor at påvirke tilblivelsen af standardiserede it-løsninger. Det er en barriere overfor teknologioptag i den offentlige sektor. Hvis der var ens regler for beskyttelse af personoplysninger ville hele markedet af offentlige nationalstaters efterspørgsel kunne bidrage til at sikre optag af nye effektive teknologier med høj sikkerhed som f.eks. cloud computing.

For det andet indebærer forslaget bl.a., at der skal udarbejdes en Privacy Impact Assessment og at der arbejdes med Privacy by Design, som omtalt ovenfor. Moderne metoder og teknologier som disse kan bidrage væsentligt til at forbedre sikkerheden ved behandling af personoplysninger, hvis de implementeres korrekt. Det er derfor betydningsfuldt at bakke op bag forslaget. Der er naturligvis forhold i Kommissionens udkast, som bør justeres. DI har ved tidligere lejligheder udtalt sig mere detaljeret om forslaget til Forordning til bl.a. Folketingets Europaudvalg, og DI henviser til mere detaljerede bemærkninger i disse henvendelser.

Tilsyn
Der findes flere forskellige tilsyn på sikkerhedsområdet. Datatilsynet fører tilsyn med behandling af personoplysninger efter Lov om behandling af personoplysninger, Finanstilsynet fører tilsyn med behandling og videregivelse af personoplysninger i den finansielle sektor, Tilsynet med Efterretningstjenesterne fører tilsyn med FE og PETs behandling af personoplysninger, osv.

Man kan ikke opnå god sikkerhed alene gennem tilsyn. Men især Datatilsynet synes at kunne have behov for en styrkelse. Sagsomfanget er i takt med digitaliseringen steget betydeligt. Det er mængden af nye teknologier, som behandler personoplysninger også. Desuden er mange af teknologierne globalt interdependente, hvad der gør det vanskeligt at skabe sig overblik. Der er behov for bedre rådgivning i form af offentliggørelse af principielle vurderinger af nye teknologier – både teknologier som bruges til behandling af personoplysninger og teknologier, som bruges til at understøtte bedre sikkerhed. Sådanne vurderinger kunne både den offentlige og den private sektor drage fordel af. Styrkelsen af Datatilsynet bør således især ske på den tekniske front.

ISO27000 er et godt framework til at opnå god sikkerhed. Der findes så vidt vides ikke nogen myndighed, der fører tilsyn med implementering af god sikkerhed, herunder efterlevelse af sikkerhedsstandarden ISO27000. Rigsrevisionen påtager sig dog med mellemrum at foretage stikprøver på området. Der er behov for, at der føres et mere systematisk tilsyn med at den offentlige sektor - og dens leverandører - efterlever ISO27000. Der ville være større sandsynlighed for, at Se og Hør-sagen kunne være undgået eller i hvert fald fået et mindre omfang, hvis man havde efterlevet sikkerhedskrav som f.eks. personalegodkendelse, dataklassifikation, adgangskontrol, kryptering, logning, funktionsadskillelse og pseudonymisering. Den offentlige sektor og dens leverandører bør finde et passende niveau for implementering af relevante korrigerende sikkerhedsforanstaltninger og kontroller på baggrund af en risikovurdering.

Det vil være nyttigt, hvis der afleveres en årlig redegørelse i form af en kortlægning af sikkerhedsniveauet i den offentlige sektor til Folketinget.

Rådet for Digital Sikkerhed
DI har gennem mange år anset det for vigtigt, at der findes et uafhængigt Råd, som bidrager til både den folkelige og den faglige debat om informationssikkerhed og privacy. DI har deltaget i de forskellige offentlige Råd og Komiteer under de daværende forskningsministre. Vi har nu, hvor sådanne ikke findes længere, været med til at stifte Rådet for Digital Sikkerhed.

Rådet for Digital Sikkerhed har bidraget meget væsentligt til debatten med høringssvar, selvstændige faglige udspil, m.v. Rådet kører imidlertid med frivillige kræfter. Det er ikke sikkert, at det kan fortsætte sådan. Rådet ville desuden kunne være endnu mere aktivt, hvis Rådet havde et sekretariat. DI foreslår, at Rådet får en mindre bevilling på Finansloven til at udføre sit arbejde – f.eks. kr. 2 millioner p.a. de næste fem år. Tanken er, at Rådet til den tid vil kunne selvfinansiere et sekretariat gennem medlemskontingenter.

Viden og awareness om sikkerhed
Der bør hos alle parter i samfundet arbejdes på at forøge viden og awareness om informationssikkerhed og privacy. For det første bør der på de forskellige niveauer i uddannelsessystemet tilvejebringes viden om informationssikkerhed i takt med, at borgerne møder forskellige it-systemer. For det andet bør der over for borgerne i almindelighed tilvejebringes informationer om sikkerhed. Endelig bør der tilvejebringes informationer om, hvordan man overordnet arbejder med at skabe en sikkerhedskultur i organisationer.

Arbejdsgruppe
DI noterer sig, at Retsudvalget ønsker at nedsætte en arbejdsgruppe med inddragelse af eksterne eksperter. Det er vigtigt, at Retsudvalget lægger vægt på at arbejdsgruppen kommer med forslag, som indebærer moderne teknologier og metoder til understøttelse af sikker behandling af personoplysninger. I forhold til det udspil, Udvalget har skitseret, synes der behov for at styrke de tekniske eksterne kompetencer.

DI har utallige gange gennem de sidste seks år argumenteret for en styrkelse af sikkerheden på den tekniske front. Anvendelse af moderne teknologier og metoder, kombineret med kravene i Lov om behandling af personoplysninger, kombineret med kravene i ISO27000 og kontrolleret af en stærk myndighed er løsningen. DI har udgivet en række vejledninger, debatoplæg og høringssvar på dette område. DI stiller sig meget gerne til rådighed for en sådan arbejdsgruppe.

Semantik
Som et lille kuriosum kan det tilføjes, at Beretningen anvender en ikke helt konsistent sprogbrug. Der tales om både personoplysningslov og persondatalov, når der formodentlig refereres til samme lov. Desuden tales i Beretningen om personfølsomme oplysninger. I Lov om behandling af personoplysninger tales der derimod om almindelige, følsomme eller fortrolige personoplysninger og ikke om personfølsomme oplysninger. Det må antages, at Retsudvalget ønsker at beskytte både de følsomme og de fortrolige personoplysninger.

DI ITEK står til naturligvis til rådighed for en uddybelse af ovenstående synspunkter.

Med venlig hilsen

Henning Mortensen
Chefkonsulent
DI ITEK

Adam Lebech
Branchedirektør
DI ITEK