TEKNOLOGI RÅDET
DBT FOUNDATION

Til møde 26. august 2014 i Parlamentarisk arbejdsgruppe vedr. databeskyttelse

LARS KLÜVER, FONDEN TEKNOLOGIRÅDET

Hovedpunkter i indlæg.

a) Situationen var forudset. Der er de sidste mindst 20 år blevet advaret mod manglen på konkrete krav til databeskyttelse og der er blevet peget på de forventelige konsekvenser for privatlivet, datakriminalitet, national sikkerhed, samfundsøkonomi, langsigtet accept af eForvaltning og i bredere forstand af internet-baserede aktiviteter.
    a. Der har **manglet en klar politisk ansvarsplacering** i forhold til at lytte til advarslerne og implementere effektive organisatoriske, juridiske og teknologiske løsninger.

b) Se og Hør sagen er en meget en synlig top af isbjerget. Nedenunder ligger der daglige indbrud i virksomheders IT-systemer; anvendelse af private data til kommercielle formål; omgåelse af regler om informationsindhentning ved ansættelser og forsikringstegning; enorme mængder spam; nedsættelse af hastighed og effektivitet i IT-systemer; identitetstyveri; økonomisk kriminalitet; og så alt det, vi ikke/sjældent hører om, som formentlig er f.eks. pengeafpresning, politisk motiveret overvågning og manipulering af andres data. Til det skal man lægge konsekvenserne af, at folk føler sig usikre ved anvendelse af IT, såsom mindre anvendelse af eForvaltning, modstand mod at sætte sig ind i og anskaffe IT, de langsigtede samfundskonsekvenser af følelsen af overvågning. Endelig vil det være uhensigtsmæssigt helt at glemme, at nogle af de svagheder, der er i systemerne også er de svagheder, som fremmede magter anvender til efterretningsvirksomhed og industrispionage.
    a. Der er behov for en **stærk og målrettet politisk indsats for at få bragt problemet ned** på et niveau, samfundet kan leve med.

c) En del IT-professionelle og debattører har desværre i mange år stået for en ikke så hensigtsmæssig tilgang til problemet, som dels er baseret på den ide, at man ikke skal lægge restriktioner på anvendelsen af IT og Internet, dels på den til tider decideret opgivende holdning, at man jo alligevel ikke kan lave helt sikre IT-systemer. Det er endt i, at det bedste har været det godes værste fjende, og at mange af de funktioner, som skulle have været frie, tværtimod er blevet kidnappet af IT-kriminelle og IT-antisociale.
    a. Der er behov for **et opgør med de forestillinger, der har ledt til, at IT og Internet er stærkt underregulerede områder**. Der bør tages fat om problemet med den tilgang, at IT- og Internetsikkerhed skal tvinges igennem til et niveau, hvor det er forbundet med betydelige omkostninger at bryde den.

d) Et kerneproblem har været, at der mangler en kobling mellem de juridiske krav til databeskyttelse og de tekniske krav. Man kan sige, at Datatilsynet sådan set ikke har kunnet lave en effektiv tilsynsmanual, som f.eks. matcher de manualer, man anvender på andre tilsynsområder, såsom indenfor arbejdsmiljø eller flysikkerhed. Hvad skal de helt konkret lede efter og kontrollere tilstedeværelsen/funktionaliteten af, når der ikke findes håndfaste krav til, hvad der skal være på plads? Programmer til databeskyttelse, anonymisering, kryptering osv. er hyldevarer hos IT-leverandørerne, men de bliver ikke efterspurgt, for der er ingen håndfaste krav om, at de skal anvendes.
    a. Der skal stilles **konkrete tekniske krav til, hvad man betragter som tilstrækkelig data/privatlivs-beskyttelse** for forskellige følsomhedsområder, og hvilken type tekniske løsninger, der skal være installeret og i funktion, før kravene er opfyldt. Kravene skal naturligvis opdateres jævnligt. Dette kan støttes af ISO-systemer, af typegodkendelse af privatlivsbeskyttende teknologi, mærkningsordninger, krav til offentlige udbud, mv.

e) Der mangler et IT identifikationsmiddel (eller, for at være mere præcis, et autentificeringsmiddel), som er nemt at anvende og tilstrækkeligt sikkert. Det har ledt til en situation, hvor det er besværligt at anvende IT-services og sikkerhedsfremmende systemer. Mange sløser derfor med sikkerheden. Flere ihændehaverbeviser er kompromitterede, CPR-numrene er de facto offentlige data for dem, som ikke skulle have adgang til dem, og det er svært at se NEM-id som den lette, ubesværede løsning, alle med glæde anvender overalt. Kombinationen af Brugernavne og Adgangskoder er udbredt, men er meget følsom overfor simpel hacking, foruden at mange håndterer dem uforsvarligt.
    a. Tiden er moden til at **etablere en smart-card-løsning**, som med eksisterende teknologi (som bankkort) entydigt og tilstrækkeligt sikkert kan identificere (autentificere) os overfor IT-systemerne. Et sådant kort kan danne basis for en fortsat udvikling, hvor andre sikre løsninger træder til, efterhånden som de kan levere samme sikkerhed som et smart-card. Det fryser altså ikke IT-sikkerheden fast, men sætter en standard, som andre løsninger mindst skal kunne leve op til. Estland har en sådan løsning, som efter alt at dømme fungerer tilfredsstillende.

f) Internettet er nærmest lovløst land, hvad angår databeskyttelse og hacking, og de få regler, der er, er forældede. Usikkerhedselementer, som er utilsigtede, såsom at have en "port" stående åben på en server, straffes med udelukkelse af serveren fra Internettet. Men hvis man på sin hjemmeside med vilje indbygger programmer, der lægger sig på de besøgendes PC'ere og aflæser deres brugernavne og passwords, får hjemmesiden lov til at bestå. Man straffer altså uforsigtighed, men ikke bevidst anvendelse af hacker-værktøjer. Teknisk er det muligt at sætte automatiske "web crawlers" – dvs programmer, der screener hjemmesider – til at finde en meget stor del af de usikre sider og iværksætte en blokering af dem indenfor f.eks. Danmark/Europa. Det er viljen, lovgivningen og etablering af en organisation, der mangler. Havde man det, ville det blive meget mere besværligt og dyrt at være hacker.
    a. Der bør arbejdes for dansk og/eller europæisk lovgivning, som muliggør aktiv modvirkning af kriminel/antisocial adfærd på Internettet ved at **blokkere aktiviteter, hjemmesider mv., der bevidst kompromitterer databeskyttelsen**. Det vil, sammen med de mulige høje fremtidige strafframmer, som netop debatteres i EU, gøre det meget mindre attraktivt at bryde IT-sikkerheden.

To afsluttende bemærkninger:

Det er desværre dårligt belyst, hvor står **social ulighed**, der formentlig er i datakriminalitet og privatlivsbrud. Det er sjældent den IT-professionelle eller den i øvrigt ressourcestærke, der rammes af identitetstyveri, fishing, osv. Det er de ressourcesvage, som på grund af funktionel analfabetisme og lav IT-kompetence er lette ofre. Der ligger derfor et ansvar hos dem, der langt hen ad vejen selv evner at håndtere truslerne, for at tage hånd om alle de mange, som ikke evner det. Det glemmes desværre ofte, når der henvises til, at det jo også er folks eget ansvar at sørge for, at deres PC er sikker, eller når man sætter sin lid til oplysningskampagner. Det, de svageste har brug for, er, at staten tager et ansvar for aktivt at beskytte deres privatliv og værdier.

Teknologirådet har i flere projekter gennemført borgerinddragelse, hvor vi har spurgt til borgernes opfattelse af databeskyttelse og trusler mod privatlivet. De forslag, jeg har nævnt i dette oplæg, ligger **på linje med, hvad borgerne ønsker** – ikke bare i Danmark, men i Europa. De føler sig magtesløse og usikre på, hvad de kan komme ud for, og de ønsker at blive aflastet for et ansvar for egen IT-sikkerhed, som de alligevel ikke kan leve op til. De ønsker med andre ord, at staten tager ansvar og etablerer IT-sikkerheden for dem.