Bemærkninger til Beretning #3

om

nedsættelse af en parlamentarisk arbejdsgruppe, der skal undersøge mulighederne for en bedre beskyttelse af personfølsomme oplysninger og et effektivt tilsyn med offentlige institutioner såvel som private virksomheders behandling af disse

Bemærkningerne er udarbejdet af CSC Danmark A/S.

Generelt:

Offentlige myndigheder har i en årrække fokuseret på digitalisering af det danske samfund med effektivisering og større tilgængelighed for borgere og virksomheder til følge.

I en tid hvor global cyber kriminalitet vokser med flere hundrede procent hvert år, øges kravene til at sikre personfølsomme data mod uautoriseret adgang. Den øgede digitalisering og det forværrede trusselsbillede har skabt en større bevidsthed hos offentlige myndigheder og politikere om nødvendigheden af at investere i øget sikkerhed. På denne baggrund hilser CSC nedsættelsen af en parlamentarisk arbejdsgruppe velkommen.

Bemærkninger til afsnit 2. "Politiske bemærkninger"

Styrkelse af Datatilsynet:

En styrkelse af Datatilsynet vil ikke i sig selv gøre de offentlige systemer mere sikre.

Der mangler snarere overordnede anvisninger og anbefalinger på det IT-sikkerhedsmæssige område. Anvisninger og anbefalinger, der instruerer offentlige myndigheder i, **hvordan** deres IT systemer skal sikres og overvåges, herunder også hvilke krav der stilles til nye driftsformer såsom cloud.

En evt. styrket offentlig tilsynsvirksomhed bør derfor have stærke IT-sikkerhedsmæssige kompetencer og fokusere på, at fællesoffentlige anbefalinger og anvisninger overholdes.

Logningsreglerne og personoplysningsloven:

Med den store mængde transaktioner og det deraf følgende store antal logs bør logningsreglerne opdateres til det nuværende trusselsscenarie. Der bør bl.a. stilles krav om realtids, automatiseret log-gennemgang, herunder korrelering og gennemgang af sikkerhedslogs på tværs af en bred vifte af systemer, applikationer og sikkerhedsopsætninger (FW, IDS/IPS, FIA etc.).

EU's nye databeskyttelsesforordning:

Den nye forordning vil stille krav om yderligere beskyttelse af persondata. Det er ikke på nuværende tidspunkt klart, om forordningen vil tilbyde tilstrækkelig beskyttelse af de meget store mængder af personfølsomme data, som den offentlige sektor er i besiddelse af.

Det nævnes, at Tyskland og Frankrig har været meget aktive i arbejdet med EU-forordningen, og det er også relevant at nævne andre landes meget regulerede tilgang til persondatabeskyttelse. Bl.a. har Tyskland og England udstukket retningslinjer for hvilke sikkerhedsløsninger, der skal være installeret, og hvorledes monitorering og opfølgning skal foretages. Kravene til disse sikkerhedsløsninger afhænger af, hvilke typer data der er tale om, og i hvilket omfang de betragtes som vitale i forhold til at beskytte den enkelte borger eller nationens sikkerhed.

I Danmark eksisterer der ikke lovgivning eller forordninger, der giver anvisninger på**, hvordan** forskellige typer af data skal beskyttes. Det eksisterende regelsæt er således ikke tilstrækkelig specifikt, når det gælder kategorisering af forskellige former for data. Og der mangler konkrete retningslinjer eller lovgivning, som regulerer metoder og processer til at understøtte sikkerheden. Det er i det store og hele op til de enkelte dataejere at etablere tilstrækkelig sikkerhed, uanset om dataejeren har den fornødne kompetence på sikkerhedsområdet. Konsekvensen er, at der i Danmark ikke er en koordineret og ensartet IT sikkerhed på tværs af ministerier, styrelser og andre offentlige myndigheder.

Behovet for samling af it- og datasikkerhed ved en ansvarlig ressortminister:

Der er behov for, at ansvaret for nationens IT sikkerhed samles ét sted. Ansvaret bør dække hele den offentlige sektor på tværs af alle niveauer og udstrækkes til de private virksomheder, der benytter personfølsomme data, som hentes hos det offentlige eller som administrerer samfundskritisk infrastruktur eller udfører samfundskritiske funktioner.

Det vil således være hensigtsmæssigt fremadrettet at have en mere holistisk tilgang til IT-sikkerhed, der dækker alle samfundskritiske og følsomme data og funktioner, uanset om de varetages af offentlige eller private virksomheder.

Man bør i tilknytning til etablering af én central IT-sikkerhedsmyndighed etablere et bredt samarbejde med alle IT-leverandører efter udenlandsk forbillede. Dette samarbejde skal sikre en hurtig udveksling af informationer leverandører og myndigheder imellem i tilfælde af IT-sikkerhedsmæssige hændelser.

Yderligere krav til både offentlige og private dataansvarlige:

Der bør stilles entydige, ensartede krav om sikkerhedsarkitektur og sikkerhedsrapportering til alle dataejere og deres leverandører. Hvis disse krav skal matche ”Best Practice”, vil det resultere i en ikke ubetydelig investering i yderligere sikkerhedsudstyr og løbende opfølgning.

Den offentlige sektors håndtering af IT er karakteriseret af mange mindre IT-organisationer og et noget fragmenteret dataejerskab. Det vil formodentlig ikke være økonomisk rentabelt at lade hver enkelt dataejer anskaffe og drive de nødvendige sikkerhedsløsninger. Ud over at centralisere det overordnede ansvar for sikkerhed, bør udførelsen således også samordnes.

I samarbejde med den private sektor og sikkerhedsleverandørerne bør det offentlige centralisere sikkerhedsovervågningen i større centre, der opererer 24X7, og som har det fornødne teknologiske

beredskab, hvis der måtte opstå problemer. Det er ligeledes vigtigt, at disse overvågningscentre er sammenkoblet med globale centre, der har adgang til internationale informationer om sikkerhedstrusler. Dette er vitalt for at kunne dæmme op for den omsiggribende internationale Cyber kriminalitet.

Obligatorisk databeskyttelsesvurdering af alle offentlige digitaliseringsprojekter:

Der bør fra centralt hold stilles konkrete sikkerhedskrav til alle offentlige IT-projekter. I den forbindelse vil det være en god ide at anvende erfaringer fra andre lande, som har arbejdet mere målrettet med IT sikkerhed end Danmark og derfor har haft mulighed for at påvirke IT sikkerhedsleverandørerne og deres service udbud.

En side gevinst ved dette er de lavere omkostninger, der følger af at anvende standard løsninger frem for specielt fremstillede løsninger til det relativt lille danske marked.