IT- og Telestyrelsen
Holsteinsgade 63
2100 København Ø

Att.: Rita Lützhøft, rla@itst.dk

Høringssvar – Begrebsmodel til brugerstyring

12. november 2009
Ref.: hip

KMD A/S har med interesse vurderet Begrebsmodel for brugerstyring, og har følgende kommentarer til modellen:

KMD A/S finder det nyttigt at der fastlægges overordnede begrebsmodeller for områder som med fordel kan standardiseres på begrebsniveau. Der findes i dag mange forskellige begrebsmodeller som hver for sig beskriver forskellige scenarier. I en implementeringssammenhæng vil den valgte løsning formentlig være stærkt afhængigt af de konkrete krav (lovkrav eksempelvis), som vil være bestemmende for hvilke modeller der mest hensigtsmæssigt finder anvendelse.

I Bilag 1 har KMD A/S anført en række svagheder ved begrebsmodellen som den er blevet opfattet af relevante fagpersoner indenfor området.

Venlig hilsen

Heidi Pedersen
Afdelingschef, Kompetencecenter Sikkerhed
KMD A/S

Direkte telefon: 44601266
E-mail: hip@kmd.dk

KMD A/S
Produktforretning
Dusager 18
8200 Århus N
Tel. 44 60 13 91
Fax 44 60 13 90
www.kmd.dk
CVR-nr. DK 26911745
Hjemsted: Ballerup

BILAG 1: Detailkommentarer

KMD A/S finder at modellen har svagheder på følgende områder:

- Det er uklart hvordan dataafgrænsning i traditionel forstand skal håndteres i henhold til modellen. Ved dataafgrænsning forstår vi afgrænsningen til at konkret bruger (aktør), autoriseret til en given funktion kun må kunne udføre funktionen på et givet objekt/gruppe af objekter. Der synes at være flere muligheder for at foretage dette i modellen (bl.a. gennem Brugerstyringsrettigheder, Brugerstyringsrollerestriktioner), så det er ikke klart hvordan modellen skal anvendes for at kunne beskrive dataafgrænsning.

- Begrebsmodellen synes at mangle redskaber til at forholde sig til risici omkring fx funktionssammenfald eller adgang til særligt kritiske funktioner. Set i forhold til implicitte krav om efterlevelse af DS-484 og anden særlig lovgivning (persondatalov, sundhedslov etc), så synes dette at være en væsentlig mangel ved begrebsmodellen. Begrebsmodellen indeholder Brugerstyringsregler og Brygerstyringsrolle-restriktioner der kan anvendes som korrigerende foranstaltninger, men ikke hjælp til at definere disse samt relationerne til hhv. Brugerstyringsrettigheder og Brugerstyringsrolletildelinger.

- Begrebet Bruger er på side 12 i beskrivelsen angivet som en kombination af en Brugers akkreditiver og dertil hørende rettigheder. Dette synes at være i modstrid med tegningen på side 11, hvor rettigheder (Brugstyringsrettigheder) er afkoblet fra brugeren gennem en Brugerstyringsrolle. I samme sætning anvendes begrebet "Brugerstyringsaktøren", som ikke er defineret andetsteds.

- Brugerstyringsrettighed synes ved eksemplerne at være uklart beskrevet. Ved handling forstår vi normalt en eller flere af Create, Read, Update, Delete (Opret, Læs, Opdater, Slet). Eksemplerne bør for forståelsens skyld opdateres med fuldgyldige beskrivelser på elementets attributter.

- Begrebet Brugerstyringsrolle er på side 12 beskrevet som "anvendes til at afgøre, hvilke handlinger en bruger må udføre i et it-system." Denne formulering er ikke i overensstemmelse med modellen, idet det her er vist at Brugerstyringsrettigheden anvendes af IT-systemet til at afgøre om en handling er i orden eller må afvises.

- Begrebet Brugerstyringsrettighedsudsteder er beskrevet på side 15. Dette element er ikke vist på diagrammet side 11. Dette leder til endnu en mangel ved begrebsmodellen. Modellen beskriver ikke hvorledes Brugerstyringsrettighedsudsteder "fødes", selv om der formentlig blot er tale om en Bruger med en eller flere specifikke Brugerstyringsrolletildelinger. Ligeledes beskriver modellen heller ikke elementerne "Service Provider" (måske i form af modellens "IT-service") og "Identity Provider", samt en beskrivelse af relationerne mellem disse, og hvordan et tillidsforhold skal vedligeholdes på tværs af organisationer. Dette er muligvis ikke intentionen med modellen, men i så fald savnes der en beskrivelse af hvordan forskellige organisationers brugerstyringsmodeller kan integreres.

- Det foranstillede "Brugerstyrings-" på mange af elementerne gør begrebsmodellen vanskeligt læselig, og virker forhindrende for en god forståelse af modellen. Eksempelvis kunne man forstå elementet

”Brugerstyringsrolle” som en rolle der har relation til eller betydning for brugerstyringsprocessen, og ikke som en betegnelse for en ”rolle”.

- Det vil være nyttigt, hvis beskrivelsen af hvert element indeholder en formålsbeskrivelse. Eksempelvis er elementet ”Brugerstyringsklassifikation” beskrevet som ”en form for ejerskab i forhold til de forskellige roller og rettigheder”, men der gives ingen nærmere beskrivelse af hvad dette ejerskabsforhold skal anvendes til.

- Der synes at være en meningsforstyrrende fejl nederst på side 15 i beskrivelsen af ”Brugerstyringsregel”. Det er umiddelbart vores opfattelse, at komplekse Brugerstyringsregler fortsat kun beskæftiger sig med regler for brugerstyringsrettigheder og ikke for regler i sig selv (jf. diagrammet), så bør der sidst i beskrivelsen stå: ”… udpege brugerstyringsrettigheder der udelukker hinanden.”