26. marts 2014
ATV's Digitale Vismænd

Emne	**Tekniske facts omkring betydningen af den fysiske placering af NETS**
Problemstilling	Store dele af den aktuelle debat om NETS har drejet sig om, hvilken betydning den fysiske placering af NETS kan få for datasikkerheden omkring de data, som NETS opbevarer eller får kendskab til, samt hvilken betydning dette kan få for driftssikkerheden. ATVs digitale vismænd ønsker med dette notat at belyse betydningen af den fysiske placering af NETS datacentre og servere i forhold til de tekniske aspekter af datasikkerhed og driftssikkerhed. DATASIKKERHED I forbindelse med datasikkerhed er det vigtigt at skelne mellem to forskellige slags data: • **PIN-koder og private nøgler**, der bruges til hhv. Dankort og digitale signaturer i NemID. • **Personfølsomme data**, f.eks. om hvilke transaktioner en bestemt kunde har gennemført. **PIN-koder og private nøgler** opbevares normalt i specielt sikrede hardware enheder, som er uhyre vanskelige at bryde ind i, selv hvis man har fysisk adgang til enheden. Enhederne er designet til aldrig at udlevere deres interne data til omverdenen. Underskrift og check af PIN-koder foregår derfor inde i enheden, og for eksempelvis NemID's vedkommende er der kontraktligt fastsatte standarder for kvaliteten af den hardware, der anvendes. De angreb, som man kan forvente mod denne slags data, er derfor angreb, der enten forsøger at lukke hele datacenteret ned ved at bombardere det med net-trafik (såkaldt denial-of-service) eller retter sig mod brugerne og/eller kortterminaler. Sådanne angreb er upåvirket af, hvor datacenteret er placeret. Brugere og terminaler vil fortsat være placeret i Danmark, og angreb over nettet på et datacenter lader sig gøre uanset den fysiske placering. **Personfølsomme data** vil normalt ikke befinde sig i sikret hardware og vil derfor i højere grad være udsat for tyveri gennem angreb, enten fra kriminelle eller fra fjentligt sindede efterretningstjenester. Sandsynligheden for, at dette sker, afhænger af, hvor veldrevet det pågældende datacenter er. Specielt i forhold til de

	sikkerhedsprocedurer og –politikker, der anvendes. Hvis NETS flytter sit datacenter til et andet sted, f.eks. i udlandet, kan det medføre ændringer i den interne organisering af centeret. Det kan derfor vise sig vanskeligt at vurdere, om den interne sikkerhed hos det nye center er bedre eller dårligere end hos det nuværende. Men risikoen afhænger ikke af den fysiske placering i sig selv, og derfor kunne den samme problemstilling opstå, hvis NETS flytter til et andet sted i Danmark. DRIFTSSIKKERHED Driftssikkerheden af et system afhænger af, hvor godt systemet er designet. Erfaringsmæssigt er det dog sådan, at alle systemer af og til går ned. Hvor skadeligt et nedbrud er i forhold til tab af data, og hvor lang tid et nedbrud varer, afhænger af systemets beredskab. Ved en eventuel ændring af NETS-servernes fysiske placering er det derfor nødvendigt at se på kravene til systemets beredskab i form af afsatte ressourcer og garantier for minimum oppetid (den procentvise tid hvor systemet er oppe - dvs. fungerer). Man bør også være opmærksom på at en placering af datacenteret som er fysisk langt væk fra Danmark vil medføre at forbindelsen til f.eks. kortterminaler vil gå via flere mellemstationer. Det kan potentielt give problemer med øget forsinkelse eller en mindre stabil kommunikation. JURIDISKE PROBLEMSTILLINGER En helt anden problemstilling er den jura, der regulerer adgangen til data. Dansk lov gælder naturligvis for data, der fysisk er placeret i Danmark og omhandler danske personer. For data placeret i udlandet er det mindre klart, hvilken lov der gælder. Vil amerikanske myndigheder med amerikansk terrorlovgivning i hånden f.eks. kunne kræve adgang til data om danske borgere, hvis et datacenter er placeret i USA? Og hvilke sanktionsmuligheder har Danmark, hvis vi mener, at danske regler er overtrådt? Endelig skal man være opmærksom på, at NETS' kontrakt med den danske stat om drift af NemID-systemet udløber om få år. Dette vil formentlig betyde, at det nuværende system vil blive afløst af et nyt, og det er ikke givet på forhånd, at NETS vil få tildelt kontrakten om driften af det næste NemID-system. Dette er selvsagt relevante problemstillinger, men falder uden for, hvad ATV's Digitale Vismænd kommenterer på.
Konklusion	Fra en teknisk betragtning er der intet grundlag for, at datasikkerheden skulle blive dårligere alene, hvis NETS flytter, enten til et andet sted i Danmark eller til udlandet. Dette hverken i forhold til PIN-koder og private nøgler eller til personfølsomme data. En ændring i NETS's organisation kan derimod have konsekvenser for både sikkerhedsniveauet og for driftssikkerheden. Det er derfor nødvendigt at have et stort fokus på kravene til sikkerhed og drift. Om de garantier, som man kan opnå for en vis standard, er tilstrækkelige, må man konkret vurdere i den givne

	situation. Det mest kritiske aspekt ved en eventuel placering i udlandet kan vise sig at være juraen vedrørende regelsæt, der regulerer adgang til data. Dette kan ikke vurderes ud fra en teknisk vinkel, og falder derfor udenfor de digitale vismænds område.
Afsendere	Notatet er skrevet på baggrund af en drøftelse på et møde i ATVs vismandsråd. **ATVs digitale vismænd er:** Professor Stephen Alstrup, KU Professor Jakob E. Bardram, ITU Professor Ivan Bjerre Damgård, AU Professor Jan Damsgaard, CBS Professor Kim Guldstrand Larsen, AAU Direktør Thomas Jakobsen, Grazper Professor Christian Søndergaard Jensen, AAU Professor Pernille Kræmmergaard, AAU og ITU Professor Jan Pries-Heje, RUC Institutdirektør Helle Rootzén, DTU Rådets formand, Direktør Ole Lehrmann Madsen, Alexandra A/S / Professor på Aarhus Universitet, deltog ikke i drøftelserne.
For yderlige spørgsmål	Professor Ivan Damgaard, AU ivan@cs.au.dk Direkte telefon: 87156258 Mobiltelefon: 20837137