Gmail **Thue Janus Kristensen <thuejk@gmail.com>**

Det åbne sikkerhedshul i Dankortet

thuejk@gmail.com <thuejk@gmail.com> 23. januar 2019 kl. 09.53
Til: finanstilsynet@ftnet.dk

Hej Finanstilsyn.

Jeg ville meget gerne have en kommentar fra jer med hensyn til det åbne sikkerhedshul i Dankort-systemet. Jeg lavede et foredrag om det her: BornHack 2018 - Thue Janus Kristensen - The Dankort is insecure and illegal. Det undrer mig at et system som Dankortet kan eksistere, når det så klokkeklart ikke opfylder de konkrete krav i Lov om Betalinger, eller best practice og almindelig sund fornuft.

Bemærk at jeg påpeger et konkret praktisk angreb på online Dankort med 2-faktor autentifikation i foredraget. Det er mit indtryk at dette (for mig ret åbenlyse) angreb ikke er bredt kendt.

Min plan er tilbyde de politiske partiers IT-ordførere et privat minifordrag om diverse sikkerhedshuller i den centrale danske infrastruktur, så som i NemID, Dankortet, og MobilePay. Det giver selvfølgelig ikke mening uden at have en kommentar med fra Finanstilsynet (Jeg har allerede en kommentar Nationalbanken).

Baggrund: Som jeg tidligere har nævnt for jer, så er der et åbent sikkerhedshul i NemID. Jeg har fået udtalelser fra de 2 førende professorer i kryptologi Danmark:

> Jeg har fremlagt dette for professor Lars R. Knudsen, som er en internationalt anerkendt kryptolog og leder af DTU's kryptologi-gruppe. Knudsen er enig i at NemID har et reelt sikkerhedshul, som ikke findes i andre browser-baserede single sign-on systemer, såsom Google's, og han "finder det besynderligt at Nets ignorerer dette problem".

og

> Når man beder folk om at taste et password på en webside, så bør man bruge de teknologiske muligheder der findes for at bekræfte identiteten af den webside, der får udleveret passwordet. Det vil i praksis sige TLS som findes i alle moderne browsere. Løsningen er på ingen måde perfekt eller ubrydelig, men klart bedre end ingenting. Det er derfor svært at forstå hvorfor NemID ikke bruger den mulighed. - Ivan Bjerre Damgård

Jeg har også spurgt Kammeradvokatens ekspert i dataret, Kirsten Petersen, om det er lovligt m.h.t. persondata (GDPR) hvis NemID har et åbent sikkerhedshul - det sagde hun ikke var lovligt. Hvilket jo måske er relevant for jer givet Lov om Betalinger §124 stk. 1. og §130 stk. 1., da bankerne giver adgang til personfølsomme data så som fagforeningstilhør via NemID, da disse kan udledes fra betalinger i kontoudtoget. En embedsmand fra Digitaliseringstyrelsen var for resten til stede da jeg fik svar fra Petersen omkring NemID og persondataoplysninger. Men Digitaliseringsstyrelsen har jo effektivt udtalt at de er ligeglade med hvad professorer i kryptologi siger om NemID, hvis jeg har forstået Digitaliseringsstyrelsens svar rigtigt, så jeg regner ikke med at Digitaliseringstyrelsen vil gøre noget.

I forbindelse med forberedelse til foredrag om NemID jeg har holdt til tekniske konferencer, og dialog med kryptologi-professorer, har jeg været tvunget til at præcisere mine argumenter og modeller. Og det gik dermed op for mig, at Dankortet har præcis samme problem med manglende brug af TLS til password-beskyttelse som NemID har. Og at Dankortet bryder Lov om Betalinger §128 stk. 1. på præcis samme måde som NemID.

Jeg har selvfølgelig også gjort Nets opmærksomme på at Dankortet har samme sikkerhedshul som NemID. Og sagt til Nets at min vurdering er at enhver professor i kryptologi vil være enig med mig.

Hilsen
Thue Janus Kristensen