Justitsministeriet
Lovafdelingen

Kontor: Formueretskontoret
Sagsnr.: 2006-7010-0045
Dok.: LHO40246

Besvarelse af spørgsmål nr. 8 af 10. maj 2006 fra Folketingets Retsudvalg vedrørende forslag til lov om ændring af lov om tinglysning og forskellige andre love (Digital tinglysning) (L 199).

Spørgsmål:

> "Ministeren bedes kommentere vedlagte artikel "TDC øger sikkerhed i digital signatur" og herunder oplyse om, hvilke konsekvenser det måtte have for digitaliseringen af tinglysningen, hvis der ikke kan stoles på den digitale signatur."

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet anmodet Ministeriet for Videnskab, Teknologi og Udvikling om en udtalelse. Videnskabsministeriet har på den baggrund indhentet følgende udtalelse fra IT- og Telestyrelsen:

"IT- og Telestyrelsen fører kontrol med, at TDC lever op til de sikkerhedskrav, der er beskrevet i de offentlige certifikatpolitikker for OCES digitale signaturer. I den forbindelse har IT- og Telestyrelsen modtaget en rapport fra TDC om en sårbarhed i forbindelse med den digitale signatur.

TDC har i relation til sagen oplyst følgende:

Der er opdaget en sårbarhed i den softwarekomponent, som TDC distribuerer sammen med den digitale signatur.

Sårbarheden, der skyldes en programmeringsfejl, er af samme type, som de sårbarheder der fra tid til anden offentliggøres i forbindelse med forskellige anvendelsesprogrammer (mail, browser etc.) på Microsoft-platformen.

Den digitale signatur anvender ligesom Windows-programmer de basale funktioner i Windows operativsystem. Sårbarheden er ikke relateret til selve den digitale signatur, men til en softwarekomponent, der distribueres til brugernes pc i forbindelse med installationen af den digitale signatur.

Sårbarheden vil, i lighed med andre sårbarheder af denne type, muliggøre, at en ondsindet hjemmeside vil kunne installere hackerværktøj på pc'en, som potentielt ville kunne anvendes af en hacker til blandt andet at stjæle en brugers digitale signatur og den tilhørende aktiverings-

kode, når den indtastes af brugeren. Det forudsætter, at detaljerne i sårbarheden er kendt af en hacker, og at brugeren lokkes til at besøge en hackers hjemmeside, samt at hackeren aktivt overvåger en transaktion med en digital signatur hos en bruger.

Der er ikke kendskab til eller indikationer på, at sårbarheden er blevet udnyttet af hackere.

Den almindelige professionelle procedure omkring håndtering af sådanne sårbarheder er, at leverandøren af produktet informeres om sårbarheden, og at sårbarheden offentliggøres ca. 45 dage herefter. Dette giver leverandøren tid til at rette fejlen og foretage det fornødne i relation til brugerne. Sårbarheder af denne type fjernes normalt ved, at fejlen rettes af leverandøren, og leverandøren oplyser herefter brugerne om, at der skal foretages en softwareopdatering af det pågældende program.

TDC har inden for den givne tidsfrist rettet fejlen i softwarekomponenten og frigivet en sikkerhedsopdatering, der lukker sårbarheden i softwarekomponenten. Oplysning om sårbarheden er foregået ved udsendelse af information til pressen den 5. maj 2006, og efterfølgende udsendelse af e-mails med den fornødne vejledning til alle brugere. Alle brugere har den 8. maj 2006 modtaget en e-mail fra TDC. Softwarekomponenten bliver automatisk opdateret, når en bruger klikker på en hjemmesideadresse i e-mailen fra TDC, eller når en bruger flytter eller fornyr den digitale signatur.

På baggrund af de fra TDC modtagne informationer er det IT- og Telestyrelsens vurdering, at fejlrettelserne er gennemført professionelt, og at opdateringen hos brugerne vil kunne foregå rimeligt problemfrit.

Når opdateringen er foretaget, vil brugerne derfor trygt kunne fortsætte med at anvende den digitale signatur.

På baggrund af TDC's redegørelse har IT- og Telestyrelsen bedt TDC om at gennemgå og dokumentere relevante kvalitetssikringsprocesser med henblik på at minimere sandsynligheden for tilsvarende fejl i fremtiden.

Det er selvfølgelig beklageligt, at leverandørerne laver fejl i software, men det er en risiko, som vi er nødt til at leve med, hvad enten fejlene stammer fra TDC's software eller Microsofts software. Microsoft har f.eks. inden for de seneste 11 måneder udsendt i alt 32 sikkerhedsopdateringer vedrørende sårbarheder af lignende art.

Derfor er brugerne af pc'er nødt til løbende at foretage sikkerhedsopdateringer i takt med at sårbarheder opdages. Dette bliver brugerne gjort opmærksom på, når de bestiller en digital signatur, ligesom bl.a. vejledninger og oplysningskampagnen "netsikker nu" omtaler problemet."

Justitsministeriet kan henholde sig udtalelsen fra Ministeriet for Videnskab, Teknologi og Udvikling.

Som det fremgår af pkt. 4.2.2. i de almindelige bemærkninger til lovforslaget, har Videnskabsministeriet over for Justitsministeriet oplyst, at OCES-signaturen teknisk set er opbygget ved

brug af en avanceret matematisk algoritme, der i forhold til det nuværende teknologiske udviklingsniveau og den nuværende datakraft almindeligvis formodes at være tilstrækkeligt sikker i 5-6 år frem i tiden. Der er således ikke i dag kendte eksempler på, at det er muligt at bryde de koder, der sikrer autenticiteten og integriteten af et digitalt dokument, der er påført en digital OCES-signatur. Hertil kommer, at gyldighedsperioden for en OCES-signatur er begrænset til 2 år, hvorefter den vil skulle fornys. Leverandøren af OCES-signaturen er i øvrigt forpligtet til at tage højde for usikkerhed, der muligvis vil kunne opstå inden for den nævnte 5-6 årige periode.

Endvidere fremgår det, at Videnskabsministeriet løbende vil foretage vurderinger af OCES-signaturens sikkerhed. Hvis det skulle vise sig at være nødvendigt, vil der i medfør af den foreslåede bemyndigelsesbestemmelse i tinglysningslovens § 7, stk. 4, jf. lovforslagets § 1, nr. 6, administrativt kunne ændres i de tekniske krav, der stilles til digitale signaturer, der anvendes til tinglysning. Det muliggør, at sikkerheden ved digital tinglysning vil kunne fastholdes på et tilstrækkeligt højt niveau.