Videnskabsministerens talepunkter til samråd UVT alm. del onsdag den 9. november 2005 vedrørende sikkerheden i den digitale signatur

1. Hvad er status på sikkerheden i den digitale signatur?

Lad mig indledningsvis slå fast, at sikkerheden omkring den softwarebaserede digitale signatur er god.

Brugeren skal sikre, at pc og programmer er beskyttet mod kendte trusler og angreb.

Brugeren skal også efterleve de nødvendige forholdsregler om beskyttelse af signaturnøglen og aktiveringskoden.

Hvis brugeren sørger for disse to ting, er risikoen er minimal.

Lad mig også understrege, at der ikke findes it-systemer eller digitale signaturer, der er 100 % sikre.

Selv Pentagon har været udsat for hackerangreb på nogle af deres it-systemer.

De eksisterende manuelle papirbaserede systemer og underskrifter er heller ikke 100 % sikre.

Dette blev f.eks. tydeligt dokumenteret ved Trads/Lublin-sagen og de forfalskede underskrifter.

Der er således altid en vis risiko for misbrug af systemer.

Denne risiko skal naturligvis nøje afvejes med omkostninger til sikkerhedsforanstaltninger og konsekvenser ved et evt. sikkerhedsbrist.

Det er da også disse overvejelser, der har ligget til grund for regeringens tilbud om en digital signatur til borgere og virksomheder.

Formålet med signaturen har været, at den skal være let at anvende inden for de fleste områder af digital forvaltning.

Signaturen er derfor som udgangspunkt en såkaldt softwarebaseret signatur.

Signaturnøglen lagres på en pc og beskyttes med en personlig aktiveringskode.

TV2 bragte torsdag den 13. oktober 2005 et indslag i nyhederne, hvor en sikkerhedsspecialist viste, at han kunne bryde ind på en læges pc og stjæle aktiveringskode og signaturnøglen.

Efter hvad jeg har fået oplyst, forsøgte sikkerhedsspecialisten sig med en række forskellige hackerangrebsmetoder.

Ved at sende en falsk e-mail og udnytte en kendt sårbarhed i et Microsoft produkt kunne specialisten indlægge et program på lægens pc.

Hermed kunne han få adgang til alt, hvad der lå på pc'en – herunder signaturnøglen.

Det er ikke nyt, at en dygtig hacker kan udnytte kendte sårbarheder og trænge ind og overtage kontrollen over en pc.

Sikkerhedsproblemet er således ikke direkte knyttet til den digitale signatur, men vedrører den generelle sårbarhed i pc'en.

Hvis pc'en havde fået installeret de seneste sikkerhedsopdateringer, ville angrebet ikke have haft succes.

Disse sikkerhedsopdateringer kan hentes gratis fra forskellige hjemmesider.

Mere end ½ million danskere har i dag en digital signatur, og der er - mig bekendt - ikke rapporteret et eneste tilfælde af misbrug eller forfalskning.

I den sammenhængen er det værd at bemærke, at der er det fornødne lovgrundlag, som vil kunne bringes i anvendelse i evt. misbrugssager.

TV2's demonstration viste en sikkerhedsbrist hos en læge.

Her må vi forvente, at de professionelle brugere er i stand til at oprette et forsvarligt sikkerhedsniveau på deres pc'er.

De skal jo også overholde persondataloven.

Hvis lægerne af en eller anden grund har problemer med sikkerhedsniveauet på deres pc'ere, findes der et alternativ til den softwarebaserede løsning.

Leverandøren af den digitale signatur tilbyder på kommercielle vilkår allerede i dag en løsning, hvor signaturen er indlejret i en hardware enhed.

En sådan løsning kan forhindre, at signaturen vil kunne kopieres fra denne enhed.

Anvendelsen af denne type løsning forudsætter stadig, at brugerne sikrer deres pc'er mod hackerangreb.

Århus amts praktiserende læger har f.eks. valgt at investere i anskaffelse af denne løsning.

Lad mig afrunde mit svar med at konkludere, at sikkerheden omkring den softwarebaserede digitale signatur er god og risikoen er minimal.

Men det forudsætter altså, at brugeren efterlever nogle enkle regler til sikring af pc'en.

2. Hvilke ændringer er planlagt for at forbedre sikkerheden i den digitale signatur?

Det er vigtigt at forstå, at der ikke findes hurtige og enkle løsninger, der med et trylleslag vil kunne skabe et 100 % sikret pc miljø.

Det er almindeligt anerkendt, at digital signatur indlejret i en hardware enhed – alt andet lige – er mere sikker end en softwarebaseret digital signatur.

Men omkostningerne hertil er også væsentligt større.

Derfor har Videnskabsministeriet sikret sig, at TDC - som er leverandør af den digitale signatur – kan tilbyde forskellige alternative løsninger.

TDC har etableret understøttelse for opbevaring af digital signatur på forskellige hardware enheder og tilbyder nu disse på kommercielle vilkår til erhvervssektoren og til borgere.

Det må forventes, at især de professionelle brugere vil tage disse løsninger til sig, hvor særlige forhold gør sig gældende.

Jeg ser det som en naturlig udvikling af informationssamfundet, at regeringen i fremtiden vil kunne tilbyde borgerne et elektronisk ID-kort med en mobil signatur.

Videnskabsministeriet har derfor i samarbejde med andre myndigheder igangsat et analysearbejde, der skal afdække mulighederne for, om sygesikringsbeviset kan udvikles til at indeholde en mobil digital signatur.

Brugerens adfærd er under alle omstændigheder et afgørende led i den samlede sikkerhed.

Relevant information og målrettet vejledning er derfor nøgleordet til at skabe en bedre sikkerhedskultur.

Videnskabsministeriet har allerede gennemført en lang række informations- og oplysningsinitiativer om it-sikkerhed rettet mod borgere, myndigheder og mindre virksomheder.

Flere af disse initiativer er permanente, og andre vil blive relanceret i forskellige sammenhænge.

Erfaringer herfra bliver løbende opsamlet, og initiativerne evalueres med henblik på hele tiden at sikre en optimal effekt for målgrupperne.

3. Hvad giver den seneste udvikling på området, ministeren anledning til af nye tiltag?

TV2's udsendelse har som tidligere nævnt ikke bragt ny viden frem om pc'ers sårbarhed eller afdækket sikkerhedsbrist i den digitale signatur.

Udsendelsen har derimod bidraget til at tydeliggøre, at en pc er sårbar over for angreb, hvis den ikke er sikret med de nødvendige sikkerhedsopdateringer, antivirusprogrammer etc.

Videnskabsministeriet skal derfor fortsat arbejde på, at der skabes en sikkerhedskultur, så borgere og virksomheder er i stand til at styre computeren uden om de største huller på informationsvejen.

På samme måde, som vi i den daglige færden instinktivt tager vores forholdsregler.

Vi ved,

- at man ikke skal opbevare koden til sit dankort ubeskyttet,
- at man ikke skal rejse fra en ulåst dør, og
- at ruder og døre i huset skal udskiftes, før det bliver alt for let for en indbrudstyv at åbne disse.

Videnskabsministeriet vil på baggrund af TV2's udsendelse målrette en oplysningsindsats over for de arbejdsgivere og læger, der via deres digitale signatur har adgang til andre personers data.

Videnskabsministeriet vil desuden etablere en hjemmeside til sårbarhedstest, hvor borgere kan kontrollere sikkerheden på deres pc'er.