Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Hermed fremsendes svar på spørgsmål nr. 8 og 9 (Alm. del) stillet af Udvalget for Videnskab og Teknologi den 11. oktober 2010. Spørgsmålene er stillet efter ønske fra Hanne Agersnap (SF).

Med venlig hilsen

Charlotte Sahl-Madsen

9. november 2010

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr. 10-096083
Dok nr. 1573766

Spørgsmål nr. 8 og 9 stillet af Udvalget for Videnskab og Teknologi den 11. oktober 2010 til Ministeren for videnskab, teknologi og udvikling (Alm. del).

Spørgsmål 8

Hvilke krav til systemer og standarder er etableret for at sikre, at sider, hvorfra der kan bruges NemID, har et tilstrækkeligt højt sikkerhedsniveau, så NemID ikke kan kompromiteres via andres sites?

Svar

For så vidt, at spørgeren refererer til sikkerheden i selve NemID-løsningen, kan jeg oplyse, at den meget høje grad af sikkerhed og driftsstabilitet i NemID, som fra fællesoffentlig side er ønsket tilvejebragt, er afspejlet i den særdeles omfattende kontrakt, som Videnskabsministeriet på vegne af staten, KL og Danske Regioner har indgået med DanID. Det er således Videnskabsministeriet, som har ansvaret for gennem en erklæring fra en statsautoriseret revisor at påse, at de bestemmelser i kontrakten med DanID, som vedrører sikkerheden med videre i NemID, overholdes.

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr. 10-096083
Dok nr. 1573766

Jeg har indhentet følgende udtalelse fra IT- og Telestyrelsen:

"De overordnede standarder og aftaler vedrørende NemID beskrives i det følgende.

Af kontrakten, som Videnskabsministeriet har indgået med DanID om NemID fremgår blandt andet følgende krav til udstedelse af NemID. DanID er forpligtet til at efterleve en OCES-certifikatpolitik, som udarbejdes og administreres af IT- og Telestyrelsen. Certifikatpolitikken har været i offentlig høring. Certifikatpolitikken indeholder blandt andet krav om overholdelse af persondataloven og DS 484, der fællesoffentligt er valgt som standard for informationssikkerhed.

For at kunne udstede NemID skal udbyderen (her DanID) indgå en kontrakt med IT- og Telestyrelsen, hvori DanID blandt andet forpligter sig til at overholde certifikatpolitikken, herunder at blive revideret af ekstern statsautoriseret revisor og indgive årlig rapportering til IT- og Telestyrelsen, som påser overholdelse af certifikatpolitikken.

For så vidt angår en virksomhed eller myndighed (en såkaldt tjenesteudbyder), der ønsker at implementere adgang til sine systemer med brug af NemID, skal der som led i kunde-leverandørforholdet mellem DanID og tjenesteudbyderen indgås en såkaldt tjenesteudbyderaftale mellem DanID og tjenesteudbyderen om anvendelse af NemID-infrastrukturen. Tjenesteudbyderen har herved ansvaret for at overholde de krav, der stilles i tjenesteudbyderaftalen. Desuden har DanID udarbejdet informationsmateriale, som udstikker en række vejledninger og anbefalinger til, hvordan tjenesteudbyderne bør implementere NemID.

Offentlige tjenesteudbydere skal overholde DS 484.

Herudover skal såvel DanID som virksomheder og myndigheder som dataansvarlige naturligvis overholde relevante love, herunder Lov om behandling af personoplysninger, (persondataloven). Af denne lov § 41, Stk. 3 fremgår: "Den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere."

Datatilsynet fører tilsyn med overholdelse af persondataloven."

For så vidt spørgeren refererer til sikkerheden i de systemer, som myndigheder og virksomheder etablerer, og hvor de bruger NemID som adgangsnøgle, kan jeg oplyse, at hver myndighed og privat virksomhed selv har det fulde ansvar for sikkerheden i deres egne systemer. Eksempelvis er det Økonomistyrelsen, som er ansvarlig for sikkerheden i NemLog-in, ligesom det er SKAT eller SU-styrelsen, som anvender NemID via NemLog-in, der har ansvaret for, at deres løsning bliver afsluttet på en sikker måde.

I denne forbindelse skal myndigheder og virksomheder naturligvis leve op til gældende lovgivning og sikkerhedsstandarder. Eksempelvis stiller forvaltningsloven krav til offentlige myndigheder om fortrolighed ved håndtering af borgernes data, og persondataloven opstiller en række krav til alle, det vil sige også til offentlige myndigheder og private virksomheder, der håndterer personoplysninger, om at sikre, at oplysningerne behandles sikkerhedsmæssigt forsvarligt. Ansvaret for egne løsninger omfatter også sikkerheden i forbindelse med, at systemerne indrettes til at modtage NemID.

IT- og Telestyrelsen har i øvrigt den opgave, at yde generel rådgivning til borgere og virksomheder om it-sikkerhed. Denne opgave løses blandt andet i den årlige netsikker nu!-kampagne. Herudover vedligeholder IT- og Telestyrelsen på sin hjemmeside en lang række råd og vejledninger om netsikkerhed til borgere og virksomheder.

Lad mig til sidst nævne, som jeg også oplyste i det åbne samråd den 7. oktober 2010, at vi har nedsat en tværoffentlig beredskabsgruppe, som kan sikre, at der hurtigt igangsættes en afhjælpning og en udmelding til offentligheden, hvis der indtræder en utilsigtet hændelse, som kan have negativ betydning for borgernes oplevelse af, at det er trygt at benytte NemID og de offentlige løsninger, der er knyttet hertil.

Spørgsmål 9

Hvem har ansvaret for at NemID ikke kompromiteres fra login sites, f.eks. ved at der ikke er log ud krav eller automatik?

Svar

I forlængelse af mit svar på spørgsmål 8 kan jeg sammenfatte, at Videnskabsministeriet på vegne af et fællesoffentligt samarbejde har indgået en kontrakt med

leverandøren DanID om leverancen af NemID. Denne kontrakt indeholder høje krav om driftsstabilitet og sikkerhed. IT- og Telestyrelsen påser gennem en statsautoriseret revisors erklæring i overensstemmelse med den indgåede kontakt, at leverandøren varetager ansvaret for sikkerhed i udvikling og drift af NemID.

DanID har ansvaret for at overholde den indgåede kontrakt med Videnskabsministeriet samt i henhold til kontrakten at implementere og driftsafvikle NemID i overensstemmelse med best practice og DS 484. Som beskrevet i kontrakten mellem DanID og Videnskabsministeriet har DanID endvidere ansvaret for at overholde persondataloven, der via sikkerhedsbekendtgørelsen stiller særlige krav til systemer, der opbevarer og behandler persondata.

En virksomhed eller en myndighed, der anvender NemID som indgang til sine løsninger, har ansvaret for at sikre, at relevante love overholdes, herunder ikke mindst persondataloven. Offentlige myndigheder skal herudover overholde den fællesoffentligt aftalte standard for informationssikkerhed, DS 484.

Det er således virksomheden eller myndigheden, der anvender NemID, der har ansvaret for at sikre, at løsninger, der anvender NemID, bliver afsluttet på en sikker måde.

Jeg henviser i øvrigt til det eksempel, som er nævnt i min besvarelse af spørgsmål 8.