

Simon Bruun Hervik

Emne: PWC vurderingsnotat

Fra: Charlotte Jacoby
Sendt: 10. september 2014 09:56
Til: 'mpo@pwc.dk'
Cc:
Emne: PWC vurderingsnotat

Kære Martin Mølgård Povlsen,

Digitaliseringsstyrelsen har modtaget PWC's vurdering af Nets' risikoanalyse af evt. ændring af minimumskrav til passwords i NemID løsningen fra 6 til 4 karakterer.

Der er nogle punkter i PWC's vurdering, der giver anledning til uklarhed, og Digitaliseringsstyrelsen har derfor nogle opklarende spørgsmål.

PwC konkluderer, at risikovurderingens konklusion "...er retvisende, såfremt de foreslæde kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet."

I indledningen skriver PwC endvidere, at PWC ikke har "...vurderet styrken og effektiviteten af de foreslæde kompenserende tiltag".

På baggrund af disse to udsagn, forekommer det, at der er to mulige fortolkninger af notatet:

1. PwC har *ikke* vurderet sikkerheden i den fremtidige løsning, men alene vurderet Nets's *beskrivelse af risici*. Med andre ord, PwC har ikke kigget på de kompenserende tiltag.
2. PwC har vurderet, at sikkerheden i den fremtidige løsning er i orden, *hvis* tiltagene implementeres, men at PwC ikke ved selvsyn har kunnet konstatere, om tiltagene rent faktisk er implementeret.

Denne uklarhed, er en svaghed i PwC's vurdering, som Digitaliseringsstyrelsen ønsker afklaret.

Digitaliseringsstyrelsen har yderligere følgende afklarende spørgsmål:

PwC skriver: "Hvad angår angreb *mod en bruger*, er vi af den opfattelse, at der ikke er udeladt væsentlige risici". Hvad betyder "mod en bruger"? Er det i modsætning til "mod Nets" (altså insider-angreb)? Det er meget uklart, om PwC her begrænser scope af vurderingen, eller om det blot er uheldigt formuleret.

Det spørgsmål, som Digitaliseringsstyrelsen grundlæggende ønsker afklaret ved notatet, er, om sikkerheden i den fremtidige NemID-løsning vil være på niveau eller bedre end sikkerheden i den nuværende løsning, hvis Nets' forslag til ændring af adgangskode-regler gennemføres, og der samtidig implementeres de kompenserende tiltag, som er beskrevet i risikovurderingen.

Styrelsen imødeser PWC's kommentarer.

Med venlig hilsen



DIGITALISERINGSSTYRELSEN

Charlotte Jacoby
Chefkonsulent

T 2287 9648

E chaja@digst.dk

Kontor for it-standardisering og sikkerhed

Digitaliseringsstyrelsen
Landgreven 4, Postboks 2193
1017 København K