Simon Bruun Hervik

Emne: VS: PWC vurderingsnotat

Fra: Mikael Buchholtz [mailto:MBZ@pwc.dk]
Sendt: 24. september 2014 13:39
Til: Charlotte Jacoby
Cc: [redacted], Mads Nørgaard Madsen
Emne: Re: VS: PWC vurderingsnotat

Kære Chalotte

Vedrørende dit første spørgsmål, så har PwC har vurderet de kompenserende tiltag, der er beskrevet i risikoanalysen "Risikoanalyse for ændring af passwords i NemID".

Vi vurderer at risikoanalysens konklusioner, der blandt andet omhandler de kompenserende tiltag, "...er retvisende, såfremt de foreslåede kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet."

Vi har ikke vurderet hvorvidt de kompenserende tiltag implementeres med tilstrækkelig styrke og kvalitet.

Vedrørende dit andet spørgsmål, så har PwC vurderet, at der ikke er udeladt væsentlige risici i risikoanalysen.

Formuleringen "mod en bruger" er ikke en begrænsning af at scopet for vores vurdering, men henviser tilbage til risikoanalysens beskrivelse af risici og skal tolkes i sammenhæng med den øvrige tekst i afsnittet.

Jeg håber at dette besvarer jeres spørgsmål.

Med venlig hilsen / Best regards

Mikael Buchholtz
PwC | Senior Manager - PhD, MScEng, ESL
Consulting
D: +45 3945 3544 | M: +45 2460 6330
Email: mbz@pwc.dk | www.pwc.dk
Strandvejen 44, DK-2900 Hellerup

From: Charlotte Jacoby <chaja@digst.dk>
To: "MXM@pwc.dk" <MXM@pwc.dk>
Cc: [redacted]@nets.eu>, "MBZ@pwc.dk" <MBZ@pwc.dk>
Date: 23-09-2014 10:20
Subject: VS: PWC vurderingsnotat

Kære Mads Nørgaard Madsen,

Efter aftale med Nets DanID genfremsendes spørgsmål til PWC's vurderingsnotat.

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

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

Kære Martin Mølgård Povelsen,

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 foreslåede kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet."
I indledningen skriver PwC endvidere, at PWC ikke har "...vurderet styrken og effektiviteten af de foreslåede 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