

Simon Bruun Hervik

Emne:

SV: Kommende POCES-certifikatpolitik (DIGST Id nr.: 550284)

Hej Simon

Det er ok – vi har ikke nogen indvendinger mod, at der gives aktindsigt i kommunikationen som er vedhæftet.

Best regards

Nets Denmark A/S
Lautrupbjerg 10, DK-2750 Ballerup
www.nets.eu

From: Simon Bruun Hervik [mailto:sibrh@digst.dk]
Sent: 23. maj 2016 15:24
Cc: Charlotte Jacoby; Thomas Vangsaa
Subject: VS: Opfølgende anmodning om aktindsigt

Hej,

Vi har modtaget en opfølgende anmodning om aktindsigt fra Christian Panton.

Det drejer sig om aktindsigt i den kommunikation, som er foregået mellem Nets DanID og Digitaliseringsstyrelsen ved Christian Pantons første anmodning om aktindsigt - sikkerhedsvurderingen af ændringerne i password krav på NemID.

Vedhæftet er materialet, som vi mener, der kan gives aktindsigt i. Jeg vil bede jer kommentere på, om der er noget væsentligt, I mener bør undtages.

Mvh
Simon

Det er ok – blot I sikrer jer det udstregede ikke kan læses. Jeg kan læse noget af det nu

-----Oprindelig meddelelse-----

Fra: Charlotte Jacoby
Sendt: 18. maj 2016 13:49
Cc: Simon Bruun Hervik; Thomas Vangsaa
Emne: Aktindsigt Panton

Hej
Her er vores bud på, hvad vi mener, der kan gives aktindsigt i. Vi har markeret med gult, hvad vi vil foreslå at undtage.

Jeg vil gerne understrege, som nævnt i min tidligere mail, at det ud over af sikkerhedsmæssige grunde, specifikt var med henblik på at have noget at læne os op ad, når 6->4 kom og ville blive kritiseret, at vi bad om disse vurderinger. Derudover kan vi kun undtage specifikke og konkrete tekster og informationer om sikkerheden og risikoen, som kan virke kompromitterende for løsningen. Det er baggrunden for vores bud på undtagelser. Hvis I mener, at der skal undtages yderligere, vil jeg bede om konkrete begrundelser herfor.

Da vi har frist i morgen, vil jeg bede om jeres kommentarer senest med udgangen af i dag.

Vh
Charlotte

-----Oprindelig meddelelse-----

Fra: Charlotte Jacoby
Sendt: 18. maj 2016 13:49
Cc: Simon Bruun Hervik; Thomas Vangsaa
Emne: Aktindsigt Panton

Hej

Her er vores bud på, hvad vi mener, der kan gives aktindsigt i. Vi har markeret med gult, hvad vi vil foreslå at undtage.

Jeg vil gerne understrege, som nævnt i min tidligere mail, at det ud over af sikkerhedsmæssige grunde, specifikt var med henblik på at have noget at læne os op ad, når 6->4 kom og ville blive kritiseret, at vi bad om disse vurderinger. Derudover kan vi kun undtage specifikke og konkrete tekster og informationer om sikkerheden og risikoen, som kan virke kompromitterende for løsningen. Det er baggrunden for vores bud på undtagelser. Hvis I mener, at der skal undtages yderligere, vil jeg bede om konkrete begrundelser herfor.

Da vi har frist i morgen, vil jeg bede om jeres kommentarer senest med udgangen af i dag.

Vh
Charlotte

-----Oprindelig meddelelse-----

Fra: Charlotte Jacoby
Sendt: 18. maj 2016 09:08
Cc: Thomas Vangsaa; Simon Bruun Hervik
Emne: SV: Sv: Kommende POCES-certifikatpolitik (DIGST Id nr.: 550284)

Hej

Det er jeg ked af at høre.

Nu kigger vi på det, men jeg tænker, at det kan blive svært at forsvare at undtage alt.

Det var også forudsætningen, da vi anmodede om en sikkerhedsvurdering, at vi skulle have noget at læne os op ad.

Så kan det jo ikke nytte noget, at vi ikke vil vise noget.

Vi vender tilbage med vores vurdering, som I så må forholde jer til med det samme, for nu haster det ifht. vores frister.

Vh
Charlotte

-----Oprindelig meddelelse-----

Sendt: 18. maj 2016 08:55
Til: Thomas Vangsaa

Emne: RE: Sv: Kommende POCES-certifikatpolitik (DIGST Id nr.: 550284)

Hej Thomas

Vi har nu internt drøftet denne sag og vores konklusion er, at vi opfatter dokumenterne som fortrolige af sikkerhedsmæssige årsager og ønsker dem behandlet på linje med den løbende risikorapportering, der ligeledes er undtaget aktindsigt.

Det kan begrundes yderligere med, at dokumenterne opstiller udtømmende lister og risici og beskriver hvordan vi vurderer og mitigerer disse. Det vil efter vor mening give personer med uærlige hensigter for megen indsigt. I forhold til PWC's vurderingsnotat "Risikoanalyse for ændring af password i NemID" mener vi også dette skal undtages, idet der øverst side 2 er et resume af sikkerhedsanalysen, det fremgår at vi arbejder med 10 risikoområder, det fremgår hvornår den seneste risikovurdering er foretaget, det fremgår at vi gennemfører kompenserende foranstaltninger og at disse kan have varierende styrke og kvalitet. Herudover giver notatet et overordnet billede af, hvordan vi anskuer sikkerhed, hvordan vi tilgår det, og hvilke parametre vi opfatter som de styrende.

Best regards

Nets Denmark A/S
Lautrupbjerg 10, DK-2750 Ballerup
www.nets.eu

-----Oprindelig meddelelse-----

Fra: Thomas Vangsaa
Sendt: 9. maj 2016 13:57
Cc: Charlotte Jacoby
Emne: VS: Sv: Kommende POCES-certifikatpolitik (DIGST Id nr.: 550284)

Hej

Vi har sendt nedenstående svar til Christian Panton, og i den forbindelse har han svaret retur og beder om aktindsigt i sikkerhedsvurderingen.

Vil i vurdere, om der er dele af den samlede sikkerhedsvurderingen der skal undtages fra aktindsigt?

Umiddelbart består sikkerhedsvurderingen af jeres sikkerhedsvurdering, PWC's vurdering samt efterfølgende korrespondance mellem DIGST og PWC.

Med venlig hilsen

Thomas Vangsaa
Specialkonsulent

M 4178 2137
E thova@digst.dk
www.digst.dk

Center for systemforvaltning og sikkerhed Landgreven 4, Postboks 2193
1017 København K
Tlf. 3392 5200

-----Oprindelig meddelelse-----

Fra: Christian Panton [mailto:christian@panton.org]

Sendt: 9. maj 2016 13:51

Til: Thomas Vangsaa

Emne: Re: Sv: Kommende POCES-certifikatpolitik (DIGST Id nr.: 550284)

Kære Thomas Vangsaa,

Jeg vil gerne bede om aktindsigt i den omtalte sikkerhedsvurdering.

Mvh

Christian Panton

On Mon, May 09, 2016 at 01:48:18PM +0200, Thomas Vangsaa wrote:

> Kære Christian Panton

>

> Tak for din henvendelse vedr. de ændrede adgangskodekrav for NemID og

> de medfølgende spørgsmål, som er adresseret nedenfor.

>

> 1) Der er ikke på nuværende tidspunkt igangsat et arbejde om revision

> af OCES-certifikatpolitikken for Personcertifikater.

>

> 2) Der er således ikke blevet sendt noget materiale i høring. Såfremt

> en revision bliver igangsat vil den også omfatte en bred offentlig høring.

>

> 3) Digitaliseringsstyrelsen har været inddraget i forbindelse med de

> ændrede adgangskodekrav. Digitaliseringsstyrelsen har i den

> forbindelse stillet krav om en ekstern sikkerhedsvurdering af NemID fra en uvildig tredjepart.

>

> Det konkluderes i den forbindelse, at NemID fortsat har et højt

> sikkerhedsniveau som hidtil, da de ændrede adgangskodekrav suppleres

> med indførelsen af mitigerende tiltag, som bl.a. inkluderer spærring

> ved 3 forkerte forsøg mod de tidligere 5 forsøg og krav til

> adgangskoden, så der ikke kan vælges fire ens cifre, en fortløbende

> talrække eller en talrække fra CPR-nummeret. Styrelsen har på baggrund

> af den samlede sikkerhedsvurdering besluttet at dispensere fra kravet i certifikatpolitikens pkt. 7.2.8.

>

> 4) I forhold til din anmodning om aktindsigt, kan styrelsen informere

> om, at der ikke på nuværende tidspunkt er igangsat et arbejde om

> revision af OCES-certifikatpolitikken for Personcertifikater. Der er

> således ikke blevet sendt noget materiale i høring.

>

> Med venlig hilsen

> Thomas Vangsaa

>

> Digitaliseringsstyrelsen

> Landgreven 4, Postboks 2193

> 1017 København K

> Tlf. 3392 5200

>

>