DIGITALISERINGSSTYRELSEN

30. maj 2016
CSS /HELKO

Datatilsynet

Borgergade 28, 5.

1300 København K

Svar på henvendelse vedrørende den sikkerhed, der opnås ved brug af NemID

Hermed følger svar på Datatilsynets henvendelse til Digitaliseringsstyrelsen d. 12. maj 2016 vedrørende ændring af krav til adgangskode i forbindelse med NemID.

På baggrund af erfaringer omkring brugervenlighed i bankerne, er det besluttet at gennemføre en ændring i kravet til den personlige adgangskode til NemID, så anvendelsen bliver mere enkel og brugervenlig, særligt fra de mobile platforme. Brugerne vil derfor fra omkring 15. juni kunne vælge at ændre deres adgangskode til fire cifre, hvis det ønskes. Brugerne kan også vælge at bevare deres eksisterende adgangskode.

Digitaliseringsstyrelsen har forud for godkendelse af beslutning herom anmodet Nets DanID om at foretage en grundig risikoanalyse og vurdering af eventuelle sikkerhedsrisici ved ændringen. Nets DanID's risikoanalyse er tillige blevet vurderet af en ekstern tredjepart. Det fremgår heraf, at NemID med ændringen fortsat til have et højt sikkerhedsniveau forbundet med to faktor autentifikation. Risikoanalyse og ekstern vurdering vedlægges dog er selve gennemgangen af risici og mitigering undtaget, jf. vedlagte version, som også er udleveret til aktindsigt.

Herunder besvares de tre stillede spørgsmål:

1) Ændringen gælder for den samlede NemID løsning og hermed også for NemID til offentlig digital signatur (OCES). Det er dog vigtigt at påpege, at der i forbindelse med anvendelse af den offentlige digitale signatur altid anvendes login med to faktorer i overensstemmelse med OCES-certifikatpolitikken.

2) Der bliver således fortsat udelukkende givet adgang til personlige og følsomme oplysninger i offentligt regi med anvendelse af brugernavn og adgangskode kombineret med brugen af nøglekort.

   Der er som nævnt gennemført en grundig risiko-analyse i forbindelse med ændringen af krav til adgangskode. Analysen konkluderer, at NemID

fortsat vil være på et højt sikkerhedsniveau selvom, brugere fremover vælger at anvende en fire cifret kode, idet der dels fortsat er spærret for udtømmende søgning – nu allerede ved tre forkerte forsøg, dels er implementeret mitigerende sikkerhedstiltag fx i form af krav til adgangskoden, så der ikke kan vælges fire ens cifre, en fortløbende talrække eller en talrække fra CPR-nummeret, der sikrer, at løsningen stadig opnår et højt sikkerhedsniveau.

Den eksterne vurdering gennemgår denne analyse, og konklusionen er, at det vil være muligt at fastholde det høje sikkerhedsniveau, så længe Nets DanID gennemfører de fremlagte sikkerhedsforanstaltninger, jf. vedlagte vurdering fra PWC.

Nets DanID har over for styrelsen bekræftet, at dette er tilfældet.

3) Digitaliseringsstyrelsen har valgt at give dispensation i forhold til kravet i OCES-Certifikatpolitik for Personcertifikater vers. 4, punkt 7.2.8 samt OCES-Certifikatpolitik for Medarbejdercertifikater vers. 5 punkt 7.2.8:

> ”Såfremt certifikatindehaverens nøglepar efter generering opbevares centralt hos CA skal følgende opfyldes:
>
> Adgangskoden skal vælges fra et udfaldsrum på mindst 36^6 mulige koder, for eksempel som 6 tegn valgt ud af 36 bogstaver, tal og specialtegn.”

Beslutningen om ændring og dispensation er truffet på baggrund af konklusionerne i risikovurderingen, hvor også spørgsmålet om insider trusler er behandlet.

Yderligere kan styrelsen oplyse, at der planlægges en mindre revisionsopdatering af Certifikatpolitikkerne frem mod ikrafttrædelse af eIDAS-forordningen, hvor ovenstående bestemmelse forventes revideret.

Med venlig hilsen

Charlotte Jacoby
Kontorchef