DATATILSYNET

Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K

Sendt via Digital Post

2. juni 2016

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2016-632-0186
Sagsbehandler
Lena Andersen
Direkte 3319 3250

Vedrørende sikkerheden ved brug af NemID

Datatilsynet blev via medieomtale bekendt med planerne om at ændre på login i forbindelse med brug af NemID. Datatilsynet vurderede umiddelbart, at ændringen af sikkerheden omkring login kunne have betydning, når NemID anvendes i bl.a. offentlige myndigheders løsninger, hvor sikkerheden skal leve op til persondatalovens krav om datasikkerhed og datakvalitet, dvs. persondatalovens § 41, stk. 3, og § 5, stk. 4. I den anledning anmodede Datatilsynet den 12. maj 2016 Digitaliseringsstyrelsen om en redegørelse.

Digitaliseringsstyrelsen har den 30. maj 2016 sendt Datatilsynet den ønskede redegørelse. Til svaret var vedlagt en risikoanalyse og ekstern vurdering.

Digitaliseringsstyrelsen har bl.a. oplyst, at der er gennemført en grundig risikoanalyse i forbindelse med ændringen af kravet til den personlige 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.

I den eksterne vurdering fra PwC er konklusionen, at PwC ikke har fundet anledning til at tro, at konklusionen i det udleverede notat fra Nets ikke er retvisende, såfremt de foreslåede kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet.

Datatilsynet skal på den baggrund understrege, at ansvaret for, at datasikkerheden i forbindelse med NemID til offentlig forvaltning er tilstrækkelig høj, efter tilsynets opfattelse ligger hos såvel certificeringscentret som Digitaliseringsstyrelsen, jf. herved også tilsynets udtalelse[1] af 3. april 2009 om OCES II løsningen.

Efter Datatilsynets opfattelse er der derfor behov for, at Digitaliseringsstyrelsen følger implementeringen af de kompenserende tiltag nøje og sikrer sig, at

[1] https://www.datatilsynet.dk/afgoerelser/afgoerelsen/artikel/datatilsynets-udtalelse-vedroerende-oces-ii-loesningen/

disse som anført af PwC implementeres med en tilstrækkelig styrke og kvalitet.

De kompenserende tiltag omfatter så vidt ses: 1) implementering af diverse tekniske faciliteter, 2) ændring af brugerregler og password politik og 3) en anbefaling af, at banker evaluerer deres tjenester og hvilken information der gives adgang til på baggrund af login med 1- faktor. Personhenførbare data såsom cpr-nummer og mobilnummer bør ikke vises.

Datatilsynet har umiddelbart følgende bemærkninger i den forbindelse:

Ad 1. Diverse tekniske faciliteter. Datatilsynet skal pege på behovet for, at Digitaliseringsstyrelsen påser, at disse implementeres som beskrevet, og at der herunder indhentes en ekstern parts vurdering af, om dette er sket.

Ad 2. Ændring af brugerregler og password politik. Efter Datatilsynets opfattelse må effekten af disse tiltag ses i lyset af, hvorvidt brugerne rent faktisk ser, forstår og iagttager de nye retningslinjer. Efter Datatilsynets umiddelbare opfattelse må dette som minimum forudsætte, at ændringerne sker på en måde, hvor de relevante ændringer er ganske tydelige for hver enkelt bruger, og at der indhentes en positiv bekræftelse fra brugeren om, at denne har set og forstået disse ændringer, samt at kun de brugere, der positivt har bekræftet ændringerne, får mulighed for at ændre deres adgangskode til fire cifre.

Ad 3. Anbefalingen om, at personhenførbare data såsom cpr-nummer og mobilnummer ikke bør vises ved login med 1-faktor. Datatilsynet finder det umiddelbart uklart, hvad der sigtes til, når begrebet "personhenførbare data" anvendes her. Efter Datatilsynets opfattelse er personhenførbare data lig med personoplysninger og omfatter også eksempelvis oplysninger om personers banktransaktioner. Datatilsynet har i øvrigt noteret sig det oplyste om, at der i forbindelse med anvendelse af den offentlige digitale signatur altid anvendes login med to faktorer i overensstemmelse med OCES-Certifikatpolitikken.

Datatilsynet kan i øvrigt konstatere, at Digitaliseringsstyrelsen efter det oplyste **har godkendt** beslutningen om at ændre kravene til adgangskoden, og at styrelsen har **valgt at give dispensation** i forhold til krav i OCES-Certifikatpolitik for Personcertifikater vers. 4, punkt 7.2.8 samt OCES-Certifikatpolitik for Medarbejdercertifikater vers. 5 punkt 7.2.8

På den baggrund har Datatilsynet besluttet sig for at foretage følgende tilføjelse på tilsynets hjemmeside, hvor tilsynets udtalelse om OCES II er offentliggjort:

> "Efterfølgende har Digitaliseringsstyrelsen godkendt ændringer til løsningen og dispenseret fra certifikat-politikken. Datatilsynets udtalelse vedrører løsningen, som den blev forelagt for tilsynet."

Datatilsynet skal endvidere anmode om, at alle tekster, der giver udtryk for, at Datatilsynet har godkendt sikkerheden bag NemID fjernes fra Digitaliseringsstyrelsens og Nets' hjemmesider herunder:

- ”Med OCES-certifikatet er der ifølge Datatilsynet skabt den nødvendige garanti for, at alle almindelige transaktioner mellem myndighed og borgere kan foregå tilstrækkelig sikkert.” på denne side http://www.digst.dk/Loesninger-og-infrastruktur/NemID/Jura-og-standarder
- ”Nets DanID har fået godkendt sikkerheden bag NemID medarbejdersignatur af Datatilsynet.” på denne side https://www.nets.eu/dk-da/løsninger/nemid/medarbejdersignatur/sikker-e-mail
- ”**Godkendt af Datatilsynet** Med OCES-certifikatet er der ifølge Datatilsynet skabt den nødvendige garanti for, at alle almindelige transaktioner mellem myndighed og borgere kan foregå tilstrækkelig sikkert.” på denne side https://www.nemid.nu/dk-da/digital_signatur/oces-standarden/

Afslutningsvis skal det for god ordens skyld oplyses, at Datatilsynet forventer at omtale denne udtalelse på sin hjemmeside.

Med venlig hilsen

Lena Andersen
Kontorchef