pwc

Nets – DanID

Vurdering af "Risikoanalyse for ændring af password i NemID"

Baggrund

I forbindelse med etablering og udrulning af en Java Script-baseret klient til NemID er det blevet praktisk muligt at anvende standardklienten på mobile enheder og på sigt på en række ikke pc-orienterede devices. Fælles for disse er, at det kan være meget besværligt eller upraktisk at indtaste et password, der lever op til de nuværende regler for kompleksitet.

Der er derfor i den finansielle sektor et ønske om at genvurdere kravet til passwords, således at der kunne anvendes et firecifret password i stedet for et password på seks karakterer.

PwC er blevet bedt om at vurdere den risikovurdering, som Nets har udarbejdet for ændringen i password-kompleksitet: "Risikoanalyse for ændring af password i NemID" af d. 22. august 2014. I nærværende notat vil vi redegøre for vores vurdering.

Vi har baseret vores vurdering på det udleverede notat. Vi har således ikke haft mulighed for at vurdere styrken og effektiviteten af de foreslåede kompenserende tiltag.

Sammenfatning af vores vurdering

Ved vores gennemgang af notatet har vi særligt lagt vægt på den ændring i arkitektur, der er sket siden 1. generation af OCES. Oprindeligt var løsningen baseret på lokalt opbevarede private nøgler, som skulle beskyttes på brugerens pc, og hvor sikkerheden i høj grad var en funktion af passwordet og beskyttelsen af den enkelte maskine, som var uden for NemID's kontrol.

Password-kompleksiteten var derfor den vigtigste beskyttelsesfaktor i den oprindelige løsning.

I dag anvendes der centralt opbevarede private nøgler, hvor både password og nøglekort[1] bidrager til den samlede sikkerhed, men bliver yderligere forstærket af muligheden for sikker programmatisk kontrol med password-afgivelsen samt løbende overvågning og alarmering. Dette giver mulighed for at mindske password-kompleksiteten, da der er etableret andre sikkerhedsmekanismer, som tilsammen kan give en tilstrækkelig sikkerhed.

Det tilbageværende spørgsmål er derfor, om den foreslåede kompleksitet på fire cifre er tilstrækkelig til at supplere de øvrige tiltag, således at den samlede sikkerhed niveau vil være det samme eller højere, efter de foreslåede kompenserende tiltag er implementeret.

---

[1] Ved anvendelse af NemID i f.eks. den finansielle sektor kan gives adgang til funktionalitet uden anvendelse af Nøglekort, men denne er begrænset til ikke kritisk læseadgang. Dette er dog ikke relevant for OCES.

Dette er der redegjort for i notatet, hvor der er fremhævet ti væsentlige risikoområder.

Vi har vurderet om disse ti områder dækker alle relevante risici, hvorvidt disse er tilstrækkeligt belyste, og om vi er enige i konklusionen på hvert område. Vi vil nedenfor redegøre for vores vurdering.

Dækkes alle relevante risici (fuldstændighed)
Der er udvalgt risici, som direkte bliver påvirket ved ændring af password-kompleksitet, og fravalgt risici, som er ens uanset password-kompleksitet. Dog er der medtaget tre risici (g, h, i), som ikke vil blive påvirket, men som er password-relevante.

Hvad angår angreb mod en bruger, er vi af den opfattelse, at der ikke er udeladt væsentlige risici.

Er risiciene tilstrækkeligt grundigt belyste

Det vores opfattelse, at risiciene er tilstrækkeligt grundigt belyste, når de enkelte beskrivelser ses i sammenhæng med risikovurderingens indledende afsnit omkring "Password-styrke" og "Statistik og sandsynlighed for brugervalgte passwords".

Vurdering af konklusionen for de enkelte områder

Vi har vurderet, at konklusionerne for de enkelte områder er retvisende, såfremt de foreslåede kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet.

Konklusion
Vi har ved vores vurdering ikke fundet anledning til at tro, at notatets konklusion ikke er retvisende, såfremt de foreslåede kompenserende tiltag implementeres med en tilstrækkelig styrke og kvalitet.

nets

Notat Risikoanalyse for ændring af password i NemID

Nets Denmark A/S
Lautrupbjerg 10
P.O. 500
DK-2750 Ballerup

T +45 44 68 44 68
F +45 44 86 09 30
www.nets.eu

CVR-nr. 20016175

[redacted]

Til Digitaliseringsstyrelsen og DanID-udvalget

Review CA-Assurance og IT-solutions.

22. august 2014

Baggrund I forbindelse med den forestående levering af NemID JavaScript (JS)-klient, ' r der i de seneste måneder været drøftelser[redacted] den manglende brugervenlighed ved indtastning af password i NemID JS i forhold til bankernes eksisterende proprietære løsninger på de mobile platforme.

[redacted]om ændring af regler for password fra de nuværende minimumskrav om seks karakterer med alfanumeriske værdier til en 4-cifret talkode. Digitaliseringsstyrelsen har som følge heraf bedt Nets DanID udarbejde en risikoanalyse og anbefaling i forhold til dette ændringsforslag.

Dette notat indeholder en analyse af ændringsforslagets eventuelle påvirkning på sikkerheden, samt de tiltag Nets DanID anbefaler at der implementeres i NemID for at opveje den reducerede længde af password, således at det samlede aktuelle sikkerhedsniveau for NemID fastholdes.

Nuværende politik Ifølge Nets DanID's gældende password politik "User Id and policy, v.1.3" skal brugeren specificere et password til NemID, som er mellem 6 og 40 karakterer. Password'et kan bestå af en kombination af 26 mulige bogstaver, tallene fra 0 til 9 samt 24 specialtegn og skal indeholde mindst et tal og et bogstav. Der skelnes ikke mellem store og små bogstaver.[redacted]

Forslag til Ændringsforslaget fra bankerne går ud på at nedsætte minimumskravet til længden

ny politik og kompleksiteten af det brugervalgte password til et 4-cifret tal.

Konklusion Det er væsentligt både for Digitaliseringsstyrelsen, bankerne og Nets DanID, at den høje sikkerhed omkring NemID bibeholdes. Borgernes og omverdenens tillid til håndtering af sikkerheden omkring NemID er afgørende.

Ændringen vil givetvis skabe debat omkring sikkerheden om NemID. Nogen vil forventeligt hævde, at der er tale om en forringelse af sikkerheden, idet best practice er at have lange komplekse password i selvbetjeningsløsninger. Specielt når passwordet udgør den eneste adgangsgivende sikkerhedsforanstaltning. Nets DanID vurderer, at ændringen i krav til password kan opvejes af kompenserende tiltag, som er tilstrækkelige til at bibeholde samme sikkerhedsniveau.

Både bankerne og Digitaliseringsstyrelsen er jævnfør persondataloven forpligtet til at beskytte personfølsomme data med fornødne sikkerhedsforanstaltninger. Selvom det samlede tekniske sikkerhedsniveau opretholdes med kompenserende tiltag, er der risiko for kritik og bekymring, som skal imødegås.

[redacted]

Analyse af password styrke

Menneskers evne til at huske gode passwords med høj tilfældighed er begrænset. Det betyder, at passwords i praksis ikke er tilfældige.

Entropi[1] er et mål for tilfældighed, som kan bruges til udtale sig om kvaliteten af brugervalgte passwords, og dermed hvor svære de er for en angriber at gætte. Jo højere entropi des stærkere password. For den nuværende password politik er den beregnede entropi[2] 14 bit. Det betyder, at man i gennemsnit[3] skal søge gennem 2^13= 8192 password for at ramme brugerens password. Tilsvarende har en selvvalgt 4-cifret talkode 10 bits entropi, hvilket medfører at man i gennemsnit skal søge gennem 2^9= 512 password for at finde en brugers password. Til sammenligning skal man for en tilfældig valgt 4-cifret talkode, som eksempelvis en Dankort PIN kode, gennemsøge 10^4/2=5000 talkombinationer for at finde frem til den

[1] Entropi er et mål for tilfældighed af en stokastisk variabel. Entropien af password kan bruges til at beregne hvor mange password man forventer at skulle teste for at finde frem til det rigtige password.
[2] Entropi beregningerne er baseret på appendix A i NIST sp-800-63-2:"Electronic Authentication Guidelines"
[3] I gennemsnit skal man søge gennem halvdelen af mængden af passwords før end man finder det rigtige pw. Når entropien er 14 bit forventer man at skulle teste 2^(14-1)=2^13 passwords.

rette.

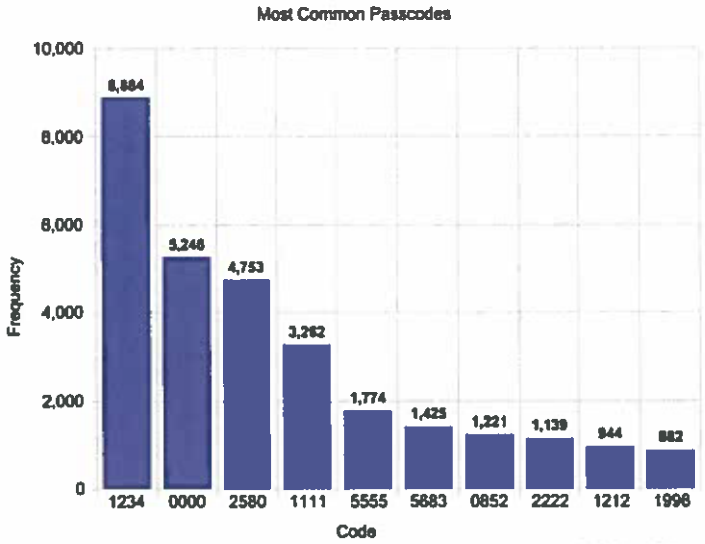
Entropi-beregningen tager imidlertid ikke højde for, at nogle password har en klar overrepræsentation, hvilket man i stedet kan belyse med password statistikker.

Statistik og sandsynlighed for brugervalgte password

Der findes forskellige undersøgelser som blandt andet baserer sig på lækkede og crackede password. Nedenfor er angivet to eksempler på sådanne statistikker. Første eksempel er taget fra www.lifehacker.com. Statistikkens grundlag er en lækket password database bestående af 3,4 millioner 4-cifrede passwords. Statistikken viser at password "1234" repræsenterer 10,713% af samtlige passwords i databasen. Det næstmest frekvente password er "1111" og repræsenterer 6,016% af databasens passwords. Samlet set repræsenterer de 5 mest brugte passwords 20,552% af hele databasen. Ved systematisk at gætte på disse fem passwords for alle brugere vil man finde frem til det rette password for hver femte bruger.

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

Næste eksempel er taget fra www.danielamitay.com, som er et projekt baseret på 204.508 iPhone passwords, registreret via en applikation. Statistikken begrænser sig ikke til 4-cifrede talkoder, hvilket sandsynligvis er grunden til de lavere procentuelle værdier.



Statistikken viser, at de ti mest brugte iPhone passwords samlet set repræsenterer 15% af alle registrerede passwords.

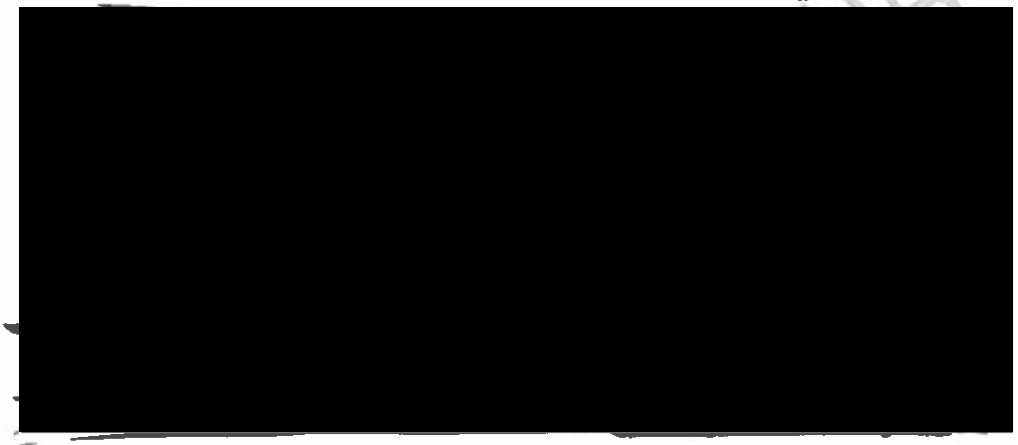
Risikoanalyse

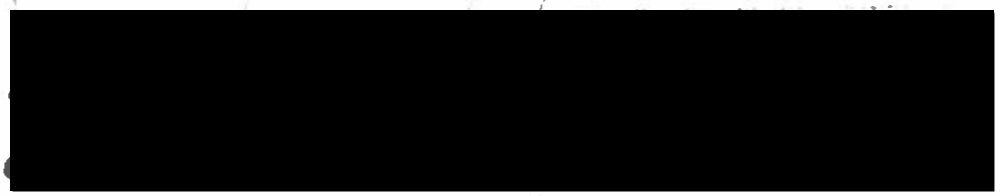
Trusselsaktører

Trusselsaktørerne vil være de samme aktører som kendes fra det generelle trusselbillede i NemID. Det vil primært være personer med intention om økonomisk kriminalitet og aktivister med interesse i at udstille sikkerheden omkring NemID som utilstrækkelig. Dertil kommer trusler som stammer fra betroede medarbejdere (insider) samt spionage og efterretningsvirksomhed.

[redacted]

[redacted]





[redacted]

Opsummering

Nets DanID har i de ovenstående afsnit analyseret risici ved ændrede krav til password og givet anbefalinger til sikkerhedsmæssige tiltag for at opretholde det høje sikkerhedsniveau som NemID er kendetegnet ved. Nets DanID anbefaler på denne baggrund, at det fremlagte ændringsforslag, herunder de kompenserende tiltag, vedtages, idet det samlede sikkerhedsniveau for NemID kan opretholdes.

Tabellen nedenfor giver et overblik over ændring i risici som følge af ændring af krav til password, Nets DanID's forslag til kompenserende tiltag og de heraf resulterende risici.