Anbefalinger om passwords

1 Baggrund

At sikre autentifikation vha passwords stiller krav til både bruger og tjenesteudbyder. I mange år har en stor del af byrden været placeret hos brugeren i form af krav til komplekse passwords, regelmæssig udskiftning, sikring mv. Dette har dog ikke givet bedre sikkerhed, og derfor er der sket et skift til at der stilles flere krav til tjenesteudbyderen og færre krav til brugeren. Dette skift ses tydelige i den seneste NIST standard: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf, som matcher et tilsvarende skift fra de britiske myndigheder; https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach. Endvidere har Center for Cybersikkerhed i oktober 2019 udgivet en vejledning til passwords: https://fe-ddis.dk/cfcs/publikationer/Documents/Vejledning-Passwordsikkerhed.pdf.

I det følgende fremføres en række anbefalinger til, hvordan tjenesteudbydere bør designe deres løsninger og til hvordan brugere bør håndtere passwords.

Det skal understreges, at disse anbefalinger bryder med den aktuelle best practice, og derfor ikke kan forventes realiseret med kort frist. Anbefalingerne er dog konsistente med de internationale trends på området og bør derfor inddrages i design af nye og revision af eksisterende systemer.

2 Forbehold

Det er vigtigt at understrege, at for følsomme tjenester[1] er autentifikation vha. password alene *aldrig* tilstrækkeligt. Anbefalingerne i dette dokument gælder *kun* for password-delen af sådanne tjenester.

3 Anbefalinger til tjenesteudbydere

#	**Anbefaling**	**Rationale**
1	Tillad kun få forsøg hvis bruger angiver forkert password (fx 10).	Dette beskytter imod online-angreb, dvs. at en angriber forsøger at gætte dit password ved at forsøge at logge ind med mange forskellige passwords.
2	Kræv skift af password ved kompromittering af password-	Dette beskytter imod offline-angreb, dvs. at en angriber forsøger at finde passwords ved

[1] Tjenester som håndterer følsomme data (fx helbredsoplysninger) eller giver adgang til at udføre følsomme transaktioner (fx overføre penge).
Begrebet bruges her bredt og dækker også tjenester som ikke nødvendigvis er følsomme i juridisk forstand. Eksempelvis bør tjenester som gør det muligt at logge ind på andre tjenester (også hvis disse tjenester ikke i sig selv er følsomme) behandles som følsomme, fordi de aggregerer viden om brugeren.

	database.	at ‘brute-force’ databasen.
3	Man må ikke bruge sikkerhedsspørgsmål (fx “hvad hedder din mor?”).	Det er meget svært at finde spørgsmål, der både er sikre, og hvor svarene kan huskes. Der har været kompromitteringer af mange brugerkonti via sikkerhedsspørgsmål.
4	Kræv passwords som er mindst 8 tegn lange uden krav om brug af specialtegn Der bør anvendes blacklisting mod en opdateret liste af svage passwords. Såfremt brugeren anvender multifaktorlogin eller lange (8 tegn eller mere) passwords er der ikke behov for at bede dem om at skifte password	Længden på passwordet er vigtigere end kompleksitet. Forudsat at de øvrige krav er opfyldt er det ikke nødvendigt at stille formmæssige krav til passwords (fx tal og specialtegn). Ved korte passwords (mindre end 8 tegn) bør man tjekke brugerens password mod en Black list, det kan fx være Troy Hunts liste, (https://haveibeenpwned.com/Passwords), hvorved det beskyttes mod simple passwords som ”Sommer19”.
5	Forudsat at de øvrige krav er opfyldt, er det ikke nødvendigt at stille krav om periodisk opdatering af passwords. Indlæg tidsforsinkelse mellem passwordforsøg	Såfremt ovenstående regler følges, er der ikke belæg for at periodisk opdatering giver bedre sikkerhed. For at beskytte mod brute force attaks bør man indlægge en tidsforsinkelse (et par sekunder) mellem hvert password forsøg. Hermed kan men tillade flere end 10 forsøg uden at kontoen låses.

Ift. nulstilling af passwords findes der forskellige brugbare alternativer fx:

- E-mail: Udfordringen ved dette er, at det forudsætter, at den benyttede e-mailkonto er passende sikret, hvilket igen delvist flytter byrden over på brugeren.
- Mobil registrering til at genskabe passwordet.
- Anden autentifikationsmetode fx NemID: NemID anbefales, når der er tale om følsomme oplysninger – fx betalingsinformationer.

4 Anbefalinger til brugere

4.1 Hovedanbefaling til brugere

Hovedanbefalingen her antager, at tjenesteudbyderen følger anbefalingerne ovenfor, og at der benyttes multifaktor-autentifikation (i form af mere end en adgangskode via mere end en kanal, f.eks. sms eller biometrisk smartcard) så snart en tjeneste er følsom.

#	**Anbefaling**	**Rationale**
1	Brug flerfaktor-autentifikation hvis muligt.	Flerfaktor-autentifikation er et af de sikringstiltag, der er mest effektive i forhold til at øge login-sikkerheden i forbindelse med adgang til kritiske informationer i it-systemer. Fler-faktor-autentifikation er karakteriseret ved, at brugeren får adgang med sit brugernavn suppleret med to eller tre af: • Noget brugeren ved (f.eks. pinkode eller password), • Noget brugeren har (f.eks. ID-kort, nøglekort, eller USB-nøgler) eller • Noget brugeren er (f.eks. ansigtsgenkendelse eller fingeraftryk), også kaldet biometrisk identifikation.
2	Lav lange passwords – gerne mere end 8 tegn, hvis det ikke er suppleret med fler-faktor-autentifikation. Brug en sætning som hjælper med at huske dit password, fx kan ”Jeg bor i nummer 38 med mine 2 hunde og 1 datter” blive til ”Jbi#38mm2ho1d”	Længden på passwordet er vigtigere end kompleksiteten.
3	Genbrug ikke passwords på tværs af tjenester.	Hvis passwordet fra en tjeneste kompromitteres, vil det have en kaskade-effekt, hvor det kan være svært at overskue, hvilke tjenester man faktisk skal skifte password ved.

4.2 Forstærkende anbefalinger til brugere

Disse anbefalinger øger sikkerheden for brugeren generelt.

#	**Anbefaling**	**Rationale**
1	Brug en password-manager til at generere tilfældige passwords på mindst 20 tegn. Her kan man have forskellige, lange og komplekse passwords til alle sine logins - uden selv at skulle huske hvert enkelt. Passwordmanagers er låst med et hovedpassword, som selvfølgelig skal være meget stærkt, for gennemskuer hackeren hovedpasswordet, er der adgang til alle brugerens gemte passwords.	En passwordmanager er et stykke software, der kan hjælpe med at opbevare ens mange unikke og sikre passwords, på en sikker måde. Adgang til de gemte passwords er beskyttet af et hovedpassword. Dette gør det lettere at overholde brugeranbefaling #1, og det sikrer generelt en høj kvalitet af brugervalgte password. Generelt er brugen af lange passwords at betragte som en alternativ løsning hvis ikke multi-faktor-autentifikation er muligt.
2	Hav et lille sæt af særligt følsomme tjenester som beskyttes ekstra godt.	Dette bør være tjenester som kan bruges til nulstilling af passwords, login-tjenester (og dermed adgang til en masse andre tjenester), eller som bruges til adgang til kritiske tjenester som fx netbank eller NemID.

5 Brug af login-tjenester

Mange brugere benytter et såkaldt fødereret login, dvs. hvor en tjeneste bruges som login-tjeneste over for andre tjenester. Et almindeligt eksempel kunne være login på Endomondo vha. Facebook.

Fordelen ved login-tjenester er, at man som slutbruger kan nøjes med at skulle huske færre passwords og logge ind mindre ofte. Ulempen er naturligvis, at man bliver afhængig af det sikkerhedsniveau, som disse tjenester tilbyder, og ikke mindst at sådanne login-tjenester (fx Facebook eller Google) får mulighed for at indsamle oplysninger om brugerens digitale færden.

På den baggrund kan det ikke generelt anbefales for den almindelige bruger at benytte login-tjenester, men det er en afvejning ift. det enkelte individs privacy-præferencer, og det skal i den sammenhæng bemærkes, at mange tjenester alligevel får adgang til oplysninger om brugerens færden igennem cookies mv.