Effektive valg af Passwords

Passwords, er et meget diskuteret emne på internettet. De fleste kender værdien af et stærkt password. Mange forestiller sig at et godt password en grumsom tegnslange der fylder 100 tilfælde tegn, tal og bogstaver, store og små. Jeg vil i denne guide genn

Skrevet den **28. Mar 2010** af **Larry1337** I kategorien **Sikkerhed / Generelt** | ⭐⭐⭐☆☆

Intro

De fleste mennesker der bruger internettet har mange profiler, og kontoer rundt omkring. Alle brugere på internettet der benytter sig at profiler har et eller flere passwords. Det er almindelig kendt at man skal have et "stærkt" password, men det bliver et tveægget svær fordi det samtidig bliver til en digital signatur, der er langt mere effektiv end f.eks. en ip eller mac adresse - Når du vælger, og bruger passwords på internettet forsvinder de jo ikke ind i et sort hul hvor de er usynlige. De ligger i databaser og kan læses af mange forskellige mennesker.Det giver en alvorlig problem stilling jeg vil uddybe i denne guide.

Regler for god brug af passwords

- 1. Genanvend aldrig "stærke" passwords på sider du ikke stoler 100% på
- 2. Brug uduelige passwords på sider du ikke stoler på / har interrese i at deltage aktivt i
- 3 Brug aldrig tilfældige proxy servere til at tilgå ting/profiler der har en eller anden betydning for dig
- 4 Udfyld aldrig det 'hemmelige spøgsmål' skema med data der giver mening
- 5 Sørg altid for at have et langt og unikt password til din email adresse
- 6 Gør ALDRIG persondata til en del af dit password (og ja din hunds navn er også person data)
- 7 Byg niveauer

1. Genanvend aldrig "stærke" passwords på sider du ikke stoler 100% på

Denne tegnsammensætning

mU-_.LfvcC#¤5&"sqw!!"RghBc

Det er et rigtig godt password hvis man betrager det ud fra hvor svært det er at gætte, eller på anden måde bryde - men der er en ulempe ved at have den slags password, for du er næsten med sikkerhed den eneste i hele verden der bruger det, og derfor kan det endnu mere sikkert end noget andet stykke data på internettet afgøre hvem du er. Du kan altså let identificeres ud fra et stærkt kodeord. Ud over det er det måske let nok at huske 1 eller 2 af denne her slags tegnslanger men ofte har man et behov for mere end 1 eller 2 profiler, der opstår altså et behov for genbrug - hvis du kun har 1 eller 2 af denne her slags passwords du bruger overalt vil dit password på et tidspunkt ende i de forkerte hænder og dine profiler/data/server og hvad du ellers måtte have vil blive et let mål.

2. Brug uduelige passwords på sider du ikke stoler på / har interrese i at deltage aktivt i

brug uduelige passwords på sider du er ligeglad med, eller ikke stoler på. Uduelige passwords er lette at huske, og du kan bruge det samme igen og igen.Ideen er at du ofte vil du oprette en profil på en side for at

få adgang til noget, en fil / artikkel, måske vil du lave et enkelt debat indlæg - I disse situationer kan og bør du bruge et udueligt password som f.eks. password, qwerty, eller 123456 - du vil på den måde ikke kunne identificeres ud fra dit password. Hvis du skulle blive glad for siden og aktiv skal du naturligvis skifte password til noget bedre. Der er ikke nogen grund til at ligge et af dine stærke passwords i hænderne på admins på en side du ikke stoler på eller har tænkt dig at bruge alligevel

3. Brug aldrig tilfældige proxy servere til at tilgå ting/profiler der har en eller anden betydning for dig

Brug aldrig tilfælde proxy servere til at tilgå profiler / servere der betyder noget for dig - når du benytter dig af en offentlig proxy kan stort set al data læses af indehaveren. Der er rigtig mange gode proxy servere der har et reelt ønske om at skabe et internet, frit af cencur og overvågning. Men der er desværre også en gruppe mennesker der opstiller proxy servere med det ene formål at 'sniffe' brugernes data. Og lad mig her understrege at det gælder alle former for proxy

4. Udfyld aldrig det 'hemmelige spøgsmål' skema med data der giver mening

Udfyld aldrig det hemmelige spøgsmåls felt i en form (til oprettelse af en profil) korrekt. Ud over at det ofte er let at gætte det såkaldte "hemmelige svar" - åbner det en kæmpe mulighed for social engineering - og derfor bør det undlades

5. Sørg altid for at have et langt og unikt password til din email adresse

Sørg altid for at have et langt og unikt password til din mail adresse, specielt den du bruger til at få tilsendt passwords/aktivering af profiler - et alternativ er

http://10minutemail.com/10MinuteMail/index.html

Det er en service der tilbyder en email adresse i 10 min - det kan være nyttig ind imellem. Men så står du uden mulighed for at få dit password tilsendt, hvis du skulle miste det.

6. Gør ALDRIG persondata til en del af dit password (og ja din hunds navn er også person data)

Hvis en person vil prøve at hacke en af dine profiler eller servere vil det letteste og sikreste (for ham/hende) simpelthen være at kende det eller gætte dit password. Folk har desværre en udbredt tendens til at bruge deres egne navne, deres kæledyrs navne, deres børns navne, fødselsdage osv osv. Derfor er det en rigtig dårlig ide at bruge dem i et 'stærkt' password -fordi det er hvad de fleste vil starte med at gætte på - der er mange metoder til at udvikle 'stærke' passwords på nettet, jeg kan anbefale en anden guide her på eksperten.dk der behandler emnet godt.

7. Byg niveauer

niveaue 1 - sider du er ligeglad med opretter en bruger for at få adgang til en resource - find 2-3 dårlige passwords du bruger

Eks : asdfgh, mickeymouse, password

[password1,2 eller 3]

nivuaue 2 - sider du er bruger på og måske ikke ville syntes om blev hacket kombiner de 2 - 3 dårlige passwords sammen med unik talrække

Eks : 321asdfgpassword321mikeymouse45678

[Talrække] [Password1], [Password2], [Talrække2][Password3][talrække3]

nivuaue 3 - Sider med meget personligt indhold, eller andet der ville være attraktivt for en hacker at få fingerne i (f.eks. en berømt youtube account, en ftp server, facebook, email, en forum profil med mange posts,ssh tilgang, en god online spiller osv.) Her bruges de stærke passwords - jeg anbefaler en lægden på omkring 20. Du kan sammensætte en godt password vha. en af de mange metoder der findes på nettet (google - how to create a password) for at gøre dit 'stærke' password stærkere kan du bruge dine uduelige passwords i forlængelse af det.

Eks : passwordNvt_tdfd9cc7aasdiosad""asdfgmikeymouse

[password1][stærkt password][password2][password3]

Du skal naturligvis finde din egen formatering mht. hvor du vil placere hvad, det er vigtigt at det falder dig naturligt at ligge de forskellige dele af passwordet hvor du gør - det værste du kan gøre er >>direkte<< at skrive af fra eksembler du finder på nettet, og dermed også fra denne guide

Den her metode giver nogle meget lange og svære (derfor gode og effektive) passwords og det er relativt let at huske - dine 2,3 uduelige passwords forøger styrken af dit 'stærke' password betydeligt. Og det er let at huske hvilket passwords der passer til hvilken side/service fordi du vil vide hvilken type side du er ved at bevæge dig ind på. Det kan være en god ide at danne et par af disse stærke passwords, du kan som en mulighed sætte det i forlængelse af sig selv. Det er vigtigt at du kun bruger dem på sider/zoner du har tillid til.

Kommentar af hejmeddig123 d. 11. Apr 2010 | 1

Derudover er det ekstremt vigtigt at passwordsene ikke indeholder ord og navne - det bliver gættet for nemt .. f.eks. er et password som "kagemand54" ekstremt nemt at cracke mens et password som "Æ^9}£h" er så godt som umuligt selvom det er langt kortere ..

Det kan også nævnes at passwords ikke er så vigtige som man skulle tro .. Det er besværligt at cracke passwords .. Det er derimod nemmere at "sniffe" dem .. og i så fald er det ligemeget om passwordet er 3 tegn eller 50 - det gør ingen forskel..

Kommentar af hejmeddig123 d. 11. Apr 2010 | 2

sorry for repost .. den preview knap gav et alt for ægte preview

det her er jo totalt paranoia .. Du har på ingen måde brug for et password på 20 tegn .. Hver gang du tilføjer et ekstra tegn, fordobler du den tid det tager at cracke passwordet 40-150 gange alt efter om du bruger store bogstaver og specialtegn.. Et password på 9 tegn er mere end rigeligt!

Derudover er det ekstremt vigtigt at passwordsene ikke indeholder ord og navne - det bliver gættet for nemt .. f.eks. er et password som "kagemand54" ekstremt nemt at cracke mens et password som "Æ^9}£h" er så godt som umuligt selvom det er langt kortere ..

Det kan også nævnes at passwords ikke er så vigtige som man skulle tro .. Det er besværligt at cracke passwords .. Det er derimod nemmere at "sniffe" dem .. og i så fald er det ligemeget om passwordet er 3 tegn eller 50 - det gør ingen forskel..