

Analyse af kodeord på nettet og iPhones

Udført juni 2011 af sikkerhedsvirksomheden Digicure ApS.

Kontaktperson: Adm. direktør Jesper Helbrandt, 40 13 00 00, jesper@digicure.dk, www.digicure.dk

Kun 0,02 % af kodeord opfylder de anbefalede krav

I den seneste tid har der været stor aktivitet blandt flere hacker grupper, hvor der er blevet udført flere angreb mod Sony, Bethesda, PBS.org, Fox.com m.fl. Dette har medført, at mange brugeroplysninger er blevet lagt offentligt tilgængeligt på nettet. Disse oplysninger inkluderer både brugernavn og kodeord, og i alt er der i den seneste tid blevet lækket minimum 128.776 brugeroplysninger. Da mange brugere benytter de samme oplysninger flere steder, betyder det, en angriber med stor sandsynlighed kan få adgang til flere af en brugers konti. De første meldinger om sådanne tilfælde kom allerede inden for et par timer efter, at de seneste brugeroplysninger blev offentliggjort med følgende citat fra en, der udnyttede lejligheden:

”

Got an Xbox Live, Paypal, Facebook, Twitter, YouTube THE WHOLE LOT! J-J-J-J-J-JACKPOT

” – twitter bruger

De 10 mest benyttede kodeord	Antal	Procent
123456	1322	1,03%
123456789	397	0,31%
password	307	0,24%
12345	167	0,13%
1234	123	0,10%
12345678	112	0,09%
123	111	0,09%
winner	110	0,09%
seinfeld	108	0,08%
1234567	101	0,08%
Samlet	2.858	2,22%

1: Top 10 kodeord baseret på 128.776 indsamlede kodeord

Firma skal beskytte deres brugere bedre

Informationslæk som disse skyldes sjældent brugerne selv, men derimod ligger ansvaret hos de virksomheder, hvor brugerne har oprettet en konto. Ofte bruges der ikke nok resurser på it-sikkerhed. Sikkerhedsforanstaltningerne er enten forældede, manglende eller slet ikke til stede. Der er overordnet to steder, hvor sikkerheden bør være bedre:

1. De sider, hvor brugere kan oprette konti, bør være sikret bedre, så kendte sårbarheder og u hensigtsmæssigheder er minimeret. Dette vil gøre det sværere for angriberne at kompromittere tjenesterne og bør udelukke flere af de automatiserede angrebsværktøjer.
2. Langt de fleste af de lækkede oplysninger har været gemt i klartekst på serverne. Dette betyder, at når angriberne har fået adgang til systemerne, skal der ikke gøres yderligere for at kunne aflæse brugernes informationer. Der bør være politikker, der sikrer, at virksomheden sikrer brugernes følsomme data ved eksempelvis kryptografisk hashing eller kryptering.

Kryptografisk hashing:

Kryptografiske hashfunktioner har til formål at danne et "fingeraftryk" af en bit information (klartekst), f.eks. en tekst [som fx et kodeord, *Digicure*] eller en datafil. Resultatet kaldes en hash eller et digitalt fingeraftryk (eng. message *digest* eller *fingerprint*). Hashen kan være af vilkårlig længde, men er typisk på mellem 32 og 256 bits. Hashfunktioner kan bl.a. bruges til digitale signaturer samt at verificere integriteten af transmitteret information.

En af de vigtigste egenskaber for en kryptografisk hashfunktion er at den er kollisionsfri, dvs. at det er "svært" (dvs. meget beregningstungt) at finde en anden klartekst med samme hash.

Kilde:

<http://da.wikipedia.org/wiki/Hashfunktion>

Ved at havde overholdt disse forholdsregler på de kompromitterede tjenester, ville situationen med stor sandsynlighed have været meget anderledes.

Brugere bør dog også sikre sig bedre

Som det kan ses af twitter-citatet ovenfor, fik en angriber adgang til flere af en brugers konti blot ved at benytte de samme oplysninger. Det er desværre et udbredt problem, at mange brugere benytter det samme brugernavn og kodeord til flere tjenester. Dette giver en angriber gode muligheder for at kompromittere flere konti blot ved at finde et sæt brugeroplysninger. Derfor bør brugere være bedre til at benytte forskellige kodeord til de tjenester denne måtte være tilmeldt, samt sørge for at kodeordene er af en tilstrækkelig kompleksitet.

Forholdsregler vedrørende kodeord

Brugere bør derfor benytte en unik kode til hver tjeneste, samt sikre sig at koderne opfylder følgende krav:

1. Der skal være minimum 12 tegn
2. Der skal være både store og små bogstaver
3. Der skal indgå tal og specieltegn
4. Kodeordet bør ikke være et ord eller en sætning
5. Undgå kodeord, der kan gættes (fødselsdag, navne osv.)

Opbygningen af kodeord	Antal	Procent
Kun små bogstaver	54768	42,53%
Kun store bogstaver	893	0,69%
Kun tal	21277	16,52%
Indeholdende specieltegn	1958	1,52%
Kun små bogstaver og tal	44977	34,93%
Kun store bog og tal	942	0,73%
Store og små bogstaver samt tal	2541	1,97%
Store og små bogstaver, tal og specieltegn	183	0,14%
Længde på mindst 8 med store og små bogstaver, tal og specieltegn	174	0,14%
Længde på mindst 12 med store og små bogstaver, tal og specieltegn	30	0,02%

Det kan ofte være svært at huske alle de mange koder, der skal bruges til forskellige tjenester. Der findes flere metoder, der kan være behjælpelige med at huske dem. Eksempelvis:

1. Benyt en fast metode til generering af koderne. Dette kan eksempelvis være en sætning, hvor startbogstavet benyttes til at danne koden:

"Jeg har 1 kat der hedder Flemming, og det er min 5. kat" bliver således til koden:

Jh1kdhF,odem5.k

2. Der findes online tjenester til generering af vilkårlige koder. Sådanne tjenester kombineret med en password manager eller –safe kan være en stor hjælp til at generere og gemme koder.

Yderligere bør kodeord skiftes ofte, så hvis et kodeord skulle blive kompromitteret, så vil perioden, hvor angriberen har adgang, være minimeret.

"

Your password should be treated like a toothbrush: you do not share it and you change it regularly !

" - security.web.cern.ch

Analyse af de lækkede oplysninger

Det gennemsnitlige kodeord er 7,6 tegn langt. 26 % procent er lige til at slå op i en [ordbog](#), der er specielt konstrueret til at bryde kodeord. 17 % indeholder kun tal, mens 43 % kun består af små bogstaver. 76 % er på 8 tegn eller mindre. '123456', '123456789' og 'password' er de 3 mest brugte kodeord.

Af de 128.776 passwords der er blevet analyseret, er det kun 30, der opfylder de anbefalede krav. Flere vil nok mene, at de anbefalede krav er meget strenge, men der er gode grunde, til at de er som de er. Som det ses, er ca. 26 % af kodeordene at finde i en ordbog, hvilket betyder, at en angriber skal bruge væsentligt færre forsøg (og mindre tid) på at opnå adgang.

Kodeord fundet i en ordbog (ftp://ftp.openwall.com/pub/wordlists/)	33454	25,98%
123456	1322	1,03%
password	307	0,24%
12345	167	0,13%
1234	123	0,10%
12345678	112	0,09%
123	111	0,09%
winner	110	0,09%
seinfeld	108	0,08%
1234567	101	0,08%
shadow	99	0,08%

Ved at benytte tal, specialtegn, samt store og små bogstaver øges det søgeområde, en angriber skal igennem for at finde koden. Hvis der eksempelvis benyttes et kodeord på 10 tegn med store og små bogstaver samt tal, kan der dannes $10^{(26 + 26 + 10)}$ kombinationer, hvilket kan sammenlignes med de ca. 4 millioner ord, der findes i den benyttede ordbog.

Antal password	Antal	Procent
Total	128776	100%
Password længde på 4:	2228	1,73%
Password længde på 5:	2652	2,06%
Password længde på 6:	37016	28,74%
Password længde på 7:	22292	17,31%
Password længde på 8:	32615	25,33%
Antal password med længde på under 9:	97299	75,56%
TOP 10 password	2858	2,22%
Passwords fundet i ordbog	33454	25,98%

Statistik for iPhones

Det er ikke kun ved internettjenester, brugere bør være opmærksomme på, hvilke kodeord der benyttes. Der er fornyeligt blevet udført en omfattende indsamling af kodeord på iPhones. Disse koder er indsamlet via en applikation (Big Brother Camera Security), hvor det kodeord, brugeren benyttede til applikationen blev sendt til forfatteren. Denne hævder, at låseskærmen på applikationen minder meget om iPhones' låseskærm, er der stor sandsynlighed for at brugeren vil benytte den samme kode begge steder. Følgende tabel viser de 10 oftest benyttede kodeord af de 204,508 kodeord der blev indsamlet.

De 10 mest benyttede kodeord på iPhone	Antal	Procent
1234	8884	4,34%
0000	5246	2,57%
2580	4753	2,32%
1111	3262	1,59%
5555	1774	0,87%

5683	1425	0,70%
0852	1221	0,60%
2222	1139	0,56%
1212	944	0,46%
1998	882	0,43%
Samlet	29530	14,44%

2: Tallene er taget fra http://amitay.us/blog/files/most_common_iphone_passcodes.php

Som det ses, udgør den samlede mængde kodeord i denne top 10 en væsentligt større andel sammenlignet med den forrige top 10. Dette skyldes højst sandsynligvis, at der er færre muligheder (10^4), samtidigt med at tal ofte er sværere at huske, hvorfor brugerne ofte vælger et genkendeligt mønster i stedet, som tilfældet med koden '2580'.

Sikkerheden som kodeord giver, afhænger derfor primært af to ting: Hvor kompleks denne er, samt hvor meget tjenesten, hvor kodeord skal benyttes, gør ud af deres sikkerhed. Det er uheldigt, at den sidstnævnte har indflydelse på dette. Men det ses ofte, at kriminelle kompromitterer virksomheders servere til at skaffe sig brugeroplysninger, da det ofte er nemmere og genvinsten (antallet af brugeroplysninger) er større. Derfor bør det være en brugers ret at kræve, at virksomhederne beskytter deres informationer bedre, men ofte er begrebet 'sikkerhed' ikke noget der tænkes over, når der oprettes en ny konto på en tjeneste. Det bør det dog være - både hos bruger og tjenesteyder.

Af Jesper Kückelhahn, Digicure