CENTER FOR CYBERSIKKERHED

Passwordvejledning

PIXI udgave

Center for Cybersikkerhed

September 2016

Brugernavn og password er i høj kurs hos hackere. Det er stadig en ofte anvendt og succesfuld angrebsmetode til at skaffe sig uautoriseret adgang til – især – offentlige og private virksomheders kritiske informationer. Passwords er i mange tilfælde nemme at få fat i og at bryde. Derfor er angrebsmetoden uhyre effektiv.

Passwords er stadig en forudsætning for at sikre, at adgangen til vigtige og måske fortrolige informationer beskyttes mod, at uønskede personer får adgang til dem. De fleste passwordvejledninger tilråder, at man skal anvende forskellige passwords til de forskellige konti, man har, og at passwords skal ændres med jævne mellemrum. Herudover er det ofte et krav, at passwords til stadighed skal være længere og mere komplicerede med det formål at gøre dem stærkere og dermed vanskeligere at bryde for hackere.

Følgende punkter er derfor hensigtsmæssige at inddrage i forbindelse med virksomhedens krav til passwords:

- Passwords skal være unikke og må ikke genbruges
- Længere passwords kan reducere krav til kompleksitet
- Anvendelse af to-faktor-autentifikation
- Anvendelse af passwordmanagere
- Periodiske skift af passwords
- Ændring af standard-passwords
- Stærke passwords til it-administrative konti
- Sikker håndtering af passwords, men ikke i klartekst

Udfordringer ved passwords

Det typiske krav til et nyt password er, at det indeholder et minimum antal tegn, en blanding af store og små bogstaver, tal og specialtegn, og i de fleste tilfælde er der krav om at ændre passwords med faste mellemrum. Som it-bruger kan man derfor være fristet til at gemme passwords på uhensigtsmæssige måder eller at genbruge passwords. Denne adfærd udfordrer den sikkerhed, som en virksomhed forventer implementeret med kravene til passwords, men adfærden er almindelig og kendt – også af hackere.

Den typiske passwordadfærd

For at gøre det nemt for sig selv og samtidig efterleve alle disse krav, når nye passwords skal sammensættes, udviser mange it-brugere en uhensigtsmæssig adfærd som f.eks.:

- Hvis passwordet skal være på minimum otte tegn, er det oftest kun på otte tegn.
- Skal passwordet indeholde et stort bogstav, bliver det store bogstav typisk anbragt som det første bogstav i passwordet.
- Hvis passwordet skal indeholde tal, bliver disse gerne placeret til sidst. Tal angives ofte mellem 0 og 99, eller som et årstal. Det er også almindeligt at ændre bogstaver med tal, der ligner et bestemt bogstav, eller som ligger tæt ved bogstavet. ”e” bliver f.eks. til ”3”, ”o” bliver til ”0” osv.
- Kravet om specialtegn løses i mange tilfælde ved at bruge ét. Nogle tegn viser sig at være mere populære end andre. Snabel-a (”@”) og udråbstegn (”!”) er nogle af de mere populære.
- Skal passwordet ændres med faste mellemrum, er der mange brugere, der anvender cykliske ord i form af ord for årstider, kvartaler, måneder osv.

- Nogle ord eller tal er meget populære og går igen i mange passwords. Blandt de mest brugte passwords er bl.a. ”123456”, ”password”, og bogstavrækker som f.eks. ”qwerty”, der følger rækkerne på tastaturet.
- Passwordet er det samme som brugernavnet eller en del af det.
- Passwordet består af navne på familie, venner, husdyr osv.
- I forbindelse med en periodisk ændring af passwordet sammensættes et nyt, som er næsten identisk med det tidligere.

Passwordstyrke

Selvom virksomheden stiller mange krav til sammensætningen af et password, og passwordet af den grund bliver betragtet som sikkert, er det ikke nødvendigvis altid tilfældet. Hvis kravet til et sikkert password f.eks. er ti tegn med en blanding af store og små bogstaver, tal og specialtegn, kan et password f.eks. se således ud:

Password2016!

Dette password opfylder alle kravene, og det er endda tre tegn længere end krævet. Måler man passwordstyrken ved hjælp af tilgængelige værktøjer på internettet, viser det sig at være **fremragende**, og at det derudover vil tage ca. 173 milliarder år at bryde passwordet med brute force fra en standard-PC. Passwordet er imidlertid meget nemt at gennemskue og derfor slet ikke så sikkert. Målinger af passwordstyrken viser således ikke altid den krævede sikkerhed, og man bør derfor ikke forlade sig alene på den type målinger.

En måde at undgå at sammensætte passwords, der er nemme at gætte, er ved at etablere en blackliste med ord, der rangerer højt på tilgængelige toplister på internettet over de mest anvend-te passwords. Denne blackliste kan også indeholde ord, der angiver en relation til virksomheden og dens opgaveløsning/produkter. Med denne viden kan man som bruger få hjælp til at undgå at anvende ord, der vil svække passwordet. Der findes flere lister på nettet med de mest almindeligt anvendte og usikre passwords f.eks. www.passwordrandom.com

Figur 1: *De mest benyttede passwords i den engelsksprogede verden.*

Genbrug af passwords er ikke tilladt

For at opnå størst mulig sikkerhed, er det vigtigt, at man som it-bruger skelner mellem de passwords, man bruger på sit private udstyr, og det eller dem, man anvender på arbejdet. Det er vigtigt at skabe awareness om dette blandt virksomhedens it-brugere. Kravene til sikkerhedsniveau vil i de fleste tilfælde være forskellige, men kompromittering af passwords i denne sammenhæng ved hjælp af f.eks. social engineering vil kunne udnyttes af hackere til også at få adgang til fortrolige, måske forretningskritiske informationer eller endda meget personlige og private informationer.

Tip 1 - Passwords, der er nemme at huske

Der findes flere metoder til at oprette stærke passwords, der samtidig ikke er alt for svære at huske, og det er vigtigt, at ikke alle medarbejdere i samme virksomhed anvender den samme metode. Anvender alle medarbejdere i virksomheden samme metode, og har en hacker viden om den, er det nemt at udnytte denne viden i et angreb.

Afhængig af systemets dataindhold, kan der ud fra en risikovurdering være forskellige krav til, hvor stærkt passwordet skal være. Er flere systemer forbundet med hinanden – som ved single sign-on bør kravet defineres af det mest kritiske system. Internetvendte systemer er ofte mere sårbare end interne systemer, der ikke har forbindelse til internettet, og som er placeret på steder med fysisk adgangskontrol.

Password med høj styrke

En metode til at oprette passwords med høj styrke, der er nemme at huske, er f.eks. at tænke på en sætning og ændre den til et password ved at forkorte den. Sætningen kan f.eks. være noget personligt og derfor nemmere at huske. For at gøre passwordet komplekst er det vigtigt at bruge både store og små bogstaver samt tal og specialtegn – gerne et fra hver kategori. Det er også vigtigt, at det har en mellemlang længde, gerne på minimum 12-14 tegn:

Følgende passwordeksempel er lavet ved at tage de to første bogstaver, det første med stort, fra sætningen. Specialtegn og tal er brugt til at erstatte ord.

Eksempel: Husk! Bestil 1000 liter olie til fyret = **Hu!Be1000L.OlTiFy**

Ordene er enten lavet til forkortelser, erstattet af specialtegn, eller der er kun benyttet det første bogstav.

Eksempel: Danmark blev nummer fire til europamesterskabet i fodbold i 1964 = ***DKb#4=EMif-64***

En anden metode er at finde på nogle tilfældige ord uden en meningsfyldt sammenhæng, der er nemme at huske, og som giver en betydelig længde – f.eks. med baggrund i en interesse. Når der bruges rigtige ord, skal man dog være opmærksom på faren ved ordbogsangreb. Ordbogsangreb kan modvirkes ved at indføre stavefejl med vilje i ordene, så de ikke kan findes i et leksikon. Det er også vigtigt at bruge både store/små bogstaver og at det som minimum er 20-25 tegn. For at gøre det nemmere for sig selv, kan man bruge en regel for, hvor de store og små bogstaver og evt. tal og specialtegn placeres i ens passwords:

Andet bogstav i hvert ord er med stort, og der er med vilje lavet stavefejl.

*Eksempel: c*ykle motion stol paradis = **sYklemOtjonsTolpAradis**

Sidste bogstav i hvert ord er med stort.

*Eksempel: a*brikos hospital zebra spark = **abrikoShospitaLzebrAsparK**

De her fremførte passwords skal selvfølgelig ikke benyttes, da de med denne vejledning er offentligt tilgængelige.

Tip 2 - Fler-faktor-autentifikation

Mange systemer giver i dag mulighed for at anvende fler-faktor-autentifikation. Fler-faktor-autentifikation kan med fordel indføres med det formål at øge sikkerheden i forbindelse med adgang til kritiske informationer i it-systemer. Anvendes fler-faktor-autentifikation kan der i de fleste tilfælde slækkes på kravet til passwordets styrke både med hensyn til længde og kompleksitet.

Fler-faktor-autentifikation er udbredt mange steder, f.eks. i forbindelse med fjernbrugeradgang. Da fler-faktor-autentifikation giver et ekstra lag af sikkerhed, er det en god idé at indføre det på systemer, hvor sikkerheden er prioriteret.

Fler-faktor-autentifikation

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 eller får (f.eks. ID kort, nøglekort, USB-nøgler eller kode på mobiltelefon) eller
- noget brugeren er (f.eks. irisscan eller fingeraftryk), også kaldet biometrisk identifikation.

Oftest benyttes to-faktor-autentifikation, hvor noget brugeren ved suppleres med noget, brugeren enten har eller er.

Center for Cybersikkerhed anbefaler, at der anvendes to-faktor-autentifikation som et godt middel til at øge sikkerheden.