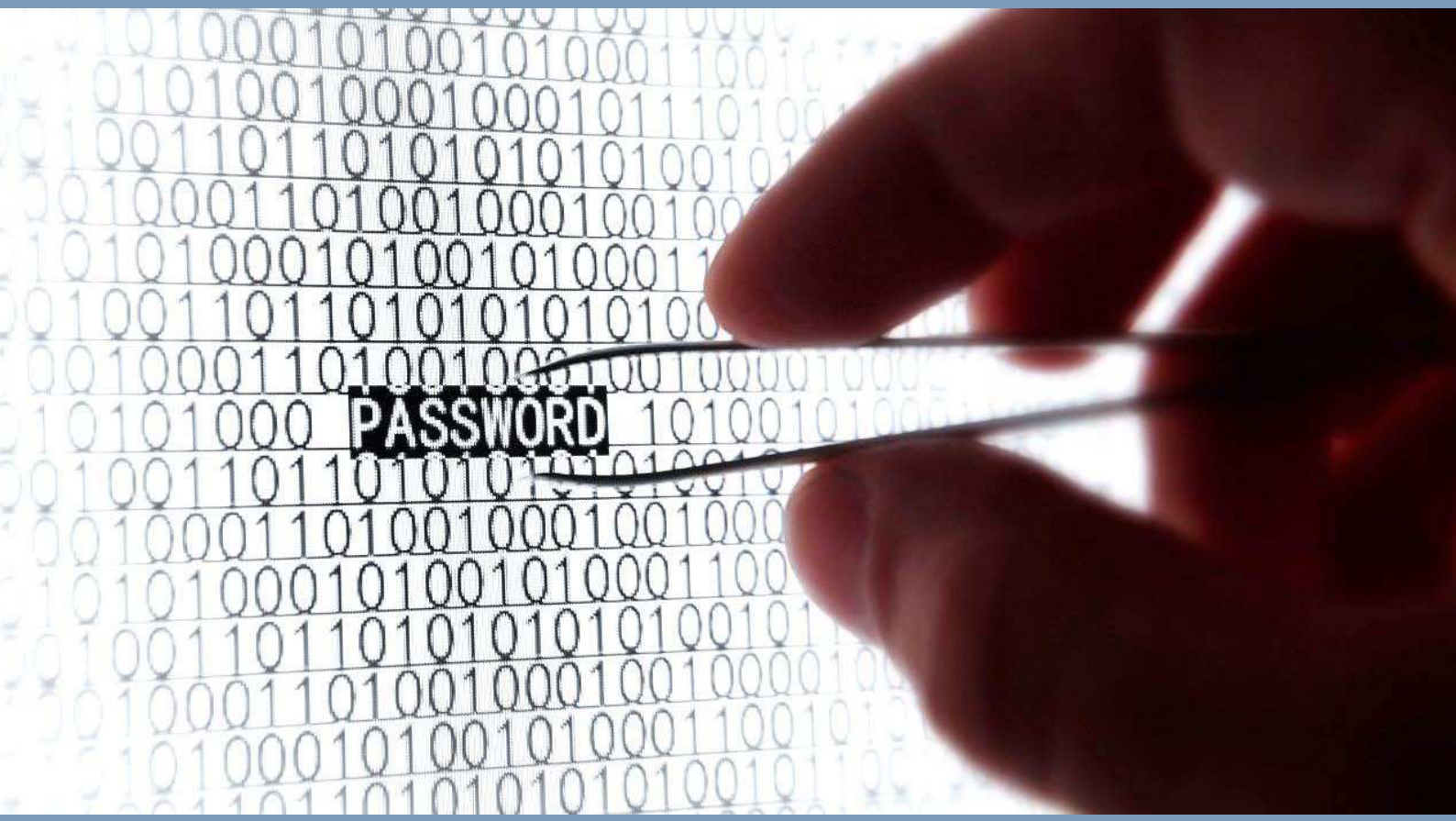
CENTER FOR CYBERSIKKERHED

Passwordvejledning



Center for Cybersikkerhed

September 2016

Indhold

Forord

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.

For mange it-brugere kan det være en udfordring med konstant nye, lange og komplicerede passwords. Det kan derfor være fristende at opbevare dem, så man hurtigt og nemt kan få fat i dem. Ikke alle opbevaringsmetoder er lige sikre, og risikoen for, at de havner i de forkerte hænder, er derfor voksende. Med andre ord, så risikerer man, at sikkerheden bliver mindre – i forsøget på at øge den.

Følgende punkter er derfor hensigtsmæssige at inddrage i forbindelse med organisationens 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

Denne vejledning indeholder en række tips til forskellige niveauer i en organisation med det formål at tilpasse passwordsikkerheden til den adfærd, der karakteriserer organisationen.

Vejledningen henvender sig til:

It-brugere, hvor vejledningen er tænkt som inspiration til at tænke passwords og deres beskyttelse på en ny måde.

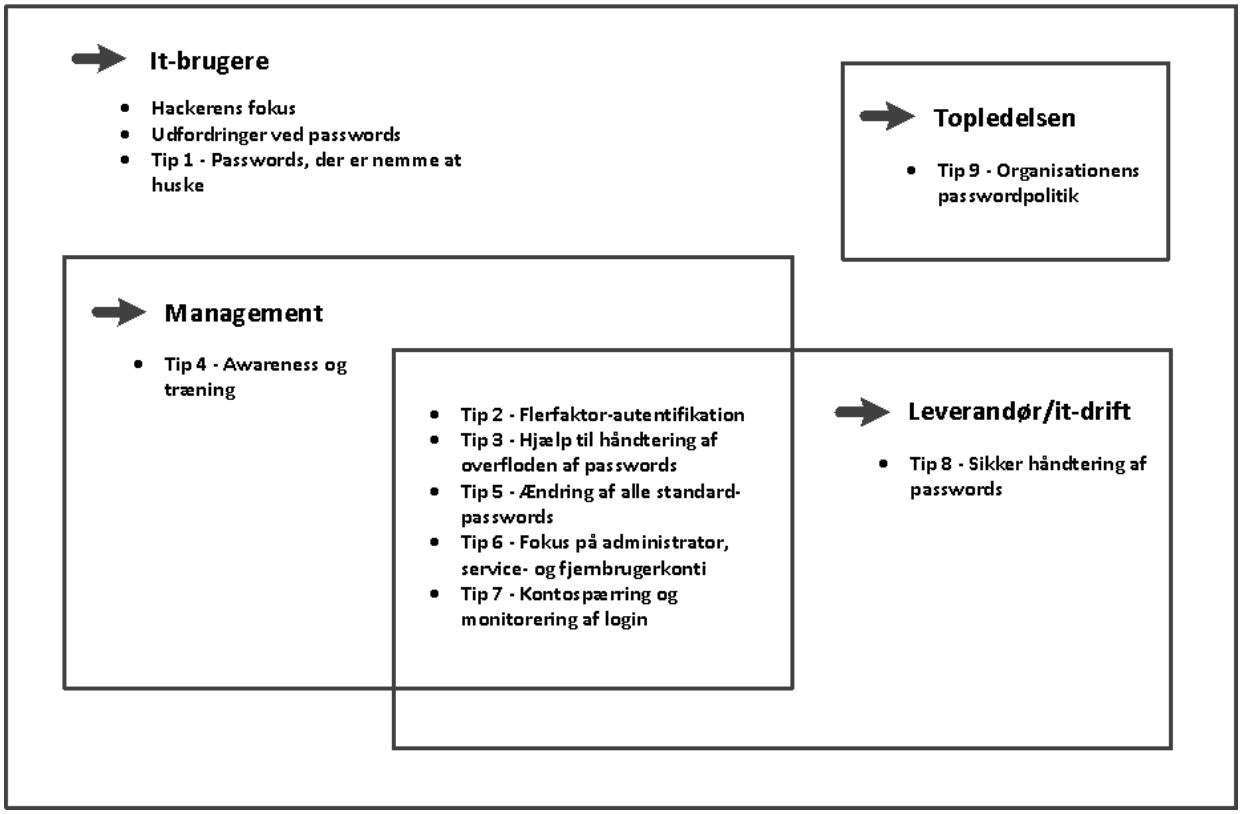
Managementniveauet, der definerer mere konkrete krav til, hvordan den overordnede passwordpolitik udmøntes i praksis. For hvilke systemer skal det f.eks. gælde, at passwords skal ændres med et bestemt mellemrum, eller at passwords skal være konstrueret på en særlig måde? Skal der investeres i understøttende it-systemer til brugere eller i it-driften til håndtering af reset af passwords?

It-driften/leverandørniveauet, hvor det kan være relevant at udarbejde konkrete procedurer defineret med udgangspunkt i organisationens behov frem for i generel best practice. It-driften vil i

mange tilfælde være den rette sparringspartner i forbindelse med anskaffelse af passende teknologier, der kan understøtte organisationens særlige behov for sammensætning, anvendelse og beskyttelse af passwords.

Topledelsen, der skal sikre, at der er fokus på sikkerheden i organisationen, herunder ved at definere rammerne for det ønskede sikkerhedsniveau. Topledelsen skal sikre, at der er tilstrækkelige ressourcer i organisationen eller tilknyttet denne, så det ønskede sikkerhedsniveau kan opfyldes.

Vejledningen beskriver nogle af de mest anvendte angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen består herudover af en række tips, som i flere tilfælde henvender sig til forskellige niveauer i organisationen. De beskrevne tips er tænkt som inspiration til at perspektivere de traditionelle måder at tænke passwords på. Organisationer og virksomheder bør overveje og vurdere de enkelte områder og deres relevante implementering, så det passer ind i egen kontekst. Nedenstående figur giver et overblik over de enkelte tips i vejledningen og den eller de målgrupper, som de er tiltænkt:



Til sidst i vejledningen er indsat en tjekliste, hvor de enkelte tips er omsat til egentlige tjekpunkter, som organisationen kan forholde sig til. Tjeklisten kan bruges af de forskellige niveauer i organisationen til at sikre, at der anvendes passwords i overensstemmelse med kravene til systemernes sikkerhed.

Hackerens fokus

Hackere målretter deres angreb ved at udnytte den viden, de har om brugere og deres passwords. Denne viden kan overføres til en række værktøjer, som hjælper hackeren til at "gætte" et password eller aflæse passwords, f.eks. gennem installation af en keylogger, der registrerer al aktivitet fra tastaturet. I de følgende afsnit beskrives en række af de metoder, som hackere særligt benytter sig af, når de forsøger at få fat i eller bryde passwords.

Social engineering

En meget benyttet metode til at få fat i passwords er såkaldt **social engineering.** Med social engineering forsøger hackeren at lokke passwordet ud af brugeren ved f.eks. i en mail at udgive sig for en person, som modtageren kender og har tillid til. Typisk vil hackeren sende en mail til målet for angrebet, hvor vedkommende anmodes om at besvare mailen med oplysninger, som giver hackeren de informationer, der skal til for at kunne gennemføre et angreb. En anden metode er at sende en tillidsvækkende mail med vedhæftet malware, som bliver aktiveret og installeret på brugerens PC. På den måde kan hackeren skaffe sig adgang til f.eks. interne it-systemer med kritiske forretningsmæssige informationer.

Phishing og spear-phishing

Populært beskrevet er et phishingangreb et angreb, hvor der "skydes med spredehagl", mens et spear-phishing er et målrettet angreb rettet mod enkeltindivider. Succesraten for, at et spear-phishingangreb lykkes, er langt højere end for et almindelig phishing–angreb.

Center for Cybersikkerhed har udarbejdet undersøgelsesrapporten *Phishing uden fangst – Udenrigsministeriet under angreb,* der indeholder en analyse af et konkret phishingangreb. Udover analysen er der et afsnit med anbefalinger til bl.a. relevante sikringstiltag til at modstå denne type angreb.

Genbrug

Mange brugere genbruger ofte passwords – og måske både på arbejde og privat. Genbrug af passwords udgør en meget stor risiko for, at en hacker får adgang til ikke blot et enkelt system, men til mange systemer.

Det er især kritisk, når passwordet er det samme både til systemer med lav sikkerhed og til systemer, der kræver høj sikkerhed.

Ordbog, brute force og rainbow table

I et såkaldt ordbogs-angreb anvender hackeren en liste med mulige – ofte almindeligt anvendte – passwords. Angrebet er en automatiseret proces, hvor listen indgår med det formål at afsløre et konkret password. I en liste med mange, vidt forskellige ord er der stor chance for at finde det password, hackeren leder efter. Problemet med denne metode set fra hackerens side er, at mange it-systemer ikke tillader et meget stort antal gæt.

Ved et brute force-angreb afprøver hackeren alle mulige sammensætninger af tegn, og denne type angreb kan derfor tage væsentligt længere tid end et ordbogsangreb. Men hvor et angreb baseret på en ordbog ikke nødvendigvis fører til afsløring af passwords, der f.eks. ikke fremgår på listen, så vil et brute force-angreb på et eller andet tidspunkt ramme rigtigt. Ligesom ved ordbogsangreb, kan det for hackeren være et problem med systemer, der ikke tillader mange antal gæt af passwords.

En rainbow table kan anvendes i forsøget på at finde et password på baggrund af en hash-værdi (læs om hash i tip 8). Metoden minder om ordbogs- og brute force-angreb, men skiller sig ud ved dels at foretage angrebet som et opslag i forudberegnede tabeller og dels som en række beregninger. Denne metode reducerer derved mængden af data i rainbow-tabellen i modsætning til en ren hash-tabel, der kun er baseret på anvendelsen af opslag. Navnet rainbow table kommer af, at der benyttes forskellige funktioner til at lave beregningerne.

'Low and Slow' brute force-angreb

Hackeren kan angribe et system ved at afprøve populære passwords på alle konti i et givent system. I en stor organisation med mange hundrede brugere, er der en god chance for, at hackeren rammer rigtigt på et tidspunkt. Da der ofte er implementeret kontospærring, sørger hackeren for kun at afprøve det tilladte antal loginforsøg, så kontoen ikke spærres.

Angrebet kaldes 'Low and Slow', fordi det kan foregå i flere uger eller måneder – og samtidig holder hackeren sig under radaren og mindsker dermed risikoen for, at angrebet blive opdaget.

Tabel 1 viser en udregning af, hvor længe det vil tage at bryde passwords af forskellig længde ved hjælp af et brute force-angreb afhængig af den anvendte computerkapacitet.

Computerkapacitet	Tid (7 tegn)	Tid (10 tegn)	Tid (12 tegn)
Standard-desktop PC	Ca. 8 dage	208 tusinde år	2 milliarder år
Hurtig desktop PC	Ca. 2 dage	52 tusinde år	459 millioner år
GPU – PC	18 timer	21 tusinde år	184 millioner år
Hurtig GPU	9 timer	10 tusinde år	92 millioner år
Parallelle GPU'er	54 minutter	87 år	9 millioner år
Mellemstort botnet	1 sekund	6 dage	2 tusinde år

Tabel 1: *Værdierne er udregnet på grundlag af http://password-checker.online-domain-tools.com/*
Tabellen tager udgangspunkt i den typiske engelske tastatur-tegnmængde ved oprettelse af passwords, hvor der er brugt en kombination af store og små bogstaver, specialtegn og tal. Der er andre tilgængelige værktøjer på internettet til kontrol af styrken af passwords.

Standard-passwords

Benyttes der standard-passwords på netværket, dvs. de passwords som hardware og software leveres med, og er der samtidig adgang til internettet, er det meget nemt for hackere at trænge ind i organisationens netværk og systemer. Hvis der er viden om den hardware og software, som

organisationen har installeret, kan standard-login findes via nettet, og informationen kan anvendes til at skaffe sig adgang til netværk og systemer.

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 organisation 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 organisationen 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 anvendte passwords. Denne blackliste kan også indeholde ord, der angiver en relation til organisationen 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. http://www.passwordrandom.com/most-popular-passwords.

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 organisationens 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 organisation anvender den samme metode. Anvender alle medarbejdere i organisationen 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.

Et password kan - afhængig af hvilke sikringstiltag der tilføjes - have forskellig styrke. Følgende tabel kan benyttes som en vejledende oversigt over, hvordan forskellige sikringstiltag kan øge styrken på et password. Tabellen tager ikke højde for organisationens øvrige sikkerhed eller brugerens passwordadfærd:

Samlet længde	Kompleksitet	Passwordstyrke		
		Lav	Mellem	Høj
Kort (<10)	a-z	X		
	a-z, A-Z	X		
	a-z, A-Z, 0-9,!"#...		X	
Mellem (10-19)	a-z	X		
	a-z, A-Z		X	
	a-z, A-Z, 0-9,!"#...			X
Langt 20+	a-z		X	
	a-z, A-Z			X
	a-z, A-Z, 0-9,!"#...			X

Andre sikringstiltag, herunder særligt fler-faktor-autentifikation, kan øge passwordstyrken væsentligt selv for passwords med lav styrke. I Tip 2 kan læses mere om fler-faktor-autentifikation.

Vær opmærksom på, at uanset hvor mange sikringstiltag, der benyttes til oprettelse af et password, vil det aldrig gøre et system 100 procent sikkert.

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.

Tip 3 - Hjælp til håndtering af overfloden af passwords

For at undgå at brugere skal håndtere for mange og for komplicerede passwords, er det vigtigt at vurdere, hvor det er nødvendigt at stille krav om anvendelse af passwords, herunder krav til længde og kompleksiteten i passwords. Er der it-systemer eller services, hvor vurderingen er, at der ikke er behov for et højt sikkerhedsniveau, er det relevant at overveje at gøre adgangen fri for passwords eller stille lave krav til passwords længde og/eller kompleksitet.

Tekniske løsninger

Tekniske løsninger kan biddrage til at hjælpe brugere med at håndtere passwords på en sikker måde.

Der kan benyttes tekniske løsninger til at reducere mængden af passwords. Med single-sign-on og passwordsynkronisering kan byrden på it-brugerne reduceres. Single-sign-on er en meget udbredt løsning, som giver samtidig adgang til flere it-systemer i organisationen. Hvis passwordet brydes, får en hacker imidlertid adgang til alle systemer, der er passwordbeskyttet, og derfor skal man også ved brug af single sign-on være opmærksom på sikkerheden.

Passwordmanagere

En passwordmanager kan anvendes til at huske passwords. Fordelen ved passwordmanagere er, at brugeren kan have forskellige, komplekse passwords til alle sine logins - uden selv at skulle huske hvert enkelt. Passwordmanagers fås både som software og som en fysisk passwordbog.

Softwareversioner af passwordmanagers er låst med et hovedpassword, som selvfølgelig skal være meget stærkt, for gennemskuer hackeren hovedpasswordet, er der adgang til alle brugerens gemte passwords. Med en passwordmanager kan man etablere en database, hvor alle passwords bliver håndteret i et sikkert format. Nogle passwordmanagers etablerer en database på den lokale PC, mens andre opbevarer databasen på en central server i organisationen eller i skyen. Valget af løsning afhænger af organisationens set-up med hensyn til PC-miljø og ønsker om central styring i form af opdatering, synkronisering og vurdering af hensigtsmæssighed ved anvendelse af cloud-løsninger.

Den fysiske passwordbog skal opbevares på et sikkert sted. I den fysiske version kan man skrive en del af passwordet, og resten bør være noget, man skal huske og tilføje, når man logger ind. For eksempel kan passwordet til et system være sJ#v78+l0o!MK1, men i passwordbogen noteres kun sJ#v78+l0o, og !MK1 er så noget, man skal huske.

Det er vigtigt at have for øje, at det ikke er alle passwords, der bør gemmes i passwordmanageren. Nogle passwords kan være så kritisk vigtige, at de ikke tåler at blive lagret.

Uanset, så vil alle it-brugere skulle huske mindst ét password af høj styrke.

Maskingenererede passwords

Tilfældigt maskingenerede passwords kan være med til at øge sikkerheden, fordi disse tilfældigt genererede passwords er meget svære at bryde. Ulempen er dog, at passwordet kan være så komplekst, at brugeren ikke kan huske det. Passwordene bør derfor genereres på grundlag af en

metode, der sikrer en sammensætning, der gør passwordene nemmere at huske. Maskingenererede passwords kan f.eks. bestå af fire tilfældige ord, eller der kan angives flere forskellige passwords, som it-brugeren kan vælge imellem, alt efter hvad der er nemmest at huske for vedkommende.

Ændring af passwords

Ændring af passwords, herunder intervallet for hvornår brugeren skal ændre det, skal vurderes på grundlag af en it-risikovurdering. I de fleste organisationer er det imidlertid fast praksis, at alle passwords skal ændres inden for 90 dage, hvilket ikke altid er det mest hensigtsmæssige.

Et kort interval giver en god sikkerhed for, at et brute force-angreb ikke uden videre vil kunne lykkes, fordi hackeren ikke kan nå at bryde passwordet, inden brugeren har skiftet det. Dermed gives der ikke adgang til forretningskritiske informationer i interne it-systemer, fordi passwords som oftest vil være ændret, inden det lykkes at kompromittere passworddatabasen. Så selvom hackeren formår at bryde en række passwords i databasen, vil vedkommende ikke kunne anvende dem.

En politik, der kræver ændring af passwords for ofte, kan imidlertid medføre irritation hos brugerne, som derved fristes til at slække på sikkerheden. Tidsintervallet for ændring af password bør derfor vurderes i forhold til normer i organisationen, herunder incitamentet for it-brugere til at efterleve organisationens passwordpolitik. Herunder bør det også overvejes hvorvidt det i det hele taget er nødvendigt med løbende ændring af passwords, hvis ellers en politik for stærke passwords efterleves.

I forbindelse med hacking af interne it-systemer skal passwords i organisationen dog altid ændres – uanset om angrebet er gennemført ved hjælp af brugernavn og password eller ej.

Center for Cybersikkerhed anbefaler, at

- **det i organisationen overvejes, hvilke tekniske løsninger det vil være hensigtsmæssigt at implementere med det formål at hjælpe it-brugeren,**
- **der benyttes en passwordmanager til at holde styr på it-brugernes personlige passwords,**
- **det ud fra en risikovurdering vurderes, med hvilket interval det er hensigtsmæssigt at stille krav om ændring af passwords.**

Tip 4 - Awareness og træning

Det er vigtigt, at organisationens it-brugere forstår passwordpolitikken og efterlever kravene til anvendelse og sammensætning af passwords uanset styrke. Herudover skal it-brugerne have kendskab til hackernes angrebsmetoder. It-brugerne skal være opmærksomme og vide, hvordan de skal reagere, hvis de bliver kontaktet af personer, der udgiver sig for at være kolleger i it-afdelingen, der f.eks. gerne vil kontrollere eller resette et password, eller hvis de modtager uventede eller underlige e-mails.

Det er ledelsens ansvar at fokusere på organisationens kultur og it-brugernes adfærd og dermed gøre opmærksom på behovet for at informere om nye angrebsmetoder. Der bør gennemføres træning i sammensætning af passwords, og det bør kontrolleres, at krav og forventninger til adfærd efterleves.

Center for Cybersikkerhed anbefaler, at ledelsen planlægger og gennemfører den fornødne awareness og træning i passwordpolitikken for organisationens it-brugere.

Tip 5 - Ændring af alle standard-passwords

It-udstyr og software leveres ofte fra leverandøren med standard-passwords. Det ved hackerne godt, og standard-passwords skal derfor ændres hurtigst muligt, og altid inden udstyr og software sættes i drift.

Standard-passwords kan være hackeres mulighed for at få adgang til en organisations it-systemer – og dermed til forretningskritiske informationer. Standard-passwords og brugernavne kan slås op på internettet, og er de ikke ændret, er det derfor i mange tilfælde meget nemt for hackeren at skaffe sig adgang.

Især er det vigtigt at være opmærksom på at ændre standard-passwords til kritiske komponenter og udstyr i infrastrukturen. Det kan f.eks. være passwords til routere, printere, logservere og firewalls.

For at kontrollere, at der ikke er implementeret hardware eller software med standard-passwords, er det vigtigt at gennemgå adgange til udstyr og software med jævne mellemrum.

Center for Cybersikkerhed anbefaler at implementere ændring af standard-passwords som en fast procedure i forbindelse med idriftsættelse af udstyr og software.

Tip 6 - Fokus på administrator-, service- og fjernbrugerkonti

Nogle konti er vigtigere at sikre end andre. Hvis administrator-, service- og fjernbrugerkonti kompromitteres, er der høj risiko for uautoriseret adgang til kritiske informationer, og der er derfor behov for ekstra beskyttelse af disse konti.

Administratorrettigheder

Almindelige it-brugere har normalt ikke behov for udvidede rettigheder til it-systemer og infrastruktur. Alle it-brugeres rettigheder skal altid tildeles i forhold til et arbejdsbetinget behov.

Opgaven som it-administrator giver adgang til opgaveløsning i relation til den systemkritiske infrastruktur og til bl.a. vedligeholdelse af interne it-systemer. Derfor er disse konti et oplagt mål for mange hackere. It-administratorer skal være særligt opmærksomme på at beskytte passwords. Passwords til administrative konti bør have høj eller meget høj styrke. Administrative konti bør kun anvendes til rene driftsopgaver, og it-administratorer bør anvende personlige konti til udførelse af opgaver udover drifts- og systemtekniske opgaver.

Fjernbrugeradgang

En fjernbruger vil ofte logge på organisationens interne systemer fra mindre sikre steder. Dette kan være fra eget personlige netværk, hotelværelset, en café eller lignende. Fælles for internetadgangen disse steder er, at organisationen ikke kan styre den lokale sikkerhed.

Center for Cybersikkerhed anbefaler, at

- **der anvendes stærke passwords til administrative konti**
- **alle fjernbrugere logger på med to-faktor-autentifikation**

Tip 7 - Kontospærring og monitorering af login

Det skal være så svært som overhovedet muligt for hackere at trænge ind i de it-systemer, der indeholder forretningskritiske informationer. Følgende løsninger kan hjælpe i forbindelse med ordbogs- og brute force-angreb.

Kontospærring

Kontospærring kan være en metode til at hindre, at en hacker ved hjælp af et online angreb formår at bryde et password og trænge ind i interne it-systemer. Brugerkontoen bliver spærret, når brugeren eller en hacker har opbrugt det definerede antal loginforsøg uden held. På denne måde kan hackeren ikke udføre sine ordbogs- og brute force-angreb.

Organisationen bør derfor udarbejde en politik for området, der fastsætter, hvor mange loginforsøg, det er hensigtsmæssigt at tillade. Er der pludselig et højt antal loginforsøg på en konto, kan det skyldes ondsindet aktivitet.

Derudover bør politikken fastsætte, hvornår de forkerte passwordforsøg skal nulstilles. Dette kan imødegå "Low and Slow"-angreb, som er beskrevet under afsnittet Hackerens fokus. Der er stor forskel på, om en hacker kan udføre det maksimale antal forkerte forsøg hver halve time eller en gang om dagen, før kontoen bliver spærret.

Det er endvidere relevant, at politikken fastsætter, hvordan låste konti bliver genåbnet. Det er problematisk, hvis en it-bruger kan ringe til servicedesk og anmode om at få sin konto låst op og med det samme få det nye, midlertidige password oplyst over telefonen. Her vil hackeren kunne udgive sig for at være brugeren og derved få adgang til kontoen. En løsning kan være, at det nye password bliver sendt til brugerens mobiltelefon eller til en kollega. Det tilsendte password skal altid kun kunne bruges ved første login.

Anvender organisationen sikkerhedsspørgsmål som f.eks. "Hvad hedder min far" til it-brugerens egen genåbning af kontoen, er der risiko for, at disse spørgsmål kan gennemskues og umiddelbart besvares af hackere ved hjælp af social engineering eller ved at google it-brugeren. Sendes SMS-kode til oplåsning af kontoen til mobiltelefonen, er det vigtigt at være opmærksom på, at telefonen skal sikres med automatisk lås med kode, samt at SIM-kort er låst med pinkode, i tilfælde af, at den mistes.

Forsinkelse på nye loginforsøg

En anden metode er såkaldt 'throttling' eller 'forsinkelse'. Her bliver kontoen ikke spærret, men for hvert fejlagtigt loginforsøg – eller efter et givet antal fejlagtige loginforsøg – er der etableret en tidsmæssig forsinkelse, før der kan gennemføres et nyt forsøg. Denne forsinkelse kan gøres eksponentielt større for hver fejlagtig session.

Monitorering af login

Center for Cybersikkerhed ser ofte, at organisationer bliver ramt af cyberangreb, hvor man efterfølgende kan konstatere, at vigtige logge fra de berørte it-systemer ikke er til rådighed til at analysere angrebet. Logning – og opsamling af disse – fra udstyr og systemer i organisationens infra-

struktur er afgørende for myndigheder og virksomheders evne til at opdage et cyberangreb hurtigt og efterfølgende effektivt afdække konsekvensen.

Center for Cybersikkerhed har udarbejdet vejledningen *Logning – en del af et godt cyberforsvar*, der indeholder en række anbefalinger og tiltag til at inddrage logning i organisationens cyberforsvar.

Center for Cybersikkerhed anbefaler, at der benyttes kontospærring eller 'throttling', og at der er strenge krav til genåbning af låste konti.

Tip 8 - Sikker håndtering af passwords

Organisationen skal have en meget restriktiv kontrol med, hvordan den teknisk håndterer sine passwords.

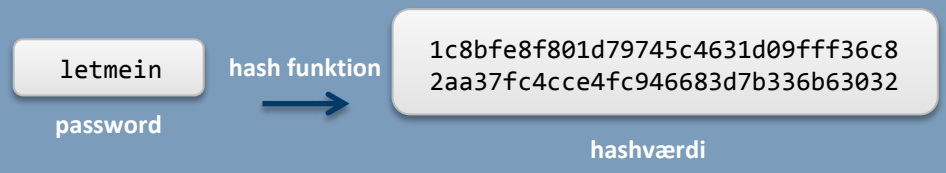
Passwords bør ikke opbevares i klartekst. Hvis passworddatabasen bliver kompromitteret, er det vigtigt, at data er gemt sikkert, så en hacker ikke umiddelbart kan bruge informationerne.

Password hash

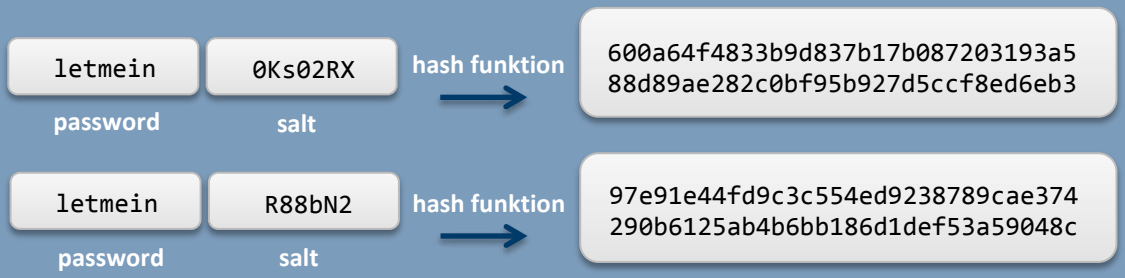
For at undgå direkte lagring af passwords, benyttes ofte en hash funktion. Ved hashing konverteres passwords af forskellig længde til en bitstreng af fast længde. Det er derved ikke muligt at gennemskue passwordets længde eller kompleksitet ud fra den hastede værdi, da den hashede værdi altid vil have den samme længde. Selv en lille ændring i passwordet vil ændre den hashede værdi fuldstændigt.

I modsætning til kryptering er metoden med at benytte konvertering af password til hash en envejsfunktion, og det er ikke muligt at finde et password ud fra hashen uden at gætte. Ved hashing er det vigtigt, at der bliver benyttet en hashfunktion, der er beregnet til passwords.

Som ekstra sikkerhed tilføjes en såkaldt 'salt' til passwordet, inden det hashes. Dette beskytter mod 'rainbow table'-angreb, hvor den hashede værdi af passwordet er kendt. I nedenstående boks kan ses et eksempel på, hvordan et hashed password ser ud.



Når der tilføjes en salt, ændres hele hash-værdien. 'Salten' er et tilfældigt unikt input, der gør, at passwordet får en anden hash-værdi, og derfor ikke vil kunne slås op i en rainbow table. Så selvom to passwords er ens, vil deres tilhørende hash værdi være vidt forskellige.



Center for Cybersikkerhed anbefaler, at passwords bliver hashed med en password-hash-funktion, at der anvendes salt, og at det kun er den hashede værdi, der bliver gemt i databasen.

Tip 9 - Organisationens passwordpolitik

For at imødegå hackerangreb hvor passwords anvendes, stilles der ofte større og større krav til passwords længde og kompleksitet. Men det kan være svært at huske mange og komplicerede passwords, og derfor kan det være fristende at genbruge passwords, eller at skrive dem ned enten fysisk eller på computeren, hvor det er nemt at få fat i dem igen.

Håndteres hackertruslen ved at lave for strenge krav til passwords, kan det således aktivere truslen fra it-brugere internt i organisationen.

Topledelsen kan med fordel tænke organisationens passwordpolitik på en ny måde, der i højere grad tager udgangspunkt i organisationens tilpassede sikkerhedsniveau, herskende kultur og brugeradfærd. Med en passwordpolitik, der bygger på ønsket om en mere enkel tilgang til passwords, er det muligt at optimere brugernes muligheder for at sammensætte passwords af forskellig styrke og huske dem.

Den overordnede passwordpolitik skal implementeres med det nødvendige ledelsesmæssige fokus og de nødvendige understøttende teknologiske løsninger. Passwordpolitikken skal udarbejdes med fokus på, at der er forskel på de sikkerhedsmæssige krav til kontrol med adgang til forskellige systemer og services. Kravene til passwords kan af sikkerhedsmæssige årsager således være forskellige for en organisations interne system og dens internet- og kundevendte system.

Den overordnede passwordpolitik kan bygge på principper som:

- Passwords anvendes, når det er nødvendigt og i relation til de sikkerhedsmæssige krav
- Undgå unødigt komplicerede passwordregler – god længde, lavere kompleksitet
- Password må ikke genbruges som adgang til flere systemer
- Anvend mindst to-faktor-autentifikation som middel til at øge sikkerheden
- Brugervenlighed – kultur og adfærd i organisationen
- Awareness, awareness, awareness
- It-understøttelse som passwordmanagers, der hjælper brugeren med at håndtere passwords
- Krav til sikker teknisk håndtering af passwords

Tjekliste

It-brugere

- ☐ Undgå det typiske password
- ☐ Lav huskeregler for oprettelse af passwords uanset styrke (tip 1)
- ☐ Undgå genbrug af passwords på tværs af konti
- ☐ Forstå begrænsningerne ved tests af passwordstyrke

Managementniveau

- ☐ Følg rådene om passwords uanset styrke (tip 1)
- ☐ Anvend to-faktor-autentifikation som middel til at øge sikkerheden (tip 2)
- ☐ Fastsæt valg af tekniske løsninger til hjælp til håndtering af passwords (tip 3)
- ☐ Fastsæt hvor ofte password skal ændres, så brugeren tilgodeses (tip 3)
- ☐ Iværksæt programmer for awareness og brugertræning (tip 4)

It-drift/leverandørniveau

- ☐ Kontroller organisationens regler for ændring af standard-passwords (tip 5)
- ☐ Iværksæt en blackliste med de mest anvendte passwords
- ☐ Hav særligt fokus på administrator-, service- og fjernbrugerkonti (tip 6)
- ☐ Iværksæt kontospærring og forsinkelse efter fejlede loginforsøg (tip 7)
- ☐ Monitorér login (tip 7)
- ☐ Sikker håndtering af passwords (tip 8)

Topledelse

- ☐ Udsend en passwordpolitik på grundlag af gennemført it-risikovurdering (tip 9)

Henvisninger

Password Guidance – Simplifying your Approach
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Logning – en del af et godt cyberforsvar

https://fe-ddis.dk/cfcs/publikationer/Documents/Vejledninger_finalapril.pdf

Phishing uden Fangst – Udenrigsministeriet under angreb

https://fe-ddis.dk/cfcs/CFCSDocuments/Phishing%20uden%20fangst.pdf

Madum, John: Bogen om password (Books on demand 2016, ISBN 978-87-7170-465-5)