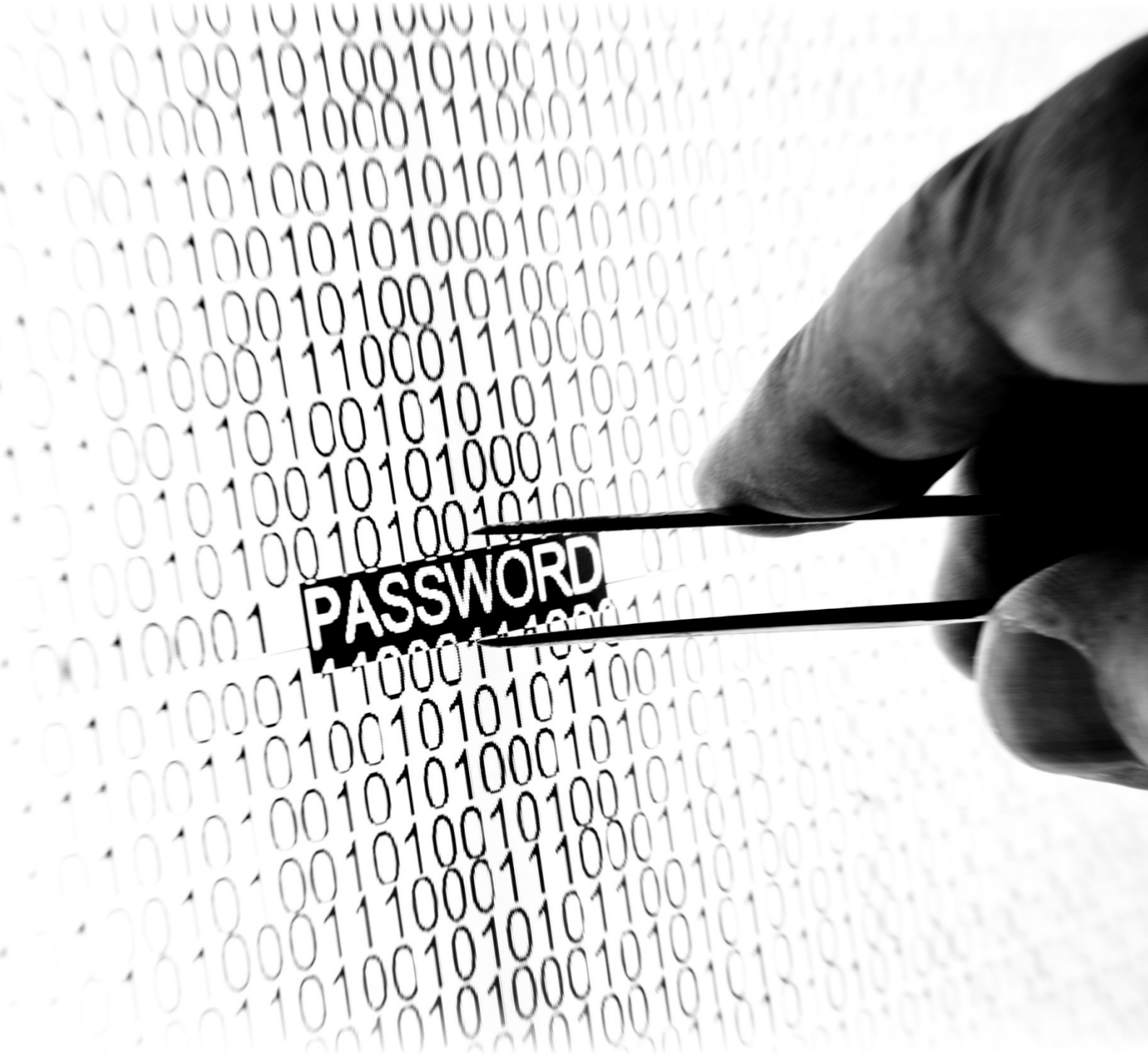
CENTER FOR CYBERSIKKERHED



Vejledning

Passwordsikkerhed

Passwordvejledning til it-brugere, -udviklere, -driftsfolk og ledelsen.

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

4. udgave, oktober 2023.

Forsideillustration: LuisPortugal/Getty Images.

Indledning

Gode passwords er en forudsætning for, at vigtige og måske fortrolige informationer beskyttes mod uønsket adgang. De fleste passwordvejledninger anbefaler, at man skal anvende forskellige passwords til forskellige konti, og at passwords til stadighed skal være længere og mere komplekse for at gøre det vanskeligere for hackere at bryde dem.

For mange it-brugere er det en udfordring med konstante krav om nye, komplekse (kombination af store og små bogstaver, tal og specialtegn) og lange passwords. Det kan derfor være fristende at opbevare dem, så man hurtigt og nemt kan få fat i dem. Men ikke alle opbevaringsmetoder er lige sikre, og risikoen for, at de havner i de forkerte hænder, er stor. Der er for eksempel stor forskel på sikkerheden i at gemme sine passwords i en fil eller i en passwordmanager.
Så selvom organisationer forsøger at øge sikkerheden med krav til hyppige skift, længden og kompleksiteten af passwords, så kan det resultere i, organisationen opnår det modsatte.

Denne vejledning beskriver nogle af de angrebsmetoder, som hackere benytter sig af, samt nogle af de eksisterende udfordringer ved passwords. Vejledningen indeholder desuden en række konkrete anbefalinger til, hvordan man – på forskellige niveauer i en organisation – bør arbejde med passwordsikkerhed.

Målgruppe

Vejledningen kan både bruges af forskellige medarbejdergrupper i en organisation, samt af it-udviklere, der skal sikre systemer. Herunder er beskrevet, hvilke kapitler hver medarbejdergruppe med fordel kan læse:

It-brugere

It-brugere er alle medarbejdere, der skal bruge passwords for at få adgang til systemer. It-brugere kan bruge vejledningen som inspiration til at lave gode passwords, og til hvordan passwords beskyttes. Læs især kapitlerne *Hvad er et godt password*, *Flerfaktor-autentifikation* og *Hjælp til håndtering af overfloden af passwords*. Se også eksempler på gode passwords i bilag 2.

It-drift og implementering

It-drift og implementering er i denne vejledning den del af organisationen, der er ansvarlige for anskaffelse eller drift af systemer og tjenester, der kræver autentifikation. Læs især kapitlerne *Ændring af alle standard-passwords*, *Fokus på privilegerede konti*, *Kontospærring og monitorering af login* og *Sikker håndtering af passwords i systemer*. Medarbejdergruppen bør også give input til forretning- og it-ledelsen

om, hvordan drift og implementering af passwords fungerer i organisationen.

Forretnings- og it-ledelsen

Forretnings- og it-ledelsen er i denne vejledning den del af organisationen, som har til opgave at kende trusler mod og potentielle sårbarheder ved passwords, vurdere risikoen og på den baggrund udarbejde en passwordpolitik. Det er også it-ledelsens ansvar, at passwordpolitikken implementeres og formidles til relevante interessenter.
Forretnings- og it-ledelsen kan benytte vejledningen som inspiration til at definere mere konkrete krav til, hvordan den overordnede passwordpolitik bør udmøntes i praksis. Læs især kapitlerne *Hvad er et godt password*, *Flerfaktor-autentifikation*, *Hjælp til håndtering af overfloden af passwords, Awareness og træning, Kontospærring og monitorering* og *Organisationens passwordpolitik*.

Topledelsen

Topledelsen kan benytte vejledningen til at få en øget forståelse for, hvordan passwords bruges i organisationen. Læs især kapitlerne *Awareness og træning* samt *Organisationens passwordpolitik*.

Vejledningen er også målrettet it-udviklere. It-udviklere kan hente inspiration til arbejdet med at sikre, at systemer udvikles, så både brugerinteraktion med passwords og lagring af password kan ske på en sikker måde. Læs især kapitlerne *Fokus på privilegerede konti*, *Kontospærring og monitorering af login* og *Sikker håndtering af passwords i systemer*.

Overordnede anbefalinger

Herunder er en samling af de overordnede anbefalinger til valg af passwords og passwordpolitikker, som gennemgås i denne vejledning. Der er dog ikke tale om en udtømmende liste, der er dækkende for alle situationer, da enhver organisation bør tage afsæt i sin egen situation og risikoprofil.

For login med passwords:

- Anvend flerfaktor-autentifikation på alle internetvendte systemer.
- Anvend flerfaktor-autentifikation hvor muligt.
- Anvend en passwordmanager til at gemme og generere passwords.
- Genbrug ikke passwords.
- Et password bør være minimum 15 tegn

Passwordpolitikker:

- Undgå unødigt komplicerede passwordregler – sigt efter god længde og lavere kompleksitet.
- Benyt tvunget passwordskift, hvis der findes tegn på eller mistanke om kompromittering.
- Anvend single sign-on for at gøre det nemt for brugerne at tilgå organisationens systemer.
- Anvend flerfaktor-autentifikation på al fjernadgang og alle privilegerede konti.
- Hav en negativliste for at forhindre brug af ofte anvendte passwords.
- Hjælp brugerne til sikker håndtering af passwords gennem regelmæssige awareness-tiltag.

Udfordringer ved passwords

Gode passwords er komplekse. Derfor stilles der typisk krav til, at et password skal indeholde en blanding af store og små bogstaver, tal og specialtegn. Der stilles også krav til minimumslængden. Og i nogle tilfælde stilles der også krav til, at passwords ændres med et fast tidsinterval.

De mange krav skaber udfordringer for it-brugeren. Særligt svært bliver det, når man skal huske mange komplicerede passwords. Det fører ofte til en uhensigtsmæssig adfærd hos brugeren, der for nemheds skyld fristes til at genbruge passwords, lave lette systemer til fornyelse af passwords eller gemme passwords på en uhensigtsmæssig måde.

Når vores adfærd er uhensigtsmæssig, opnår vi ikke den sikkerhed, som gode passwords skal være med til at give vores organisationer. Det gør vi ikke, fordi hackerne kender til vores uhensigtsmæssige adfærd og udnytter den til at kompromittere it-brugeren. Ud over metoder som phishing og social engineering, hvor hackerne forsøger at franarre brugeren deres password, benytter hackerne også metoder som brute force, rainbow table, ordbogsangreb og password spraying. Metoderne er nærmere beskrevet i Bilag 1, Hackerens fokus på s.23.

Den typiske og uhensigtsmæssige passwordadfærd
For at gøre det nemt for sig selv og samtidig efterleve de mange krav til sammensætningen af nye passwords, udviser mange it-brugere en uhensigtsmæssig adfærd som for eksempel:

- 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 erstatte 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 tegn. Nogle tegn har vist 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 tasternes rækkefølge på tastaturet.
- Passwordet er det samme som brugernavnet eller en del af det.
- Passwordet består af navne på familie, venner, husdyr osv.

Hvis der gennemtvinges periodisk ændring af passwordet, sammensætter brugere ofte et nyt, som er næsten identisk med det tidligere.

Passwordstyrke

Selv om 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 15 tegn med en blanding af store og små bogstaver, tal og specialtegn, kan et password se således ud:

Password123456!

Udbredte passwords

Som i eksemplet ovenfor, hvor et password lever op til de formelle krav, men stadig ikke kan betragtes som sikkert, kommer mange til at vælge et password, som andre også har valgt, og derfor nemt kan gættes af en hacker. Lister over de mest udbredte passwords er frit tilgængelige på internettet og kan afprøves på et enkelt brugernavn eller på tværs af mange i et password spraying-angreb.

De mest benyttede passwords i den engelsksprogede verden.

Brug af lækkede passwords

Når en samling af brugernavne og passwords bliver lækket på internettet fra eksempelvis en kompromitteret hjemmeside, indgår disse også hurtigt i en hackers arsenal og tilføjes til listen af passwords, der kan være værd at afprøve. På https://haveibeenpwned.com kan man tjekke, om ens egne kontooplysninger eller konti fra ens domæne har optrådt i kendte lækager. Man bør ikke tjekke med passwords, man aktivt bruger.

Hvad er et godt password?

Det er svært at komme med konkrete og præcise råd om valg af passwords, der passer til alle situationer og trusselsbilleder. Det er derfor vigtigt, at der på baggrund af en risikovurdering findes en kombination af sikringstiltag, der giver en passende balance mellem sikkerhed og anvendelighed i relation til, hvad passwordet giver adgang til.

Er flere systemer forbundet med hinanden, som ved single sign-on, bør kravet til passwords defineres af det mest forretningskritiske system. Internetvendte systemer er ofte mere sårbare end interne systemer, der ikke har forbindelse til internettet.

Selv om kompleksitet reducerer risikoen for, at eksempelvis et brute force-angreb lykkes, er længden på passwordet en vigtigere faktor. Da krav om kompleksitet kan føre til forudsigelige mønstre i valg af passwords, bør der i stedet overvejes at stille højere krav til længde og supplere med andre sikringstiltag. Se kapitlet *Kontospærring og monitorering af login s.188* for yderligere information om sikringstiltag, der kan reducere risikoen for brute force-angreb.

Et af de sikringstiltag, der er mest effektivt som supplement til ethvert password, uanset styrke, er flerfaktor-autentifikation. Se kapitlet

Flerfaktor-autentifikation *s.10* for yderligere information.

Alternativt kan man, hvis organisationens autentifikationsplatform tillader det, i nogle tilfælde helt undgå passwords. Se afsnittet *Adgang uden password s.9* for mere information.

Vær opmærksom på, at uanset hvor mange sikringstiltag, der etableres som supplement til passwords, vil de aldrig gøre et system 100 procent sikkert.

Passwords og passphrases
Der findes mange forskellige råd til valg af passwords. Uanset hvilken metode man vælger, er det vigtigt, at metodevalget ikke deles med andre. Det er også vigtigt, at passwordet har en tilstrækkelig længde. Passwords bør være på minimum 15 tegn, særligt hvis det ikke er muligt at indføre flerfaktor-autentifikation. Se mere herom i kapitlet

Flerfaktor-autentifikation *s.10.*

Eksempler på password:
En metode kan være at bruge det første bogstav fra hvert af ordene i en sætning:

Jcgpa,nss,m-hdr = *Jeg cykler gerne på arbejde, når solen skinner, men ikke hvis det regner*
(Her er ordet "ikke" erstattet med tegnet "-")

En anden metode kunne være at vælge en sangtitel og kombinere den med kunstnernavn og tegn/tal:

HvalenValborg1976Shu-Bi-Dua

En anden tilgang kan være at konstruere en passphrase, der består af nogle tilfældige ord, der er nemme at huske, og som giver en betydelig længde. Hvis man anvender en kombination af almindelige ord, er det vigtigt at øge længden til minimum 20 tegn.

Eksempler på passphrases:
En metode kan være at kombinere ord inspireret af et rum i hjemmet:

GryderOpskriftKnivSkabMad

En anden metode kan være at kombinere ord inspireret af den seneste rejse, man har været på:

CafeMuseumPoolSolFerie

Det er også muligt at øge kompleksiteten af sin passphrase ved at erstatte nogle af bogstaverne med tal og specialtegn, f.eks. ændre dobbelt o til % og l til 1. Så vil tidligere eksempel blive til:

CafeMuseum.P%1So1Ferie

De angivne eksempler på passwords og passphrases skal selvfølgelig ikke benyttes, da de med denne vejledning er offentligt tilgængelige.

Hvis man anvender en passwordmanager, og dermed ikke har brug for at kunne huske alle sine unikke passwords, kan man stadig med fordel bruge meget komplekse og lange passwords. Ofte kan disse genereres af passwordmanageren.

Adgang uden password
Da passwords kan være svære at huske og nemme at gætte, og da de ofte genbruges og kan optræde i datalæk, har der i internationale fora været arbejdet på at finde en erstatning for dem.

Med vedtagelsen af FIDO2[1]-standarden er det nu blevet muligt at tilbyde nem og sikker adgang til hjemmesider og operativsystemer baseret på en offentlig/privat nøgle i stedet for passwords. Autentifikation baseret på FIDO2 løser mange af de problemer, der er forbundet med den klassiske anvendelse af passwords, og er samtidig nem at anvende for brugeren.

For at en bruger kan få adgang uden password til eksempelvis en onlineservice, skal brugerens konto registreres, og et unikt offentligt/privat nøglesæt genereres. Først vælger brugeren en autentifikator, der kan accepteres af serviceudbyderen (eksempelvis mobiltelefon eller USB-sikkerhedsnøgle). Brugeren låser den valgte autentifikator op med eksempelvis fingeraftryk, hardware-nøglens knap eller en pinkode, hvorefter et unikt nøglepar genereres. Nøgleparret er unikt knyttet til både autentifikatoren, brugerens konto og udbyderen. Den offentlige nøgle sendes til udbyderen, som gemmer den til brug for senere brugervalidering.

Når brugeren senere tilgår udbyderens service og angiver sit brugernavn, sender udbyderen et stort og tilfældigt tal (en såkaldt "nonce") til brugerens enhed. Det eneste, brugeren skal gøre, er at låse autentifikatoren op, ligesom under registreringen (eksempelvis med fingeraftryk). Enheden finder den relevante private nøgle, krypterer det tilsendte tal med nøglen og sender resultatet tilbage til udbyderen. Udbyderen validerer det tilsendte ved hjælp af den offentlige nøgle, der er gemt på vegne af brugeren, og kan på den måde bekræfte, at brugeren har adgang til sin private nøgle. Er valideringen succesfuld, gives brugeren adgang til servicen.

Ved anvendelse af FIDO2-baseret autentifikation sendes der således ikke noget password over internettet, og udbyderen af den service, der tilgås, gemmer ikke noget password eller anden information, der ikke må opsnappes eller lækkes. Man undgår derfor flere af de risici, der er forbundet med den klassiske anvendelse af passwords, samtidig med at metoden er nem at anvende i daglig brug.

CFCS anbefaler, at

- et password bør være minimum 15 tegn.
- hvis passphrases benyttes, bør de bestå af 5 ord, der tilsammen er minimum 20 tegn.
- passwords aldrig indeholder oplysninger, der kan associeres med brugeren eller organisationen, såsom varemærker.
- passwords ikke genbruges.

Flerfaktor-autentifikation

Mange systemer giver i dag mulighed for at anvende flerfaktor-autentifikation. Flerfaktor-autentifikation er et af de sikringstiltag, der er mest effektivt i forhold til at

[1] Læs mere om FIDO2 på siden: https://fidoalliance.org/fido2/

øge login-sikkerheden i forbindelse med adgang til kritiske informationer. Anvendes flerfaktor-autentifikation, kan der i de fleste tilfælde slækkes på kravet til passwordstyrke – både med hensyn til længde og kompleksitet.

Flerfaktor-autentifikation er karakteriseret ved, at brugeren får adgang med sit brugernavn suppleret med to eller tre af nedenstående faktorer:

- Noget brugeren ved (eksempelvis pinkode eller password)
- Noget brugeren har (eksempelvis ID-kort, nøglekort eller USB-sikkerhedsnøgler)
- Noget brugeren er (eksempelvis ansigtsgenkendelse eller fingeraftryk), kaldes også biometrisk identifikation

Oftest benyttes flerfaktor-autentifikation, hvor eksempelvis et password (noget brugeren ved) suppleres med godkendelse på mobiltelefonen (noget brugeren har).

Flerfaktor-autentifikation er allerede vidt udbredt og anvendes ofte eksempelvis i forbindelse med fjernadgang og netbank. Da flerfaktor-autentifikation øger login-sikkerheden markant, er det en god idé at introducere metoden, hvor det er muligt, og som minimum på systemer, hvor sikkerheden er prioriteret. Hvis en mailkonto kan bruges til at nulstille glemte passwords på andre konti, bør den eksempelvis beskyttes med flerfaktor-autentifikation.

Der findes flere forskellige flerfaktor-autentifikationsmetoder, for eksempel mobil-applikationer, der genererer engangskoder eller beder om bekræftelse ved loginforsøg, biometri som fingeraftryk eller ansigtsgenkendelse og USB-sikkerhedsnøgler (der også kan anvendes til adgang uden password).

Flerfaktor-autentifikation baseret på koder sendt via SMS er usikre og bør derfor ikke benyttes. Hvis det dog er eneste mulighed, så giver det bedre sikkerhed end brug af password alene.

Hvilken metode, der passer bedst til den enkelte organisation eller det enkelte formål, afhænger bl.a. af sikkerhedskravene og tilgængelige resurser til administration og teknologi.

Ved fjernbrugeradgang
Flerfaktor-autentifikation bør altid benyttes ved fjernbrugeradgang. En fjernbruger vil ofte logge på organisationens interne systemer fra mindre sikre steder. Det kan være fra brugerens eget personlige netværk, et hotelværelse eller en café. Fælles for internetadgangen disse steder er, at organisationen ikke kan sikre netværket eller styre den lokale sikkerhed og derfor kan være mere sårbar over for kompromittering af passwords.

CFCS anbefaler, at

- der anvendes flerfaktor-autentifikation hvor muligt.
- der altid anvendes flerfaktor-autentifikation på konti med privilegerede rettigheder.
- der altid anvendes flerfaktor-autentifikation ved fjernadgang til interne systemer.

Hjælp til håndtering af overfloden af passwords

For at undgå at brugerne skal håndtere mange og komplekse passwords, børorganisationen vurdere, hvor det er nødvendigt at stille krav om anvendelse af passwords, herunder krav til længden og kompleksiteten af passwords. Er der it-systemer eller services, hvor det vurderes, 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 passwordlængde og/eller -kompleksitet.

Single sign-on
Med single sign-on kan byrden på brugerne reduceres. Single sign-on er en meget udbredt løsning internt i organisationer, som giver brugerne adgang til flere it-systemer uden at skulle logge separat på hvert enkelt system. Hvis passwordet kompromitteres, får en hacker imidlertid adgang til alle de systemer, brugerens konto har adgang til, og derfor er en høj grad af sikkerhed også af afgørende betydning ved brug af single sign-on.

Denne vejledning forholder sig ikke til, hvilke leverandører man bør benytte til single sign-on ved login til hjemmesider og serviceydelser.

Passwordmanagere
En passwordmanager er software, der kan opbevare brugernes mange unikke og stærke passwords på en sikker måde. Fordelen ved en passwordmanager er, at brugerne kan have forskellige, lange og komplekse passwords til alle de steder, de skal logge ind, uden selv at skulle huske hvert enkelt. Passwordmanagers er låst med et hovedpassword, som selvfølgelig skal være meget stærkt, for hvis en hacker bryder hovedpasswordet, er der adgang til alle brugerens gemte passwords.

Der findes forskellige typer passwordmanagers:

- Browser-indbyggede passwordmanagers
- Browser-integrerede passwordmanagers
- Selvstændige passwordmanagers

Browser-indbyggede passwordmanagers bruges i de mest anvendte browsere til at gemme passwords til de hjemmesider, man besøger. Passwordmanageren kan synkronisere passwords på tværs af enheder via producentens tilknyttede cloudtjeneste. Denne løsning er nem at anvende, men understøtter oftest kun passwords til hjemmesider, og den tilbyder kun begrænset funktionalitet og begrænsede krypteringsmuligheder. Selv om de gemte passwords er krypterede, er selve adgangen til at kunne anvende dem afhængig af sikkerheden på den anvendte enhed. Denne løsning bør ikke anvendes til kritiske systemer.

Browser-integrerede passwordmanagers installeres som et plug-in i browserne. Funktionaliteten er udvidet i forhold til browser-indbyggede passwordmanagers. De kan ofte hjælpe brugeren med at generere sikre passwords, tjekke om passwordet

tidligere har været lækket på internettet, eller om passwordet er anvendt ofte og derfor frarådes. Passwords gemmes krypteret hos producenten og synkroniseres på tværs af enheder gennem dennes cloudtjeneste. Denne løsning bør ikke anvendes til kritiske systemer.

Selvstændige passwordmanagers er som udgangspunkt ikke integreret med browseren, og de har en reduceret angrebsflade. Når der skal logges ind på en hjemmeside, aktiveres passwordmanageren med et tastetryk, eller man kan selv kopiere passwordet fra den og sætte ind. Mange af disse passwordmanagers har samme funktionalitet som, de browser-integrerede produkter, nogle har endda bedre funktionalitet. Brugerne kan selv vælge, hvor de vil gemme deres krypterede passworddatabase. Nogle produkter understøttes automatisk af de større cloudtjenester, men brugeren kan også vælge at have databasen liggende lokalt eller hos en anden cloudtjeneste efter eget valg.

Hvis den krypterede passworddatabase opbevares i en cloudtjeneste, kan man nemt synkronisere på tværs af de computere og mobile enheder, man anvender, og dermed tilgå sine passwords, hvor man har brug for dem. Man skal dog sikre sig, at man ikke nøjes med at have en enkelt kopi af databasen hos en enkelt leverandør. Man skal altid have adgang til passwordmanageren, eksempelvis i tilfælde af at tjenesten lukker, oplever et kritisk nedbrud eller lider et uopretteligt datatab. Understøttelse af backup og mulighed for at eksportere data bør derfor være et parameter i forbindelse med valg af produkt.

Der bør vælges blandt veletablerede og gennemprøvede passwordmanagers. Passwordmanagers skal holdes opdateret, således at eventuelle sikkerhedsrettelser kan afhjælpe kendte sårbarheder i produktet.

Uanset platform er det vigtigt, at det hovedpassword, der bruges til at låse op for adgangen til de krypterede passwords, er meget stærkt. Det kan med fordel suppleres med en flerfaktor-autentifikation som eksempelvis USB-sikkerhedsnøgle og/eller biometrisk adgangskontrol.

I organisationer med integreret single sign-on og få passwords er der som regel ikke brug for passwordmanagers. Der kan dog være enkelte afdelinger, der i kraft af deres funktion har behov for at gemme mange passwords. Det kan eksempelvis være it-driftsfunktionen, kommunikationsafdelingen eller indkøbsafdelingen. Der findes produkter på markedet, der kan understøtte rettighedsstyring af adgang til passwords, systematisk ændring af passwords på kritiske servicekonti og logning af, hvem der har tilgået hvilke passwords hvornår, som organisationer med behov for at administrere mange privilegerede konto-oplysninger kan benytte. Ligeledes bør passwordmanagers, der bruges til arbejdsrelaterede passwords, ikke benyttes til passwords, man benytter i sit privatliv.

De passwords, der måtte være nødvendige for reetablering i forbindelse med større kritiske driftshændelser, bør opbevares i fysisk form et sikkert sted, så adgangen til dem ikke er afhængig af en normal driftssituation.

Indkøb af passwordmanager

Organisationen bør sikre sig, ved indkøb af en passwordmanager, at den valgte løsning også lever op til organisationens vedtagne sikkerhedskrav. CFCS har udarbejdet en række anbefalinger, som organisationen bør sikre sig, at passwordmanageren kan leve op til.

- Ved tilgang til passwordmanageren:
  - bør brugerens hovedpassword følge organisationens passwordregler.
  - bør brugeren benytte flerfaktor-autentifikation.
- Passwordmanageren bør være produceret og driftet i et land, som organisationens risikovurdering ikke betegner som højrisiko.
- Passwordmanageren bør:
  - generere tilfældige passwords, som efterlever både organisationens passwordregler og det eksterne systems eller hjemmesides passwordkrav.
  - opbevare passwords som hashede og saltede værdier ved brug af velafprøvede password hash-funktioner.
  - kunne udfylde brugerens loginoplysninger automatisk på tidligere tilgåede hjemmesider og systemer.
  - kunne slette passwordet fra udklipsholderen efter en bestemt tidsperiode når passwordet er kopieret.
  - kunne informere organisationen og brugeren, hvis en tidligere tilgået hjemmeside og/eller et system er blevet kompromitteret.
  - informere brugeren, i tilfælde af at organisationens passwordregler ikke overholdes ved oprettelse af et nyt password.
  - være tilgængelig på alle brugernes operativsystemer.
  - være under aktiv support for sikkerhedsopdateringer.
  - logge aktiviteten på passwordmanageren.
- Hvis der benyttes onlinesynkronisering, skal der være end to end-kryptering.

Maskingenererede passwords

Maskingenerede passwords kan være med til at øge sikkerheden, fordi disse tilfældigt genererede passwords er mindre forudsigelige og svære at bryde. Ulempen er dog, at passwordet kan være så komplekst, at brugeren ikke kan huske det. Anvendes der ikke en passwordmanager, bør passwords genereres ved hjælp af en metode, der sikrer en sammensætning, der gør dem nemmere at huske. Maskingenererede passwords kan eksempelvis bestå af fem 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. Anvendes der en passwordmanager, kan maskingererede password have lang længde og høj kompleksitet, da brugeren i dette tilfælde ikke selv behøver at kunne huske det.

Ændring af passwords
Hvor det tidligere har været betragtet som god praksis at gennemtvinge regelmæssige skift af passwords, er det ikke nødvendigvis tilfældet mere. Baggrunden for praksis med at skifte password f.eks. hver tredje måned var at begrænse den tid, en hacker havde til rådighed til at kompromittere og anvende et password. Den hyppige ændring af passwords har dog vist sig at føre til, at mange brugere vælger svagere passwords, der er nemmere at huske, eller bruger en fast fremgangsmåde til at vælge et nyt password, der eksempelvis kan være baseret på månedsnavn/tal, årstid el.lign., der er nemt at knække for en hacker.

Hvis en organisation har implementeret sikringstiltag, der reducerer risikoen for kompromittering af passwords, kan den på baggrund af sin risikovurdering vælge ikke at kræve regelmæssig ændring af passwords. Disse sikringstiltag bør inkludere:

- Awareness-træning af brugere i håndtering og valg af sikre passwords.
- Politikker understøttet af tekniske kontroller, der sikrer relevant passwordlængde og evt. -kompleksitet.
- Kontrol med at ofte anvendte eller allerede lækkede passwords ikke vælges.
- Kontrol med at brugeren ikke skifter tilbage til et af brugerens tidligere benyttede passwords.
- Begrænsning af antal mulige loginforsøg eller throttling (se kapitel *Kontospærring og monitorering af login s.188*).

Hvis der er mistanke om eller bevis for, at et eller flere passwords er kompromitteret, bør et passwordskift dog altid gennemtvinges.

CFCS anbefaler, at

- passwordmanagers anvendes, når der er behov for at gemme mange unikke passwords.
- valg af løsning baseres på, hvad passwords giver adgang til, og at det sker i henhold til organisationens risikovurdering.
- tvunget passwordskift kun bør benyttes, hvis der findes tegn på kompromittering.
- der implementeres en procedure for at gennemtvinge passwordskift ved mistanke om kompromittering.
- det i organisationen overvejes, hvilke tekniske løsninger der vil være hensigtsmæssige at implementere med det formål at hjælpe it-brugeren.

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 f.eks. udgiver sig for at være kolleger i it-afdelingen, som gerne vil kontrollere eller nulstille et password, eller hvis de modtager uventede eller mistænkelige mails.

Det er ledelsens ansvar at fokusere på organisationens kultur og it-brugernes adfærd og dermed være opmærksom på om der er behov for at informere om nye angrebsmetoder. Der bør gennemføres awareness-træning i valg af gode passwords samt god sikkerhedspraksis i almindelighed, og det bør kontrolleres, at krav og forventninger til adfærd efterleves.

CFCS anbefaler, at

- ledelsen planlægger og gennemfører den nødvendige awareness-træning i passwordpolitikken for organisationens it-brugere.

Ændring af alle standard-passwords

It-udstyr og software leveres ofte fra leverandøren med systemkonti og standard-passwords. Det ved hackerne godt, og standard-passwords bør derfor altid ændres, inden udstyr og software tages i brug.

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 hackere at skaffe sig adgang. Især er det vigtigt at være opmærksom på at få udarbejdet en procedure for ændring af standard-passwords, så ændringen foretages ved opsætning af et system. Det kan eksempelvis 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.

CFCS anbefaler, at

- implementere ændring af standard-passwords som en fast procedure, i forbindelse med at udstyr og software tages i brug.

Fokus på privilegerede konti

Nogle konti er vigtigere at sikre end andre. Hvis administrator-, service- eller systemkonti kompromitteres, er der høj risiko for uautoriseret adgang til kritiske informationer, og der er derfor behov for ekstra beskyttelse af disse privilegerede konti. Derfor bør adgangen til dem sikres med flerfaktor-autentifikation, og der bør anvendes længere og mere komplekse password.

Administratorrettigheder
Almindelige it-brugere har normalt ikke behov for udvidede rettigheder til it-systemer og -infrastruktur. Alle it-brugeres rettigheder skal altid tildeles på baggrund af et arbejdsbetinget behov.

Rollen 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 bør være særligt opmærksomme på at beskytte deres passwords. Adgangen til administrative konti bør sikres med flerfaktor-autentifikation. Er dette ikke muligt, bør der anvendes lange og komplekse passwords. Administrative konti bør alene anvendes til de opgaver, hvor de udvidede rettigheder er påkrævet.

Til daglige opgaver såsom håndtering af mails og internetadgang bør der anvendes en almindelig brugerkonto uden administrative rettigheder.

En administrativ konto bør være personlig, og passwordet til en sådan konto må kun kendes af den administrator, kontoen er tildelt. Ved afgang af personale med administrative rettigheder bør den personlige privilegerede konto straks lukkes, og passwords på alle service-konti, administratoren har haft kendskab til, skiftes. Denne proces kan i nogle kommercielle produkter til administration af privilegerede konti automatiseres eller helt undgås gennem anvendelse af engangspasswords.

Håndtering af privilegier
For bedre at holde styr på privilegerede konti kan organisationen benytte et Privileged Access Management (PAM)-system. PAM-løsninger bygger på at styre, monitorere og sikre brugen af privilegerede rettigheder og kan benyttes til at centralisere og effektivisere styring af privilegerede konti.

CFCS anbefaler, at

- administrative konti kun anvendes, når der udføres aktiviteter, der kræver administrative privilegier.
- privilegerede konti sikres med flerfaktor-autentifikation.

- der følges en fast og dokumenteret proces for nedlukning af privilegeret adgang for afgående administratorer.

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 mod flere forskellige typer af hackerangreb, der er beskrevet i Bilag 1 s.23:

Kontospærring
Kontospærring kan være en metode til at hindre, at hackere ved hjælp af et online-angreb formår at bryde et password og få adgang til interne it-systemer. Brugerkontoen bliver spærret, når brugeren eller hackere uden held har opbrugt det tilladte antal loginforsøg. På denne måde kan hackere ikke udføre brute force- og ordbogsangreb.

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

Politikken bør fastsætte, hvornår antallet af registrerede mislykkede loginforsøg skal nulstilles. Dette kan imødegå password spraying-angreb, som er beskrevet i Bilag 1 *Hackerens fokus s.23*. Der er stor forskel på, om en hacker kan udføre det maksimalt tilladte antal forkerte forsøg hver halve time eller én gang om dagen, før kontoen bliver spærret.

Det er desuden 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 en hacker kunne udgive sig for at være brugeren og derved få adgang til kontoen. En løsning kan være, at et midlertidigt engangspassword udleveres via en kollega eller nulstilles på baggrund af en eksisterende flerfaktor-autentifikationsmetode.

Organisationen bør ikke benytte sikkerhedsspørgsmål som eksempelvis ”Hvad hedder min far” til it-brugerens egen genåbning af kontoen, da der er risiko for, at disse spørgsmål kan gennemskues og umiddelbart besvares af hackere ved hjælp af social engineering eller åbne kilder som f.eks. sociale medier.

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 givent antal fejlagtige loginforsøg – er der etableret en tidsmæssig forsinkelse, før der kan gennemføres et nyt forsøg. Denne forsinkelse kan gøres eksponentielt større for hvert fejlagtigt loginforsøg.

Notifikation af bruger ved login
Hvis en bruger logger på fra en enhed, der ikke før har været anvendt, kan en notifikation til brugeren om dette login, eksempelvis via mail eller SMS, være med til at øge muligheden for at opdage kompromitterede konti, så brugeren og organisationen hurtigt kan tage de nødvendige foranstaltninger.

Monitorering og logning af login
For at imødegå potentielle brud på sikkerheden bør organisationen monitorere loginforsøg. Monitoreringen vil ofte blive foretaget automatisk via software, der advarer de relevante medarbejdere, hvis, for eksempel, antallet af loginforsøg afviger fra organisationens normalbillede. Advarsler fra monitoreringsværktøjet kan justeres i forhold til, hvor kritisk eller sensitivt det pågældende system er. Derudover kan CFCS konstatere, at organisationer, der bliver ramt af cyberangreb, ofte ikke har de nødvendige logfiler fra de berørte it-systemer til rådighed til at analysere angrebet. Logning af udstyr og systemer i organisationens infrastruktur er afgørende for at kunne opdage et cyberangreb hurtigt og efterfølgende effektivt afdække konsekvensen.

CFCS har udarbejdet vejledningen *Logning – en del af et godt cyberforsvar (2023)*, der indeholder en række anbefalinger og tiltag til at inddrage logning i organisationens cyberforsvar.

CFCS anbefaler, at

- der benyttes kontospærring eller *throttling.*
- organisationen har en fast procedure med krav til genåbning af låste konti.
- loginforsøg logges og monitoreres.

Sikker håndtering af passwords i systemer

Organisationen bør sikre sig, at fortroligheden beskyttes i forbindelse med både anvendelse, kommunikation og opbevaring af passwords.

Anvendelse af passwords
Login-sider på systemer udbudt af organisationen bør tillade, at passwords kan kopieres ind i passwordfeltet, så anvendelse af passwordmanagers er understøttet. Det bør ligeledes ikke begrænses, hvor lange password der kan vælges, eller hvilke bogstaver eller tegn der er tilladt. Det anbefales yderligere, at brugeren ved valg af password bliver forhindret i at benytte et password, hvis det er udbredt eller kendt fra tidligere lækager. Til understøttelse af dette findes offentligt tilgængelige negativlister over ofte anvendte passwords og databaser af lækkede passwords, der kan integreres via et API (se eksempelvis https://haveibeenpwned.com).

Så vidt muligt bør organisationen understøtte flerfaktor-autentifikation på udbudte systemer i organisationen og overveje understøttelse af FIDO2-baseret adgang uden passwords ved opsætning og drift af nye systemer.

Kommunikation af passwords
På alle sider, hvor passwords indtastes eller på anden måde udveksles mellem enheder/systemer over et netværk, bør kommunikationskanalen være krypteret.

Opbevaring af 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.

I modsætning til kryptering er metoden, der anvendes ved konvertering af passwords 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 benyttes en standardimplementering af en velafprøvet hash-funktion, der er beregnet til passwords.

Som ekstra sikkerhed tilføjes et unikt salt til hvert password, inden det hashes. Dette sikrer, at den resulterende værdi, der gemmes, er unik for selv identiske passwords og beskytter således mod rainbow table-angreb (se Bilag 1 s.23).

Password hash
For at undgå direkte lagring af passwords benyttes der en hash-funktion. Ved hashing udregnes der på baggrund af et password en hash-værdi i form af en bitstreng af fast længde. Det er ikke muligt at gennemskue passwordets længde eller kompleksitet ud fra den hashede værdi, da den hashede værdi altid vil have den samme længde. Selv en lille ændring i passwordet vil ændre den hashede værdi fuldstændigt.

Salt
Tilfældig værdi, der tilføjes passwords, inden de hashes, således at den resulterende værdi altid er unik.

Såfremt et system understøtter adgang uden password via FIDO2-standarden, reduceres behovet naturligvis for at sikre opbevaring af passwords.

CFCS anbefaler, at

- brugergrænseflader tillader brug af passwordmanagers.
- brugergrænseflader tilpasses til at hjælpe brugeren med at vælge sikre passwords.
- der benyttes en negativliste for at forhindre brug af udbredte passwords.
- al kommunikation af passwords sker over krypterede forbindelser.
- der kun gemmes hashede værdier med unikke salt baseret på standardimplementeringer af velafprøvede password-hash-funktioner.

Organisationens passwordpolitik

For at imødegå hackerangreb stilles der ofte høje krav til passwordlængde 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 på papir eller på computeren, hvor det er nemt at få fat i dem igen.

Håndteres hackertruslen ved at stille for strenge krav til passwords, kan det utilsigtet føre til dårlig passwordpraksis, hvis passwordet ikke understøttes af eksempelvis single sign-on eller passwordmanagers.

Ledelsen kan med fordel tænke organisationens passwordpolitik ind i organisationens risikovurdering, herskende kultur og brugeradfærd. Passwordpolitikken bør implementeres med det nødvendige ledelsesmæssige fokus og de nødvendige understøttende teknologiske løsninger. Den bør 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 systemer.

CFCS anbefaler, at organisationen udarbejder en passwordpolitik, der er baseret på følgende punkter:

- Anvend passwords, når det er nødvendigt, og i relation til de sikkerhedsmæssige krav.
- Undgå unødigt komplicerede passwordregler – sigt efter god længde og lavere kompleksitet.
- Genbrug ikke passwords på tværs af systemer.
- Husk at passwords er personlige og ikke må deles.
- Anvend flerfaktor-autentifikation til at øge sikkerheden.
- Implementer og understøt brugen af passwordmanagers.
- Hav fokus på sikker teknisk håndtering af passwords.

Referencer

Australian Cyber Security Centre. (2021). Implementing Multi-Factor Authentication https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication

Canadian Centre for Cyber Security. (2019). Best practices for passphrases and passwords *https://cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032*

Center for Cybersikkerhed. (2023). Logning – en del af et godt cyberforsvar https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/

Grassi, P. A. et al. (2020). *Digital Identity Guidelines.* (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-3, Rev. 3, Includes updates as of February 3, 2020

Hunt, T. (2022). *Have I been pwned*. *https://haveibeenpwned.com/*

National Cyber Security Centre. (2018). password administration for system owners https://www.ncsc.gov.uk/collection/passwords

Bilag 1: Hackerens fokus

It-systemer tilgås ofte med brugernavne og passwords, som derfor er værdifulde for hackere. Samtidig målretter hackere deres angreb ved bl.a. at udnytte den viden, de har om brugere og deres passwords. Denne viden kan overføres til en række værktøjer, som hjælper hackeren med at bryde passwords, eksempelvis en keylogger, der registrerer al aktivitet fra tastaturet. I de følgende afsnit beskrives en række af de metoder, som hackere benytter, når de forsøger at få fat i eller bryde passwords.

Social engineering
Social engineering er en teknik, hvor der anvendes psykologiske greb til at få offeret til i god tro at udføre en handling, vedkommende ellers ikke ville have udført. Det kan eksempelvis være at afgive loginoplysninger eller videregive informationer om organisationen, dens processer, systemer eller kunder.

Mere avanceret social engineering anvender hackeren ofte informationer om ofret eller arbejdspladsen, som er fundet på hjemmesider eller sociale medier ved forudgående rekognoscering.

Social engineering kan bl.a. ske via mail (phishing), sms (smishing) eller telefon (vishing).

Phishing
Phishing er forsøg på at narre mailmodtagere til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller opnå uretmæssig adgang til bl.a. it-systemer.

Ofte vil hackeren ved hjælp af simpel social engineering forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer.

Phishing-mails sendes ofte bredt ud til mange tilfældige modtagere uden at være tilpasset den enkelte modtager.

Spear phishing
Spear phishing minder om almindelig phishing, men adskiller sig ved at være målrettet den enkelte modtager og anvende teknikker fra social engineering. Spear phishing-mails er typisk udformet, så de virker særligt relevante, overbevisende og troværdige for modtageren. Dette opnås ved for eksempel at anvende navne eller andre personspecifikke informationer, som er indsamlet på baggrund af en forudgående rekognoscering.

Genbrug
Mange genbruger ofte passwords. 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, når et password bliver lækket eller på anden måde kompromitteret.

Brute force

Ved et brute force-angreb afprøver hackeren alle mulige forekommende sammensætninger af tegn, tal og bogstaver. Denne type angreb kan tage meget lang tid, men vil altid lykkes, hvis der er tilstrækkelig tid og computerkapacitet.

Ordbogsangreb
Ordbogsangreb er en variation af et brute force-angreb. Her forsøger hackeren at gætte et password ved at bruge ofte anvendte ord og kombinationer af ord fundet i forskellige ordbøger. På en liste med mange vidt forskellige ord, samt kombination af disse, er der stor chance for at finde det password, hackeren leder efter.

Rainbow table
Passwords gemmes næsten aldrig i klartekst. I stedet bliver passwords bearbejdet af en matematisk envejsfunktion, en såkaldt hash-funktion. For at bryde disse hashes kan en hacker benytte sig af en rainbow table. En rainbow table indeholder en lang række forudberegnede hash-værdier, hvor man kender det oprindelige password, de er baseret på. Hvis en hacker kan finde en matchende hash-værdi i en rainbow table, er passwordet derfor brudt.

Password spraying
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 sandsynlighed for, at hackeren rammer rigtigt på et tidspunkt. Dette kaldes password spraying. Da der ofte er implementeret kontospærring, sørger hackeren for kun at afprøve få passwords på hver konto, så kontoen ikke spærres.

Standard-passwords
Når organisationer indkøber og idriftsætter ny hardware eller software, er disse ofte udstyret med standard-passwords fra producentens side. Hvis disse standard-passwords ikke ændres, kan hackere bruge deres kendskab til dem til at opnå administratoradgang.

Bilag 2 beskriver eksempler på metoder til opbygning af gode passwords eller passphrases. Vær opmærksom på, at de givne eksempler ikke bør anvendes, som de fremstår her.

Bilag 2

Eksempler på passwords (min 15 tegn)

Metode 1:

- Vælg land og hovedstad
- Fjern sidste bogstav i landet
- Indsæt min 2 tegn eller tal imellem ordene

Eksempler:

1. Vilnius#05Litaue
2. Paris17/&Frankri

Metode 2:

- Forbogstav for alle ord i en lang sætning
- Erstat evt. specifikke bogstaver med tal eller tegn

Eksempler:

1. Jcgpa,nss,m-hdr
   (Jeg cykler gerne på arbejde, når solen skinner, men ikke hvis det regner eller sner)
2. Ekøsd,0skdhismis
   (En kold øl smager dejlig, og så krummer det heller ikke så meget i sengen)

Metode 3:

- Titel på sang og kunstnernavn adskilt med tegn eller tal

Eksempler:

1. 1dagtilbage#Nik&Jay
2. HvalenValborg1976Shu-Bi-Dua
3. 8660$PeterSommer
4. Sjakaline?%Tessa

Eksempler på passphrases (min 20 tegn)

Metode 4:

- 5 ting/begreber fra et rum i hjemmet, ens seneste rejse, indkøbskurven mv. – start alle ord med stort

Eksempler:

1. GryderOpskriftKnivSkabMad
2. CafeMuseumPoolSolFerie
3. FrugtYmerKiwiKagerKaffe

Vær opmærksom på, at brugen af danske bogstaver i passwords og passphrases kan give udfordringer nogle steder. Erstat evt. disse med valgfrie tegn.