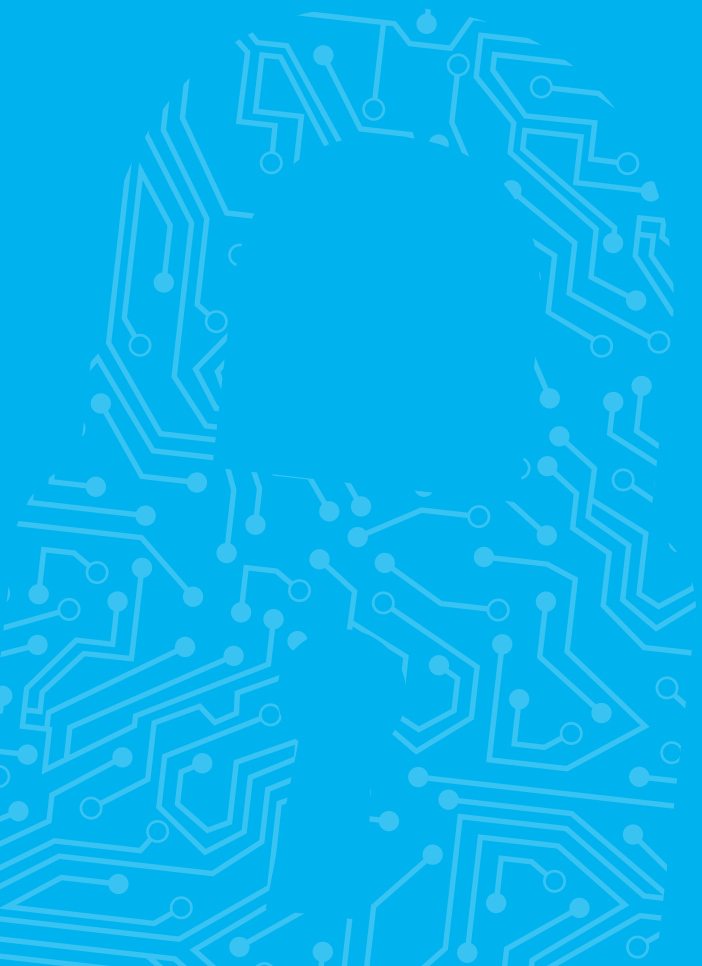
Glemte passwords koster – ikke længere!

– en grundig guide til sikkert valg af password self-service



SignaturGruppen

"FORKERT BRUGERNAVN ELLER PASSWORD."

Meldingen er frustrerende at blive mødt med, men den er ikke desto mindre dagligdag for tusindvis af medarbejdere i danske virksomheder og organisationer hver dag.

Et opkald til IT Helpdesk løser problemet, men det koster i begge ender af røret, og samtidig rummer den traditionelle måde at håndtere glemte passwords en række sikkerhedsmæssige udfordringer.

Både de ressource- og sikkerhedsmæssige udfordringer kan dog løses med password self-service, som giver brugeren mulighed for selv at nulstille sit password, vælge et nyt og komme hurtigt videre med arbejdet.

Vi har skrevet denne guide for at give et overblik over mulighederne inden for password self-service og et indblik i fordele og ulemper ved de forskellige løsningstyper.

Vi håber, du finder guiden brugbar. God læselyst!

Vidste du, at ..

... det 5. mest benyttede password på verdensplan er "football"?

Nummer 1 er "123456".

Indholdsfortegnelse

Vidste du, at ..

... at eksperter anbefaler passwords på mindst 13 karakterer, som ikke indeholder almindelige ord og består af både store og små bogstaver, tal samt specialkarakterer?

Hvad koster glemte passwords din organisation?

Det koster på flere måder, når en medarbejder har svedt sit password ud i sommerferien. Ikke nok med at både medarbejderen og IT Helpdesk skal bruge dyrebar tid, så giver det også anledning til overtræk på sikkerhedskontoen.

Men lad os starte med det, der er lettest at gøre op, nemlig de omkostninger, som IT Helpdesk har på håndtering af et glemt password. Ifølge Gartner beløber det sig til 22 dollars per opkald vedrørende glemte passwords, svarende til omtrent 145 kroner (2016).

En enkel måde at udregne omkostningen for de glemte passwords er altså at gange antallet af opkald vedrørende glemte password med 145.

Selvom beløbet i de fleste organisationer bliver ganske stort i sig selv, fortæller det kun én side af historien. For det rammer jo både medarbejderen og it-supporteren, når der skal bruges tid på glemte passwords.

Omkostningen på brugersiden er mere diffus, men givetvis en del højere end IT Helpdesks, da man som bruger kan risikere, at supporten ikke er åben, at man kommer til at vente i kø eller slet og ret ikke får fat i en supporter. Og imens tiden går, står arbejdet stille.

HØJ PRIS FOR DØGNSUPPORT

Vil man som organisation sikre, at ens medarbejdere kan arbejde på alle tider af døgnet, har man brug for en 24–7 support, og etablering af en sådan ordning er ganske kostbar.

Hvis supportens manuelle håndtering af glemte passwords er ét af argumenterne for at oprette en 24-7 support skal denne omkostning altså også tages med i betragtning.

GLEMTE PASSWORDS KOSTER PÅ SIKKERHEDSKULTUREN

Hvis man glemmer sit password og ikke kan komme igennem til IT Helpdesk, er det fristende lige at låne en kollegas loginoplysninger, så man kan komme videre med at løse sine arbejdsopgaver. Og har man gjort det én gang, kan man jo lige så godt gøre det samme næste gang, så man slipper for at ringe til supporten.

Det kan i situationen virke harmløst, men det er en direkte vej til en dårlig sikkerhedskultur, og det sætter de 'venlige' kollegaer i en urimelig konflikt mellem det personlige ansvar for it-sikkerhed og ønsket om at hjælpe en kollega med at få løst et problem.

GLEMTE PASSWORDS GIVER MINUS PÅ BRUGERVENLIGHEDSKONTOEN

Oven i de økonomiske og sikkerhedsmæssige omkostninger, er det også værd at tage mere diffuse parametre som frustration og service med i betragtning. Det er svært at regne om til kroner og ører, men det koster noget, at medarbejdere får en frustrerende oplevelse, når de egentlig bare ville i gang med at gøre deres arbejde.

Glemte passwords er (også) et spørgsmål om sikkerhed

Når man snakker håndtering af glemte passwords, vil mange organisationer ofte primært fokusere på brugervenlighed og effektivisering. Men sikkerheden må ikke overses, når man undersøger, hvordan man vil håndtere glemte passwords i fremtiden.

De fleste it-organisationer er i en løbende modningsproces, hvad angår intern it-sikkerhed, eksempelvis styret af compliance-krav i forhold til ISO 27000-standarderne.

ISO 27000-standarderne har password management som et centralt fokusområde. Det gælder både den indledende registrering af brugeren, sikker udlevering af password samt sikring af, at kun brugeren kender passwordet efterfølgende.

FLERE SVAGHEDER VED BRUG AF IT HELPDESK

En af de kritiske processer er håndtering af glemte passwords, og den meget udbredte praksis, hvor brugeren ringer til IT Helpdesk og beder om et nyt password, har flere svagheder.

- Hvordan validerer IT Helpdesk, at de snakker med den rigtige bruger?
- Hvordan kontrollerer organisationen, at IT Helpdesk ikke overtager en brugers konto med deres superadministrator rettigheder? Eventuelt blot midlertidigt?
- Hvordan sikres fortrolighed af passwords i medarbejderens dagligdag?

Det traditionelle svar på disse spørgsmål er at opretholde et kontinuerligt fokus på, hvordan sikkerheden holdes høj, blandt andet gennem oplæring af supportere, regelmæssig auditering og stikprøver for at tjekke, om der har været misbrug. Dette er tunge processer, som let kan blive nedprioriteret i en travl dagligdag, hvis man ikke er meget stærkt styret på it-sikkerhed.

„DET VAR IKKE MIG, NOGEN MÅ HAVE LÅNT MIT PASSWORD!“

Disse forhold skal man have styr på, hvis man vil kunne holde en medarbejder ansvarlig for de handlinger, der udføres med vedkommendes login og passwords. Har man ikke det, kan medarbejderen med god ret hævde, at det lige så godt kan have været en administrator eller en kollega, som har udført de givne handlinger.

De it-sikkerhedsudfordringer, som den traditionelle måde at nulstille passwords giver, kan man komme udenom, hvis man i stedet vælger en sikker password self-service løsning – altså en løsning, som giver brugerne mulighed for på egen hånd at nulstille sit password og vælge et nyt.

Men hvordan sikrer vi, at kun den rigtige bruger kan vælge et nyt password? Det er helt afgørende for sikkerheden, og i det næste afsnit vurderer vi fire forskellige autentifikationsmekanismer, man kan vælge til password self-service.

Hvilken password self-service løsning skal jeg vælge?

Skal det være et NemID papkort med engangskoder, en sms, en e-mail eller navnet på dit kæledyr, der åbner døren til det forjættede land, hvor du kan vælge et nyt password og komme videre med dit arbejde?

Mulighederne for at give medarbejderne adgang til password self-service er mange, og vi har derfor valgt at sammenligne de fire primære autentifikationsmekanismer på parametrene sikkerhed, brugervenlighed og effekt.

Sikkerhed: Hvor høj er sikkerheden i forhold til at forhindre, at passwordet bliver kompromitteret? (Høj, mellem, lav)
Brugervenlighed: I hvor høj grad er det nemt og intuitivt for brugeren at benytte løsningen? (Høj, mellem, lav)
Effekt: I hvor høj grad vil det lykkes brugeren selv at nulstille sit password med løsningen? (Høj, mellem, lav)

	SIKKERHED	BRUGERVENLIGHED	EFFEKT
NEMID	**HØJ** NemID er forbundet med høj sikkerhed i brugerens bevidsthed. Man bruger det til sin netbank og vil derfor ikke låne det ud. Korrekte CPR-oplysninger har organisationen allerede registreret troværdigt i lønsystemet.	**HØJ** Det er almindeligt at have sit NemID nøglekort på sig, og brugerne husker som udgangspunkt altid koden, da de benytter den regelmæssigt.	**HØJ** Der er ingen nævneværdige barrierer i forhold til at vælge nyt password, og især for de løsninger, der præsenteres direkte på login-skærmen er effekten høj.
SMS	**MELLEM** Mobiltelefonen har mange mennesker et afslappet forhold til. Den kan blive lånt ud eller lagt på skrivebordet, hvor den bliver tilgængelig for andre. Det er en udfordring for organisationen at holde de korrekte telefonnumre på brugerne registreret sikkert og løbende.	**HØJ** Vi har næsten altid vores mobiltelefon på os og er vant til at bruge den til en lang række forskellige formål.	**HØJ** Der er ingen barriere i forhold til vælge nyt password, men det kræver, at brugerne har holdt organisationen opdateret ved skift af mobilnummer. For at fungere skal alle mobilnumre registreres indledningsvist og holdes opdateret på en sikker måde, så en svindler ikke kan få registreret sit eget mobilnummer.
E-MAIL	**LAV** Generelt en for svag autentifikationsmekanisme til vigtige passwords, da for mange (netværksudbyder, netværksadministrator, mailudbydere osv.) har mulighed for at aflæse mails.	**HØJ** Alle er fortrolige med at bruge mail, så det vil være nemt at gå til.	**HØJ** Der er ingen barriere i forhold til at vælge nyt passwords, hvis brugeren vel at mærke beholder og husker den samme e-mail adresse, som er blevet registreret i første omgang.
SPØRGSMÅL-SVAR	**MELLEM** Vi er tilbøjelige til at vælge spørgsmål, som det er muligt at gætte eller Google sig frem til svaret på.	**MELLEM** Hvis brugeren har fået valgt sine spørgsmål og tilhørende svar, vil man almindeligvis også kunne huske de korrekte svar.	**LAV** Man er typisk ikke motiveret for at indstille spørgsmål og svar, før skaden er sket, og det er for sent.

Risikoanalyse: Password self-service med NemID vs. SMS

Ovenstående matrix peger altså på, at de to mest velegnede autentifikationsmekanismer til håndtering af glemte passwords er NemID og SMS.

Herunder har vi lavet en kort sikkerhedssammenligning af de to løsningstyper ved at se på risici og potentielle konsekvenser af disse risici.

Sandsynlighed og konsekvens scores fra 1–5, hvor 5 er højest. Risikoværdien fås ved at gange de to tal.

Risiko for et falsk nulstillet password for én bruger scores til konsekvens 3, mens risiko for falsk nulstillet password for mange brugere scores til konsekvens 5.

Sandsynligheden for de enkelte risikotyper, tager her udgangspunkt i et generelt billede af en stor organisation med mange it-brugere. Man bør derfor forholde sig konkret til, om sandsynligheden og konsekvenserne er større eller mindre for de enkelte scenarier i ens egen organisation.

RISIKOTYPE	BESKRIVELSE	SANDSYNLIGHED	KONSEKVENS	RISIKOVÆRDI	TIPS TIL FOREBYGGELSE
SMS **SMS opsnappet**	Anden person får adgang til engangskode sendt pr. SMS. Eksempelvis pga.: » Telefon mistet » Telefon efterladt på skrivebordet » Telefon hacket til at omdirigere SMS » Aflytning i telenetværket	3	3	**9**	Kræv personlig kode på telefon inden visning af SMS, undlad flash SMS som vises uden kode. Sørg for device management fra arbejdsgiveren, så telefonens sikkerhed er høj.
SMS **Forkert mobilnummer registreret på brugeren**	Svindler får tilsendt engangskode på grund af forkert registreret mobilnummer på brugeren.	2	4	**8**	Implementér sikre procedurer for registrering og ændring af tilknyttede mobilnumre.
SMS & NEMID **Server til nulstilling af passwords kompromitteret**	Driftsserver for password nulstilling hos organisationen bliver kompromitteret. Dermed kan en angriber ændre alle organisationens passwords.	1	5	**5**	Implementér patch management, netværkssegmentering, hardening og sikre driftsprocedurer og overvågning for serveren.
SMS & NEMID **Brugers arbejdsstation kompromitteret**	Brugerens arbejdsstation bliver hacket. Dermed kan en angriber indlægge et fjernkontrolværktøj, som muliggør misbrug.	2	4	**8**	Etablér beskyttelse af de arbejdsstationer, man kan foretage password nulstilling fra.
NEMID **NemID kompromitteret**	Brugerens NemID bliver kompromitteret og kan dermed anvendes til falske password nulstillinger.	1	4	**4**	Understøt medarbejder i at spærre NemID ved kompromittering.
NEMID **Forkert CPR-nummer registreret på brugeren**	Hvis en angriber kan få registreret et CPR-nummer, som knytter sig til et NemID, han kontrollerer, kan det anvendes til falsk password nulstilling.	2	4	**8**	Etablér sikre arbejdsgange for registrering og ændring af CPR-nummer tilknyttet brugerens konto.

Undgå to klassiske faldgruber

Når man som organisation skal finde ud af, hvordan man får implementeret password self-service på en effektiv måde, er der to faldgruber, som mange organisationer gennem tiden er havnet i.

Den ene handler om urealistiske forventninger til brugerne, den anden om kommunikation.

MOTIVATIONEN KOMMER OFTEST FOR SENT

Hvis man skal have succes med sin password self-service løsning, skal man ikke forudsætte, at brugerne aktivt skal foretage sig noget for at blive klar til at foretage password self-service.

Mange brugere er ganske enkelt ikke motiverede til at lave den nødvendige registrering, inden behovet opstår – og så er det for sent. Resultatet er, at de i stedet ringer til IT Helpdesk.

REKLAMÉR FOR JERES SELF-SERVICE LØSNING

Og uanset hvor nem løsningen bliver at tage i brug for medarbejderne, må man ikke undervurdere behovet for at kommunikere den nye løsning ud – særligt i starten, men også kontinuerligt. Hvis medarbejderne ikke kan finde løsningen, når de har brug for den, eller ikke oplever, at password self-service giver dem værdi, vil en stor del af dem fortsætte med at ringe til IT Helpdesk, ligesom de plejer.

Hvor skal brugeren kunne tilgå password self-service? I overvejelserne om password self-service er det altså vigtigt at vælge en løsning, som er let tilgængelig for brugeren. Vi ser i tabellen herunder på fire muligheder.

	TILGÆNGELIG PÅ INTRANET (BASIS)	TILGÆNGELIG FRA LOGIN-SKÆRM	TILGÆNGELIG FRA HJEMMEARBEJDS-PLADS	TILGÆNGELIG FRA MOBILE DEVICES
OVERVEJELSER	Dette er den almindelige løsning. Det kan være svært for brugeren at finde løsningen, så den kræver en del 'reklame'. Brugere kan være nødt til at låne en kollegas PC, da de ikke kan komme på netværket/ Intranet uden password.	Ved at synliggøre løsningen direkte på login-skærmen får brugeren muligheden, lige der hvor behovet opstår. Der kan etableres begrænset netværksadgang direkte til password self-service, så brugeren kan nå denne uden at kende sit netværks password.	Både Intranet og login-skærm-løsningerne kan også tilbydes fra hjemmearbejdsplads, såfremt både computer og autentifikationsmekanisme er tilstrækkelig sikker. Der bør laves en risikovurdering før ibrugtagning af denne type løsninger.	En del organisationer har brugere som sjældent eller aldrig anvender en almindelig computer. Ud over den tekniske understøttelse af mobile devices, gælder der typisk samme sikkerhedsovervejelser for disse løsninger, som ved adgang fra hjemmearbejdsplads.

Så for at opsummere: Hvis I skal have en høj succesrate med jeres password self-service løsning, skal I kunne svare ja til disse tre spørgsmål:

- Kan medarbejderen bruge password self-service uden at have gjort noget på forhånd – besvaret nogle spørgsmål, registreret et mobilnummer eller lignende?
- Kan medarbejderne lære, at de ikke bare skal ringe til IT Helpdesk, sådan som de plejer?
- Kan medarbejderen selv finde hen til password self-service?

Se video!

Se hvor enkelt det er for brugeren at gennemføre Password Reset med NemID direkte i loginskærmen.

signaturgruppen.dk/kampagner/glemtepasswords/video

Signaturgruppen og Password Reset med NemID

Signaturgruppen er en it-specialistvirkomhed, der hjælper private og offentlige organisationer med at udnytte potentialet i NemID-infrastrukturen.

Signaturgruppen har udviklet løsningen **Password Reset med NemID**, som gør det muligt for medarbejderne at bruge deres private NemID til at vælge et nyt password, når de har glemt den gamle kode. Enkelt og sikkert og uden at trække på ressourcerne i IT Helpdesk.

Løsningen understøtter også anvendelse af SMS, men vi gør meget ud af at være med til at vurdere og anbefale sikkerhedsløsningen.

Anvendelse af NemID er baseret på CPR-nummer og fungerer således straks, uden at medarbejderen skal gøre noget for at tilmelde sig, svare på spørgsmål eller blive belemret med velkomstmails.

Password Reset med NemID kører i dag i en lang række danske virksomheder og organisationer – og selvbetjeningsløsningen bliver flittigt benyttet. En statistik baseret på 2015-tal fra 15 af Signaturgruppens kunder viser, at der i gennemsnit bliver foretaget 1.070 password nulstillinger med NemID årligt hos hver enkelt kunde.

Det giver i sig selv en betragtelig besparelse i IT Helpdesk, men det økonomiske aspekt er dog kun én side af sagen.

Ofte handler password nulstilling lige så meget om at give medarbejderne mulighed for at komme hurtigt og sikkert videre med deres arbejde. Det er blandt andet tilfældet i Aalborg Kommune, som har indført Password Reset med NemID i forbindelse med implementeringen af Fælles Medicinkort (FMK).

Janni Bøgsted Kjærgaard, projektleder for FMK i Aalborg Kommune, fortæller:

„Det er enormt vigtigt, at personalet selv kan nulstille deres passwords, for de er fuldstændige afhængige af at kunne få adgang til FMK for at give borgene den korrekte pleje – også i weekenderne og uden for normal kontortid. Og vi skal sikre, at de har adgang, så alternativet ville være en 24/7 support, som ville være temmelig dyr at drive."

„Vi har opnået større sikkerhed med løsningen. Tidligere så personalet sig nødsaget til at låne hinandens passwords, hvis de havde glemt deres eget, og det må de naturligvis ikke. De sætter deres faglige autorisation på spil ved at låne deres 'identitet' ud. Nu er der heldigvis ingen undskyldninger for det længere."

Signaturgruppen A/S
Incuba - Navitas
Inge Lehmanns Gade 10
8000 Aarhus C

Telefon: 7025 6425
E-mail: info@signaturgruppen.dk

I Signaturgruppen er vi eksperter i løsninger med NemID og digital signatur. Vores mission er at hjælpe virksomheder og organisationer med at realisere potentialet i den danske digitale signaturinfrastruktur

SignaturGruppen