

Det är viktigt att man i sin policy tänker på att det skall vara praktiskt att hantera lösenord enligt policy.

- När och hur man får dokumentera lösenord
- Om och i så fall när man får dela lösenord
- Krav på att lösenord skall hållas hemliga
- Hur ofta man får lov att återanvända ett lösenord
- Hur ofta man måste byta lösenord
- Krav på typer av tecken som måste kombineras
- Minsta antalet tecken ett lösenord får ha

senord, vilken bl.a. kan beakta följande:

Inom organisationen bör det finnas en policy för lösenord, vilken bl.a. kan beakta följande:

Policy för lösenord

da lösenord som är svåra att lista ut.

senord som är 100 % säkra, men man däremot använda- Det är i praktiken närmast omöjligt att ta fram lö-

En användaridentitet kan i normalfallet vara känt för alla, men lösenord är något som skall hållas hemligt.

För att göra det möjligt att kontrollera åtkomst till IT-system och den information som hanteras, är det nödvändigt att använd en teknik för identifiering som omfattar en användaridentitet och verifiering av identiteten, t.ex. ett lösenord.

Introduktion

För att göra det möjligt att kontrollera åtkomst till IT-

MiniGuide

Vad är starka lösenord

IT- & Informationssäkerhet



Några tips för att skapa och hantera lösenord

Lösenord skall vara enkelt att komma ihåg men samtidigt vara svårt för en utomstående att lista ut. En enkel teknik för att skapa ett lösenord är att använda en ramsa eller fras där första bokstaven i varje ord väljs ut. Ett exempel på detta är frasen "1 Askunge och 7 dvärgar på julåttan", vilket ger lösenordet 1Ao7dpj.

När du skapar lösenordet måste du följa den policy

för lösenord som finns inom organisationen. Saknas en sådan policy finns det som regel inget hinder att du följer goda råd som exempelvis att det bör vara mer än 7 tecken med en blandning av småbokstäver, stora bokstäver, siffror och specialtecken (@, \$, !).

När du har skapat ett lösenord måste du hålla detta

hemligt. Detta innebär att du inte skall lämna ut ditt lösenord till någon annan, även om det är en person du känner eller till servicepersonal som behöver se hur din dator beter sig vid ett eventuellt problem.

Metoder för verifiering av identitet

Följande tre metoder kan användas för verifiering:

Något man här - Magnetkort, lösenordsgenerator
Någon egenskap man är - Biometrisk information (fingeravtryck, öga, röst, namnteckning)

IT Ledarskap

Vi erbjuder spjutspetskompetens med hög integritet för att hjälpa företag och organisationer till ett effektivt utnyttjande av IT med målsättning att verksamhetsprocesser skall leverera och skapa värde.