

## IT sikkerhedsregnskab

De fleste virksomheder er afhængige af deres IT systemer. Systemer som ikke fungerer eller fungerer med nedsat effektivitet, kan betyde ekstra personaleudgifter, tabte ordrer, dårligt image m.v. Og de kan endvidere betyde, at vital information går tabt eller havner hos de forkerte.

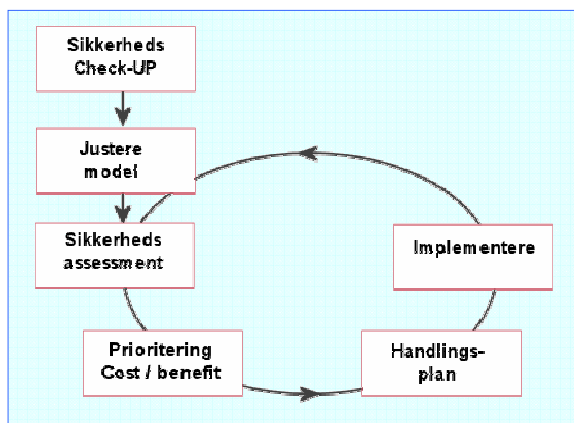
Der bruges mange ressourcer på at sikre IT systemerne og beskytte dem mod interne og eksterne trusler. Men spørgsmålet er, om ressourcerne bruges rigtigt? Ved at udarbejde et IT sikkerhedsregnskab får man ikke blot en bred vurdering af IT systemernes sikkerhedsniveau. Man får også mulighed for at vurdere, om ressourcerne bruges optimalt. IT sikkerhedsregnskabet fortæller, om indsatsen modsvarer af en tilsvarende høj forretningsmæssig sikkerhed samt reduktion i tab og ekstraudgifter.

IT sikkerhedsregnskabet er et værktøj til at fokusere indsatsen. Målet er at beskytte virksomheden mod tab, samtidig med at sikkerhedsløsningerne giver forretningsmæssig værdi. Udgangspunktet er et *IT sikkerheds check-UP* med en gennemgang af virksomhedens aktuelle sikkerhedsrisici og de eksisterende sikkerhedsløsningers evne til at dæmme op for disse risici.

### IT sikkerhedsregnskab

Et IT sikkerhedsregnskab er virksomhedens værktøj til at vurdere og beregne den forretningsmæssige nytteværdi af IT sikkerhedstiltag. Målet er en prioritering, der giver mest sikkerhed med størst bidrag til forretningen for pengene.

IT sikkerhedstiltag bliver ofte indført ud fra et forsigtighedsprincip: *Det er bedre at sikre for meget end for lidt*. Det er klart at sikkerheden ikke må være lemfældig, men overdreven sikkerhed har også en bagside. Ikke blot koster sikkerhed penge, men kan også hæmme forretningsmuligheder: *Overdreven sikkerhed er i bedste fald spild af ressourcer, i værste fald ødelægger det virksomhedens konkurrencedygtighed*.



Første trin i LELLOs model for implementering af et IT sikkerhedsregnskab er et IT sikkerheds check-UP, der giver status på virksomhedens IT sikkerhed.

### IT sikkerheds check-UP

Et IT sikkerheds check-UP giver virksomheden svar på om der er væsentlige sikkerhedsrisici som ikke er beskyttet tilstrækkeligt samt om de ressourcer som anvendes på sikkerhed anvendes på de rigtige områder.

Analysen, som gennemføres i løbet af et par uger, giver svar på om:

- Virksomhedens sikkerhedstiltag er fokuseret mod at beskytte virksomhedens kerneværdier.
- Sikkerhedstiltagene tilfører en forretningsmæssig værdi.
- De reelle og vigtige sikkerhedsrisici afbødes med de eksisterende tiltag.

Ved at anvende en cost/benefit betragtning får virksomheden mulighed for at vurdere omkostninger og nytteværdi ved eksisterende sikkerhedstiltag og sætte det i relation til deres forretningsmæssige nytteværdi.

Et IT sikkerheds check-UP gennemføres i et kort intensivt forløb og munder ud i en kortfattet rapport, som indeholder de væsentligste observationer, herunder et antal 'quick fixes', der umiddelbart kan iværksættes, og en business case for eventuelle ændringer til de eksisterende IT sikkerhedstiltag.

### Vil du vide mere?

Kontakt LELLO for et uforpligtende møde, hvor vi gennemgår dine aktuelle sikkerhedsspørgsmål og vurderer værdien af et IT sikkerheds check-UP og et IT sikkerhedsregnskab i din virksomhed.