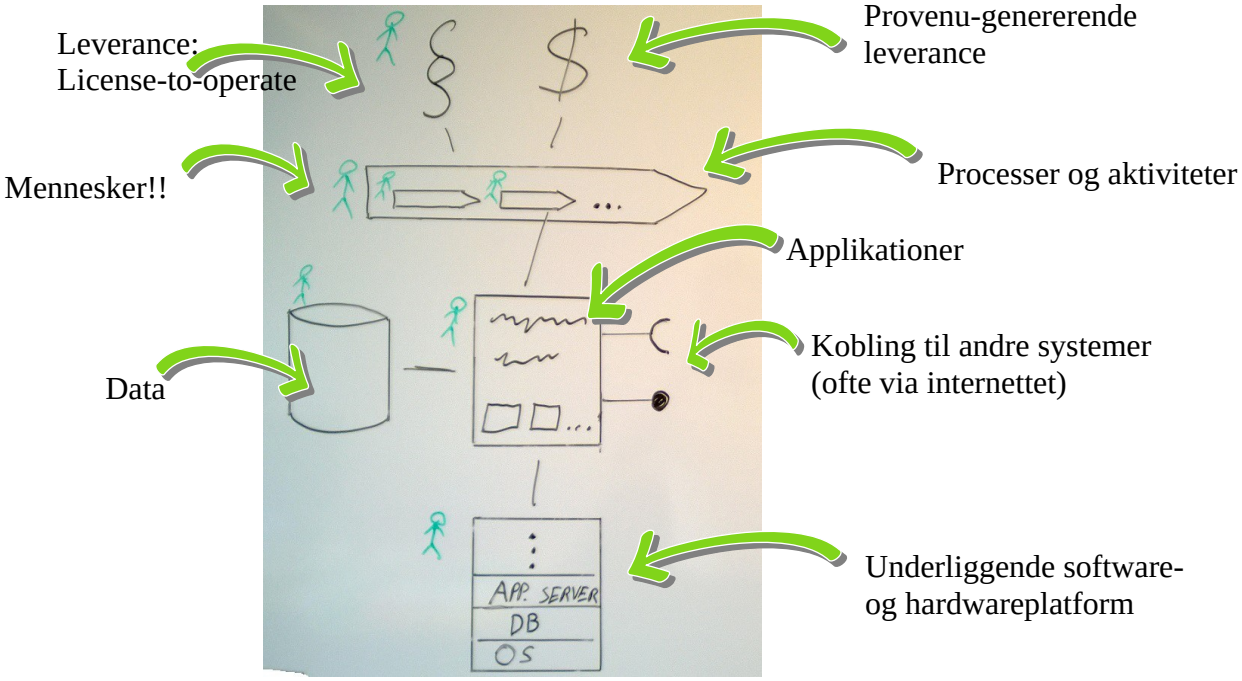
IT Sikkerhedsledelse

Mange virksomheder, specielt SMV, har utilstrækkelig IT-sikkerhed og beredskab. Det skyldes dels, at de fleste ikke har IT som deres primære kompetenceområde, dels, at de mangler det overblik, der skal til for at komme i gang. Det er der god grund til, for området er komplekst. Men det er er også ærgerligt, for man kan komme langt med den relativt simpelt tilgang, der skitseres i det følgende.

Udgangspunktet for prioritering: Virksomhedens aktiver

Når vi skal beslutte, hvilke aktiver, vi skal forsvare, og hvilke sikkerhedsindsatser vi skal implementere, er udgangspunktet at forsvare vores værdiskabelse. Så udgangspunktet er overblik over vores leverancer, i prioriteret rækkefølge. Det er her vigtigt, at man tænker virksomheden 'hele vejen rundt'. Leverancer er ikke bare varer og ydelser men også f.eks. regnskab eller dokumentation for korrekt behandling af kemikalier.

Næste skridt er at kortlægge de processer og aktiviteter, der skaber leverancerne – eller i hvert fald de leverancer, vi ønsker at forsvare. For hver af disse ser man skridt for skridt på, hvilke data, der benyttes og gennem hvilke systemer, data tilgås. Og: Hvilke systemer disse primære systemer vekselvirker med for at tilbyde brugeren denne funktionalitet. Dette giver følgende, meget enkle model for en virksomheds IT- og forretningsarkitektur:



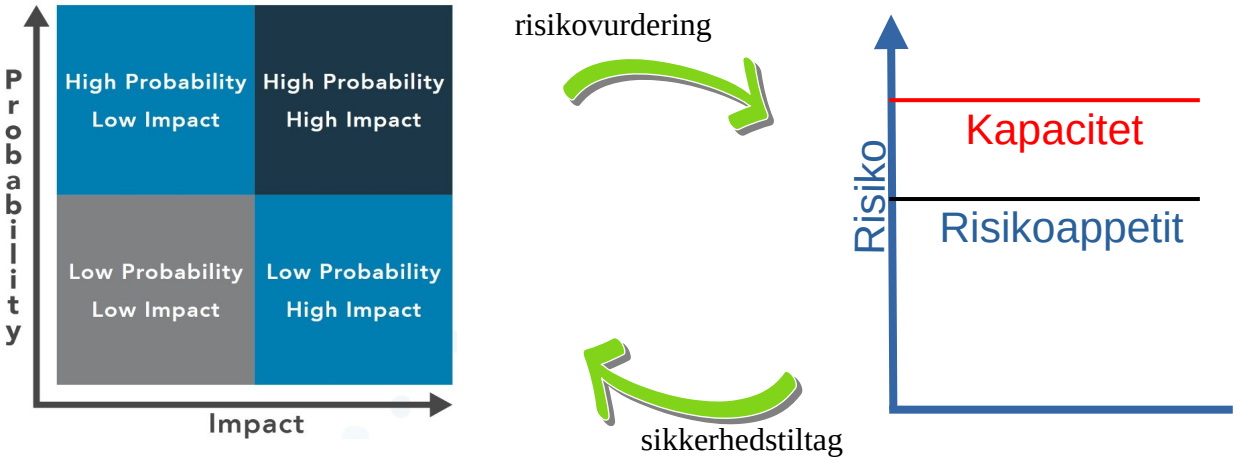
I praksis er billedet selvfølgelig mere kompliceret: Der er flere formål og derfor flere processer, processerne kan være ganske komplekse og benytte adskillige applikationer, der igen vekselvirker med mange eksterne systemer. Og al sammen på forskellig computer-infrastruktur. Men konceptuelt er det simpelt, hvilket åbner det op for, at alle (også alle virksomhedens ansatte) kan være med.

Risikostyring

Det er ledelsens opgave at sikre en bæredygtig forretning, og fordi IT er så integreret i moderne virksomhedsdrift afkræver stort set alle rammeværker og regelsæt (f.eks. NIS2) virksomhedens ledelse at arbejde med en risikobaseret tilgang til IT-sikkerhed. Dette gøres ved systematisk at vurdere;

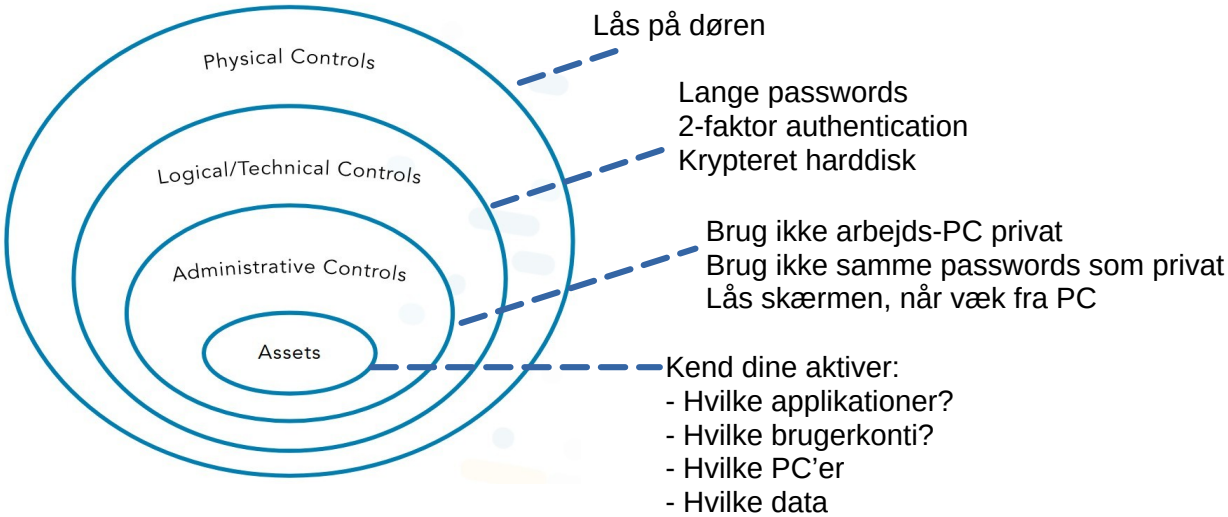
- hvilke trusler der er mod de forskellige aktiver
- hvor sandsynligt det er, at dette aktiv vil kunne kompromitteres af en given trussel
- konsekvenserne for virksomhedens aktiviteter, i fald aktivet kompromitteres

Den anden side af mønten er at etablere en klar ide om, hvor meget man kan holde til, før driften bliver udfordret (risikokapaciteten) – og hvor tæt på denne grænse, man tør gå (risikoappetitten). Risikostyringen går så i al sin enkelthed ud på at man for de risici, der ligger uacceptabelt højt, laver tiltag der enten mindsker sandsynligheden for, at de indtræffer, eller konsekvensen af, at de indtræffer, eller begge dele. Hvorefter der foretages en ny vurdering, og processen gentages:



Sikkerhedsforanstaltninger

De sikkerhedstiltag (kaldet 'kontroller'), man kan tage, deles op i; fysiske (lås på døren), logisk-tekniske (systemet stiller krav til passwords) og administrative (instrukser til medarbejderne). Samlet taler man om 'forsvar i dybden'; hvis låsen på døren bliver brudt op, er PC'en krypteret og password-beskyttet. Hvilke foranstaltninger, man implementerer, afhænger af virksomheden, men rådene i figuren er universelle:



Og når det går galt

Beredskabet skal være tænkt igennem, inden man har et problem. Det er for sent at købe brandslukkeren, når huset står i flammer. Men også her gælder reglen, at simpelt er godt. For de fleste er det tilstrækkeligt med en beredskabsplan indeholdende (Print planen på papir. Det er ikke sikkert, der er adgang til PC'en.)

Beredskabsplan ('A4')

- Navn og kontaktinformation på den/dem, der indgår i beredskabet.
  - Hvis der er flere, skal deres rolle fremgå
  - Det skal fremgå, hvem der leder beredskabet.
- Navne på andre der skal/kan kontaktes :
  - IT-leverandører
  - IT-tjenester (regnskab, løn, web osv.)
  - Bank
  - Forsikring
  - osv.
- Kriterier for, hvornår beredskabet aktiveres
- Aktiveringsprocedure

Lidt større virksomheder vil skulle lave scenarieplanlægning, fordi forskellige folk vil involveres afhængig af krisens karakter. Men uanset størrelsen er opgaven:

Krisehåndtering

- Stop blødningen
- Inddæm skaden
- Påbegynd genopbygningen

Det kræver en forståelse af den hændelse, der er indtruffet og forståelse af virksomhedens IT-infrastruktur, at stoppe skadevolderen. Det kræver forståelse af virksomhedens virke (og af dens IT) at minimere skaden. Og det kræver ofte en god backup at kunne genopbygge:
Mange opdager for sent, at driftsstabilitet – f.eks. opnået ved at spejle systemer eller lægge dem i skyen – ikke må forveksles med IT-sikkerhed; korrumperede data har overskrevet ens backup, så systemet kan ikke umiddelbart bringes til live igen. Her har man et noget bedre udgangspunkt, hvis man har en offline backup af, som minimum, applikationskonfigurationer og forretningsdata.

Slutbemærkning

Alle internetvendte IT-systemer er under konstant angreb. Der går højest minutter fra en server sættes på nettet, til den angribes. Men det er ikke bare servere, der angribes; det kunne også være en 'smart home' loftslampe eller radiatortermostat, hvis den er eksponeret mod nettet. Eller medarbejder-PC'en. Så din virksomhed er under angreb. Hele tiden.

Derfor er der heller ikke nogen vej uden om: Man er nødt til at forholde sig til sin IT-sikkerhed. For de fleste er denne opgave cirka lige så kærkommen som momsregnskabet. Den er også næsten lige så vigtig. Det er håbet, at nærværende pamflet har givet dig tilstrækkeligt afsæt til at komme i gang med arbejdet. Ellers er feedback velkommen.

God Arbejdslyst
Karsten Bormann