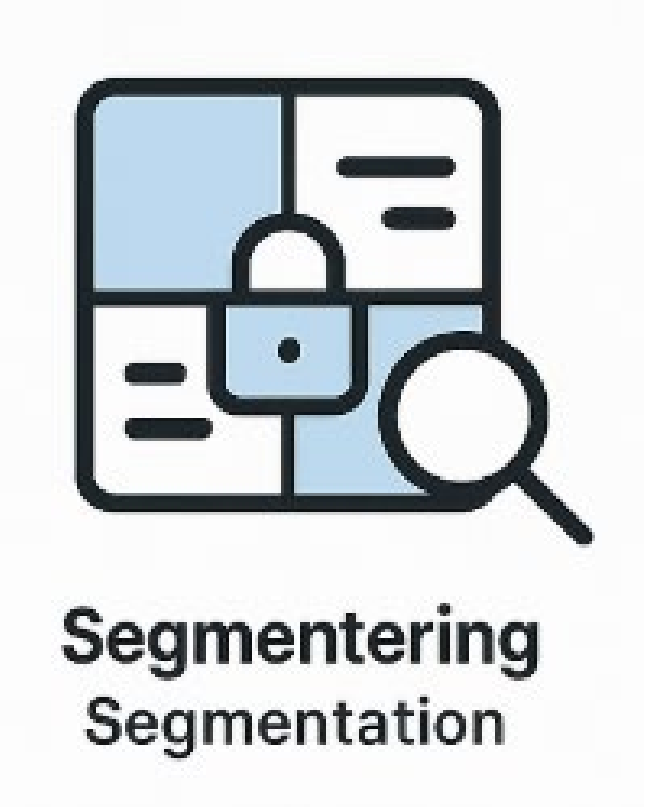
4. Leverandør-prioritering

www.cyber-smv.dk



Formål, deltagere og anvendelse

- **Formål**
  - Leverandører kan udgøre en direkte cybersikkerhedsrisiko. Derfor er det vigtigt, at vurdere hvilke leverandører, der skal have et prioriteret fokus, hvad angår tiltag indenfor cybersikkerhed.
- **Deltagere**
  - Ansvarlige for leverandører/sourcing og IT.
- **Anvendelse**
  - Del af arbejdet med at segmentere leverandører som typisk sker årligt.

Introduktion

- Traditionelt vil virksomheden lave en kategorisering af leverandørerne på baggrund af den relative værdi og forsyningsrisiko.
- Se eksempel her.
- I forbindelse med cybersikkerhed bør virksomheden dog også inddrage dette element i sine overvejelser i leverandørevalueringer .

Fremgangsmåde (1/2)

- Lav et udtræk af virksomhedens aktive leverandører.
- Start med at fokusere på de direkte leverandører (leverandører af råvarer, materialer, komponenter m.v. til produkterne).
- Vurder hver enkelt leverandør ud leverandørens cybersikkerhedsprofil:
  - Det kan f.eks. være adgang til følsomme date, systemintegration, sikkerhedscertificeringer, historik over databrud/sårbarheder, geopolitisk risiko, afhængighed ved systemkompromittering, osv.
- Brug en vægtnings- og scoringsmodel.

Fremgangsmåde (2/2)

- Kategoriser i f.eks. Høj, Middel og Lav risiko.
- Udarbejd handleplan pr. gruppe (f.eks.):
  - Høj: Audit, kontraktkrav, kontrolbesøg
  - Middel: Årlige self assesments, evt. audits.
  - Lav: Minimal overvågning.
- Implementer, følg op og juster over tid.
- Årlige vurderinger og exitstrategier.

Cybersikkerhedseksempel

Kriterium	Lav risiko (1)	Mellem risiko (3)	Høj risiko (5)
Adgang til følsomme data	Ingen persondata	Ikke følsomme data	Følsomme data
Teknisk integration	Ingen integration	Begrænset integration	Fuld adgang
Sikkerhedscertificeringer	ISO 27000/NIS2 eller lignende	Egenkontrol	Ingen dokumentation
Tidligere sikkerhedshændelser	Ingen historik	Mindre hændelse	Kendt brud/dårlig respons
Leverandørens modenhed	Høj cyber modenhed	Medium cyber modenhed	Lav cyber modenhed
Geopolitisk/leverandørrisiko	Leverandøren er placeret i lavrisiko land	Leverandøren er placeret i mellemrisiko land	Leverandøren er placeret i højrisiko land
Osv.	xx	xx	

Cybersikkerhedseksempel inkl. vægtning

Kriterium	Vægt	Eksempel score (1 = lav risiko, 5 = høj risiko)
Adgang til følsomme data	30%	5
Teknisk integration	25%	4
Sikkerhedscertificeringer	15%	3
Tidligere sikkerhedshændelser	15%	2
Leverandørens cyber modenhed	10%	2
Geopolitisk/leverandørrisiko	5%	3
Osv.	xx	xx

For eksemplet gælder = (0,3x5) + (0,25x4) + (0,15x3) + (0,15x2) + (0,1x2) + (0,05x3) = **3,6**.

Da leverandøren tenderer mod medium/mellemhøj risiko bør den overvåges og evt. undergå en audit.