8. Involvering af partnere ved cyberhændelser

www.cyber-smv.dk

Formål, deltagere og anvendelse

- **Formål**
  - For en SMV (små og mellemstore virksomhed) er det vigtigt at have en enkel, men effektiv, proces for at sikre, at relevante leverandører og tredjeparter inddrages ved en cyberhændelse.
- **Deltagere**
  - Ledelse, IT, indkøb og andre relevante funktioner.
- **Anvendelse**
  - Ved hver ny cyberhændelse.

Fremgangsmåde

- De følgende **fem** trin, kan implementeres af en SMV virksomhed.

1. Forberedelse og planlægning

- Identificér kritiske leverandører og tredjeparter (fx IT-support, hosting, cloud, softwareleverandører).
- Udarbejd kontaktliste med navne, roller, telefonnumre og e-mails.
- Indgå aftaler (f.eks. i kontrakter eller SLA'er), der beskriver:
  - Hvordan og hvornår de skal kontaktes ved hændelser.
  - Hvilket ansvar de har i en genopretningssituation.

Fremgangsmåde

2. Hændelsesdetektion og vurdering

- Når en hændelse opdages:
  - Vurder hurtigt typen og omfanget.
  - Brug en simpel skabelon til at dokumentere hændelsen (f.eks. dato, systemer ramt, mistanke om årsag).

3. Aktivering af beredskab og kontakt

- Hvis hændelsen vurderes som alvorlig:
  - Aktivér en intern ”incident response”-gruppe (kan være 2-3 nøglepersoner).
  - Kontakt relevante leverandører/tredjeparter ud fra kontaktlisten.
  - Brug en standardbesked til at informere dem hurtigt og klart.

Fremgangsmåde

4. Koordination og genopretning

- Afhold korte statusmøder (online eller telefonisk) med leverandører.
- Del nødvendige oplysninger sikkert (f.eks. via krypteret e-mail eller samarbejdsværktøj).
- Følg en simpel tjekliste for genopretning (f.eks. genskab backup, skift adgangskoder, opdater systemer).

5. Evaluering og læring

- Efter hændelsen:
  - Afhold et kort evalueringsmøde.
  - Opdater kontaktliste og processer baseret på erfaringer.
  - Del læring med relevante medarbejdere og leverandører.

Eksempel på checkliste til genopretning efter en cyberhændelse

Trin	Handling	Ansvarlig	Status
1	Bekræft hændelsens omfang og berørte systemer	IT-ansvarlig	
2	Informér interne nøglepersoner og ledelse	Ledelse	
3	Kontakt relevante leverandører og tredjeparter	IT/Indkøb	
4	Afbryd adgang til kompromitterede systemer	IT	
5	Genskab data fra backup (hvis muligt)	IT	
6	Skift adgangskoder og opdater sikkerhedsindstillinger	IT	
7	Udfør teknisk analyse og loggennemgang	IT/Leverandør	
8	Dokumentér hele hændelsesforløbet	IT/compliance	
9	Evaluer og opdater beredskabsplaner	Ledelse	
10	Informér relevante eksterne parter (f.eks. kunder, myndigheder)	Ledelse/PR	