8. Involving partners in cyber incidents

www.cyber-smv.dk

Purpose, participants and application

- **Purpose**
  - For an SME, it is important to have a simple yet effective process to ensure that relevant suppliers and third parties are involved in the event of a cyber incident.
- **Participants**
  - Management, IT, procurement, and other relevant functions.
- **Application**
  - With each new cyber incident.

Approach (1/5)

The following five steps can be implemented by an SME company.

1. **Preparation and planning**
   - Identify critical suppliers and third parties (e.g., IT support, hosting, cloud, software providers).
   - Prepare a contact list with names, roles, phone numbers, and emails.
   - Enter into agreements (e.g., in contracts or SLAs) that describe:
     - How and when they should be contacted in the event of incidents.
     - What responsibilities they have in a recovery situation.

Approach (2-3/5)

2. Incident detection and assessment

- When an incident is detected:
  - Quickly assess the type and scope.
  - Use a simple template to document the incident (e.g., date, systems affected, suspected cause).

3. Activation of contingency and contact

- If the incident is assessed as serious:
  - Activate an internal incident response group (can be 2–3 key persons).
  - Contact relevant suppliers/third parties based on the contact list.
  - Use a standard message to inform them quickly and clearly.

Approach (4-5/5)

4. Coordination and recovery

- Hold short status meetings (online or by phone) with suppliers.
- Share necessary information securely (e.g., via encrypted email or collaboration tool).
- Follow a simple recovery checklist (e.g., restore backup, change passwords, update systems).

5. Evaluation and learning

- After the incident:
  - Hold a short evaluation meeting.
  - Update contact list and processes based on lessons learned.
  - Share learnings with relevant employees and suppliers.

Example of incident recovery check list

Step	Action	Responsible	Status
1	Confirm the scope of the incident and affected systems	IT-responsible	
2	Inform internal key personnel and management	Management	
3	Contact relevant suppliers and third parties	IT/purchasing	
4	Cut off access to compromised systems	IT	
5	Restore data from backup (if possible)	IT	
6	Change passwords and update security settings	IT	
7	Perform technical analysis and log review	IT/supplier	
8	Document the entire course of the incident	IT/compliance	
9	Evaluate and update contingency plans	Management	
10	Inform relevant external parties (e.g., customers, authorities)	Management/PR	