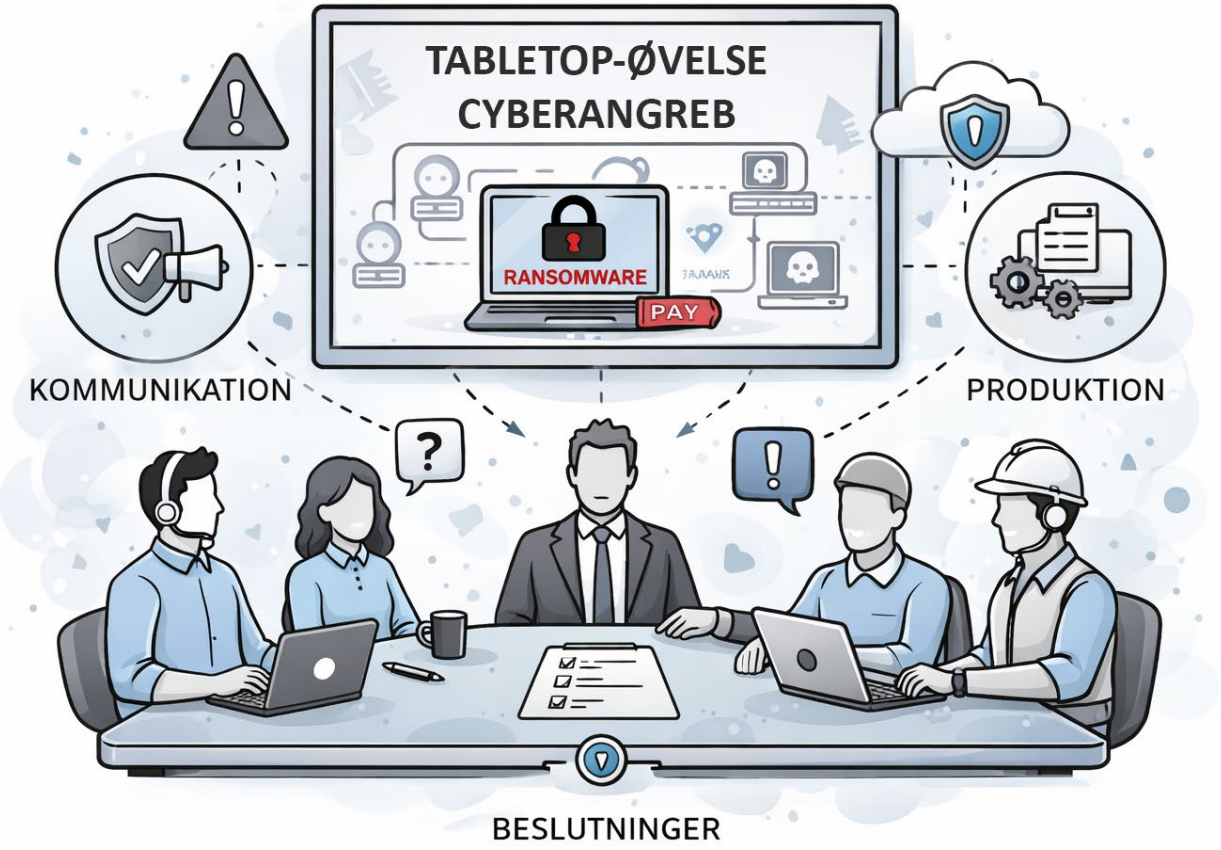
Tabletop-øvelser



Værktøjet er tilvejebragt i projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), der er støttet med midler fra Industriens Fond. Dato for publicering: 09.01.2026

Tabletop-øvelser*

- En tabletop-øvelse er en struktureret gennemgang af et realistisk cyberangreb, hvor relevante roller (ledelse, Informationsteknologi (IT), operationel teknologi (OT), drift, kommunikation m.fl.) diskuterer:
  - Hvad sker der?
  - Hvem gør hvad?
  - Hvilke beslutninger skal træffes – og hvornår?
  - Hvordan kommunikeres der internt og eksternt?
- Formålet med øvelsen er at teste:
  - Organisationens beredskab ved en cyberhændelse.
  - Samspillet mellem IT og OT.
  - Beslutningsprocesser under pres.
  - Kommunikation internt og eksternt.
- Øvelsen foregår typisk som et møde med en facilitator – ingen systemer bliver slukket eller angrebet i praksis.

*Det hedder en tabletop-øvelse, fordi øvelsen oprindeligt foregik rundt om et bord (“tabletop”), hvor deltagerne arbejdede med kort, planer, scenarier og beslutninger i fællesskab – uden at udføre handlingerne i virkeligheden.

Scenarie-faser

- Fase 1: Opdagelse.
- Fase 2: Eskalation og beslutning.
- Fase 3: IT / OT påvirkning.
- Fase 4: Kommunikation.
- Fase 5: Genopretning.

Udbytte

- Roller og ansvar (udfyldes under øvelsen):
  - Rolle, navn, ansvar for f.eks. lederen af hændelseshåndteringen, IT-ansvarlig, produktionsansvarlig, kommunikationsmedarbejder, eksterne deltagere (kunder eller leverandører).
- Nedfæld identificerede styrker.
- Nedfæld identificerede svagheder.
- Forbedringstiltag.
  - List tiltag, ansvarlig og deadline.
- Opfølgning:
  - Hvornår gentages øvelsen?
  - Skal cyberberedskabsplanen opdateres?
  - Skal der gennemføres tekniske tests (f.eks. backup eller PLC failover)?

Eksempler på tabletop-øvelser

	Ransomware rammer ERP – produktionen påvirkes indirekte	Angreb spreder sig fra kontor-IT til produktionsnetværk	Leverandøradgang misbruges (fjernsupport)	Databrud med medarbejder- eller kundedata
Type	IT → OT	IT ↔ OT	Supply chain / OT	IT / compliance
Scenarie	En medarbejder klikker på et phishing-link ERP-systemet bliver krypteret Produktionsplanlægning og ordrestyring er utilgængelig	IT opdager malware på flere pc'er OT-ansvarlig bemærker ustabilitet i SCADA Risiko for stop i produktionen	Ekstern leverandør har fjernadgang til PLC/SCADA Kontoen kompromitteres Uautoriserede ændringer opdages	HR- eller kundedata lækkes Presse eller kunder henvender sig Tidsfrist for anmeldelse til Datatilsynet
Tabletop-fokus	Hvornår erkender vi, at det er ransomware? Hvem beslutter at lukke systemer? Kan produktionen fortsætte manuelt? Hvornår og hvordan informeres kunder?	Er IT og OT tilstrækkeligt adskilt? Hvem må beslutte at stoppe produktionen? Hvornår prioriteres sikkerhed frem for output?	Hvordan opdages misbruget? Hvem kontakter leverandøren? Lukkes al ekstern adgang – og hvornår? Dokumentation og ansvar	Hvornår er det et databrud? Hvem anmelder til Datatilsynet? Hvad siger vi offentligt – og hvornår?
Tester især	Ledelsesbeslutninger Backup og genopretning Kommunikation	Samspil mellem IT og produktion Beslutningskompetence Eskalation	Leverandørstyring Adgangskontrol Beredskab uden for normal arbejdstid	Juridisk forståelse Kommunikationsberedskab Ledelsens rolle