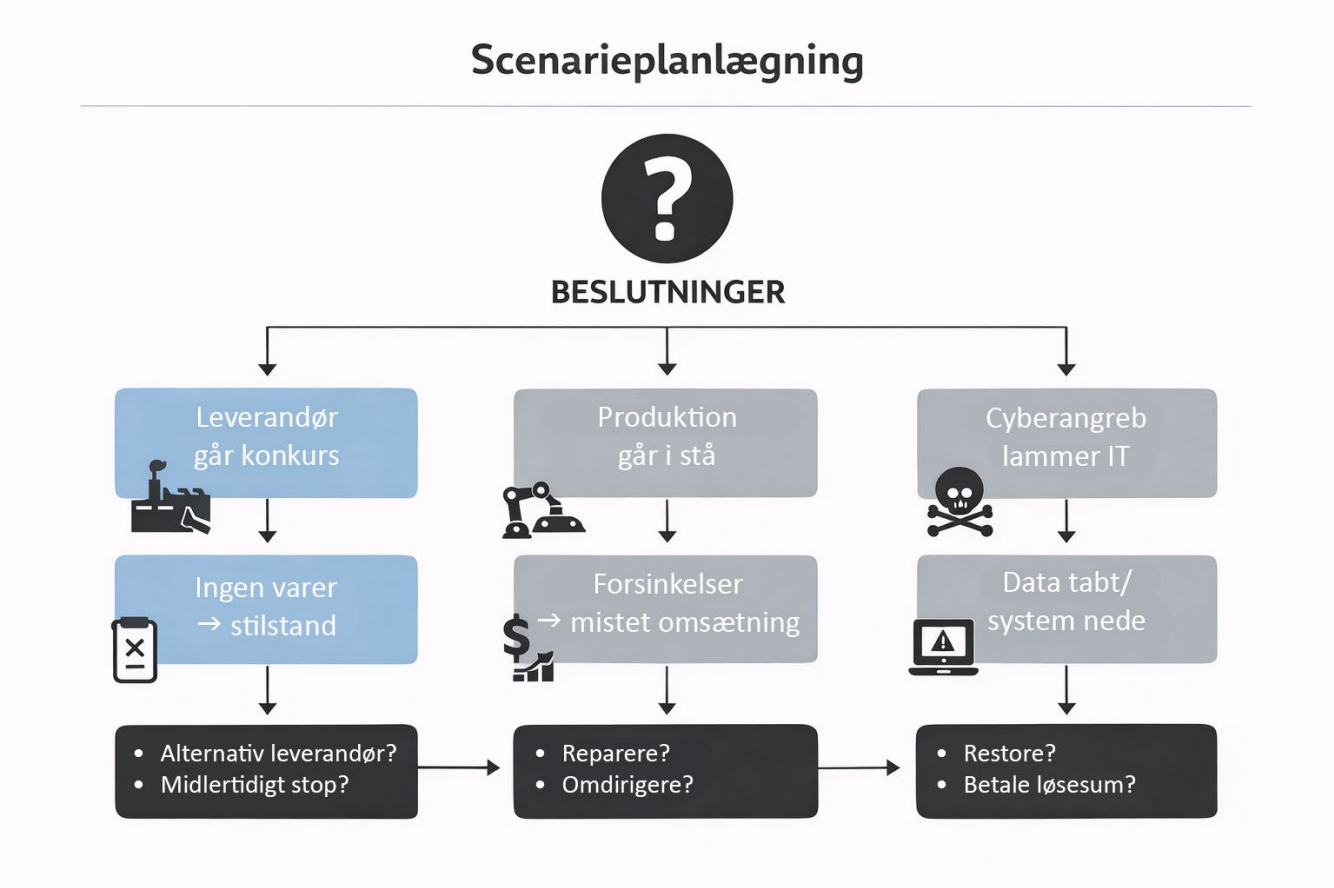
Scenarieplanlægning



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

Scenarieplanlægning for cybersikkerhed (IT og OT)

- Scenarieplanlægning for cybersikkerhed for Informationsteknologi (IT) og operationel teknologi (OT) er en metode, hvor en virksomhed systematisk forbereder sig på konkrete cyberangreb ved at gennemgå realistiske hændelsesscenarier – både for IT og OT.

- **Formål og omfang**
  - Formål: Eksempelvis identificere kritiske cybertrusler, vurdere konsekvenser og planlægge beredskab og sikre en hurtig og kontrolleret håndtering af cyberhændelser (f.eks. ransomware, phishing og systemnedbrud).
  - Omfang: Eksempelvis IT-systemer (ERP, CRM, netværk), OT-systemer (PLC'er, SCADA, produktionsudstyr), data, medarbejdere og eksterne parter.

Fremgangsmåde

1. Sæt teamet: Sammensæt et tværfunktionelt team med IT, OT, produktion og ledelse.
2. Kortlæg aktiver: Identificer kritiske IT- og OT-systemer.
3. Identificer trusler/scenarier: Brainstorm mulige cybertrusler og fejlscenarier for både IT og OT.
4. Foretag konsekvensanalyse
5. Prioriter scenarier: Vurder hvilke trusler, der kræver mest fokus.
6. Udarbejd strategier: Beskriv forebyggende og reaktive tiltag.
7. Planlæg træning og test: Simuler scenarier og evaluer.
8. Vedligehold: Opdater planen årligt, efter ændringer i teknologi eller organisation, og efter øvelser.

Kortlæg aktiver: Identificer kritiske IT- og OT-systemer

System	Type (IT/OT)	Beskrivelse	Kritikalitet (H, M, L)	Ejer

Note: H = Høj, M = Mellem, L = Lav

Kortlæg aktiver: Identificer kritiske IT- og OT-systemer (eksempler)

System	Type (IT/OT)	Beskrivelse	Kritikalitet (H, M, L)	Ejer
ERP-system	IT	Styrer økonomi, lager, indkøb, planlægning; uden det kan ordrebehandling og indkøb stoppe.	Høj	IT-chef
MES-system	OT	Styring af maskiner Overvåger produktionsplaner, ressourceallokering og workflow; kritisk for effektiv produktion.	Høj	Produktionschef
SCADA-system	OT	Fjernovervågning af procesanlæg; stopper produktionen hvis utilgængelig.	Høj	Produktionschef
Backup-system	IT	Sikrer dataredundans; kritisk for hurtig genoprettelse ved IT-hændelser.	Høj	IT-chef
E-mail og kommunikationssystemer	IT	Intern og ekstern kommunikation; essentiel for koordinering og krisestyring.	Høj	IT-chef
Sensorer/IoT-enheder	OT	Fysiske enheder, der indsamler data fra omgivelserne (f.eks. temperatur, tryk, vibration, fugt eller position) og sender dataene digitalt til andre systemer via netværk (internet, lokalnet, mobilnet m.m.).	Medium	OT-ansvarlig

Note: H = Høj, M = Mellem, L = Lav

Identificer trusler / scenarier (eksempler)

Trussel/scenarie	Angrebstype	Sandsynlighed	Konsekvens	Prioritet	Indikatorer
Ransomware på ERP	IT	Medium	Høj	Høj	Usædvanlig filkryptering, login-fejl
Phishing-angreb mod medarbejdere	IT	Høj	Medium	Høj	Mistænkelige e-mails, uautoriserede login-forsøg
Malware på produktionsstyring (PLC / SCADA)	OT	Lav	Høj	Høj	Unormale maskinbefalinger, produktion stopper
DDoS-angreb mod netværk	IT	Medium	Medium	Medium	Netværksnedbrud, langsom internetadgang
Sabotage via eksterne leverandører	OT	Lav	Høj	Høj	Usædvanlig aktivitet i OT-systemer

Note: DDoS = *Distributed Denied-of-Service* (er et cyberangreb, hvor mange computere samtidig overbelaster en server eller et netværk, så en hjemmeside eller digital tjeneste bliver langsom eller helt utilgængelig for normale brugere).

Konsekvensanalyser

For hver trussel/scenarie beskrives:

1. Produktionsstop (timer/dage).
2. Økonomisk tab.
3. Sikkerhedsrisiko for medarbejdere.
4. Omfang af datatab eller læk.
5. Omdømmerisiko.

Strategier og beredskab

Trussel/scenarie	Forebyggende strategier	Reaktive strategier	Ansvarlig
Ransomware på ERP	Antivirus, firewall, træning, backup	Gendan fra backup, isoler systemer, informer krisestab	IT-chef
Phishing-angreb mod medarbejdere	Security awareness-træning, e-mail-filtrering	Lås kompromitterede konti, ændr passwords	IT-chef
Malware på produktionsstyring (PLC / SCADA)	Segmentering af OT-netværk, softwareopdatering	Isoler påvirket PLC, manual drift, sikkerhedsteam aktiveres	OT-ansvarlig
DDoS-angreb mod netværk	Redundant netværk, cloud-beskyttelse	Trafikfiltrering, kontakt ISP	IT-chef
Sabotage via eksterne leverandører	Adgangskontrol, kontraktkrav, overvågning	soler systemer, revision af logs, krisestab aktiveres	OT-ansvarlig

Træning og test (eksempler)

IT

- Phishing-simulationer.
- backup-gendannelse.
- Netværksangrebstest.

OT

- SCADA / PLC failover test (en planlagt test, hvor man kontrollerer, om et redundant PLC-setup automatisk og korrekt kan overtage styringen, hvis den primære PLC fejler eller tages ud af drift).
- Manuel drift under angreb.
- Scenarieøvelser med krisestab.

Vedligeholdelse

- Opdater scenarier minimum årligt eller efter større ændringer i IT/OT.
- Revidér kontaktinformationer, roller og ansvarlige.
- Evaluer trænings- og testresultater og tilpas strategier.