CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Sådan gennemføres en Tabletop scenarieøvelse

www.cyber-smv.dk

Værktøjet er tilvejebragt i forbindelse med projektet **Cybersikkerhed og Forretningskontinuitet** støttet af Industriens Fond. Offentliggjort den 09.01.2026.

Roller

Facilitator: En person, der leder diskussionen, stiller spørgsmål i relation til scenariet.

Penneфører: En person dedikeret til at tage noter om centrale diskussionspunkter, identificerede svagheder og foreslåede handlinger.

Deltagere: Det tværfaglige team fra Supply Chain Resilience proces-modellen.

Spilleregler

01

Dette er en læringsøvelse, ikke en test. Målet er at finde svagheder i virksomheden.

02

Der er ingen forkerte svar, kun muligheder for diskussion og forbedring.

03

Fokuser på de nuværende processer og kapabiliteter og ikke på, hvad du ville ønske, du havde. Vær ærlig.

04

Løs ikke scenarierne i sig selv: Tænk over, hvordan scenariernes temaer påvirker din virksomhed.

Processen

Læs historien: Facilitatoren læser scenarieopsummeringen og de specifikke chok højt.

Gennemgå dit øjebliksbillede: Se kort på resultaterne fra Supply Chain Resilience proces-modellen.

Gennemgå spørgsmålene: Facilitatoren guider teamet gennem diskussionsspørgsmålene til det pågældende scenarie.

Konklusioner fra indsamlingen: Notér de mest centrale resultater.

Scenarie 1: USA's tilbagetrækning fra Europa

Historien: Efter et skift i amerikansk udenrigspolitik reducerer USA dramatisk sine sikkerhedsforpligtelser over for Europa, trækker tropper ud af regionen og skaber et lederskabsvakuum i NATO. For at kompensere er europæiske nationer, herunder Danmark, tvunget til at øge forsvarsudgifterne betydeligt, hvilket fører til nedskæringer på andre områder. Det globale handelsmiljø bliver mere fjendtligt.

Chokkene for din virksomhed:

→ *Supply Chain Shock*: USA implementerer en ny universel handelstold, der øger omkostningerne ved din eksport til det amerikanske marked og de komponenter, du importerer fra amerikanske leverandører, betydeligt.

→ *Cybertrusler*: Med den svækkede amerikanske sikkerhedsparaply iværksætter Rusland en konstant, lavniveau-kampagne af sofistikerede cyberangreb rettet mod europæisk infrastruktur og dens leverandører, herunder virksomheder som din.

Scenarie 1: USA's tilbagetrækning fra Europa

Guidet diskussion (Tabletop-øvelsen – detaljeret eksempel):

- → **Detektion og vurdering:** Hvordan ville vi først høre om de nye toldsatser? Hvem i vores virksomhed er ansvarlig for at overvåge international handelspolitik? Hvordan ville vores nuværende IT-sikkerhedssystemer skelne et statsstøttet cyberangreb fra et almindeligt kriminelt angreb?

- → **Øjeblikkelig reaktion:** Hvad er vores første tre handlinger inden for 24 timer efter toldmeddelelsen? Hvem er i vores øjeblikkelige reaktionsteam ved et større cyberangreb? Har vi kontaktoplysninger til juridiske rådgivere og retsmedicinske eksperter let tilgængelige?

- → **Forretningskontinuitet:** Kan vores forretningsmodel overleve en told på 20 % på vores primære eksportprodukt? Hvor længe kan vi operere, hvis vores primære logistikpartner bliver lammet af et cyberangreb? Har vi undersøgt alternative leverandører uden for USA for kritiske komponenter?

- → **Sårbarheder afsløret:** Når vi ser på vores overblik over modstandsdygtighed, hvordan udnytter dette scenarie vores specifikke svagheder? Hvilke nye sårbarheder afslører det?

Scenarie 2: USA-Kina konfrontation om Taiwan

Historien: En mindre maritim hændelse i det Sydkinesiske Hav eskalerer hurtigt. Kina indfører en fuldstændig militærblokade af Taiwan, et globalt knudepunkt for avanceret produktion, hvilket sætter en kritisk del af den globale økonomi i stå.

Chokkene for din virksomhed:

→ *Supply Chain Shock*: Din forsyning af kritiske komponenter fra Taiwan (f.eks. halvledere, specialiseret elektronik) er fuldstændig afbrudt. Din produktionslinje vil stoppe inden for få uger.

→ *Cyber Threat*: Mens dit indkøbsteam desperat kæmper for at finde nye leverandører, bliver de mål for yderst sofistikerede og overbevisende phishing-angreb forklædt som kommunikation fra potentielle nye partnere.

Eksempel på diskussioner: Hvor afhængige er vi af leverandører med én enkelt lokation placeret i geopolitiske følsomme regioner? Hvad er vores proces til at godkende nye leverandører under ekstremt tidspres? Hvad er sikkerhedsrisiciene ved denne hurtige sourcingproces? Hvad er den fulde økonomiske konsekvens af et komplet, månedlangt produktionsstop?

Scenarie 3: Klimaforandringer

Historien: En række ekstreme vejrbegivenheder forårsager omfattende forstyrrelser. En større oversvømmelse i Tyskland afskærer vigtige europæiske transportveje i ugevis. Som svar på klimamål implementerer EU nye energibesparende regler, der har utilsigtede konsekvenser for digital infrastruktur.

Chokkene for din virksomhed:

- → *Supply Chain Shock*: Jeres primære landrute for europæisk distribution er ufremkommelig. Samtidig bliver en nøgleleverandør, der allerede er stresset af klimabegivenheden, ramt af et ransomware-angreb og går offline.

- → *Cyber Threat*: De nye EU-regler begrænser brugen af beregningsintensiv kunstig intelligens, hvilket tvinger din cloud-sikkerhedsudbyder til at deaktivere sine mest avancerede trusselsdetekteringssystemer. Dette gør din virksomhed mere sårbar over for angreb, netop når cyberkriminelle udnytter dette kaos.

→ **Eksempel på diskussioner:** Tager vores plan for forretningskontinuitet højde for samtidige fysiske og digitale forstyrrelser? Er vores forsikringsdækning tilstrækkelig til klimarelaterede driftsafbrydelser? Hvordan vurderer vi andenordens konsekvenser af nye reguleringer, der synes at være irrelevante for vores kerneforretning?

Scenari 4: Økonomisk polarisering

Historien: Vedvarende økonomisk usikkerhed og inflation krymper den europæiske middelklasse og udhuler kundebasen for mange virksomheder. Denne økonomiske angst giver næring til politisk ekstremisme og social uro. I sanktionerede økonomier rekrutteres teknologisk dygtige, men arbejdsløse unge i stigende grad organiseres i cyberkriminalitet.

Chokkene for din virksomhed:

- → *Supply Chain Shock*: En mindre kritisk leverandør i din lokale forsyningskæde er ramt af et ransomware-angreb. Da de mangler ressourcer til at komme sig, går de konkurs, hvilket skaber et pludseligt og uventet hul i dit lokale forsyningsnetværk.
- → *Cyber Threat*: Din virksomhed står over for en dramatisk stigning i økonomisk motiveret cyberkriminalitet, især ransomware-as-a-Service-angreb, der er sofistikerede, men billige at udføre. Angriberne er ikke statsstøttede, men er yderst professionelle kriminelle virksomheder.

Eksempel på diskussioner: Hvordan vil et vedvarende fald i markedsefterspørgslen på 15% påvirke vores forretning? Hvor godt forstår vi den økonomiske og cybermodstandsdygtighed hos vores mindre lokale leverandører? Hvordan adskiller vores plan for håndtering af hændelser sig, når vi har at gøre med en kriminel virksomhed versus en statslig aktør?

Scenarie 5: Når AI går amok

Historien: For at forbedre effektiviteten implementerer din virksomhed en generisk AI-drevet software-as-a-service (SaaS) platform til at styre en kritisk forretningsfunktion, såsom lagerstyring eller produktionsplanlægning. Valget er baseret på marketingpåstande og brugervenlighed med minimal uafhængig sikkerhedsverifikation.

Chokkene for din virksomhed:

- → *Supply Chain Shock*: Tredjepartsudbyderen af AI-tjenester lider under et langvarigt ransomware-angreb. Dine kritiske driftsdata hostes på deres servere og er nu fuldstændig utilgængelige. Din produktion er sat på pause på ubestemt tid, fordi du ikke ved, hvilke materialer du har eller har brug for.

- → *Cyber Threat*: Angrebsvektoren er ikke dit eget netværk men en betroet tredjepartsleverandør. Dette understreger den enorme risiko ved at outsource kritiske funktioner uden robust sikkerhedskontrol, klare kontraktlige beskyttelser og en uafhængig databackupstrategi.

Eksempel på diskussioner: Hvad er vores proces til evaluering af sikkerheden hos nye softwareleverandører? Specificerer vores kontrakter med SaaS-udbydere deres ansvar i tilfælde af brud og garanterer os adgang til vores data? Har vi vores egne sikkerhedskopier af data, der er gemt på tredjepartsplatforme? Hvilken kritisk institutionel viden risikerer vi at miste til "black box"-AI-systemer?