CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Reduktion af risici ved indgåelse af leverandør- eller andre tredjepartsrelationer

www.cyber-smv.dk

Værktøjet er tilvejebragt i forbindelse med projektet **Cybersikkerhed og Forretningskontinuitet** (www.cyber-smv.dk), støttet af Industriens Fond.
Offentliggjort den 08.01.2026.

Formål, deltagere og anvendelse

- **Formål**
  - At identificere, vurdere og reducere cybersikkerheds- og digitale forsyningskæderisici på forhånd, før der etableres tillid, adgang, datadeling eller operationel afhængighed.
- **Deltagere**
  - Data- og IT-chefer, juridisk/compliance-funktioner samt produkt- og tjenesteejere.
- **Anvendelse**
  - Anvendes før indgåelse af formelle relationer med leverandører, kunder, partnere eller andre tredjeparter.

Fremgangsmåde

Overvejelserne i resten af dette dokument kan anvendes af virksomheder på følgende måder før indgåelse af formelle relationer med leverandører, kunder, partnere eller andre tredjeparter:

- Som et afdækningsværktøj i den tidlige dialog og i forbindelse med udbud og tilbudsprocesser (Request for Proposals – RFP).
- Til at tilpasse spørgeskemaer og kontraktklausuler baseret på den faktiske risiko.
- Til at beslutte eskalationsniveauer, kompenserende kontroller eller eventuel afvisning.
- Til at skelne mellem acceptabel og uacceptabel restrisiko.

Bemærk: Ikke alle krav er nødvendigvis relevante, og organisationer bør derfor udvælge de krav, der er relevante i den konkrete sammenhæng.

Dækkede aspekter

1. Forretningskontekst og relationens kritikalitet.
2. Dataeksponering og informationsfølsomhed.
3. Adgangs- og forbindelsesmodel.
4. Leverandørens cybersikkerhedsmæssige modenhed og praksis.
5. Hændelseshistorik, detektion og beredskab/reaktionsevne.
6. Afhængigheder og gennemsigtighed i forsyningskæden.
7. Regulatoriske og juridiske forhold.
8. Assurance, dokumentation og gennemsigtighed.
9. Kontraktuel parathed.
10. Forandrings- og varighedsforventninger.
11. Kulturelle og samarbejdsmæssige signaler.

Forretningskontekst og relationens kritikalitet

Overvejelser

- Hvilke forretningsprocesser, tjenester eller produkter vil dette samarbejde understøtte?
- Hvor kritisk er relationen for kerneforretningen, sikkerheden eller indtjeningen?
- Hvilken påvirkning ville leverandørsvigt, kompromittering eller driftsafbrydelse have?
- Er relationen operationel, strategisk, taktisk eller varebaseret?
- Er der tale om et engangssamarbejde eller en langsigtet afhængighed?

Dataeksponering og informationsfølsomhed

Overvejelser

- Hvilke typer data vil blive tilgået, behandlet, lagret eller transmitteret (f.eks. personoplysninger, fortrolige forretningsdata, intellektuel ejendom, legitimationsoplysninger, nøgler eller driftsdata)?
- Vil data forlade jeres organisations kontrollerede miljø?
- Er der krav til dataresidens eller datasuverænitet?
- Deles data ensrettet, tovejs eller aggregeres de på tværs af kunder?
- Hvilke mekanismer for datasegregering er etableret (særligt relevant for SaaS- og MSP-leverandører)?

Adgangs- og forbindelsesmodel

Overvejelser

- Hvilke typer adgang vil tredjeparten have (fx netværk, applikation eller applikationsprogrammeringsgrænseflade (API))?
- Vil tredjeparten have administrativ eller privilegeret adgang?
- Er adgangen vedvarende eller tidsbegrænset?
- Er integrationer direkte, indirekte eller via mellemmænd?
- Hvordan oprettes, autentificeres og tilbagekaldes identiteter?
- Kan adgangen teknisk begrænses efter princippet om mindst mulige rettigheder (least privilege)?
- Indgår der fjernadgangsværktøjer, servicekonti eller automatisering?

Leverandørens cybersikkerhedsmæssige modenhed og praksis

Overvejelser

- Findes der en defineret styringsstruktur for informationssikkerhed?
- Er roller og ansvar inden for cybersikkerhed klart fastlagt?
- Er sikkerhedspolitikker dokumenteret og periodisk gennemgået?
- Findes der en sikker udviklingslivscyklus (for software- og tjenesteleverandører)?
- Er processer for sårbarhedshåndtering og patching etableret?
- Hvordan håndteres medarbejdernes sikkerhedsbevidsthed?
- Er underleverandører underlagt tilsvarende sikkerhedskrav?

Hændelseshistorik, detektion og beredskab/reaktionsevne

Overvejelser

- Har organisationen oplevet væsentlige sikkerhedshændelser?
- Hvordan blev hændelser opdaget, håndteret og afhjulpet?
- Findes der en dokumenteret beredskabsplan for hændelseshåndtering (incident response)?
- Bliver kunder/partnere underrettet inden for fastsatte tidsfrister?
- Er der koordinering mellem tekniske, juridiske og kommunikationsteams?
- Gennemføres der tabletop-øvelser eller simuleringer?

Afhængigheder og gennemsigtighed i forsyningskæden

Overvejelser

- Hvem er de kritiske underleverandører, cloud-udbydere eller teknologipartnere?
- Er afhængigheder *upstream* oplyst og bliver de periodisk gennemgået?
- Bliver softwarekomponenter og biblioteker registreret og sporet (f.eks. Software Bill of Materials (SBOM))?
- Er der etableret foranstaltninger til at undgå forfalskede eller gråmarkeds-komponenter?
- Hvilke antagelser lægges der til grund for tillid til leverandører?

Regulatoriske og juridiske forhold

Overvejelser

- Hvilke love og regler er gældende (f.eks. databeskyttelse, sektorspecifik regulering)?
- I hvilke jurisdiktioner vil data blive behandlet eller tilgået?
- Er der geopolitiske risici eller risici relateret til sanktioner?
- Gælder der forpligtelser til adgang for retshåndhævende myndigheder eller offentlige myndigheder?
- Er de regulatoriske rapporteringsforpligtelser afstemt mellem parterne?

Assurance, dokumentation og gennemsigtighed

Overvejelser

- Hvilken sikkerhedsdokumentation kan fremlægges (certificeringer, rapporter, erklæringer)?
- Er der uafhængig assurance tilgængelig (f.eks. tredjepartsrevisioner)?
- Hvor aktuel og relevant er dokumentationen?
- Kan virksomheden understøtte revisioner eller vurderinger efter behov?
- Er gennemsigtighed løbende, eller er den begrænset til onboarding?

Kontraktuel parathed.

Overvejelser

- Kan sikkerhedskrav håndhæves kontraktligt?
- Er ansvar og forpligtelser klart fordelt mellem parterne?
- Er tidsfrister for hændelsesunderretning realistiske og afstemte?
- Er styring af ændringer og brug af underleverandører adresseret?
- Er krav til exit, ophør samt returnering eller sletning af data gennemførlige?
- Er ansvar, ansvarsbegrænsninger og skadesløsholdelse afstemt med eksponeringen for cyberrisici?

Forandrings- og varighedsforventninger

Overvejelser

- Hvordan vil væsentlige ændringer blive identificeret og vurderet (f.eks. nye tjenester, arkitekturændringer, fusioner og opkøb)?
- Hvor ofte bør revurdering finde sted?
- Er der defineret triggere for gengodkendelse eller eskalation?
- Findes der en klar exitstrategi, hvis risikoen bliver uacceptabel?

Kulturelle og samarbejdsmæssige signaler

Overvejelser

- Hvor transparent og responsiv er organisationen under due diligence?
- Bliver sikkerhed betragtet som et fælles ansvar eller som en barriere?
- Bliver sikkerhed betragtet som en omkostning eller en investering?
- Bliver problemstillinger og risici fremstillet defensivt eller konstruktivt?
- Er der vilje til løbende forbedring over tid?