CYBERSIKKERHED OG FORRETNINGSKONTINUITET

INDUSTRIENS FOND

SDU

FORSVARSAKADEMIET

Sikkerhedspraksisser i forsyningskæden set fra et produkt- og tjenestelivscyklus-perspektiv

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**
  - Integration af sikkerhedspraksisser i forsyningskæden i cybersikkerheds- og virksomhedens risikostyringsprogrammer.
  - Overvågning af praksissernes effektivitet gennem hele teknologiens produkt- og tjenestelivscyklus.
- **Deltagere**
  - **Interne:** Data- og IT-chefer, juridisk/compliance-funktioner samt produkt- og tjenesteejere.
  - **Eksterne:** Leverandører og underleverandører samt eventuelt revisorer/auditorer, hvis certificering er et mål.
- **Anvendelse**
  - Bør gennemføres risikobaseret og hændelsesdrevet – rutinemæssigt (f.eks. årligt eller ved kontraktfornyelse) samt når der sker væsentlige ændringer (f.eks. større opdateringer, hændelser, ejerskabsændringer eller nye kritiske afhængigheder).

Fremgamgsmåde

Ud fra praksisserne i resten af dette dokument udvælger organisationer de praksisser, der står mål med en given leverandørs kritikalitet, risikoprofil og rolle.

1. Udvælg relevante livscyklusfaser for leverandøren (f.eks. SaaS-leverandør (software som en service) vs. hardwareleverandør).
2. Anvend proportionalitet baseret på kritikalitet og risiko.
3. Kortlæg de udvalgte praksisser til interne kontroller for cybersikkerhed og Enterprise Risk Management (ERM).
4. Følg udviklingen ved hjælp af KPI'er/KRI'er over tid.

Dækkede aspekter

1. Styring (governance) og integration af risici.
2. Koncept-, design- og kravfase.
3. Leverandør-due diligence og udvælgelse.
4. Kontraktindgåelse og onboarding.
5. Udvikling, produktion og integration.
6. Levering, implementering og godkendelse.
7. Drift, vedligeholdelse og support.
8. Udfasning og ophør.

Styring (governance) og integration af risici

Formål:

- At sikre, at sikkerhedsrisici i forsyningskæden systematisk indarbejdes i virksomhedens governance, cybersikkerhed og risikostyring.

Praksisser

- Fastlæggelse af en strategi for forsyningskædesikkerhed og tilpasning af denne til målsætninger for cybersikkerhed og Enterprise Risk Management (ERM).
- Etablering af en formel politik for cybersikkerhed i forsyningskæden (Cybersecurity Supply Chain Risk Management – C-SCRM).
- Definition af risikoappetit og risikotolerance for leverandørrelaterede cyberrisici samt indarbejdelse af leverandørrisici i virksomhedens risikoregistre.
- Etablering af en eksplicit sammenhæng mellem leverandørrisici og business impact-analyse (BIA).
- Definition og opfølgning på KPI'er/KRI'er for performance inden for forsyningskædesikkerhed.
- Fastlæggelse af faste intervaller for rapportering til den øverste ledelse eller risikokomitéer.

Koncept-, design- og kravfase

Formål:

- At forebygge risiko ved at indarbejde sikkerhedskrav tidligt.

Praksisser

- Identifikation af kritiske leverandører, underleverandører og serviceafhængigheder.
- Kortlægning af produktkomponenter og tjenester i forhold til forretningskritiske processer.
- Fastlæggelse af sikkerhedskrav til hardware, software og tjenester, herunder definition af tillidsgrænser og trusselsmodeller, der også omfatter leverandører.
- Fastlæggelse af krav til privatlivsbeskyttelse og databeskyttelse.
- Etablering af sikre designgennemgange, der inkluderer trusler i forsyningskæden (f.eks. manipulation og forfalskede komponenter).

Leverandør-due diligence og udvælgelse

Formål:

- At vælge leverandører, der er i stand til at opfylde sikkerhedskravene.

Praksisser

- Etablering af en risikobaseret leverandørklassificering (kritisk, høj, middel, lav), der omfatter vurderinger af finansielle, operationelle, juridiske og geopolitiske risici samt leverandørens cybersikkerhedsmodenhed (politikker, kontroller, certificeringer).
- Løbende opfølgning på leverandørers certificeringsstatus (f.eks. ISO/IEC 27001, NIS2).
- Etablering og vedligeholdelse af et overblik over leverandørers hændelseshistorik og praksis for sårbarhedshåndtering.
- Krav om gennemsigtighed og oplysning om underleverandører samt outsourcet udvikling og processer.

Kontraktindgåelse og onboarding

Formål:

- Gør sikkerhedsforpligtelser håndhævelige.

Praksisser

- Fastlæggelse af kontraktligt håndhævelige forpligtelser vedrørende cybersikkerhed og forsyningskædesikkerhed.
- Etablering af kontrakter med revisionsret (right-to-audit) og adgang til dokumentation og sikkerhedserklæringer.
- Definition af tidsfrister for hændelsesunderretning og krav til samarbejde i kontrakter.
- Etablering af krav om underretning ved væsentlige ændringer (ejerskab, underleverandører, arkitektur).
- Fastlæggelse af forpligtelser vedrørende sikker ophør og sletning af data.
- Etablering af overgangs- og kontinuitetskrav for at reducere risikoen for leverandørlåsning.
- Etablering af kontroller til håndhævelse af godkendelseskrav ved underleverandørbrug til kritiske funktioner.
- Regelmæssig genvalidering af kontraktuelle sikkerhedskontroller.
- Fornyet godkendelse af leverandører efter fusioner, opkøb eller ændringer i ejerskab.

Udvikling, produktion og integration

Formål:

- At forebygge kompromittering under udvikling og integration.

Praksisser

- Etablering af sikre praksisser for softwareudvikling, herunder sikre kodningsstandarder, peer reviews, automatiseret sikkerhedstest samt beskyttelse af build-pipelines og signeringsnøgler.
- Implementering af chain-of-custody (kronologiske dokumentation, der sporer beslaglæggelse, opbevaring, kontrol, overdragelse, analyse og endelig disposition af fysiske eller digitale beviser eller materialer)-kontroller og anvendelse af manipulationssikret emballage.
- Etablering af praksisser for fysisk sikring af faciliteter og baggrundstjek af personale.
- Etablering af kontroller for at undgå gråmarkeds- eller forfalskede komponenter.
- Anvendelse og vedligeholdelse af en Software Bill of Materials (SBOM).

Levering, implementering og godkendelse

Formål:

- At sikre integritet mellem leverandør- og kundemiljøer.

Praksisser

- Verificering af leverandørens hærdnings- og konfigurationskrav.
- Validering af, at leverede komponenter svarer til de godkendte versioner.
- Gennemførelse af sikkerhedstest før ibrugtagning i produktion.
- Verificering af sikre konfigurationsbaselines før accept af produkter og tjenester.
- Etablering af godkendelsesporte, der er knyttet til risikogodkendelse.

Drift, vedligeholdelse og support

Formål:

- At håndtere udviklende risici i forsyningskæden over tid.

Praksisser

- Løbende revurdering af leverandørrisici.
- Overvågning af sårbarheder, der påvirker leverandørkomponenter.
- Indsamling af trusselsinformation relateret til leverandørøkosystemet.
- Fastlæggelse af tidsfrister og ansvar for patching, herunder koordinering ved offentliggørelse af kritiske sårbarheder.
- Etablering af integrerede hændelsesberedskaber og -reaktioner i samarbejde med leverandører.
- Etablering af processer til at anvende erfaringer (lessons learned) i opdatering af leverandørers risikoprofiler.

Udfasning og ophør

Formål:

- At forebygge resterende risici efter udfasning af tjenester eller produkter.

Praksisser

- Etablering af processer for sikker nedlukning og destruktion af data.
- Etablering af processer for tilbagekaldelse af adgange og legitimationsoplysninger.
- Gennemførelse af en risikovurdering efter ophør.