

5. Cybersikkerhed i kontrakter

www.cyber-smv.dk



Kravspecifikation
Requirements
specification



Formål, deltagere og anvendelse

- **Formål**

- Denne tjekliste har til formål at sikre, at cybersikkerhedsrisici håndteres effektivt gennem kontraktuelle krav og løbende opfølgning i relationer med leverandører og tredjeparter. Listen kan bruges som et styringsværktøj ved kontraktudarbejdelse, evaluering og leverandørstyring.

- **Deltagere**

- Ansvarlig for sourcing/leverandører, jura og økonomi.

- **Anvendelse**

- I udarbejdelser af kontrakter og samarbejdsaftaler.

Checkliste (1/6)

1. Forberedelse og risikobaseret tilgang

- ☐ Er der foretaget en systematisk risikovurdering for hver leverandørtype (baseret på dataadgang, systemintegration, geografisk placering mv.)?
- ☐ Er leverandører prioriteret ud fra kritikalitet for forretningsdrift, compliance og informationssikkerhed?
- ☐ Er der udarbejdet leverandørprofiler med kravniveauer (f.eks. niveau 1 = kritisk IT-drift, niveau 2 = konsulenttydelser, mv.)?
- ☐ Indgår cybersikkerhed i tidlige faser af leverandørudvælgelsen (Request for Information/Request for Proposal)?

Checkliste (2/6)

2. Formulering af kontraktuelle cybersikkerhedskrav

- ☐ Er cybersikkerhedskravene konkretiseret og nedskrevet i kontraktens hovedtekst eller bilag?
- ☐ Er der differentierede krav afhængigt af leverandørens risikoprofil?
- ☐ Indgår følgende emner:
 - ☐ Adgangsbegrænsning og brugerrettigheder?
 - ☐ Kryptering af følsomme data (i transit og i hvile)?
 - ☐ Backup og gendannelsesstrategier?
 - ☐ Sikker softwareudvikling (hvis relevant)?
 - ☐ Behandling af personoplysninger (GDPR)?
 - ☐ Brug af underleverandører og krav til dem?
- ☐ Henvises der til specifikke standarder og frameworks (f.eks. ISO 27001, NIS2, NIST osv.)?

Checkliste (3/6)

3. Ret til kontrol, tilsyn og dokumentation

- ☐ Giver kontrakten ret til auditering og inspektion, herunder varslet og uvarslet tilsyn?
- ☐ Er der krav om dokumentation for sikkerhedsforanstaltninger, f.eks. årlig ISAE 3000/3402-erklæring?
- ☐ Skal leverandøren fremvise resultater fra for eksempel:
 - ☐ Penetrationstests?
 - ☐ Sårbarhedsscanninger?
 - ☐ Incident response-øvelser?
- ☐ Fremgår det, at manglende dokumentation er kontraktbrud?

Checkliste (4/6)

4. Hændeshåndtering og ansvar

- ☐ Er der beskrevet krav om hændelsesrapportering inden for fast tidsramme (f.eks. 24 timer)?
- ☐ Er der fastlagt en kontaktstruktur og kommunikationsplan ved sikkerhedshændelser?
- ☐ Er roller og ansvar ved hændeshåndtering og efterforskning klart defineret?
- ☐ Skal leverandøren deltage i fælles hændelsesøvelser eller testscenarier?
- ☐ Indeholder kontrakten bestemmelser om f.eks.:
 - ☐ Erstatningsansvar ved datatab eller driftstab?
 - ☐ Dækning af retslige og regulatoriske konsekvenser?

Checkliste (5/6)

5. Sanktioner og misligholdelse

- ☐ Er der tydelige sanktionsmekanismer for brud på sikkerhedskrav, f.eks.:
 - ☐ Konventionalbod?
 - ☐ Suspendering af samarbejdet?
 - ☐ Kontraktophævelse?
- ☐ Er cybersikkerhed integreret i Service Level Agreements (SLA'er), inkl.:
 - ☐ Svar- og afhjælpningstider?
 - ☐ Antal årlige hændelser?
- ☐ Er der krav om økonomisk sikkerhed eller forsikring ift. sikkerhedsbrud?
- ☐ Er der etableret mekanismer til opfølgning og reaktion ved gentagne overtrædelser?

Checkliste (6/6)

6. Kontraktstyring, opfølgning og opdatering

- ☐ Er der en proces for løbende evaluering af cybersikkerhedskrav i takt med:
 - ☐ Nye trusler?
 - ☐ Nye teknologier=
 - ☐ Ændringer i leverandørens tjenester?
- ☐ Er ansvarlige internt for kontraktopfølgning og sikkerhedsovervågning udpeget?
- ☐ Er cybersikkerhed medtaget i kontraktændringsprocesser (ændringsbilag, fornyelser, forlængelser)?
- ☐ Foreligger der en centralt vedligeholdt oversigt over hvilke kontrakter, der har hvilke cybersikkerhedskrav?

Særligt i forhold til prioritering i kontrakter

- ☐ Er der indført et klassifikationssystem, hvor leverandører med høj forretningskritikalitet får:
 - ☐ Flere og skarpere sikkerhedskrav
 - ☐ Højere niveau af tilsyn
 - ☐ Hurtigere responstider?
- ☐ Er cybersikkerhedskravene tilpasset i forhold til leverandørens rolle (databehandler, systemintegrator, hardwareleverandør)?
- ☐ Indgår prioritering af cybersikkerhed som en del af kontraktforhandling og -scoring?