

Teknisk dokumentation

Den tekniske dokumentation er hjørnestenen i compliance-arbejdet under CRA. Den skal kunne dokumentere, at produktet **overholder de væsentlige cybersikkerhedskrav** i hele dets livscyklus, og fungere som **dokumentation overfor markedsovervågningsmyndigheder** og tredjepart.

Dokumentationen skal være: - Udarbejdet **inden produktet bringes i omsætning** - **Løbende ajourført**, når der sker ændringer i produktets funktion, arkitektur eller risikovurdering - **Opbevaret i hele supportperioden** – og mindst i 10 år

▮ Et produkt **må ikke bringes i omsætning**, før den tekniske dokumentation er klar og opfylder kravene.

Hvad skal dokumentationen indeholde?

Ifølge artikel 31 og bilag VII skal dokumentationen dække alle relevante tekniske og proceduremæssige forhold ved produktet, herunder:

- Generel beskrivelse af produktets formål og funktion
- Versionsnumre på software og firmware samt angivelse af patchniveau og udgivelsesdatoer (hvis relevant)
- Arkitektur og designbeskrivelser
- Vurdering af cybersikkerhedsrisici (trusler, sandsynlighed, konsekvens)
- Begrundelse for fastsat **supportperiode**
- Processer for **sårbarhedshåndtering**, opdateringer og sikkerhedsopdateringers formidling til brugere
- Oplysninger om anvendte **harmoniserede standarder** eller alternative tekniske løsninger
- Liste over **softwarekomponenter og afhængigheder (SBOM)**, herunder:
 - Komponenter indlejret i produktet
 - Komponenter hentet via **API'er, cloudtjenester eller eksterne moduler**
- Versioner og evt. licensinformation
- Reference til **overensstemmelseserklæring** (jf. bilag V)
- Navn og kontaktoplysninger på den **ansvarlige person**, som har underskrevet erklæringen og kan kontaktes af myndigheder

- Resultater fra tests og sikkerhedsvalidering (penetrationstest, fuzzing, statisk analyse mv.)
- **Ændringslog** over væsentlige ændringer i dokumentationen eller produktet

▮ Hvis produktet integrerer med eksterne tjenester eller API’er, skal disse medtages i SBOM og risikovurdering – **også selvom det er tredjepartskontrollerede systemer.**

Eksempler på dokumentationselementer

Dokumenttype	Formål
Risikovurderingsrapport	Identificere trusler og dokumentere cybersikkerhedsbeskyttelse
Arkitekturdiagram	Visualisering af systemdesign og komponentintegrationer
SBOM inkl. API’er og services	Sporing af alle softwarekomponenter – også tredjepart
Testresultater (f.eks. fuzzing)	Dokumentation for cybersikkerhedsniveau
Patch- og updateprocedurer	Forklaring af hvordan og hvornår opdateringer leveres
Ændringslog og versionshistorik	Sporbarhed for dokumentationens ajourføring

Tilgængelighed og sprog

Dokumentationen skal: - Være tilgængelig i hele supportperioden - Udarbejdes på **et officielt EU-sprog**, der anerkendes af medlemsstaten - Kunne fremvises på anmodning fra myndigheder – både **i digitalt og fysisk format**

- ▮ Husk: Teknisk dokumentation er ikke kun en engangsopgave – den skal leve og opdateres i takt med produktets udvikling og cybersikkerhedslandskabets ændringer.
- ▮ Se også [10_sbom.md](#) for uddybning af dokumentationskravene til softwarekomponenter og afhængigheder.

Last update: 2025-10-30 12:07:19