

SBOM og sårbarhedshåndtering

CRA stiller klare krav til, hvordan producenter skal håndtere cybersikkerhed i hele produktets livscyklus. To centrale elementer i denne indsats er:

- En **Software Bill of Materials (SBOM)** – en detaljeret oversigt over anvendte softwarekomponenter
- En struktureret proces for **sårbarhedshåndtering** og rapportering

Disse krav fremgår især af **Bilag I, del II**, samt af flere centrale **præambler** og **artikler**, herunder 13, 31 og 54–60.

SBOM – Software Bill of Materials

SBOM er en struktureret liste over alle softwarekomponenter i produktet – herunder open source, tredjepartsbiblioteker, egne moduler og integrerede services. CRA kræver, at denne dokumentation:

- **Opbevares som en del af den tekniske dokumentation** (jf. bilag VII)
- **Kan fremlægges på anmodning** fra markedsovervågningsmyndigheder (præambel 22)
- **Omfatter alle relevante komponenter**, inkl. API'er og tjenester, som produktet er afhængigt af (præambel 34)

□ Også software og services integreret via API'er – selv hvis det er tredjepart – skal indgå i SBOM og vurderes i risikovurderingen, hvis de er væsentlige for produktets funktion eller sikkerhed.

SBOM skal typisk inkludere:

- Navn og version på hver komponent
 - Leverandør eller oprindelse (f.eks. OSS-projekt)
 - Licensinformation
 - Kendte sårbarheder (CVE'er), hvor relevant
 - Brugsmønster og funktion (fx lokal, cloud, ekstern service)
-

SBOM via Software Composition Analysis (SCA)

En SBOM kan opbygges automatisk ved brug af **Software Composition Analysis (SCA)** – en metode til at analysere kildekode, build-systemer og afhængighedsstyring.

SCA identificerer:

- Direkte og indirekte afhængigheder
- Versioner og udgivelsesdatoer
- Kendte sårbarheder (CVE'er)
- Licensoplysninger og rettighedsforhold

▮ **Vigtigt:** SCA kan kun bruges på komponenter, hvor fabrikanten har **adgang til kildekoden eller de anvendte artefakter** (f.eks. compiled libraries, pakker eller container images). Det kan **ikke anvendes på black-box-komponenter** eller eksterne API'er, hvor der ikke er adgang til komponentens indhold.

Opdateringer og adskillelse af funktionalitet

CRA fastsætter, at **sikkerhedsopdateringer skal leveres særskilt fra funktionalitetsopdateringer** (jf. præambel 57 og bilag I, del II). Det betyder:

- Brugere må ikke tvinges til at installere nye funktioner for at modtage sikkerhedsrettelser
- Opdateringsmekanismen skal tydeligt skelne mellem sikkerhedsrettelser og nye features
- Brugeren skal informeres om opdateringens formål

Dette princip sikrer, at **cybersikkerhed prioriteres** – og at brugere trygt kan modtage opdateringer uden at frygte utilsigtede ændringer i funktionalitet.

Sårbarhedshåndtering og opdateringer

CRA forpligter fabrikanten til at identificere, håndtere og afhjælpe sårbarheder i hele produktets **supportperiode**. Dette omfatter både interne komponenter og eksterne afhængigheder.

Kravene omfatter:

- **Overvågning og identifikation** af sårbarheder i hele produktets livscyklus
- **Reaktion og afhjælpning**, herunder udarbejdelse og udrulning af sikkerhedsopdateringer
- **Underretning** af relevante aktører, herunder:
 - Brugere (jf. præambel 67)
 - Markedsovervågningsmyndigheder

- **CSIRT og ENISA ved aktivt udnyttede sårbarheder** (jf. artikel 14 og præambel 65)
- **Opdateringsmekanismer**, der muliggør nem og rettidig levering til brugere (præambel 56–57)

□ CRA forbyder at bringe produkter i omsætning, hvis de har **kendte sårbarheder** på tidspunktet for markedsføring (præambel 38).

Supportperiode og ajourføring

- Producenten skal **fastsætte en supportperiode** i overensstemmelse med produktets forventede levetid (præambel 59)
- Supportperioden skal som hovedregel være mindst **5 år** (præambel 60)
- **Dokumentation, SBOM og risikovurderinger skal ajourføres**, når produktet ændres, opdateres eller nye trusler identificeres
- Ved supportens ophør opfordres det til at:
- **Frigive kildekoden**, eller
- **Overdrage ansvaret** til anden part (præambel 61)

Centrale krav i bilag I, del II – Sårbarhedshåndtering

Krav	Beskrivelse
Kendte sårbarheder	Produktet må ikke indeholde kendte sårbarheder ved lancering
Rapportering	Brugere skal kunne rapportere sårbarheder via kontaktpunkt
Sikkerhedsopdateringer	Skal være gratis, rettidige og særskilt fra funktionsopdateringer
Ændringsstyring og logning	Ændringer og hændelser skal kunne spores og logges
Underretning ved aktiv udnyttelse	Fabrikanten skal informere myndigheder og brugere

□ CRA forpligter fabrikanten til **proaktiv sikkerhedsledelse**: Det er ikke nok at reagere – man skal **forudsige, dokumentere og forebygge** sårbarheder aktivt.

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