The EU Cyber Resilience Act (CRA)

Key facts at a glance

The EU Cyber Resilience Act (CRA) is an upcoming legislation that will place strict cyber security requirements on any product with digital elements made available on the EU's internal market. The act is expected to enter into force in mid 2024, and the latest draft foresees compliance grace periods of 21 and 36 months. Hence, vendors should plan for partial CRA compliance by early 2026. Full compliance will be required by mid 2027.

Scope

The CRA is set to cover all software and hardware products that (i) are made available on the EU market, and (ii) include any form of data connectivity. Coverage includes remote (cloud) data processing associated with the product. Excluded are certain medical, automotive, aviation, maritime, and military products, as well as services (e.g. SaaS, PaaS, IaaS).

Product requirements

The CRA requires vendors to design their products with security in mind. It lists several concrete product requirements. These include, among others:

- Products must be supplied without any known exploitable vulnerabilities.
- Products must have access control mechanisms.
- Data protection must be provided.
- Products must be resistant against Denial of Service (DoS) attacks.
- Products must include (automated) distribution of security updates.
- Security information and instructions must be provided.

Process requirements

Additionally, the CRA requires manufacturers put in place several security-related processes. These include, but are not limited to:

- Identifying and documenting product-related cybersecurity risks.
- Maintaining a software bill of materials (SBOM).
- Efficient handling of vulnerabilities (incl. updates) during a predefined support period covering a product's expected lifetime.
- Publicly disclosing information about patched vulnerabilities.
- Establishing a vulnerability reporting mechanism available to third parties.
- Performing security assessments and testing.
- Recalling products as appropriate.
- Notifying the EU (within 24h) and users about security incidents.

Demonstrating compliance

Depending on the product class, compliance can be demonstrated through (i) self-declaration, (ii) the use of standards, (iii) type-approval, (iv) a purpose-certified internal quality assurance mechanism, or (v) a European cybersecurity certification scheme.

Penalties

Depending on the type of violation, non-compliance may be penalised with fines of up to €15 million, or 2.5% of total worldwide annual turnover, whichever is higher.

Published by
Zühlke Engineering AG, Zürcherstrasse 39J, CH -8952 Schlieren
www.zuehlke.com
Contact: Dr. Piet De Vaere, piet.devaere@zuhlke.com