Press Release

Add value.
Inspire trust.

Cyber Resilience Act

November 20, 2024

TÜV SÜD makes digital products cyber fit

Munich. With its promulgation in the EU OJ on 20 November 2024 the Cyber Resilience Act (CRA) has tightened the requirements for digital products in the EU. Manufacturers, importers and distributors need to adjust their cybersecurity policies and practices in accordance with the new law. The focus is on comprehensive vulnerability management, mandatory CE marking, the cybersecurity of digital products and strict obligations governing the reporting of security incidents.

The CRA introduces new, binding and comprehensive cybersecurity requirements for connected hardware and software products in the European Union. “The aim is that ‘products with digital elements’ are more secure and that manufacturers remain responsible for cybersecurity throughout a product’s life cycle thereby protecting businesses and consumers“, says Maxime Hernandez, Cybersecurity Program Manager at TÜV SÜD. The new regulation applies to products such as smart TVs, firmware, sensors used for the monitoring of machinery and even products used in industrial plants. However, its scope excludes products such as medical devices, and safety systems used in motor vehicles and civil aviation, all of which are governed by separate industry-specific requirements. Manufacturers, importers or distributors of digital products that are not in conformity with the CRA are risking high fines and will lose their approval for the EU market. “To prepare for increasingly complex cybersecurity threats, companies need to consider not only the operational phase of the digital product but its entire life cycle which includes design, development, production, etc”, explains Maxime Hernandez.

- The proof of CRA conformity required depends on the risk class of a product. For digital products that are not classified as either Important or Critical manufacturers can self-declare conformity as outlined in module A accompanied by technical documentation demonstrating compliance with the essential requirements. For important products, by contrast, manufacturers and distributors must obtain assessment by a notified body, like TÜV SÜD and apply harmonized standard when they become available. This applies to class I products such as network management systems, password managers or smart home products with security functionalities. Class II includes digital products with a

higher cybersecurity risk level, such as firewalls, tamper-resistant microprocessors, tamper-resistant microcontrollers. Maxime Hernandez points out, “We provide audits, testing and risk assessment based on our longstanding experience with relevant product category standard”

Secure by design

The CRA will require connected products to offer the possibility to encrypt relevant data, protect from unauthorised access and provide a secure-by-default configuration. Simply proving a product’s cybersecurity when placing it on the market will no longer be enough. Instead, manufacturers need to assess the cybersecurity risks throughout the life cycle of their products. “When purchasing components, for example, manufacturers must perform due diligence to exclude any security gaps and vulnerabilities in the finished products caused by the purchased components”, says Maxime Hernandez. Vulnerability handling is a central obligation for manufacturers. “To respond adequately, manufacturers need to discover and assess vulnerabilities at an early stage.” Manufacturers must ensure security updates throughout the expected lifetime of their products. If a security issue is identified in this period, manufacturers must publish security advisory messages and release security patches and updates free of charge.

Manufacturers also have the obligation to report security incidents to the European Union Agency for Cybersecurity (ENISA), the product user and, where applicable, any parties commissioned with the maintenance and repair of the product. Digital product users need to respond particularly quickly in the case of a vulnerable product by patching when an update is available or isolating the product while waiting for the patch. TÜV SÜD helps manufacturers to implement the processes needed for reporting these incidents and ensuring compliance with the CRA requirements for technical documentation.

Transparent communication and documentation

The CRA also requires comprehensive product documentation that lists all important characteristics and security functions. The documentation must state which cybersecurity risks may occur under which circumstances, and give details of contact point in case of a cybersecurity vulnerability. It must also point out where the CE marking and the software bills of material can be found. The latter provides a detailed list of all software elements and facilitates security management.

All the CRA requirements will come into force following a 36-month transition period. “Nevertheless, manufacturers, distributors and importers should start to address the CRA at an

early stage, to ensure their users' security and avoid competitive disadvantages later on. Manufacturers need to start a new journey on improving their products and it cannot be done overnight", says Maxime Hernandez. Given this, TÜV SÜD has already started to offer a comprehensive training and testing program on cyber resilience.

Further information:

- tuvsud.com/en/resource-centre/stories/cyber-resilience-act-a-new-era-in-product-cybersecurity
- www.tuvsud.com/en/themes/cybersecurity
- Regulation - 2024/2847 - EN - EUR-Lex

Media Relations:

TÜV SÜD AG Corporate Communications Westendstr. 199 80686 Munich, Germany	Dirk Moser-Delarami Phone +49 89 5791-1592 E-Mail dirk.moser-delarami@tuvsud.com Internet tuvsud.com/newsroom