

CRA, NIS-2 & Co. – leveraging new regulations for greater cybersecurity

Regulations such as the Cyber Resilience Act (CRA), NIS-2 and IEC 62443 Machinery Directive set new standards for the security level of digital products and infrastructures. Fraunhofer AISEC shows how companies can meet regulatory requirements, build security and future-proof their digital business models by implementing minimum standards.

Digitalisation is advancing in Germany and Europe, but with it, the attack surface for cybercriminals is also growing. The number of cyber attacks is rising rapidly – according to a Bitkom study on the cyber security situation in Germany in 2024, 91 percent of German companies reported incidents of data theft, espionage or sabotage, with an estimated economic loss of 267 billion euros. Critical infrastructures are particularly affected and are increasingly becoming the target of attacks from abroad. The threat situation is exacerbated by new attack methods using artificial intelligence.

Against this backdrop, new cybersecurity requirements such as the Cyber Resilience Act (CRA), NIS 2 Directive and IEC 62443 machine directive aim to strengthen trust in digital products and promote the European single market and digital business models.

CRA, NIS-2 and IEC 62443 as new guidelines

The CRA establishes uniform requirements for the cybersecurity of digital hardware and software products across Europe for the first time. Manufacturers, importers and distributors must implement comprehensive security measures, including risk assessments, vulnerability management and inventory lists for software components (known as software bills of materials). Companies that violate these regulations risk heavy fines and loss of market access.

The NIS 2 Directive extends the scope of cybersecurity requirements to numerous sectors, including health-care, transport and energy. It obliges companies to introduce cyber risk management and report security incidents. Violations can be punished with fines of up to ten million euros.

In addition, the IEC 62443 standard defines security requirements for industrial automation and control systems. It sets standards for secure product development processes and the 'secure by design' approach in order to minimise risks right from the design phase.

Companies, especially SMEs, find compliance with these regulations very challenging. The multitude of requirements appears complex and their implementation resource-intensive.

However, intelligent automation can make compliance with regulatory requirements efficient and resource-friendly, while also strengthening a company's own cyber security in the long term. 'There are already a number of technologies and measures in place that provide effective protection against many attacks. The new EU regulations now provide companies with helpful guidelines for implementing minimum standards,' explains Prof. Dr. Claudia Eckert, Director of the Fraunhofer AISEC.

Implement minimum standards and establish effective protection

A key element for the effective implementation of the various regulations is the creation of a mapping between the diverse requirements in order to identify overlaps and exploit efficiency potential. This reduces redundant measures and creates a security basis based on the identified minimum standards. 'This not only enables companies to secure market access, for example to the EU single market by means of CE marking, or avoid sanctions for legal violations, but also protects them against misuse, data loss and espionage,' says Eckert.

Eckert identifies the following key commonalities in the requirements to be met:

- the implementation of risk assessment processes
- the implementation of vulnerability management, for example with patches and updates throughout the entire product lifecycle
- the assurance of business continuity, for example by means of backup and crisis management
- the assurance of the security of the digital supply chain, for example by recording the hardware and software components used with the Software Bill of Materials (SBOM)
- the implementation of an information security management system (ISMS) in which access rights are securely managed and clear rules for handling passwords and emails are established
- the implementation of a continuous reporting and notification system, for example with regular proof of compliance and continuous documentation of the precautions taken and their effectiveness

- the implementation of appropriate security measures in line with the state of the art, such as zero trust, multi-factor authentication, etc.

Automation as a factor for success

(Partially) automated tools enable continuous monitoring and documentation of compliance with these measures and the creation of proof of compliance. AI solutions can significantly increase the speed of cyber defence and minimise the effort required for effective protection.

Fraunhofer AISEC supports companies with technology- and application-oriented security solutions, e.g. as open source tools that facilitate the implementation of regulatory requirements based on (partially) automated technologies. The tools developed at Fraunhofer AISEC support the identified minimum standards such as risk assessment, vulnerability management, supply chain and policy management, and declaration of conformity.

Fraunhofer AISEC thus strengthens the reliability, trustworthiness and tamper resistance of IT-based systems and products, enabling companies to build confidence in the security of their products. This is a decisive factor in sustainably strengthening digital business models and securing competitive advantages in the German and European single market.



Contact

Prof. Dr. Claudia Eckert
 Managing Director
 Phone: +49 89 3229986-292
 claudia.eckert@aisec.fraunhofer.de

More Information



Spotlight 'Cyber Resilience Act'

The identification of assets, the establishment of protection and the achievement of compliance

RISK-ASSESSMENT

'**QuBA**' (**Questionnaire-Based Assessment**) is a questionnaire-based, quick and easy risk assessment method tailored to simple products with uniform protection requirements. (Contact: Daniel Angermeier, daniel.angermeier@aisec.fraunhofer.de)

VULNERABILITY MANAGEMENT

The **analysis tool 'Codyze'** automatically checks software code for compliance with applicable regulations for communication, encryption, compliance, and certification. It identifies potential security vulnerabilities and recommends specific actions to remedy them. (Contact: Christian Banse, christian.banse@aisec.fraunhofer.de)

The '**Clouditor**' continuously checks the secure configuration of cloud services on cloud platforms. Using defined catalogues, it monitors security and compliance requirements as well as data encryption, access management and data protection compliance. (Contact: Christian Banse, christian.banse@aisec.fraunhofer.de)

The **library 'kotlin-csaf'** enables the parsing, importing and validation of CSAF documents. With the help of the library, the implementation of the provider can be automatically checked for correctness. (Contact: Christian Banse, christian.banse@aisec.fraunhofer.de)

SUPPLY CHAIN MANAGEMENT

The **open source framework 'Connector Measurement Component (CMC)'** records all software components used and enables the establishment of certified communication networks in heterogeneous, cloud-based infrastructures, regardless of the hardware used. (Contact: Sascha Wessel, sascha.wessel@aisec.fraunhofer.de)

POLICY MANAGEMENT

The '**GyroidOS**' platform protects the integrity, confidentiality and availability of data and software with numerous security functions and contributes significantly to meeting security requirements. It also supports certification processes in accordance with industry standards DIN SPEC 27070 and IEC 62443-4-2 as well as Common Criteria. (Contact: Sascha Wessel, sascha.wessel@aisec.fraunhofer.de)

DECLARATION OF CONFORMITY

'**Confirmate**' can be used to perform automated conformity checks on software components. The tool combines static code analysis with a compliance evaluation and checks the conformity of third-party software against vulnerability databases. (Contact: Christian Banse, christian.banse@aisec.fraunhofer.de)



Website 'Codyze'



'Clouditor' on GitHub



'kotlin-csaf' on GitHub



'CMC' on GitHub



Website 'GyroidOS'



Press release 'Confirmate'