

Cyber Resilience Act:

Why Cybersecurity Is Becoming a Product Feature

Starting in 2027, the Cyber Resilience Act will fundamentally change the requirements for products with digital elements. For manufacturers, machinery builders, and operators, this means that cybersecurity will no longer be viewed as a downstream IT task, but rather as an integral part of the product throughout its entire lifecycle.

TOX® is already an active part of this development. The TOX® system ecosystem is consistently designed to meet the upcoming requirements for secure, updatable, and resilient products.

The CRA Sets a New Standard for Digital Products

The Cyber Resilience Act, or CRA for short, is EU Regulation 2024/2847 for products with digital elements. It applies to hardware and software made available on the EU market, including separately marketed components. The goal is to develop digital products more securely, address vulnerabilities more effectively, and provide users with greater transparency regarding cybersecurity.

The EU is thus responding to a well-known problem: While many connected products are becoming increasingly powerful, they are not always provided with sufficient security, clear update processes, or transparent information about risks and support. This is precisely where the CRA comes in.

What's Changing for Manufacturers and Users

The CRA is primarily aimed at manufacturers. In the future, they must be able to demonstrate that cybersecurity has already been taken into account during planning, development, production, deployment, and maintenance. This includes, among other things:

- Risk assessment for products with digital elements
- Secure development and technical documentation
- Procedures for handling vulnerabilities
- Provision of security updates during the support period

- Conformity assessment and CE marking
- Reporting requirements for actively exploited vulnerabilities and serious security incidents

For users and machine builders, this means that the selection of digital components will become more strategic. What matters is not only whether a product works today, but whether it can be operated securely, updated, and evaluated transparently throughout its lifecycle.

Key Deadlines

The CRA entered into force on December 10, 2024. Implementation will occur in phases:

Date	Significance
June 11, 2026	Start of requirements for conformity assessment bodies
September 11, 2026	Start of reporting obligations for manufacturers
December 11, 2027	Full application of the essential CRA requirements

No later than December 11, 2027, affected products that do not meet the requirements may no longer be made available on the EU market.

Why the CRA Is More Than Just Compliance

The CRA is not just a regulatory issue. It sends a signal to the industry: connectivity, data capabilities, and digital product logic require a new understanding of safety.

In modern production environments, it is no longer sufficient to view individual components in isolation. Machines, drives, control systems, software, network interfaces, and data flows form an integrated system. The more closely these elements are connected, the more important secure architectures, clear responsibilities, and updatable platforms become.

Cybersecurity thus becomes a quality attribute of industrial products. It influences availability, investment security, and trust in automated processes.

TOX® is CRA-ready

TOX® is actively embracing this transformation. With TOX® drive and system solutions, cybersecurity is considered an integral part of product development from the very beginning.

This is not just about individual technical functions, but about future-proof system logic: networked drive technology, software, process monitoring, data connectivity, and lifecycle capability must work together seamlessly.

TOX® drive technology combines integrated control and process logic, quality data acquisition, network connectivity, and software into a modular overall system. This modular system forms the foundation for the TOX® MultiTechnology Platform. TOX® software serves as the central element of the system architecture.

With its drive and system solutions, TOX® provides the foundation that enables customers to operate safely and with future-proof capabilities, even in a more heavily regulated, networked production environment.

Conclusion

The Cyber Resilience Act makes it clear: The future of industrial products is not only digital but also cyber-resilient. This creates a shared responsibility for manufacturers and users. Products must be developed securely, documented transparently, and provided with security updates throughout their intended support period.

TOX® is already addressing these upcoming requirements today and supports customers in using modern drive technology in a secure, connected, and future-proof manner.

4,817 characters including spaces

Service for editorial offices:

Meta title: Cyber Resilience Act: TOX® Focuses on Secure and Resilient Systems

Meta description: The Cyber Resilience Act makes cybersecurity a product attribute. TOX® is adapting its drive and system solutions to meet the new requirements.

Keywords: TOX® PRESSOTECHNIK; Cyber Resilience Act; CRA; cybersecurity; cyber resilience; machine safety; drive technology; TOX® software; industrial software; connected production; IT security; process monitoring; lifecycle; security updates; mechanical engineering; automation

Image caption:



Image 1: The TOX® software combines operation, process monitoring, and data processing, making it a central component of safe and connected production processes.

Image: TOX® PRESSOTECHNIK SE & Co. KG

About the company:

TOX® is a supplier of presses, systems as well as components for sheet metal joining and assembly technology. Since its foundation in 1978, the family business has become a global player with more than 1500 employees worldwide, over 500 of which are based at the headquarters in Weingarten near Ravensburg, Germany. The success story started with one pneumohydraulic drive – the TOX® Powerpackage. The “Components” division now includes pneumohydraulic and electromechanical drives as well as controls, sensors and software for process monitoring and quality assurance. In addition to a large range of presses, the system range comprises manual, machine and robot tongs. Another mainstay are modern sheet metal joining procedures, also incorporating the TOX® Clinching Technology, which makes the company today’s market leader.

Drives, processes and systems from TOX® can be found at automotive manufacturers and their suppliers as well as at industrial businesses for household appliances, electronic components, furniture and much more. Special versions of the TOX® Drives are also approved for the food industry.

TOX® is represented worldwide: 17 subsidiaries, amongst others in the USA and South America, Europe and South Africa, India, China and the entire Pacific Region. 18 representatives in many other markets support and advise local customers.

In case of questions, contact:

TOX® PRESSOTECHNIK SE & Co. KG

presse@tox-de.com

Riedstraße 4

88250 Weingarten, Germany

Tel.: +49 751 5007- 0

www.tox.com

Please send us a copy of any publication:

presse@tox-de.com