

CYBER RESILIENCE ACT

Mitsubishi Electric sichert CE-Konformität mit Resilienz Management

Der Cyber Resilience Act (CRA) verpflichtet Hersteller, Importeure und Händler, Cybersicherheit über den gesamten Lebenszyklus von Produkten mit digitalen Elementen nachweisbar umzusetzen. Für die industrielle Automatisierung bedeutet das, dass Produkte von Anfang an sicher entwickelt werden („Secure by Design“), mit voreingestellten Sicherheitsfunktionen ausgeliefert werden („Secure by Default“), bekannte Schwachstellen aktiv behoben werden und über den gesamten Lebenszyklus kostenlose Sicherheitsupdates verfügbar sind.

Die Verordnung (EU) 2024/2847 wurde am 20. November 2024 veröffentlicht. Ab dem 11. September 2026 greifen Meldepflichten für aktiv ausgenutzte Schwachstellen, ab dem 11. Dezember 2027 gelten alle Anforderungen vollständig. Damit wird Cybersicherheit zu einem zentralen Bestandteil der CE-Konformität.

Für Betreiber vernetzter Produktionsanlagen steigern verbindliche Update- und Meldeprozesse die Planbarkeit und reduzieren Risiken in der Lieferkette. Steuerungen, HMIs und Netzwerktechnik müssen künftig nicht nur leistungsfähig, sondern auch auditierbar cyberresilient sein. Mitsubishi Electric integriert die CRA-Vorgaben konsequent in Entwicklung, Betrieb und Support. Ein Product Security Incident Response Team (PSIRT)

koordiniert das Schwachstellenmanagement und veröffentlicht Gegenmaßnahmen. Als CVE Numbering Authority (CNA) kann Mitsubishi Electric Sicherheitslücken eindeutig kennzeichnen und transparent kommunizieren. Ergänzend setzt das Unternehmen auf signierte Firmware-Updates, rollenbasierte Zugriffskontrollen und Monitoring-Konzepte, die den Betrieb schützen und Compliance sicherstellen. Alle Maßnahmen orientieren sich an internationalen Standards wie IEC 62443-4-2 und schaffen eine belastbare Grundlage für Audit und Nachweisführung.

Von HMI bis SPS: Technische Maßnahmen für auditierbare Cyberresilienz

Mitsubishi Electric ist dabei, diese Anforderungen erfolgreich umzusetzen. Bei HMIs, wie zum Beispiel bei der neuen GOT3000-Serie kommen signierte Firmware-Updates, restriktive Standardkonfigurationen und eine rollenbasierte Benutzerverwaltung zum Einsatz. SPS-Systeme wie die neuen Plattformen MELSEC MX-F und MX-F werden durch getrennte Engineering- und Betriebsnetze, verschlüsselte Fernzugriffe und definierte Update-Prozesse gegen Cyberattacken resilient gemacht. Typische Nachweise umfassen eine vollständige SBOM, dokumentierte Patch-Prozesse, Log-Export und die Kommunikation des Supportzeitraums. Für Antriebe, Roboter und Engineering-Software gelten vergleichbare Prinzipien: sichere Kommunikationspfade, dokumentierte Lebenszyklus-Supportzeiten und Offenlegung bekannter CVEs (Common Vulnerabilities and Exposures). Diese Maßnahmen erhöhen die Resilienz gegenüber Manipulationen und unterstützen die Nachweisführung im Rahmen der CE-Kennzeichnung.

Aktuelle Bedrohungslage und regulatorischer Druck

Die Relevanz des CRA wird durch aktuelle Entwicklungen unterstrichen. Laut Dragos Report stieg die Zahl der Ransomware-Angriffe auf Industrieorganisationen im Jahr 2024 gegenüber 2023 um mehr als 87 Prozent, parallel wurden neue ICS-spezifische Malware-Familien identifiziert. Gleichzeitig verschärft Deutschland mit dem NIS-2--Umsetzungsgesetz die Anforderungen an Unternehmen: Rund 29 000 Unternehmen fallen seit Ende 2025 unter erweiterte Sicherheits- und Meldepflichten, Cybersecurity wird ausdrücklich zur Leitungsaufgabe. Damit steigt der Compliance-Druck entlang der industriellen Lieferkette erheblich und ergänzt die Vorgaben des CRA.

Mehr Vertrauen in industrielle Systeme

Der CRA eröffnet Chancen für mehr Transparenz und Vertrauen in Automatisierungslösungen. Mitsubishi Electric bietet Lösungsansätze für eine sichere, zukunftsfähige Produktion, von sicheren Firmware-Updates über Zugriffskontrollen bis hin zu Monitoring-Konzepten. Ergänzend stellt das Unternehmen Checklisten und Security Advisories bereit, um die Nachweisführung für Audits zu erleichtern. Praxisbeispiele wie wöchentliche Patchfenster für HMIs oder SPS-Engineering über Jump-Hosts nach dem Bastion-Prinzip verdeutlichen den Nutzen für den Betrieb.

Autor: Silvia von Dahlen, Marketing Communications Manager

Mitsubishi Electric Europe B.V. Industrial Automation

Weitere Informationen unter:

[Cyber Resilience Act CRA - Cyber Security für die Industrie](#)

Quellen

Verordnung (EU) 2024/2847 *<https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng>

Dragos report: <https://www.dragos.com/resources/press-release/dragos-reports-ot-ics-cyber-threats-escalate-amid-geopolitical-conflicts-and-increasing-ransomware-attacks>

NIS-2-Umsetzungsgesetz: [BSI - Presse - NIS-2-Umsetzung: Bundestag beschließt Cybersicherheitsgesetz](#)

Bilder



Bild 1: Secure by Default und Design. Mitsubishi Electric integriert die CRA-Vorgaben konsequent in Entwicklung, Betrieb und Support.

(Quelle: Getty Images)



Bild 2: Keine Chance für Ransomware-Angriffe dank CRA.

(Quelle: Getty Images)

Das/die Bild(er), das/die mit dieser Pressemitteilung verteilt wird/werden, ist/sind nur für den redaktionellen Gebrauch bestimmt und unterliegt/unterliegen dem Urheberrecht. Das/die Bild(er) dürfen nur zur Begleitung der hier genannten Pressemitteilung verwendet werden, eine andere Verwendung ist nicht gestattet.

Über Mitsubishi Electric Corporation

Mit mehr als 100 Jahren Erfahrung in der Bereitstellung zuverlässiger und qualitativ hochwertiger Produkte ist Mitsubishi Electric ein weltweit anerkannter Marktführer in der Herstellung, dem Marketing und dem Vertrieb von elektrischen und elektronischen Geräten für die Informationsverarbeitung und Kommunikation, Weltraumentwicklung und Satellitenkommunikation, Unterhaltungselektronik, Industrietechnologie, Energie, Mobilitäts- und Gebäudetechnologie sowie Heiz-, Kälte- und Klimatechnologie. In Anlehnung an „Changes for the Better“ ist Mitsubishi Electric bestrebt, die Gesellschaft mit Technologie zu bereichern. Das Unternehmen erzielte zum Ende des Geschäftsjahres am 31.03.2025 einen konsolidierten Umsatz von 36,8 Milliarden US-Dollar*. In über 30 Ländern sind Vertriebsbüros, Forschungsunternehmen und Entwicklungszentren sowie Fertigungsstätten zu finden. Seit 1978 ist Mitsubishi Electric in Deutschland als Niederlassung der Mitsubishi Electric Europe vertreten. Mitsubishi Electric Europe ist eine hundertprozentige Tochter der Mitsubishi Electric Corporation in Tokio. Weitere Informationen finden Sie unter www.MitsubishiElectric.com.

**Die Beträge in US-Dollar werden von Yen zum Kurs von ¥150=US\$1 umgerechnet, dem ungefähren Kurs auf dem Tokioter Devisenmarkt am 31. März 2025.*

Über die Mitsubishi Electric Factory Automation Business Group

Mitsubishi Electric bietet eine breite Palette an Automatisierungs- und Verarbeitungstechnologien, darunter Steuerungen, Antriebsprodukte, Produkte zur Energieverteilung und -steuerung, Funkenerosionsmaschinen, Elektronenstrahlmaschinen, Laserbearbeitungsmaschinen, numerische Computersteuerungen und Industrieroboter, und trägt so zu einer höheren Produktivität - und Qualität - in der Fertigung bei. Darüber hinaus bieten die umfangreichen Servicenetzwerke rund um den Globus eine direkte Kommunikation und umfassende Unterstützung für die Kunden. Der globale Slogan "Automating the World" verdeutlicht den Ansatz des Unternehmens, durch den Einsatz fortschrittlicher Technologien, die Weitergabe von

Know-how und die Unterstützung der Kunden als vertrauenswürdiger Partner die Automatisierung zum Wohle der Gesellschaft zu nutzen.

Weitere Informationen über die Geschichte von "Automating the World" finden Sie hier:

www.MitsubishiElectric.com/fa/about-us/automating-the-world

Mitsubishi Electric Industrial Automation

Die Mitsubishi Electric Europe B.V., Industrial Automation hat ihren Hauptsitz in Ratingen bei Düsseldorf. Sie ist Teil der Mitsubishi Electric Europe B.V., die seit 1978 in Deutschland vertreten ist, einer hundertprozentigen Tochtergesellschaft der Mitsubishi Electric Corporation, Japan. Ihre Aufgabe ist es für den Bereich Industrial Automation den Vertrieb, Service und Support in der gesamten DACH-Region und Benelux zu steuern.

Weitere Informationen finden Sie unter de.mitsubishielectric.com/fa

Weitere Informationen:

de.mitsubishielectric.com

Folgen Sie uns weiter:



youtube.com/Benutzer/MitsubishiFAEU



twitter.com/MitsubishiFAEU



<https://www.linkedin.com/showcase/mitsubishi-electric-europe-industrial-automation>



https://www.instagram.com/mitsubishi_electric_fa_emea/

Pressekontakt:

Mitsubishi Electric Europe B.V.

Industrial Automation

Silvia von Dahlen

Manager Marketing Communications

Mitsubishi-Electric-Platz 1

40882 Ratingen, Deutschland

Tel.: +49 (0)2102 486-5160

Fax: +49 (0)2102 486-7170

silvia.von.dahlen@meg.mee.com

de.linkedin.com/in/silvia-von-dahlen

