

Cyber Resilience Act @Balluff – So wollen wir die CRA-Konformität erreichen

Der Cyber Resilience Act (CRA) der Europäischen Union setzt neue, verbindliche Standards für die Cybersicherheit von Produkten mit digitalen Elementen. Für Balluff hat der CRA große Bedeutung, da er nicht nur die Sicherheit vernetzter Produkte stärkt, sondern auch deren Konformität auf dem europäischen Markt sicherstellt. Gemeinsam schaffen wir so eine widerstandsfähigere digitale Infrastruktur.

Wir haben sorgfältig geprüft, welche unserer Produkte unter den Anwendungsbereich des CRA fallen. Stand heute gehen wir davon aus, dass alle unsere Produkte, die BUS- und IIoT-Protokolle sowie IO-Link nutzen, in den Geltungsbereich des CRA fallen. Dies betrifft einen großen Teil unserer vernetzten Komponenten, die Sie täglich in Ihren Anlagen und Maschinen einsetzen.

Balluff verpflichtet sich, die Anforderungen des CRA proaktiv und während des gesamten Produktlebenszyklus – von der Entwicklung bis zum Auslaufen – umzusetzen und einzuhalten. Unser Ziel ist es, alle CRA-konformen Produkte gemäß der bewährten Normenfamilie IEC 62443-4-1 zu gestalten. Dieser Ansatz stellt sicher, dass unsere Produkte nicht nur die CRA-Anforderungen erfüllen, sondern sich auch optimal in die Sicherheitskonzepte Ihrer Anlagen und Maschinenbauer integrieren lassen – für eine sinnvolle und praxisnahe Anwendung. So stellen wir die Umsetzung sicher:

Gezielte Projektarbeit:

Wir haben ein bereichsübergreifendes Projektteam gebildet, das die CRA-Anforderungen im Hinblick auf globale Prozesse, Methoden und Produkte sorgfältig analysiert und diese zeitnah umsetzt.

Sichere Entwicklungsprozesse:

Wir integrieren einen standardisierten Secure Product Development Lifecycle (SPDLC) in unseren bestehenden Produktentwicklungsprozess und stellen so sicher, dass Sicherheitsaspekte von Anfang an fest in der Produktentwicklung verankert sind.

2026 werden wir die Zertifizierung unserer Prozesse und Methoden gemäß der Norm IEC 62443-4-1 anstreben.

Integration von Sicherheitsprinzipien und Best Practices:

Wir übernehmen die Prinzipien und Standards der IEC62443-4-1 und IEC62443-4-2 in unsere Prozesse und Produkte und richten unseren Entwicklungsansatz eng an diesen aus, um unseren Kunden sichere und zuverlässige Lösungen zu bieten.

Koordiniertes Schwachstellenmanagement:

Um proaktiv auf potenzielle Sicherheitslücken reagieren zu können, richten wir ein zentrales, dediziertes Product Security Incident Response Team (PSIRT) ein und führen ein koordiniertes Schwachstellenmanagement in Zusammenarbeit mit CERT@VDE ein. Das gewährleistet die koordinierte Annahme, Analyse, Behebung und Offenlegung aller sicherheitsrelevanten Schwachstellen.

IT-Sicherheitszertifizierung:

Zur Unterstützung unserer internen Prozesse streben wir aktuell die Zertifizierung unserer IT-Sicherheitsmanagementprozesse nach IEC 27001 an, die die Informationssicherheit unserer Geschäftsprozesse und IT-Systeme adressiert. Damit unterstreichen wir unser Engagement für höchste Sicherheitsstandards in unseren internen Abläufen und Systemen.

Ihr Feedback ist uns wichtig!

Wir sind überzeugt, dass eine starke Produktsicherheit ein zentraler Bestandteil der Produktstrategie ist. Wir freuen uns auf den Dialog mit Ihnen. Wenn Sie Fragen zur CRA-Konformität oder zum Produktsicherheitsansatz von Balluff haben oder spezielle Anforderungen, bei denen wir Sie unterstützen können, wenden Sie sich bitte an Ihren Ansprechpartner für weitere Informationen oder einen Austausch.

Wir freuen uns auf Ihr Feedback und Ihre Anregungen!



i.A Heiko Mahr, Product Security Manager



i.V. Dr. Ingo Kleinschroth, CISO (acting)