

Information zu Cyber Resilience Act (CRA) und Maschinenverordnung (EU) 2023/1230

Stadtbergen, 01.07.2026

Sehr geehrte Damen und Herren,

derzeit erreichen uns vermehrt Anfragen im Zusammenhang mit der bevorstehenden verpflichtenden Umsetzung der Anforderungen aus der EU-Maschinenverordnung sowie dem Cyber Resilience Act (CRA), zu denen wir mit diesem Schreiben Stellung nehmen möchten.

Wir als Erhardt+Leimer GmbH sind uns der Bedeutung der angefragten Themen im Kontext des Cyber Resilience Act (CRA) sowie der Maschinenverordnung (EU) 2023/1230 bewusst und arbeiten daran, die jeweils relevanten Anforderungen innerhalb der vorgesehenen Fristen umzusetzen.

Als Lieferant von Komponenten und unvollständigen Maschinen richtet sich der Umfang der umzusetzenden Maßnahmen nach unserer Rolle innerhalb der Lieferkette sowie der bestimmungsgemäßen Verwendung unserer Produkte. Bestimmte Maßnahmen, insbesondere netzwerkseitige Schutzmechanismen wie Firewalls, liegen außerhalb unserer Systemgrenzen und sind im Rahmen der Gesamtintegration durch den Maschinenhersteller sowie im Betrieb durch den Betreiber sicherzustellen.

Unsere Produkte erfüllen bereits heute die wesentlichen Anforderungen des Stands der Technik im Bereich Cybersecurity und orientieren sich an den Vorgaben der IEC 62443-4-2. Beispielsweise verfügen Komponenten mit EL.NET-Technologie über rollenbasierte Zugriffskontrollen sowie Protokollierungsfunktionen. Diese Sicherheitsfunktionen werden sukzessive auf weitere Produktlinien ausgeweitet.

Da unsere Komponenten typischerweise nicht direkt mit öffentlichen Netzen verbunden werden, jedoch in vernetzten Umgebungen eingesetzt werden können, und die Entscheidung, wann Software ersetzt oder geändert wird, dem Betreiber oder dem Maschinenhersteller obliegt, werden wir sicherstellen, dass Firmware- und sicherheitsrelevante Updates künftig strukturiert über geeignete Portale zur Verfügung gestellt werden.

Ein Prozess zum Umgang mit Schwachstellen und Sicherheitsvorfällen wird etabliert und im Einklang mit den Anforderungen des CRA weiterentwickelt. Dies umfasst auch die fristgerechte Meldung an die zuständigen Behörden sowie die Information betroffener Kunden. Bei bekannten Schwachstellen oder Sicherheitsvorfällen treten wir – wie bereits heute praktiziert – proaktiv mit unseren relevanten Kunden in Kontakt.

Die Prinzipien Security-by-Design und Security-by-Default werden systematisch in unsere Entwicklungsprozesse integriert und aktuell unternehmensweit weiter ausgebaut.

Zukünftig werden Software-Stücklisten (SBOM) in strukturierter und geeigneter, perspektivisch auch in maschinenlesbarer Form bereitgestellt, um Transparenz über eingesetzte Softwarekomponenten sicherzustellen.

Bei unseren EL.NET-Komponenten kommen überwiegend selbst entwickelte sowie proprietäre Softwarelösungen zum Einsatz. Die jeweils installierten Versionen können bereits heute über das Web-Based Management (WBM) der Komponenten sowie über die dort generierbare Systemstückliste bzw. Ersatzteilliste eingesehen werden.

Wir hoffen, Ihnen mit den vorstehenden Informationen weitergeholfen zu haben. Da die Harmonisierung der einschlägigen Normen derzeit noch nicht abgeschlossen ist und sich die regulatorischen Anforderungen weiterhin in Entwicklung befinden, können wir zum aktuellen Zeitpunkt keine verbindlichen oder weitergehenden Detailauskünfte zu den genannten Themen geben. Unser Webauftritt der Erhardt+Leimer GmbH wird um den Bereich Security entsprechend erweitert werden, damit Sie in Zukunft die Möglichkeit haben dort alle relevanten Informationen zu diesem Thema zu erlangen.

Mit freundlichen Grüßen



Joachim Tatarczyk
Managing Director | Group COO

Erhardt+Leimer GmbH