

CRA-Meldepflicht: Warum Unternehmen jetzt unter Handlungsdruck stehen



Seit dem 11. September 2026 gilt die Meldepflicht des Cyber Resilience Act. Wer diese Ausgabe zur SPS 2026 in Nürnberg in der Hand hält, trägt das Risiko nicht erst ab heute, sondern bereits seit dem Spätsommer. IT-Sicherheit für Komponenten in der Produktionsautomatisierung ist längst zur handfesten Einkaufsfrage geworden. Was Beschaffung, Konstruktion und Qualitätssicherung jetzt nachholen müssen.

Der Cyber Resilience Act wirkt längst in der Praxis

Messebesucher der SPS, sehen sich selten als „Einkauf“ im klassischen Sinn, sind es aber doch. Denn die Beschaffungsentscheidung fällt nicht erst im Lastenheft der kaufmännischen Einkaufsabteilung, sondern oft schon in diesen Messehallen von Konstrukteuren, Systemintegratoren und Automatisierungstechniker.



*Autor:
Michael Enslin
Experte für Software- und
Systems Engineering
ITQ GmbH
www.itq.de*

Genau hier setzt bereits der Cyber Resilience Act (CRA) an. Schon seit 2024 in Kraft, blieb er für viele im Maschinenbau eine abstrakte EU-Verordnung. Seit September gelten nun die ersten scharfen Pflichten. Bei aktiv ausgenutzten Sicherheitslücken oder Sicherheitsvorfälle, müssen Hersteller von „Produkten mit digitalen Elementen“ binnen 24 Stunden eine Erstmeldung auf der zentralen Meldeplattform ENISA abgeben, gefolgt von Nachmeldung und Abschlussbericht. Schwachstellen müssen künftig systematisch erkannt, bewertet und offengelegt werden, Dokumentationen auf Anfrage unverzüglich bereitstehen. Verstöße sind keine Lappalie und werden mit Bußgeldern bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes geahndet.

Wer ist betroffen?

Das betrifft jedoch längst nicht nur Software-Hersteller. Erfasst sind im CRA IoT-Geräte, Industrie-PCs, Robotik und Bildverarbeitung, Steuerungen, Sensorik mit Firmware, kurz: praktisch jede vernetzte Komponente, die heute in einer automatisierten Fertigungslinie verbaut wird. Damit sind nicht nur die offensichtlichen IT-Systeme betroffen, sondern auch Komponenten, die bislang eher als „klassische“ Automatisierungstechnik galten und deren digitale Bestandteile in der Beschaffung bisher kaum eigenständig bewertet wurden.

Sicherheit als Fundament für Industrial AI

Die Dringlichkeit dieses Themas trifft auf einen zweiten großen Trend der Branche: Auf der SPS 2026 in Nürnberg steht „Industrial AI“ und die Weiterentwicklungsmöglichkeiten durch Künstliche Intelligenz in Automatisierung, Antriebstechnik, Sensorik und Software im Mittelpunkt. Zentrale Fragen sind dabei, wie sich KI und Cyber

Security vereinbaren lassen. Eine Fertigung, die zunehmend auf KI-gestützte Entscheidungen setzt, von der vorausschauenden Wartung bis zur automatisierten Bildverarbeitung, braucht eine Basis aus vertrauenswürdiger, nachweisbar sicherer Hardware und Software. Security by Design ist damit keine Bremse für Innovation, sondern deren Voraussetzung. Wie viel Nachweisaufwand das im Einzelfall bedeutet, hängt jedoch vom Risiko der jeweiligen Komponente ab.

Nicht jede Komponente wiegt gleich schwer

Der CRA unterscheidet mehrere Risikoklassen, und gerade im Umfeld von Industrie-PCs lohnt sich der genaue Blick: Die meisten Steuerungen, Sensoren und Antriebe fallen in die Standardklasse, für die eine Selbstbewertung durch den Hersteller ausreicht. Netzwerkmanagement-Systeme, Router oder das Betriebssystem eines Industrie-PCs sowie VPN-Lösungen für die Fernwartung gehören bereits zur Klasse „Wichtig I“. Wer virtualisierte Steuerungsarchitekturen einsetzt, landet mit Firewalls, Intrusion-Detection-Systemen oder Hypervisoren sogar in Klasse „Wichtig II“. „Kritische“ Produkte mit digitalen Elementen sind unter anderem Hardwaregeräte mit Sicherheitsboxen, Smart-Meter-Gateways und Chipkarten. Für die Beschaffung heißt das: Je näher eine Komponente an Netzwerksicherheit und Virtualisierung liegt, desto höher der Prüfaufwand, der bereits beim Lieferanten beginnen muss.

Qualitätsanspruch auch für Software

Firmen würden nie eine Maschine ohne Sicherheitsprüfung in Betrieb nehmen. Beim Thema Software, die heute in jeder Komponente steckt, war diese Selbstverständlichkeit lange nicht da. Mit dem CRA verständigen sich die Unternehmen darauf, den gleichen Qualitätsanspruch, der aus dem klassischen Maschinenbau bekannt ist, konsequent auf Software und vernetzte Systeme zu übertragen.

Das ist kein zusätzlicher Aufwand um seiner selbst willen, sondern die Übertragung von etwas, das im Engineering längst bewährt ist.

Diese Übertragung ist der Kern der Herausforderung: Strukturen, die im mechanischen Anlagenbau seit Jahrzehnten selbstverständlich sind, wie Nachweispflichten, Freigabeprozesse, Lebenszyklusverantwortung, müssen jetzt für Software und vernetzte Komponenten mit derselben Konsequenz aufgebaut werden.

Nicht-EU-Lieferanten: Wenn der Einkauf zum Importeur wird

Ein Punkt, der in der Beschaffungspraxis oft übersehen wird: Der CRA gilt für jedes Produkt,

das auf dem EU-Markt in Verkehr gebracht wird, dabei ist der Sitz des Herstellers selbst irrelevant. Ein großer Teil der Industrie-PC-Hardware und eingebetteten Boards stammt aus Fertigungsstandorten außerhalb der EU. Wird eine solche Komponente direkt bei einem Hersteller außerhalb der EU eingekauft, kann das einkaufende Unternehmen dadurch selbst zum „Importeur“ im Sinne des CRA werden. Als Importeur muss es nach Art. 19 CRA lediglich prüfen, dass der Hersteller Konformitätsbewertung, technische Dokumentation, CE-Kennzeichnung und EU-Konformitätserklärung vorgelegt hat, erstellt werden diese weiterhin vom Hersteller. Zum vollwertigen Hersteller wird das Unternehmen erst, wenn es das Produkt unter eigener Marke vertreibt oder wesentlich verändert (Art. 21/22 CRA). „Wir kaufen nur ein“ schützt trotzdem nicht vor der Prüfpflicht: Ohne einen in der EU ansässigen Bevollmächtigten des Herstellers fällt die Verantwortung direkt dem Importeur zu.

Nicht nur eine Sache der IT. Der Einkauf spielt mit

Bislang war Produktsicherheit meist Sache der Entwicklung oder der IT-Abteilung. Seit dem 11. September 2026 gilt: Wer Komponenten beschafft, haftet als Teil der Lieferkette mit, dabei ist es irrelevant, ob als Hersteller einer Maschine, als Systemintegrator oder als Importeur von Zulieferteilen. Wer heute Antriebe, Steuerungen, Sensorik oder Industrie-PCs einkauft, ohne sich mit dem Lieferanten über Meldewege, Update-Fähigkeit und Dokumentationspflichten verständigt zu haben, kauft ein Risiko mit ein, das sich erst im Schadensfall zeigt.

Für die Beschaffung heißt das konkret: Sicherheitsnachweise, Schwachstellenmanagement und Update-Zusagen gehören ab jetzt so selbstverständlich in die Lieferantenbewertung wie technische Datenblätter oder Zertifikate. Wer das versäumt, schiebt das Risiko nicht weg, er übernimmt es unbemerkt!

Die regulatorische Verdichtung 2026/2027

Ab dem 20. Januar 2027 verankert die neue EU-Maschinenverordnung Cybersicherheit erstmals verbindlich als Teil der Maschinensicherheit mit Anforderungen an sichere Konnektivität und den Schutz sicherheitsrelevanter Hardware und Software vor Manipulation. Ab Dezember 2027 greifen die vollständigen CRA-Pflichten: CE-Kennzeichnung, eine Software Bill of Materials (SBOM) sowie Sicherheitsupdates über den Produktlebenszyklus.

In der Praxis bedeutet das: Safety und Security verschmelzen zu einer gemeinsamen Anforderung an jede Maschine und jede Komponente. Wer heute beschafft, entscheidet bereits über die Compliance-Fähigkeit von morgen.



Was der Einkauf konkret prüfen muss

Für die Beschaffung heißt Security by Design vor allem eines: Nachweisbarkeit einfordern, bevor der Auftrag erteilt wird. Folgende Fragen sollten gestellt werden:

- Kann der Lieferant eine SBOM liefern?
- Gibt es ein dokumentiertes Schwachstellenmanagement, an das ich mich im Ernstfall wenden kann?
- Und wie lange werden Sicherheitsupdates zugesagt?

Diese Fragen entscheiden heute über die Zukunftsfähigkeit einer Beschaffungsentscheidung.

Drei Punkte, die sich in jedem Lastenheft und jeder Lieferantenbewertung wiederfinden sollten:

- erstens die Fähigkeit des Lieferanten, Softwarebestandteile und Abhängigkeiten transparent zu dokumentieren;
- zweitens ein belastbarer, benannter Prozess für Meldung und Behebung von Schwachstellen;
- drittens eine vertraglich fixierte Zusage zur Update-Versorgung über die geplante Nutzungsdauer der Maschine hinweg.

Wer diese drei Punkte jetzt in Lieferantengespräche einbringt, holt den Rückstand aus dem September auf und verschafft sich zugleich einen Vorsprung, den die Verordnung ab 2027 ohnehin verbindlich einfordern werden.

Wer diese Nachweise noch nicht liefern kann, muss nicht bei null anfangen: Modulare, dokumentierte Systemarchitekturen lassen sich nachträglich aufbauen, Update- und Meldeprozesse können in bestehende Entwicklungsabläufe integriert werden. Anbieter wie die ITQ GmbH unterstützen dabei in drei Schritten: Selbstbewertung anhand einschlägiger Normen, Priorisierung der Verbesserungspotenziale und praktische Umsetzung der Änderungen.

Future Skills: Wer die Sicherheitsanforderungen von morgen umsetzt

CRA, NIS2 und die kommende Maschinenverordnung verlangen nicht nur neue Prozesse, sondern Ingenieure, die Security by Design von Anfang

an mitdenken. Genau hier setzt ein zweites ITQ-Engagement auf der SPS 2026 an, das auf den ersten Blick wenig mit Gesetzestexten zu tun hat, im Kern aber genau darauf einzahlt: der MAKEATHON. Für ITQ ist das keine Randaktivität, sondern gelebte Überzeugung: Digital Education ist eine von vier Kernkompetenzen des Unternehmens, das bereits seit 2016 MAKEATHONS veranstaltet – weil Vorschriften wie der CRA nur so gut wirken wie die Ingenieure, die sie später umsetzen. Wer Security by Design erst nach dem Studium lernt, lernt es zu spät für die Praxis.

Auf der SPS 2026 initiiert ITQ bereits zum zweiten Mal gemeinsam mit der Mesago Messe und New Automation einen MAKEATHON: Studierende bearbeiten in kurzer Zeit echte Industry Challenges und bauen erste Prototypen. Ein Besuch der MAKEATHON-Area zeigt, woher die Fachkräfte kommen, die SBOM, Schwachstellenmanagement und Update-Prozesse künftig in der Praxis umsetzen. Sicherheit und Nachwuchsförderung sind damit zwei Seiten derselben Zukunftsfähigkeit.

Was die Studierenden hier in wenigen Stunden als Prototyp bauen, müssen Unternehmen morgen als geprüften, dokumentierten Nachweis liefern – der MAKEATHON trainiert also genau die Kompetenz, die der CRA einfordert: Sicherheit von Anfang an mitzudenken, nicht nachträglich aufzusetzen.

Beides entscheidet darüber, ob Unternehmen die nächste Frist wieder erst im Rückspiegel erkennen oder sie diesmal aktiv gestalten.

Wer schreibt:

Michael Enslin ist Ingenieur mit Abschluss der Technischen Universität München und seit über 15 Jahren bei der ITQ GmbH tätig. In dieser Zeit hat er umfassende Erfahrung in Software- und System-Engineering-Projekten gesammelt und begleitet Lösungen entlang der gesamten Wertschöpfungskette, vom Sensor bis hin zur Cloud. Ein besonderer Schwerpunkt seiner Arbeit liegt im Bereich IT-Security. Er war mehrere Jahre in Fachgremien des DKE zu Sicherheitsstandards für die Industrie aktiv und bringt dieses Wissen gezielt in Kundenprojekte ein, in denen er Security-Lösungen konzipiert und umsetzt. ◀