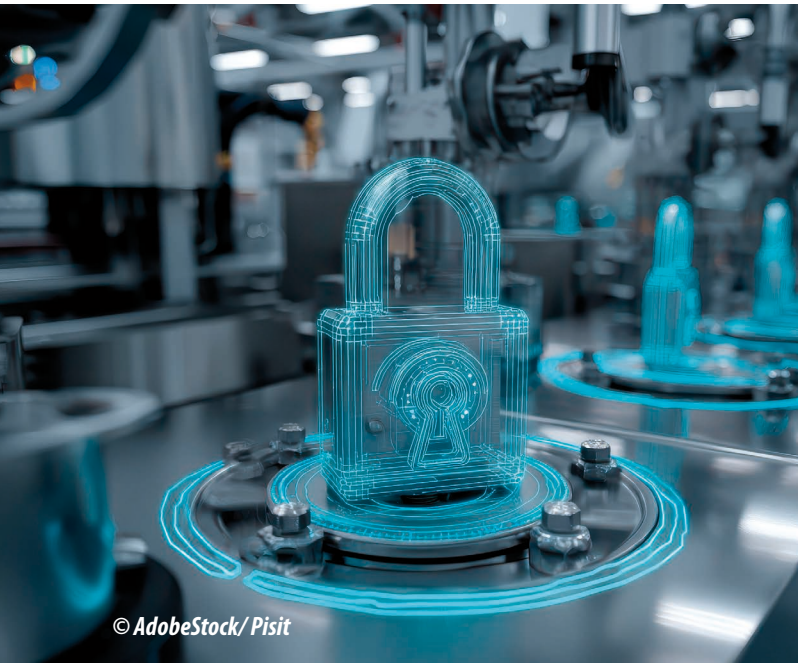


Sicherheits- und Compliance-Anforderungen erfüllen

Fünf Tipps zur Vorbereitung auf die neue EU-Maschinenverordnung



© AdobeStock/Pisit

Der Countdown läuft: Im Januar 2027 tritt die neue Maschinenverordnung (2023/1230/EU) der Europäischen Union (EU) in Kraft und ersetzt die Maschinenrichtlinie 2006/42/EG. Für Fertigungsunternehmen bedeutet das: Nur noch zwölf Monate Zeit, um sich auf verschärfte Anforderungen vorzubereiten – insbesondere beim Schutz vor Cyberangriffen.

Die Dringlichkeit ist real

Cyberattacken auf Produktionsanlagen können nicht nur teure Ausfallzeiten verursachen, sondern die Existenz ganzer Unternehmen gefährden. Die neue Verordnung reagiert auf diese Bedrohung und macht Cybersecurity zur Pflicht. Das bedeutet für Maschinenbauer: Sie müssen bereits bei der Konstruktion Schutzmaßnahmen einbauen. Industrieunternehmen wiederum müssen ihre Geräte sorgfältig bedienen und warten.

Doch wo anfangen? Die Automatisierungsexperten von Omron haben fünf praxisnahe Tipps zusammengestellt, mit denen sich Unternehmen jetzt optimal auf die neuen Anforderungen vorbereiten können.

1. Neue Vorschriften verstehen und strategisch umsetzen

Egal ob nun Maschinenbauer oder anwendendes Unternehmen: Wer die neuen Vorschriften gut umsetzen und einhalten möchte, muss sie zunächst einmal verstehen. Das übergeordnete Ziel der neuen Verordnung ist dabei dasselbe wie zuvor: Es geht um die Gewährleistung einer sicheren Konstruktion, Herstellung und Verwendung von Maschinen. Jetzt sollen aber auch Lücken in der ursprünglichen Richtlinie geschlossen werden, vor allem angesichts der Fortschritte in der digitalen Technologie und der Komplexität der modernen Fertigung. Die neue Verordnung beinhaltet neben einem strukturierteren Ansatz für Konformitätsbewertungen auch spezielle Regelungen zu Digitalisierung und Cybersicherheit. Ein fundiertes Verständnis dieser Bestimmungen ist essenziell.

2. Neue Standards frühzeitig einführen

Es gibt keine Übergangsfrist zwischen den beiden Rechtsvorschriften. Das bedeutet: Unternehmen müssen bis zum 20. Januar 2027 umfassende Konformität erreichen. Zu diesem Zeitpunkt müssen alle Maschinen auf dem EU-Markt so konstruiert sein, dass sie unbefugtem Zugriff oder Manipulationen standhalten, die sicherheitskritische Funktionen beeinträchtigen könnten. Dazu gehören Schutzmaßnahmen gegen böswillige Eingriffe über physische Verbindungen wie USB-Anschlüsse und digitale Kanäle wie vernetzte Systeme.

Die Verordnung schreibt außerdem ausdrücklich vor, dass sicherheitskritische KI-Systeme strengen Risikobewertungen und in vielen Fällen Konformitätsbewertungen durch Dritte unterzogen werden müssen, um die Einhaltung der Vorschriften zu überprüfen. Die Einrichtung und Erprobung von Prozessen und Protokollen zur Sicherstellung der Konformität kann einige Zeit in Anspruch nehmen. Je früher Unternehmen mit der Umsetzung der erforderlichen neuen Standards beginnen, desto einfacher wird der Übergang.

3. Vorhandene Maschinen und Systeme überprüfen

Der nächste Schritt besteht darin, alle vorhandenen Maschinen und Systeme hinsichtlich der neuen Standards zu überprüfen. Ein umfassendes Audit hilft festzustellen, welche Maschinen vernetzt sind, welche KI- oder adaptive Systeme enthalten und welche sicherheitskritischen Komponenten für Cyberangriffe anfällig sein könnten. Für Maschinenbauer kann das bedeuten, dass sie Konstruktionspläne, Softwarearchitektur und Netzwerkintegrationspunkte bewerten müssen. Für Endnutzer bedeutet es, dass sie überprüfen müssen, wie Maschinen tatsächlich in der Fertigung betrieben werden. Hierzu gehören auch alle

Ad-hoc-Modifikationen oder ältere Anschlüsse. Ziel ist es, Lücken zu erkennen, risikoreiche Systeme zu priorisieren und Upgrades oder zusätzliche Sicherheitsvorkehrungen rechtzeitig vor Ablauf der Frist im Januar 2027 zu planen.

4. Schulungen entwickeln und durchführen

Selbst die sichersten Maschinen sind nur so sicher wie die Menschen, die sie bedienen. Maschinenhersteller sollten deshalb klare Anleitungen und Dokumentationen zu Cybersicherheitsmaßnahmen bereitstellen. Endanwender wiederum müssen sicherstellen, dass Bediener, Wartungspersonal und Vorgesetzte umfassend in sicherer Nutzung, zuverlässigem Betrieb und der Reaktion auf Vorfälle geschult sind. Ein Hinweis: Die neue Verordnung erlaubt es Herstellern, Online-Benutzerhandbücher bereitzustellen. Das kann helfen, Umweltbelastung und Betriebskosten zu reduzieren. Um Regelkonformität zu gewährleisten, müssen digitale Ressourcen mindestens zehn Jahre nach Markteinführung eines Produkts zugänglich bleiben.

5. Auf verlässliche und erfahrene Partner setzen

Die Anforderungen der neuen Maschinenverordnung an die Cybersicherheit können komplex sein. Deshalb lohnt es sich, mit erfahrenen Lieferanten und Integratoren zusammenzuarbeiten, um so den Übergang zu erleichtern. Unternehmen mit einer nachgewiesenen Erfolgsbilanz in Bereichen wie sicheres Design, Automatisierung und Compliance bieten umfassende Lösungen für die industrielle Automatisierung, die von Grund auf bewährte Verfahren für Cybersicherheit integrieren. Die Kooperation mit vertrauenswürdigen Partnern wie Omron verhilft zu sicheren und regelkonformen Maschinen, die sich gegen neue Cyberbedrohungen behaupten können. ◀

OMRON

<https://industrial.omron.de/de/home>