Cybersicherheit in der neuen EU-Maschinenverordnung

Das müssen Hersteller und Betreiber beachten

© TheDigitalArtist/pixabay

Im vergangenen Sommer ist die neue EU-Maschinenverordnung in Kraft getreten. Zwar bleibt den Unternehmen bis Anfang 2027 Zeit, um die neuen Vorgaben anzuwenden, doch sollten sie mit der Umsetzung nicht allzu lange warten. Denn neuerdings sind auch auf dem Gebiet der Cybersecurity umfangreiche Maßnahmen zu ergreifen.

Relevanz der Cybersicherheit steigt

Cybersicherheit ist nicht nur in traditionellen Industriezweigen von großer Bedeutung, sondern gewinnt auch in der Elektronikbranche zunehmend an Relevanz. Die erstmalige Integration von Cybersicherheitsmaßnahmen in die neue EU-Maschinenverordnung EU) Nr. 2023/1230 reflektiert die wachsende Vernetzung elektronischer Geräte und unterstreicht die Notwendigkeit, robuste Schutzmechanismen zu implementieren.

In Anbetracht der steigenden Bedrohungen im digitalen Raum ist es entscheidend, dass Hersteller und Betreiber der Elektronikindustrie proaktiv handeln, um die Sicherheit ihrer Produkte und Systeme zu gewährleisten.

Autor:
Stefan Fleckenstein
Head of Cybersecurity
MaibornWolff
www.maibornwolff.de

Anspruchsvolle Vorgaben

Die neuen Vorgaben müssen Unternehmen künftig umsetzen, um auch weiterhin das CE-Kennzeichen zu erhalten. Im Unterschied zur alten Maschinenrichtlinie 2006/42/EG gilt die Verordnung für alle EU-Länder und muss nicht erst in nationale Gesetze gegossen werden. Obgleich sie erst ab dem 20. Januar 2027 anzuwenden ist, stellt die neue EU-Maschinenverordnung im Bereich der Cybersecurity anspruchsvolle Vorgaben, auf die sich die Unternehmen mit einem Bündel an unterschiedlichen Maßnahmen frühzeitig vorbereiten sollten.

Hersteller in der Bringschuld

Die neue EU-Verordnung nimmt vor allem die Hersteller in die Pflicht. Sie sind künftig dazu angehalten, die notwendigen Vorkehrungen zu treffen, um ihre Maschinen wirksam gegen Cyber-Angriffe zu sichern. Doch bedeutet dies nicht, dass damit die anderen Akteure aus der Verantwortung entlassen wären – insbesondere die Anwender werden zu einer gewissenhaften Nutzung angehalten.

Die Neuerungen im Detail

Schutz gegen Korrumpierung und größere Steuerungssicherheit: Die neuen Vorgaben zur Cybersecurity finden sich größtenteils in Anhang III der Verordnung. Relevant sind hier vor allem folgende Aspekte:

- „**Schutz gegen Korrumpierung**“ (Protection against corruption) (Artikel 1.1.9)
  Die Maschine muss so gebaut sein, dass ihre Verknüpfung mit anderen Geräten oder dem Internet zu keiner „gefährlichen Situation“ führt, wie es in der Verordnung heißt. Software und Daten, die dem sicheren Betrieb der Maschine dienen, müssen zudem benannt und geschützt werden. Schließlich sind auch alle (rechtmäßigen wie unrechtmäßigen) Eingriffe in sicherheitsrelevante Software zu dokumentieren.

- „**Sicherheit und Zuverlässigkeit von Steuerungen**“ (Artikel 1.2.1)
  Auch für die Sicherung der Maschinensteuerung haben die Hersteller Sorge zu tragen. So dürfen weder im Falle von Hacker-Angriffen, noch bei versehentlichen Anwenderfehlern Gefährdungssituationen entstehen. Die Grenzen der Sicherheitsfunktionen von Maschinen müssen überdies vorab genau abgesteckt werden und vor nachträglichen Veränderungen geschützt sein. Dies gilt ausdrücklich auch für selbstlernende, d. h. KI-basierte Systeme. Die Verordnung sieht außerdem vor, dass Rückverfolgungsprotokolle zu absichtlichen oder unabsichtlichen Eingriffen bis zu fünf Jahre lang gespeichert werden und zugänglich sein müssen.


© NoName/pixabay

Vorgaben zu After-Sales-Pflichten und KI-Systemen

Doch hat die neue EU-Maschinenverordnung nicht nur Auswirkungen auf Herstellung und Risikoanalyse – auch Nachmarktpflichten finden sich explizit aufgeführt. Sollten Maschinen nicht mehr verordnungskonform sein, ist der Hersteller unverzüglich dazu aufgefordert, Korrekturmaßnahmen zu ergreifen oder aber Rückrufaktionen einzuleiten bzw. das Produkt vom Markt zu nehmen. Auch die zuständigen nationalen Behörden sind in einem entsprechenden Fall zu unterrichten.

KI-Systeme

Eine wichtige Neuerung betrifft zudem Maschinen, die über Systeme mit sog. „**selbstentwickelndem Verhalten**“ (sprich: KI-Systeme) verfügen. Sie werden künftig zu den Hochrisikomaschinen gerechnet, was das Konformitätsbewertungsverfahren deutlich aufwendiger werden lässt. So werden die Hersteller gemäß der neuen EU-Verordnung eine Baumusterprüfung oder ein umfassendes Qualitätssicherungssystem vorzuweisen haben, um die Konformität von Maschinen mit KI-Software garantieren zu können.

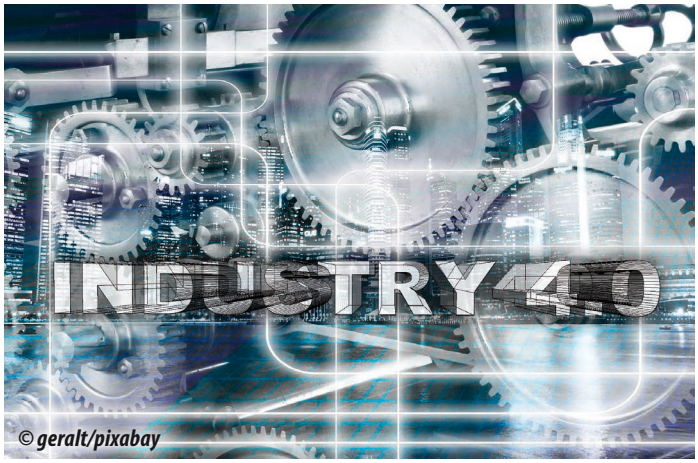
Welche Maßnahmen können Hersteller ergreifen?

Letztlich bleibt es den Herstellern überlassen, welche konkreten Maßnahmen zu ergreifen sind, um den Anforderungen der neuen

EU-Verordnung Genüge zu leisten. Als Leitfaden kann jedoch die internationale Normenreihe IEC 62443 dienen, die sich mit der IT-Sicherheit von „Industrial Automation and Control Systems“ befasst. Hervorzuheben sind hier im Besonderen die Dokumente IEC 62443 4-1 (Secure product development lifecycle requirements) sowie 62443 4-2 (Technical security requirements for IACS components): Sie behandeln ausführlich, welche Aspekte im Hinblick auf einen sicheren Software-Entwicklungsprozess zu beachten sind.

Bedrohungsmodellierung

Ratsam erscheint zuvorderst eine Bedrohungsmodellierung, durch die sich aufklären lässt, auf welchen unterschiedlichen Wegen (etwa über das Bedienterminal, USB-Zugänge oder das Netzwerk) die Maschine angegriffen werden kann.



© geralt/pixabay

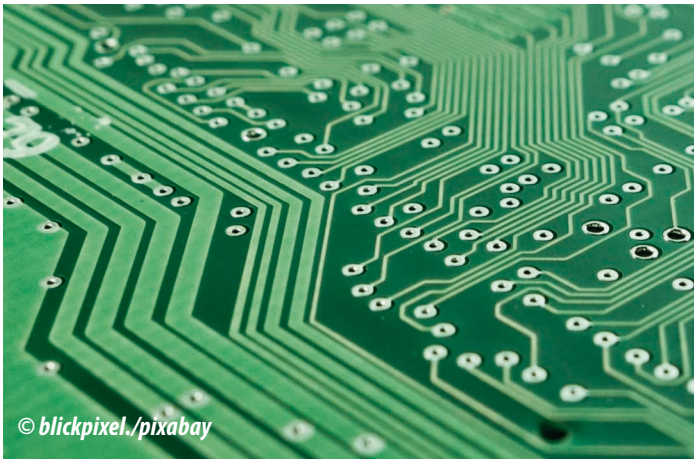
Auf Grundlage eines solchen Modells lässt sich in einem nächsten Schritt eine individuelle Risikobewertung vornehmen. Auf diese Weise ist sichergestellt, dass ein passgenauer und zielorientierter Maßnahmenplan ausgearbeitet werden kann.

Maßnahmen

Folgende Maßnahmen sollten in Betracht gezogen werden:

- eine **starke Verschlüsselung** sämtlicher Netzwerkverbindungen zur Maschine. Dafür sollten Hersteller stets auf die Anwendung der aktuellsten Logarithmen und Parameter achten.
- Einführung eines **Identitäts- und Zugangsmanagements**, das sicherstellt, dass die Anmeldung ausschließlich berechtigten Personen gestattet ist. Die Sicherheitsparameter müssen zudem so festgelegt sein, dass der Aktionsraum des Benutzers klar umrissen ist. Ein solches Least-Privilege-Prinzip sollte nicht nur für Anwender, sondern auch für die Verbindung mit anderen Maschinen oder Systemen gelten.
- eine minutiöse **Protokollierung sämtlicher Anmelde- und Abmeldevorgänge** durch das installierte Software-Programm. Darüber hinaus müssen alle Modifizierungen der Software protokolliert werden – ganz gleich, ob sie autorisiert (etwa in Form von Updates) oder unautorisiert (schlimmstenfalls durch Hacker-Angriffe) vorgenommen wurden. Die Speicherung der Daten sollte direkt auf der Maschine oder auf einem zentralen Server erfolgen. Auch die Bereitstellung dieser Dokumentation für Prüfstellen oder Behörden ist vom Hersteller jederzeit zu garantieren.


© geralt/pixabay


© blickpixel./pixabay

- ein **Vulnerability-Management** für alle installierten Software-Programme, im Zuge dessen fortlaufend mögliche Schwachpunkte (schwach geschützte Zugangscodes, riskante Netzwerkverbindungen etc.) identifiziert werden. Aufgrund der neu hinzukommenden After-Sales-Verpflichtungen sollten Hersteller auch logistisch darauf vorbereitet sein, Defizite und Mängel rasch beseitigen zu können.

Erforderliche Maßnahmen angehen

Unternehmen in der Elektronikbranche sollten nicht zögern, sich auf die Anwendung der neuen EU-Maschinenverordnung vorzubereiten. Die Aspekte der Cybersicherheit erfordern eine frühzeitige Auseinandersetzung, da die zunehmende Vernetzung elektronischer Geräte neue Herausforderungen mit sich bringt. Nur durch eine enge Zusammenarbeit zwischen Herstellern und Betreibern kann die effektive Bekämpfung von Cyberkriminalität gelingen.

Fazit

Auch wenn einige Formulierungen in der neuen EU-Maschinenverordnung unter Umständen Raum für Diskussionen lassen, weisen die Vorgaben zur Cybersecurity in die richtige Richtung.

Die Verordnung reagiert auf ein Problem, das die Unternehmen in den kommenden Jahren immer stärker beschäftigen wird, und nimmt Hersteller, aber auch Betreiber im Kampf gegen Cyberkriminalität in die Pflicht. Zumal auf Hersteller-Seite nun möglichst frühzeitig Vorkehrungen getroffen werden müssen: Diese reichen von einer umsichtigen Risikoanalyse aufgrund von Bedrohungsmodellierungen über verlässliche Verschlüsselungsverfahren und Identitätsprüfungen bis hin zu einem fortlaufenden Vulnerability-Management, das immer auch die Anwender in die Sicherheitsmaßnahmen einbindet.

Klar ist: Nur im Schulterschluss von Herstellern und Betreibern wird die Bekämpfung von Cyberkriminalität gelingen. Die Komplexität dieser Aufgabe erfordert ein planvolles Handeln, auch wenn die Verordnung erst Anfang 2027 verbindlich anzuwenden ist.

Wer schreibt:

Nach langjähriger Tätigkeit in der Softwareentwicklung übernahm Stefan Fleckenstein von 2010 bis 2020 als CIO die Verantwortung für die interne IT-Infrastruktur und Softwareentwicklung von MaibornWolff, zusätzlich zu seiner Arbeit in Kundenprojekten. Die Informationssicherheit wurde in dieser Zeit zu einem der Schwerpunkte seiner Arbeit, in der er MaibornWolff zur ISO 27001-Zertifizierung führte. ◄