Stay Ahead. Stay Secure.

STÖBER Security.

Worum geht es?

Die wachsende Bedrohung aus dem Cyber-Raum und die zunehmende Digitalisierung von Produktionsanlagen machen Security zu einem maßgeblichen Thema in der Antriebstechnik. Auch ein Thema für die EU – im Einklang mit deren Cyber-Strategie werden für den Maschinen- und Anlagenbau in naher Zukunft nachfolgende Richtlinien gelten.

EU-Richtlinie NIS 2.

Die NIS (Netz- und Informationssicherheit) wurde bereits 2016 zur allgemeinen Stärkung der Cyber-Sicherheit verabschiedet. Der Nachfolger NIS 2 gilt seit Anfang 2023. Ursprünglich nicht die Antriebstechnik als Branche betreffend, müssen mit NIS 2 jetzt auch Unternehmen im Maschinen- und Anlagenbau nachweisen, dass sie Maßnahmen zum Schutz vor Security-Vorfällen ergreifen. Dazu gehört zunächst die Risikoanalyse von bestehenden Systemen auch in Produktionsumgebungen.

Neue Maschinenverordnung (EU) 2023/1230.

Das Thema „Security“ wird durch die neue Maschinenverordnung (EU) 2023/1230 zur Herstellerpflicht. Sie ersetzt die bisherige Maschinenrichtlinie und trat am 19. Juli 2023 in Kraft. Zwar haben Maschinenhersteller 42 Monate für die Umsetzung Zeit, jedoch müssen die neuen Anforderungen an die Security bis 2024 vollständig erfüllt werden. Das bedeutet, Hersteller müssen zukünftig sicherstellen, dass die Sicherheitsfunktionen einer Maschine in keiner Weise, weder unbeabsichtigt noch vorsätzlich beeinträchtigt werden.

Cyber Resilience Act.

Die Europäische Kommission hat im September 2022 den Entwurf eines Cyber Resilience Acts (CRA) vorgelegt. Ziel ist, die Cyber-Sicherheit von Produkten, die miteinander oder mit dem Internet verbunden werden können, entscheidend zu verbessern.

Hauptziele dieser Verordnung.

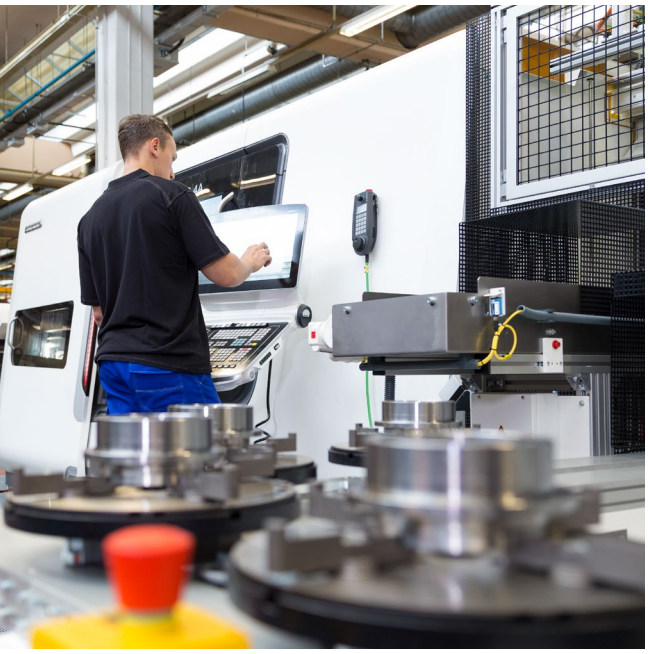
- Produkte mit digitalen Bestandteilen, die auf den EU-Markt gebracht werden, sollen weniger Schwachstellen aufweisen.
- Hersteller sind für die Cyber-Security Ihrer Produkte während eines definierten Zeitraums verantwortlich, und …
- … sie verpflichten sich, Sicherheitslücken während des gesamten Produktlebenszyklus zu schließen.
- Mehr Transparenz über die Sicherheit von Hard- und Softwareprodukten.
- Eine höhere Sicherheit für Nutzer.

Hersteller und Entwickler sind nun gefordert, die hohen Anforderungen des CRA umzusetzen. Denn Produkte, die den Vorschriften nicht entsprechen, dürfen ab 2026 nicht mehr in den Markt eingeführt werden.
Und genau damit wird die Security zu einem essentiellen Bestandteil für deren Verkauf in der EU.

Warum ist das so wichtig?

Je digitaler die Fertigung, desto größer die Gefahr von Cyber-Angriffen. Diese können zu Spionage sowie zur Sabotage führen. Eine einzige Lücke im System reicht da schon aus. Und je länger die Produktion lahmliegt, umso dramatischer sind die wirtschaftlichen Defizite: zum einen finanziell durch verpasste Einnahmen, zum anderen schädigt dies das Vertrauen der Kunden und den Ruf des Unternehmens.

Weitere, sehr schwerwiegende Folgen von Cyber-Angriffen können Personenschäden sein. Gerade dann, wenn die Safety, d. h. die funktionale Sicherheit, die dafür verantwortlich ist, Schaden an Menschen und Sachen zu verhindern, manipuliert wird.



Sicherheit auf operativer Ebene.

Während kontinuierliche Maßnahmen für die Cyber-Security auf IT-Ebene selbstverständlich sind, wird die Operational-Technology (OT)-Ebene meist vernachlässigt. Dabei sind Anlagen keine abgeschlossenen Einheiten und gerade mit der zunehmenden Digitalisierung öffnen sie sich für Datenströme und Fernzugriffe – und damit auch für Hacker.

Unsere Security-Strategie basiert auf dem internationalen Standard IEC 62443, der Security-Norm für industrielle Automatisierungssysteme.

Sie beinhaltet

- Richtlinien und Best Practices für die Sicherheit Ihrer Informations- und Steuerungssysteme in industriellen Umgebungen.
- Konkrete Maßnahmen, um Zugriffe zu kontrollieren und Netzwerke zu schützen.

Die sicherheitsgerechte Auslegung von Prozessen, beispielsweise, dass zwischen dem Versand von Produkten und der Ankunft beim Kunden kein Unbefugter Produkte manipulieren kann.

STÖBER Antriebstechnik GmbH + Co. KG
Kieselbronner Straße 12
75177 Pforzheim
Tel. +49 7231 582-0
mail@stoeber.de
www.stober.com