ISSN-Nr. 1612-1848

01 | 2025 | 35. Ausgabe

FTS/AMR FACTS

Fachmagazin für autonomen Transport

www.home-of-intralogistics.de

Cybersecurity für mobile Roboter

Auch in unserer Welt der mobilen Robotik holt uns das Thema Cybersecurity ein. In der heutigen Logistikbranche gewinnen mobile Roboter und Fahrerlose Transportsysteme zunehmend an Bedeutung. Diese Technologien revolutionieren die Art und Weise, wie Waren bewegt und verwaltet werden. Doch mit der zunehmenden Vernetzung und Automatisierung steigt auch das Risiko von Cyberangriffen. Daher ist es unerlässlich, Cybersecurity in den Entwicklungs- und Betriebsprozess mobiler Roboter zu integrieren.

Unterschiede zwischen IT und OT

Ein grundlegendes Verständnis der Unterschiede zwischen Informationstechnologie (IT) und Betriebstechnologie (OT) ist entscheidend, um die Bedeutung der Cybersecurity für unsere Branche zu verstehen: Während IT-Systeme in der Regel eine Nutzungsdauer von drei bis fünf Jahren haben und relativ gut standardisiert sind, zeichnen sich OT-Systeme durch eine längere Lebensdauer von 15 bis 20 Jahren und eine Vielzahl von unterschiedlichen Komponenten aus. Dies ist z.B. ein Unterschied, welcher spezifische Ansätze zur Cybersecurity notwendig macht.

Herausforderungen in der Cybersecurity

Die Kommunikation in OT-Systemen erfolgt zyklisch und in Echtzeit. Verzögerungen von wenigen Millisekunden in der Kommunikation zwischen einzelnen OT-Komponenten können bereits einen Produktionsstillstand verursachen.

Updates in OT-Umgebungen kommen in der Regel nicht so häufig zum Einsatz, wie in regulären IT-Systemen, werden aber dafür umso komplexer in der Durchführung. Es existieren keine Test-Umgebungen im OT-Umfeld, daher muss der Patch direkt in der produktiven Umgebung eingespielt werden. Während in der IT bereits umfassende Erfahrungen mit Cybersecurity aus den letzten Jahren bestehen, ist das Bewusstsein und die Expertise in der Maschinenwelt noch begrenzt.

Um die Cybersecurity für mobile Roboter effektiv zu gestalten, sind Experten erforderlich, die sowohl über Fachwissen im Bereich der Cybersecurity als auch über Erfahrung in der Automatisierungstechnik verfügen. Diese Fachkräfte sind derzeit rar, und Unternehmen müssen oft eigene Schulungsprogramme entwickeln, um die erforderlichen Kompetenzen intern aufzubauen.

Aus heutiger Sicht sind es drei europäische Verordnungen, mit denen wir es diesbezüglich zu tun haben (werden):

1. Richtlinie über Sicherheitsanforderungen für Netz- und Informationssysteme (NIS-2)

Ziel und Anwendungsbereich: NIS-2 ist eine EU-Richtlinie, die darauf abzielt, die Cybersicherheit in der EU zu verbessern, insbesondere für Organisationen, die kritische Infrastrukturen betreiben. Sie umfasst auch Unternehmen, die eine bedeutende Rolle in der digitalen Wirtschaft spielen.

Wichtige Punkte:

- Kritische Infrastruktur: NIS-2 richtet sich an Organisationen mit einem Jahresumsatz von mindestens 10 Millionen Euro oder 50 Mitarbeitern, sowie an besonders wichtige Organisationen mit einem Umsatz von 50 Millionen Euro oder 250 Mitarbeitern.
- Sicherheitsanforderungen: Die Richtlinie legt spezifische Sicherheitsanforderungen fest, die Unternehmen erfüllen müssen, um ihre Netz- und Informationssysteme zu schützen, bezogen auf alle Prozesse im Unternehmen.
- Berichtspflichten: Unternehmen sind verpflichtet, Sicherheitsvorfälle zu melden und entsprechende Maßnahmen zur Risikominderung zu ergreifen.

2. Maschinenverordnung (MVO)

Ziel und Anwendungsbereich: Die Maschinenverordnung regelt die Sicherheit und den Gesundheitsschutz von Maschinen in der EU. Sie muss ab dem 20. Januar 2027 angewendet werden. Sie legt Anforderungen fest, die sicherstellen sollen, dass Maschinen sicher betrieben werden können.

Wichtige Punkte:

- Sicherheits- und Gesundheitsschutzanforderungen: Die Verordnung enthält spezifische Anforderungen zum Schutz von Personen, Haustieren, Sachen und der Umwelt.

Die drei EU-Verordnungen ergänzen sich.

- Cybersicherheitsanforderungen: Diese Anforderungen sind im Zusammenhang mit den Sicherheits- und Gesundheitsschutzanforderungen zu betrachten. Sie betreffen insbesondere die Steuerungen von Maschinen und deren Widerstandsfähigkeit gegen böswillige Angriffe.
- Protokollierung: Es gibt Anforderungen zur Protokollierung von sicherheitsrelevanten Eingriffen über einen Zeitraum von fünf Jahren.

3. Cyber Resilience Act (CRA)

Ziel und Anwendungsbereich: Der Cyber Resilience Act ist eine neue EU-Verordnung, die darauf abzielt, die Cybersicherheit von vernetzten Produkten zu verbessern. Ab dem 11. Dezember 2027 müssen alle Anforderungen der Verordnung eingehalten werden. Bereits ab dem 11. September 2026 sind Hersteller von vernetzten Produkten verpflichtet Schwachstellen und Sicherheitsvorfälle zu melden.

Wichtige Punkte:
- Sicherheitsanforderungen für Produkte: Der CRA legt spezifische Sicherheitsanforderungen für Produkte mit digitalen Elementen fest, um sicherzustellen, dass diese Produkte von Anfang an sicher gestaltet sind.
- Der CRA betrifft praktisch alle Produkte, die in irgendeiner Form mit anderen Geräten oder Netzwerken kommunizieren können. Dies schließt auch Produkte ein, die Datenfernverarbeitung nutzen, etwa durch Cloud-Backends.
- Marktzugang: Produkte, die nicht den Anforderungen des CRA entsprechen, dürfen nicht auf dem EU-Markt angeboten werden.
- Verantwortlichkeiten der Hersteller: Hersteller sind verpflichtet, kostenlose Sicherheitsupdates bereitzustellen und Sicherheitsvorfälle zu melden.

Im Folgenden wollen wir kurz die Gemeinsamkeiten und Unterschiede dieser drei Verordnungen aufzeigen.

Gemeinsamkeiten:

- Ziel der Verbesserung der Cybersicherheit: Alle drei Regelungen zielen darauf ab, die Cybersicherheit zu erhöhen und Organisationen zu schützen, die kritische Infrastrukturen oder Produkte mit digitalen Elementen betreiben.
- Regulierungsrahmen: Sie schaffen einen rechtlichen Rahmen, der Unternehmen verpflichtet, Sicherheitsmaßnahmen zu implementieren und Vorfälle zu melden.
- Fokus auf Risikominderung: Alle drei Regelungen betonen die Notwendigkeit, Risiken zu identifizieren und geeignete Maßnahmen zur Risikominderung zu ergreifen.

In jeder Ausgabe macht sich Dr.-Ing. Günter Ullrich seine „Mobilen Gedanken".

Unterschiede:

- Anwendungsbereich: NIS-2 konzentriert sich auf die Informationssicherheit in den Unternehmensprozessen, während die Maschinenverordnung spezifisch für Maschinen und deren Sicherheit definiert ist. Der CRA hingegen bezieht sich auf vernetzte Produkte. Security-Grundwerte: Während die Anforderungen aus NIS-2 und CRA auf Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität abzielen, liegt der Schwerpunkt der MVO auf Safety im Sinne des Personenschutzes.
- Zeitliche Aspekte: Die MVO muss ab dem 20. Januar 2027 angewendet werden, während der CRA ab dem 11. Dezember 2027 vollständig umgesetzt werden muss. Die NIS-2 Richtlinie muss in nationales Recht umgewandelt werden, was noch nicht in allen EU-Ländern, einschließlich Deutschland, geschehen ist. Derzeit wäre daher die EU-Richtlinie direkt anwendbar in den EU-Staaten, die noch kein nationales Gesetz verabschiedet haben.
- Sicherheitsanforderungen: Während NIS-2 und der CRA spezifische Anforderungen an die Cybersicherheit stellen, legt die Maschinenverordnung einen stärkeren Fokus auf den physischen Schutz von Personen und der Umwelt in Verbindung mit Cybersicherheitsanforderungen.

Diese Unterschiede und Gemeinsamkeiten verdeutlichen, dass es wichtig ist, die jeweiligen Anforderungen und Zielsetzungen der verschiedenen Regelungen zu verstehen, um die Cybersicherheit in der modernen Industrie und Logistik effektiv zu gewährleisten.

Zusammenfassung

Die Integration von Cybersecurity in die Entwicklung und den Betrieb mobiler Roboter ist nicht nur eine technische Herausforderung, sondern auch eine strategische Notwendigkeit. Cybersicherheit gibt es schon lange in der IT, aber bisher wurde noch kaum in der Maschinenwelt über das Thema Cybersicherheit gesprochen.

Die best practices und Arbeitsweisen der klassischen IT kann in der Maschinenwelt zum aktuellen Zeitpunkt nur bedingt funktionieren. OT-Cybersecurity-Experten benötigen neben Fachwissen im Bereich der Cybersecurity zwingend Erfahrung im Bereich der

Automatisierungstechnik. Diese Leute gibt es nicht. Diese muss man sich selbst ausbilden.

HINWEIS: Die Cybersecurity ist ein Schwerpunktthema auf dem Anwenderforum „Mobile Robotik" auf der LogiMAT 2025. Kostenlose kompetente und neutrale Beratung erfolgt durch Fachexperten auf der Messe.

Autoren:
Dr.-Ing. Günter Ullrich,
Leiter VDI Fachausschuss FTS und Forum-FTS,
M.C.Sc. Peter Stoiber,
Senior Consultant im Forum-FTS,
M.Sc. Regina Stoiber, Geschäftsführerin
Datenbeschützerin GmbH, Regen

INFO

Bilder: Forum-FTS

www.forum-fts.com/community-2/anwenderforum

Mitautor Peter Stoiber ist Senior Consultant im Forum-FTS.

Mitautorin Regina Stoiber ist Geschäftsführerin der Datenbeschützerin GmbH.