AMKmotion

MEMBER OF THE ARBURG FAMILY

# Cyber-Security bei AMKmotion

Vorgaben. Zuständigkeiten. Unsere Lösungen.



# 01 Einführung Cyber Resilience Act (CRA)

# 01 Cyber Resilience Act

- CRA ist die erste europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind.
- Ziel ist es, die Cybersicherheit innerhalb der Europäischen Union zu erhöhen.
- Die neuen Vorschriften gelten in allen EU-Mitgliedsstatten.
- Die Umsetzung erfolgt in verschiedenen Etappen bis Ende 2027.



# 02 Warum Cyber-Security?

- **Mehr Vernetzung = mehr Risiko**
  - Maschinen und Produktionsanlagen sind heute eng mit IT- und OT-Systemen* verbunden
  - Technologien wie Ethernet, Remote-Zugriff und digitale Services sind Standard
  - → Dadurch entstehen neue Angriffsflächen für Cyberangriffe
- **Mögliche Folgen von Angriffen**
  - Maschinenstillstände & Produktionsausfälle
  - Datenverlust & Verlust von Know-how
  - Angriffe können sicherheitsrelevante Funktionen von Maschinen direkt beeinflussen.
- **Cyber-Security ist die Grundlage für**
  - Funktionale Sicherheit & Vertraulichkeit
  - Verfügbarkeit & Zuverlässigkeit
  - Wettbewerbsfähigkeit

*IT = Information Technology
OT = Operation Technology

# 03 Relevanz für Maschinenbauer und Betreiber

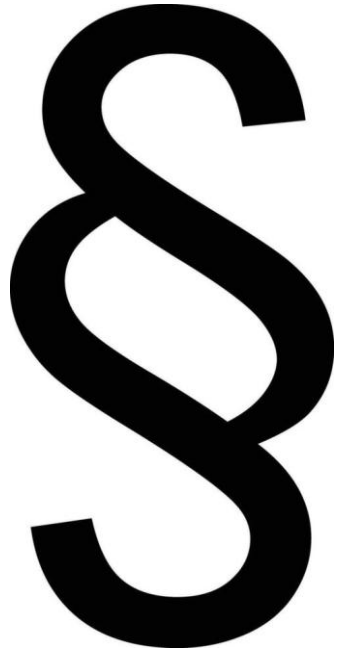
- **Cyber-Security wird Produktanforderung**
  - Relevanz für Maschinen, Steuerungen und Antriebssysteme
- **Betrifft den gesamten Lebenszyklus**
  - Entwicklung → Inbetriebnahme → Service → Retrofit
- **Verantwortung liegt in mehreren Bereichen**
  - Nicht nur IT betroffen
  - Auch Maschinenbau & Automatisierung in der Pflicht
- **Direkte Auswirkungen bei Sicherheitsvorfällen**
  - Sicherheit der Bediener
  - Produktion & Lieferfähigkeit
  - Betriebssicherheit
  - Reputation & Haftung



# 04 Regulatorischer Rahmen für Cyber-Security

- **Cyber-Security wird zur Pflicht**

- **Wichtige Rahmenwerke im Überblick**
  - **IEC 62443**
    → Stand der Technik für industrielle Systeme
  - **NIS-2**
    → Anforderungen an Organisation, Betrieb & Umgang mit Sicherheitsvorfällen (Incident Handling)
  - **Cyber Resilience Act (CRA)**
    → Anforderungen an Produkte mit Software und Schnittstellen sowie deren Hersteller



# 02 Aufgaben und Verantwortlichkeiten

# 05 Verantwortung der Hersteller

- **CE-Kennzeichnung – als rechtlicher Anker**
  - CE-Kennzeichnung nur zulässig, wenn alle CE-relevanten EU-Vorschriften erfüllt sind
  - Hersteller bestätigt die Konformität eigenverantwortlich

- **CE-relevante Richtlinien & Verordnungen**
  - Maschinenrichtlinien/Maschinenverordnung
  - Niederspannungs- & EMV-Richtlinie
  - Weitere produktspezifische Vorgaben
  - **Neu: Cyber Resilience Act (CRA)**

- **Risiken bei falscher Kennzeichnung**
  - Ordnungswidrigkeit oder Straftat
  - Maßnahmen der Marktüberwachung
  - Bußgelder & Haftungsrisiken

- **Was ändert sich durch CRA**
  - Cyber-Security wird **Teil der CE-Konformität**
  - Gilt für alle Produkte mit digitalen Elementen
  - Hersteller tragen Verantwortung über den **gesamten Produktlebenszyklus**

# 06 Cyber-Security in Antriebssystemen – Verantwortlichkeiten

## Sicherheit entsteht im Zusammenspiel

### AMKmotion (Komponentenebene)

- **Physischer Schutz**
  - Abgedeckte Serviceschnittstellen
  - Zentrale Geräte im Schaltschrank geschützt
- **Sichere Kommunikation**
  - EtherCAT mit Single-Master-Prinzip
  - Kontrollierter Datenfluss über Master
  - Kein IP-Datenverkehr -> reduzierte Angriffsfläche
- **Manipulationsschutz**
  - Firmware-Echtheitsprüfung
  - Keine Schadsoftware in Drives möglich
- **Zugriff & Daten**
  - Nur eigene Protokolle zugelassen
  - Kommunikation via AIPEX 5 ist verschlüsselt

### Maschinenbauer/Betreiber (Systemebene)

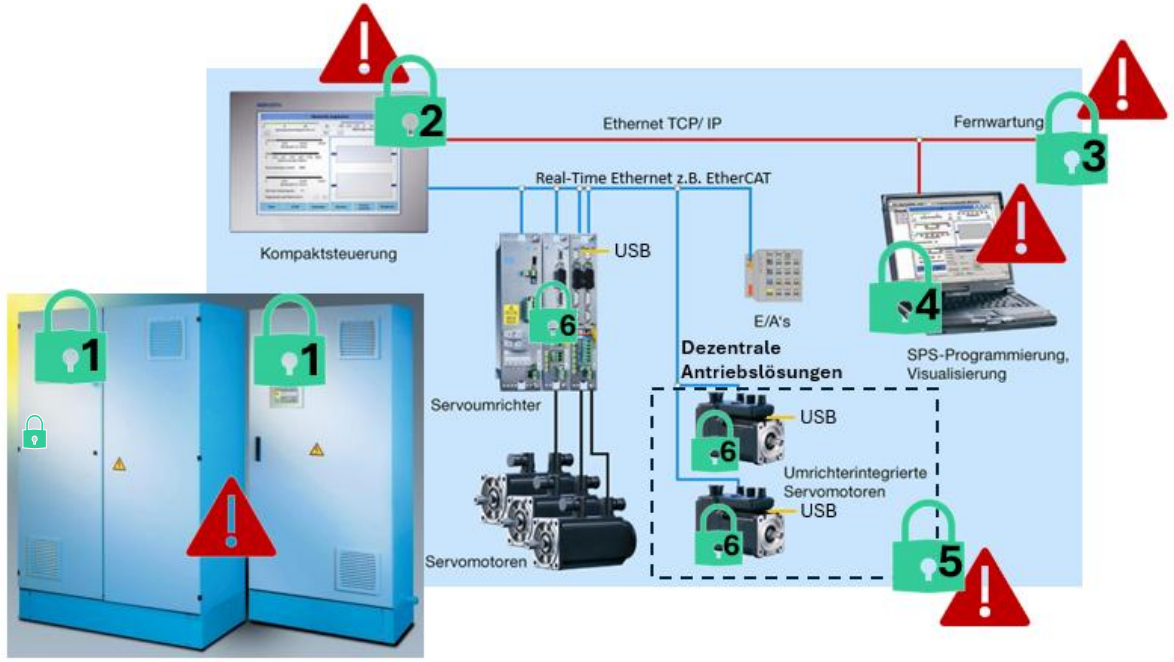
- **Zugriffsmanagement**
  - Keine globalen Admin-Zugänge
- **Remote-Zugriff**
  - Unsichere Verbindungen vermeiden
- **Risikomanagement**
  - Sicherheitsrisiken frühzeitig analysieren
  - Fehlanwendungen berücksichtigen und verhindern
- **Ganzheitliche Sicherheit**
  - Zusammenspiel von Komponenten & System sicherstellen

# 07 Risiko- und Bedrohungsanalyse bei Maschinen

## Betroffene Schnittstellen – Checkliste für die Risikoanalyse von Maschinenbauern

**Typische Gefahrenstellen:**

1. **Physischer Zugriff**
   – Zugang zu Produktionsstätten, Anlagen und Schaltschränken nur für autorisierte Personen
2. **Steuerung & Feldbus**
   – Schutz vor Schadsoftware und Absicherung des Feldbus-Netzwerkes in der Steuerung
3. **IT- & Netzwerk**
   – IT-Sicherheit, zum Schutz von Firmen- und Anlagennetzwerken
4. **PCs & drahtlose Verbindungen**
   – Absicherung von Industrie-PCs gegen Schadsoftware, keine unsicheren WLAN-/Hotspot-Verbindungen verwenden
5. **Dezentrale Systeme**
   – Schutz vor unbefugtem Zugriff auf Anlagen mit dezentralen Geräten
6. **AMKmotion sichert zentrale Gefahrenstellen an den Antriebskomponenten**




Potentielle Gefahrenstellen

Schutzeinrichtungen

# 08 Schwachstellenmanagement & Transparenz

## Warum ist das wichtig?

- Umgang mit Sicherheitslücken wird verpflichtend
- Transparenz über den gesamten Produktlebenszyklus erforderlich

## Zeitliche Anforderungen

- **Ab Sept. 2026 → Meldepflicht für aktiv ausgenutzte Sicherheitslücken**
- **Ab Dez. 2027 → Verpflichtendes, strukturiertes Schwachstellenmanagement**

## Zielsetzung

- Sicherheitslücken frühzeitig erkennen
- Risiken nachvollziehbar bewerten
- Maßnahmen schnell umsetzen

# 09 Schwachstellenmanagement & Transparenz

## Anforderungen an Maschinenbauer

- Sicherheitslücken bei Maschinen und Komponenten aktiv überwachen
- Klare Bewertungs- und Entscheidungsprozesse für sicherheitsrelevante Informationen etablieren
- Security-Risiken transparent an Kunden & Betreiber kommunizieren

## Schlüsselbausteine

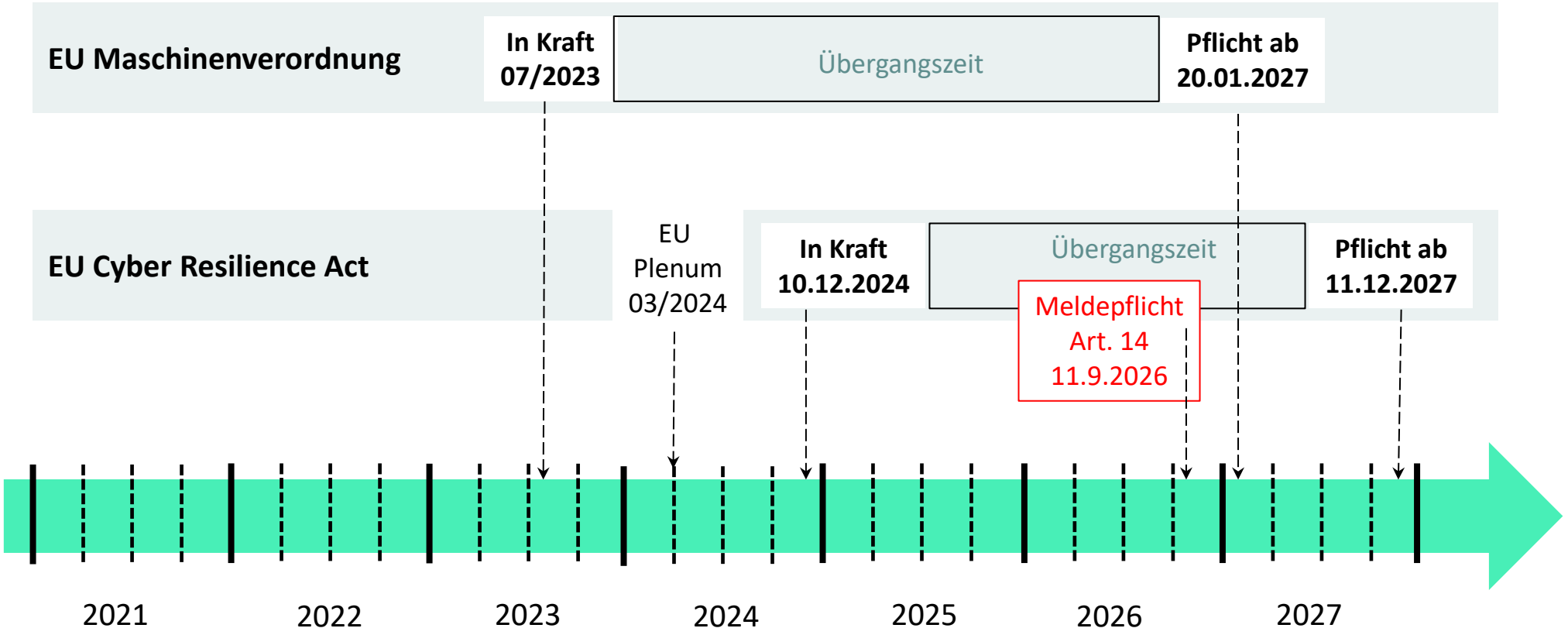
- **PSIRT** (Product Security Incident Response Team) → zentrale Einheit für Sicherheitsvorfälle
- **SBOM** (Software Bill of Materials)
  - Strukturierte Übersicht der eingesetzten Software-Bausteine
  - Darstellung von Abhängigkeiten innerhalb eines Produktes

**Strukturiertes Erfassen und Nachverfolgen von Sicherheitsrisiken wird zur Pflicht**
und zum festen Bestandteil der Produktverantwortung

AMKmotion
MEMBER OF THE ARBURG FAMILY

# 02 Zeitliche Einordnung relevanter EU-Regelwerke

# 10 Zeitliche Einordnung relevanter EU-Regelwerke



# 03 Cyber-Security bei AMKmotion

# 11 Cyber-Security bei AMKmotion - Status und nächste Schritte

## Bereits umgesetzt

- Schnelle Reaktion durch PSIRT (Product Security Incident Response Team)
- Klare Prozesse für
  - Meldung, Bewertung und Priorisierung von Security-Vorfällen
  - Regelmäßige Überwachung sicherheitsrelevanter Themen
- Zentrale Security-Kontaktadresse mit Ticketsystem
  - Strukturierte Erfassung und Nachverfolgung von Security-Fällen
  - Klare Zuständigkeiten im PSIRT

## In Umsetzung

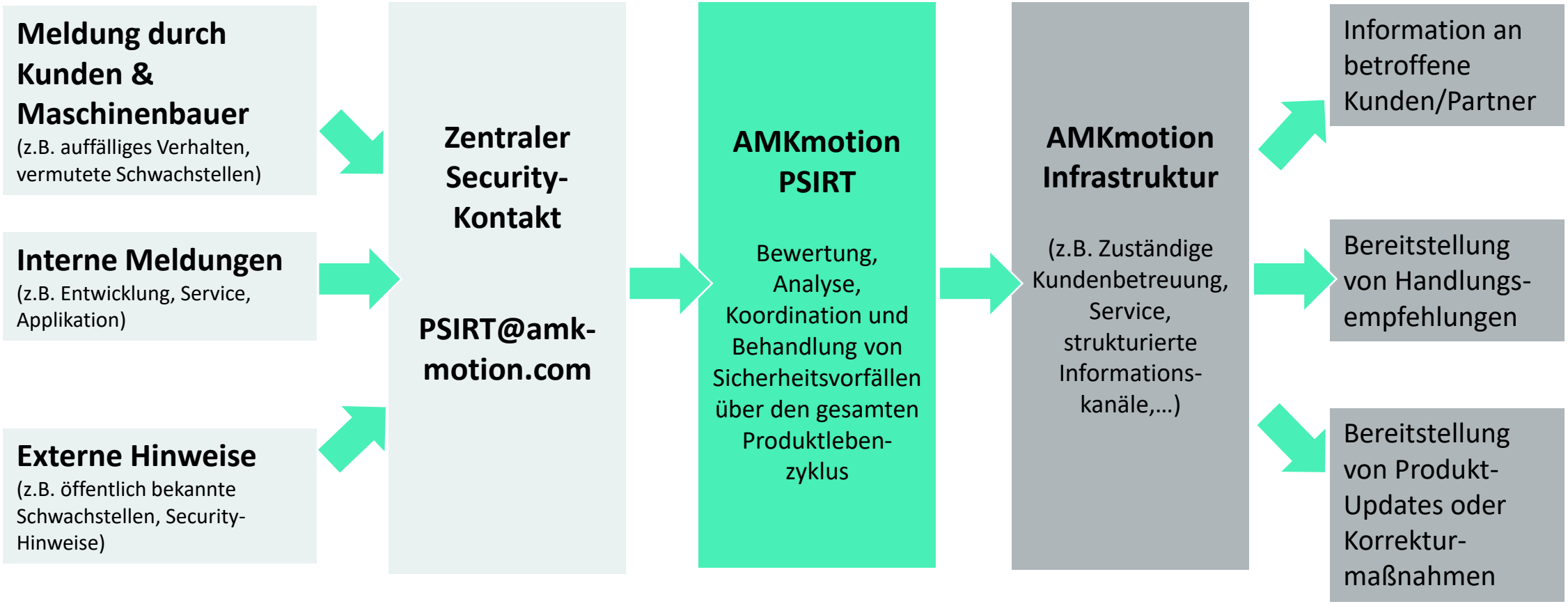
- Risikoanalysen für AMKmotion-Produkte
- Erstellung von Software-Stücklisten SBOM (Software Bills of Materials)
- Entwicklung einer kundenorientierten Patch- & Update-Strategie
- Etablierung strukturierter Security Tests
- Regelmäßige Code-Reviews für Security-relevante Funktionen

## Weiterer Ausbau

- Strukturierte, externe Kommunikation von Security-Informationen
- Stufenweiser Ausbau von Prozessen und Transparenz entlang des Produktlebenszyklus
- Enge Abstimmung zwischen internen Fachbereichen, wie Entwicklung, Produkt-management, Applikation, IT.

**AMKmotion hat die organisatorischen und technischen Grundlagen für Cyber-Security geschaffen und richtet seine Prozesse konsequent an CRA-Anforderungen aus.**

# 12 Meldekette für Sicherheitsvorfälle



# 13 AMKmotion PSIRT-Team



**PSIRT@amk-motion.com**

AMKmotion

MEMBER OF THE ARBURG FAMILY


## AMKmotion GmbH + Co KG

Gaußstraße 37-39
73230 Kirchheim unter Teck
Germany

+49 7021 5005 0
info@amk-motion.com