AMKmotion

MEMBER OF THE ARBURG FAMILY

Cyber-Security bei AMKmotion

Security by Design für moderne Antriebssysteme



AMKmotion
MEMBER OF THE ARBURG FAMILY

01 Einführung Cyber Resilience Act (CRA) und Relevanz für Maschinenbauer & -betreiber

01 Warum Cyber-Security?

- Die zunehmende Vernetzung von Maschinen und Anlagen führt zu einer immer engeren Verbindung von *IT- und OT-Systemen. **Ethernet-basierte Kommunikation, Remote-Zugriffe und digitale Services sind heute fester Bestandteil moderner Automatisierungslösungen**. Gleichzeitig entstehen dadurch neue Angriffsflächen für Cyberangriffe.
- Cyber-Security betrifft daher nicht mehr nur klassische IT-Systeme, sondern zunehmend auch Maschinen und Produktionsanlagen. Mögliche Folgen sind **Maschinenstillstände, Produktions-ausfälle sowie der Verlust von Daten und applikationsspezifischem Know-how**.
- Cyber-Security wird damit zu einer grundlegenden Voraussetzung für funktionale Sicherheit, Verfügbarkeit, Zuverlässigkeit und Wettbewerbsfähigkeit. Manipulationen oder Angriffe können sicherheitsrelevante Funktionen von Maschinen direkt beeinflussen.

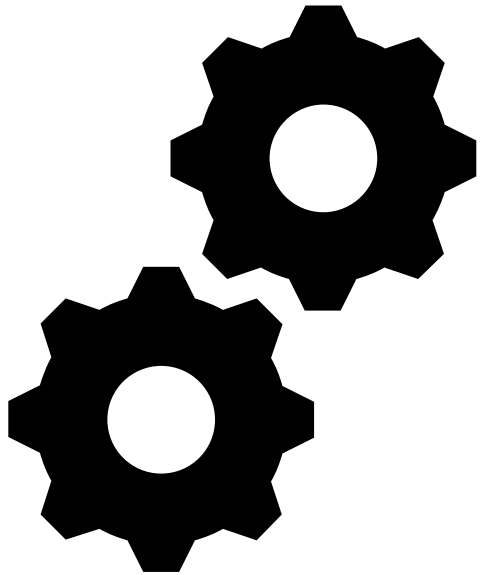


* IT (Information Technology): Systeme zur Verarbeitung, Speicherung und Übertragung von Daten, z. B. Office-IT, Server, Netzwerke und Cloud-Dienste.
OT (Operational Technology): Systeme zur Steuerung und Überwachung von Maschinen und Anlagen, z. B. Steuerungen, Antriebe, Sensoren und industrielle Netzwerke.

02 Relevanz für Maschinenbauer und Betreiber

Cyber Security als Pflicht und Verantwortung

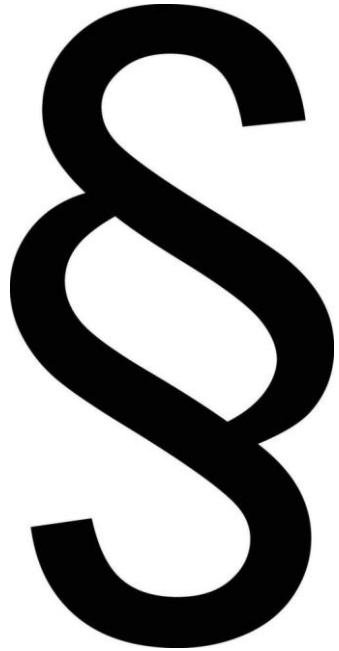
- Cyber Security schützt die **funktionale Sicherheit, Verfügbarkeit, Integrität** und **Vertraulichkeit** von Maschinen und Anlagen
- Maschinen und Antriebssysteme sind zunehmend Teil vernetzter Gesamtsysteme. Sicherheitsvorfälle wirken sich direkt auf:
  - Sicherheit der Bediener
  - Produktion und Lieferfähigkeit
  - Betriebssicherheit
  - Reputation und Haftung
- Cyber Security betrifft den **gesamten Lebenszyklus** einer Maschine – von Entwicklung und Inbetriebnahme bis Service und Retrofit
- Die Verantwortung liegt nicht nur in der IT, sondern auch beim **Maschinenbau und der Automatisierung**



03 Regulatorischer Rahmen für Cyber-Security

Cyber-Security wird regulatorisch verpflichtend

- Relevante Rahmenwerke im Überblick
  - **Normenreihe DIN EN 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
- Cyber Security ist kein IT-Thema allein, sondern **produkt- und maschinenrelevant**



02 CE-Kennzeichnung als rechtlicher Anker

CE-Kennzeichnung – Verantwortung des Herstellers

- **CE-Kennzeichnung darf nur erfolgen, wenn ein Produkt allen relevanten EU-Rechtsvorschriften entspricht**
- Der Hersteller erklärt damit eigenverantwortlich die Konformität , z.B. mit der
  - Maschinenrichtlinie / Maschinenverordnung
  - Niederspannungs- und EMV-Richtlinie
  - Weitere produktspezifische Rechtsakte
  - Und neu auch die Konformität mit der CRA-Verordnung
    Somit wird CRA Tel der CE-Konformität für alle Produkte (Komponenten, Maschinen) mit digitalen Elementen. Hersteller tragen Verantwortung über den gesamten Produktlebenszyklus.

- **Rechtliche Folgen bei falscher CE-Kennzeichnung**
  - Ordnungswidrigkeit oder Straftat
  - Maßnahmen der Marktüberwachung
  - Bußgelder und Haftungsrisiken

03 Aufgaben & Verantwortlichkeiten

05 Aufgaben und Verantwortlichkeiten

Rechtsvorschrift	CRA	NIS-2
Rechtliche Verantwortung	AMKmotion Maschinenbauer	Maschinenbetreiber AMKmotion Nur im Rahmen als Betreiber des eigenen Maschinenparks
Zuordnung zu Produkten, Komponenten, Maschinen	Produkte • Firmware (Hardware-gebundene Software) • Software Maschinenkonzepte	Firmeninfrastruktur • IT & OT Netzwerk • Produktion & Logistik • Office-Bereiche

AMKmotion als Hersteller von Komponenten

- Unterstützt Maschinenbauer bei der Umsetzung von Cyber Security-Anforderungen durch geeignete Produkte und Funktionen
- Erfüllt **relevante rechtliche und normative Anforderungen**
- Ein spezialisiertes **Product Security Incident Response Team (PSIRT)** reagiert im Sicherheitsfall schnell und gezielt
- Agiert als **technischer Experte und Sparringspartner**

Maschinenbauer als Hersteller des Systems

- Erstellt das **Cyber-Security-Konzept für die Maschine** und das Gesamtsystem
- Verantwortet den Schutz von **eigenen sowie betreiberrelevanten Daten und Know-how** auf Maschinenebene
- Trifft technische und organisatorische Maßnahmen zur **Sicherstellung der Verfügbarkeit und Sicherheit** der Maschine
- Erfüllt die anwendbaren **rechtlichen und normativen Anforderungen** (z. B. CE-Kennzeichnung, CRA-Pflichten für die Maschine, Aufstellung eines PSIRT-Teams)
- Etabliert Prozesse zum **Umgang mit Sicherheitsvorfällen** im Betrieb der Maschine

06 Schwachstellenmanagement & Transparenz

Umgang mit Sicherheitslücken, Meldeanforderungen und Transparenz entlang des Produktlebenszyklus

Zeitliche Anforderungen

Ab September 2026

- Verpflichtung zur Meldung von **aktiv ausgenutzten Sicherheitslücken und Sicherheitsvorfällen**

Ab Dezember 2027

- Einführung eines **dauerhaften und strukturierten Schwachstellenmanagements**

Zielsetzung:

- Sicherheitslücken frühzeitig identifizieren
- Risiken nachvollziehbar bewerten
- Geeignete Maßnahmen zeitnah umsetzen

Anforderungen an Maschinenbauer

Maschinenbauer sind künftig gefordert

- Sicherheitslücken in Maschinen sowie eingesetzte **Komponenten systematisch zu beobachten**
- **Bewertungs- und Entscheidungsprozesse** für sicherheitsrelevante Informationen zu etablieren
- Relevante Security-Risiken **transparent an Betreiber und Kunden zu kommunizieren.**

Schlüsselbausteine zur Umsetzung

PSIRT – Product Security Incident Response Team

- Zentrale organisatorische Einheit für den Umgang mit sicherheitsrelevanten Ereignissen

SBOM – Software Bill of Materials

- Strukturierte Übersicht der eingesetzten Software-Bausteine
- Darstellung von Abhängigkeiten innerhalb eines Produktes

Das strukturierte Erfassen und Nachverfolgen von Sicherheitsrisiken wird unverzichtbar und ist regulatorisch gefordert

07 Cyber-Security in Antriebssystemen – Verantwortlichkeiten

Sicherheit entsteht im Zusammenspiel

AMKmotion (Komponentenebene)

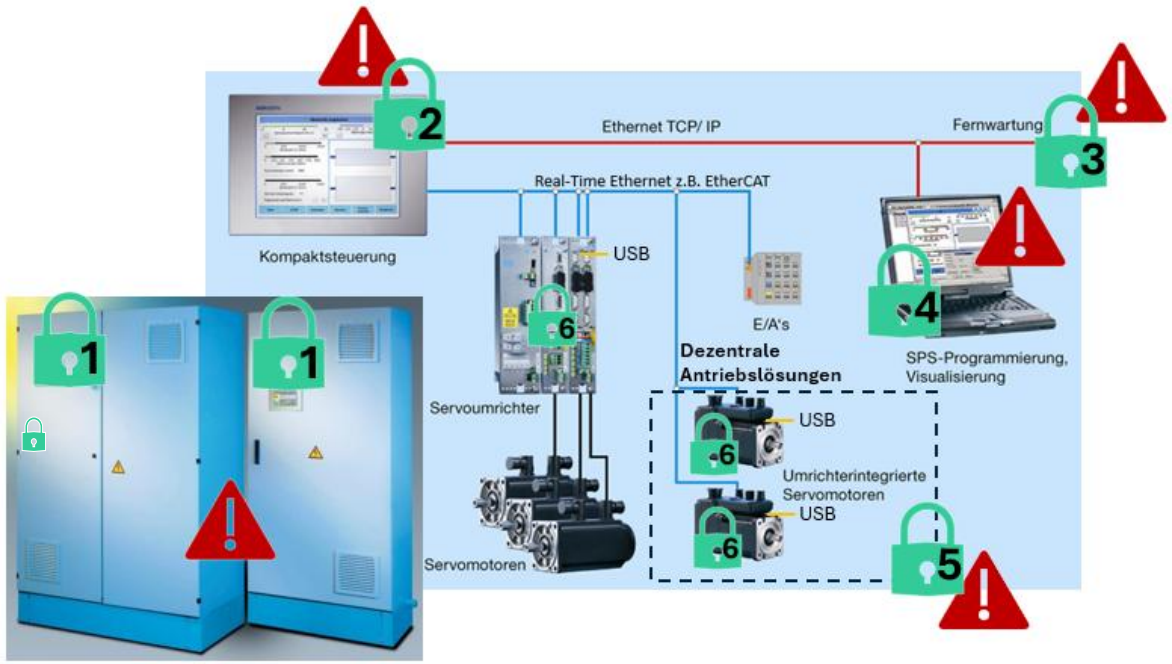
- **Physischer Schutz**
  - Abgedeckte Serviceschnittstellen
  - Zentrale Geräte im Schaltschrank geschützt
- **Sichere Kommunikation**
  - EtherCAT mit Single-Master-Prinzip
  - Kontrollierter Datenfluss über Master
  - Kein IP-Datenverkehr -> reduzierte Angriffsfläche
- **Manipulationsschutz**
  - 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

08 Risiko- und Bedrohungsanalyse bei Maschinen

Betroffene Schnittstellen – Checkliste für die Risikoanalyse von Maschinenbauern



Potentielle Gefahrenstellen

Schutzeinrichtungen

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**

09 Risiko- und Bedrohungsanalyse bei Maschinen

Durch sicherheitsgerichtete Designmaßnahmen schützt AMKmotion die Antriebskomponenten:

- Serviceschnittstelle an „Dezentralen Antrieben“ sind mit Verschraubungen abgedeckt
- „Zentrale Geräte“ sind im Schaltschrank vor unbefugtem Zugriff geschützt
- EtherCAT ist eine offene und hoch performante Schnittstelle, architektonisch abgesichert durch
  - **Single Master System**, wodurch Risiken von SubDevices nahezu eliminiert werden
  - Allein der EtherCAT Master kann die EtherCAT Schnittstelle schützen und kontrolliert die Daten zu und von den Antrieben
  - **Kein IP-Datenverkehr**, was die Angriffsfläche auf die Komponenten deutlich reduziert

- Firmwarepakete werden im Antrieb auf Echtheit geprüft. So können Manipulationen erkannt werden und es kann sich keine Schadsoftware in den Drives verstecken
- Neben der Steuerungskommunikation werden von AMKmotion Antrieben lediglich auf dem hauseigenen Kommunikationsprotokoll basierende Daten akzeptiert. Dieses Protokoll wird von der Inbetriebnahme-Software AIPEX 5 genutzt. So werden die Angriffsvektoren minimiert.
- Weitere Kommunikation von AIPEX 5 ist stets verschlüsselt und grundsätzlich abhängig vom Schutzniveau des PC bzw. der IT-Infrastruktur

09 Risiko- und Bedrohungsanalyse bei Maschinen

AMKmotion schützt durch sicherheitsgerichtete Designmaßnahmen die Antriebskomponenten

- Serviceschnittstelle an „Dezentralen Antrieben“ sind mit Verschraubungen abgedeckt
- „Zentrale Geräte“ sind im Schaltschrank vor unbefugtem Zugriff geschützt
- EtherCAT ist eine offene und hoch performante Schnittstelle, architektonisch abgesichert durch
  - **Single Master System**, wodurch Risiken von SubDevices nahezu eliminiert werden
  - Allein der EtherCAT Master kann die EtherCAT Schnittstelle schützen und kontrolliert die Daten zu und von den Antrieben
  - **Kein IP-Datenverkehr**, was die Angriffsfläche auf die Komponenten deutlich reduziert
- Firmwarepakete werden im Antrieb auf Echtheit geprüft. So können Manipulationen erkannt werden und es kann sich keine Schadsoftware in den Drives verstecken
- Neben der Steuerungskommunikation werden von AMKmotion Antrieben lediglich auf dem hauseigenen Kommunikationsprotokoll basierende Daten akzeptiert. Dieses Protokoll wird von der Inbetriebnahme-Software AIPEX 5 genutzt. So werden die Angriffsvektoren minimiert.
- Weitere Kommunikation von AIPEX 5 ist stets verschlüsselt und grundsätzlich abhängig vom Schutzniveau des PC bzw. der IT-Infrastruktur

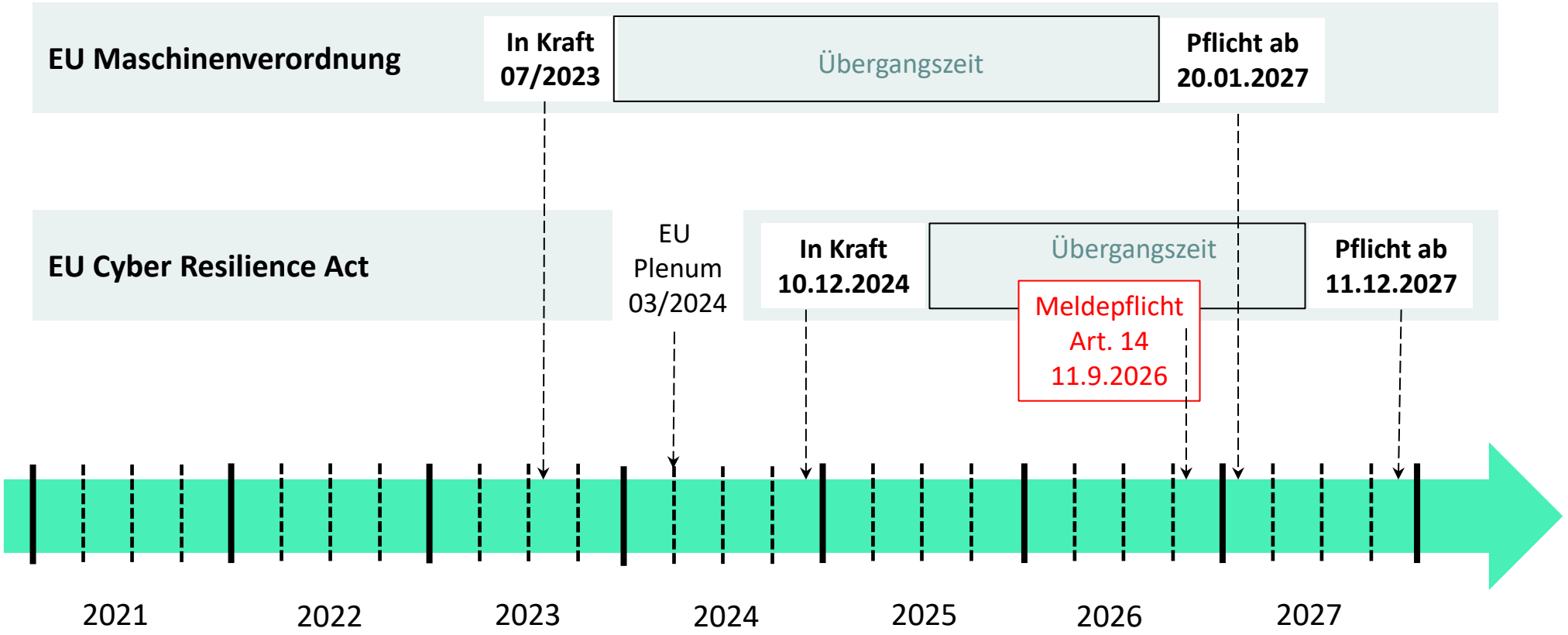
10 Risiko- und Bedrohungsanalyse bei Maschinen

Weitere Systemmaßnahmen durch Maschinenbauer und Betreiber

- Die Absicherung erfolgt im Zusammenspiel zwischen Komponenten und übergeordnetem System
- Richten Sie keine globalen Administratorzugänge für die Anlage ein
- Unterbinden Sie unzureichend gesicherte Remotezugänge
- Analysieren Sie im Rahmen der Risikoanalyse vorhersehbar Fehlanwendungen und versuchen Sie diese zu unterbinden.

04 Zeitliche Einordnung relevanter EU-Regelwerke

11 Zeitliche Einordnung relevanter EU-Regelwerke



05 Cyber-Security bei AMKmotion

12 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

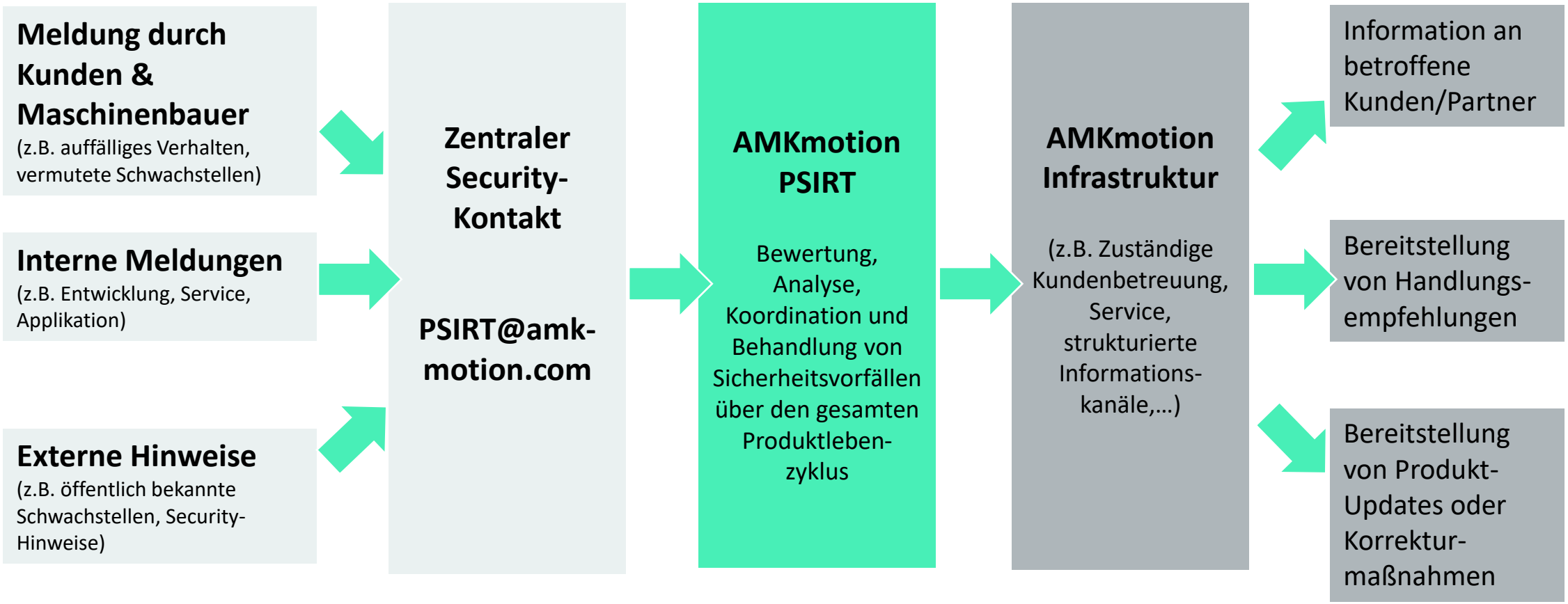
- Risikoanalysen für AMKmotion-Produkte
- Erstellung von Software-Stücklisten SBOM (Software Bills of Materials)
- Entwicklung einer kundenorientierten Patch- & Update-Strategie
- Etablierung strukturierter Security Tests
- Regelmäßige Code-Reviews für Security-relevante Funktionen

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 bereits heute an künftigen regulatorischen Anforderungen (CRA) aus.

13 Meldekette für Sicherheitsvorfälle



14 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

