

SICHERE MASCHINEN UND ANLAGEN: CYBERSECURITY AUS SICHT DER BETREIBER





Florian Vetter

EUCHNER GmbH + Co. KG - Safety Services

Experte für Arbeits- und Maschinensicherheit (TÜV Thüringen)

ISA/IEC 62443 Cybersecurity Fundamentals Specialist (CFS)

Telefon +49 711 7597-474

Mobil +49 162 3608 742

E-Mail florian.vetter@euchner.de

➤ Was uns stark macht

- **42 Tochtergesellschaften** und Handelspartner im In- und Ausland
- **> 900 Mitarbeiter** international
- **> 7.000 hochwertige Produkte** für den Maschinen und Anlagenbau





- > **Consulting**
Beratung und Dokumentation für Hersteller und Betreiber
- > **Engineering**
Modifikation und Überprüfung von Maschinen
- > **Training**
Praxisnahe Schulungen für Hersteller und Betreiber

- **Geltungsbereich des Cyber Resilience Acts**
- **Betreiberpflichten durch den CRA**
 - Anforderungen aus der TRBS 1115 Teil 1
 - Betrachtung der „wesentlichen Änderung“ nach CRA
- **Fazit zur Cybersecurity für Betreiber**

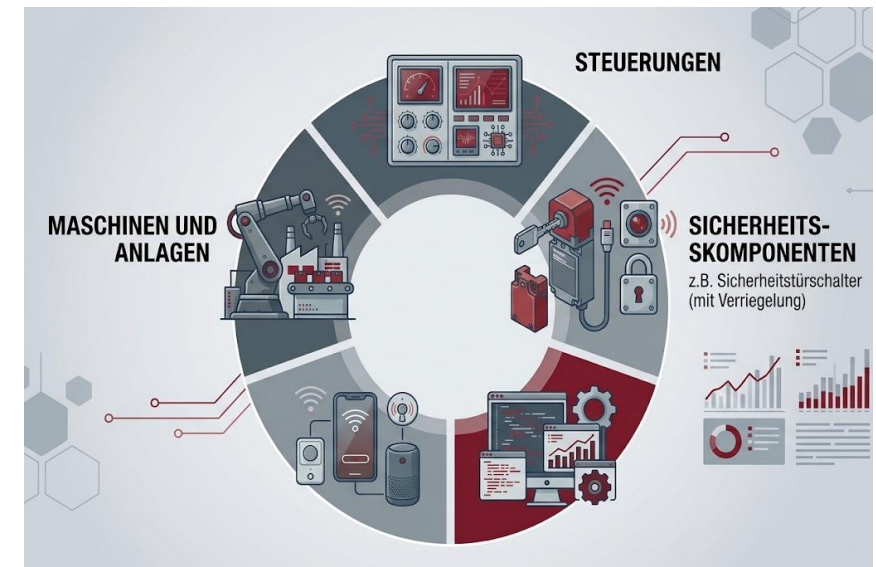
EUCHNER

More than safety.

GELTUNGSBEREICH DES CYBER RESILIENCE ACTS

➤ **Verordnung 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – Cyberresilienz-Verordnung**

- Produkte **mit digitalen Elementen**, sind Produkte, die Daten verarbeiten oder mit anderen Systemen kommunizieren können, z.B.
- Steuerungen
 - Sicherheitskomponenten
 - Software
 - Vernetzte Geräte
 - Maschinen und Anlagen



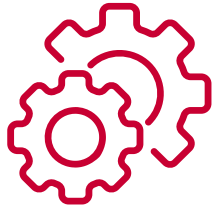
Maschinenhersteller sind auch Hersteller digitaler Produkte.

➤ **Verordnung 2024/2847 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen – Cyberresilienz-Verordnung**

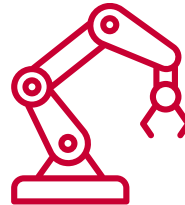


➤ **Drei zentrale Gruppen entlang der Wertschöpfungskette im Fokus des CRA**

**Hersteller von
Komponenten**



**Maschinenhersteller
(Integratoren)**

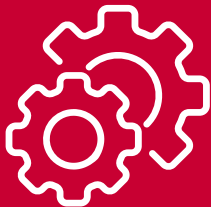


**Betreiber /
Anwender**

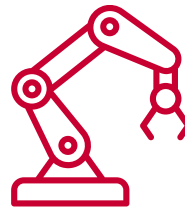


➤ **Drei zentrale Gruppen entlang der Wertschöpfungskette im Fokus des CRA**

**Hersteller von
Komponenten**



**Maschinenhersteller
(Integratoren)**



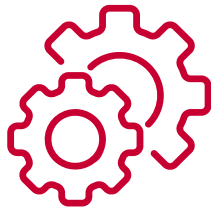
**Betreiber /
Anwender**



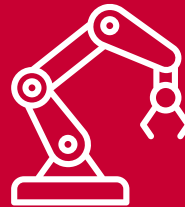
- Integration von Cybersicherheit in Design und Entwicklung
- Bereitstellung cybersicherer Produkte und Dokumentation
- Bereitstellung von Sicherheitsupdates über den definierten Lebenszyklus

➤ **Drei zentrale Gruppen entlang der Wertschöpfungskette im Fokus des CRA**

**Hersteller von
Komponenten**



**Maschinenhersteller
(Integratoren)**



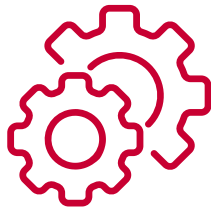
**Betreiber /
Anwender**



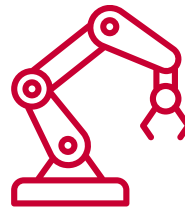
- Auswahl geeigneter, cybersicherer Komponenten
- Cybersichere Systemintegration
- Vollständige Dokumentation der Gesamtmaschine

➤ **Drei zentrale Gruppen entlang der Wertschöpfungskette im Fokus des CRA**

**Hersteller von
Komponenten**



**Maschinenhersteller
(Integratoren)**



**Betreiber /
Anwender**



- Bewertung von Cybersicherheitsrisiken
- Umsetzung von Empfehlungen und Updates
- Cybersicherer Betrieb über den gesamten Lebenszyklus

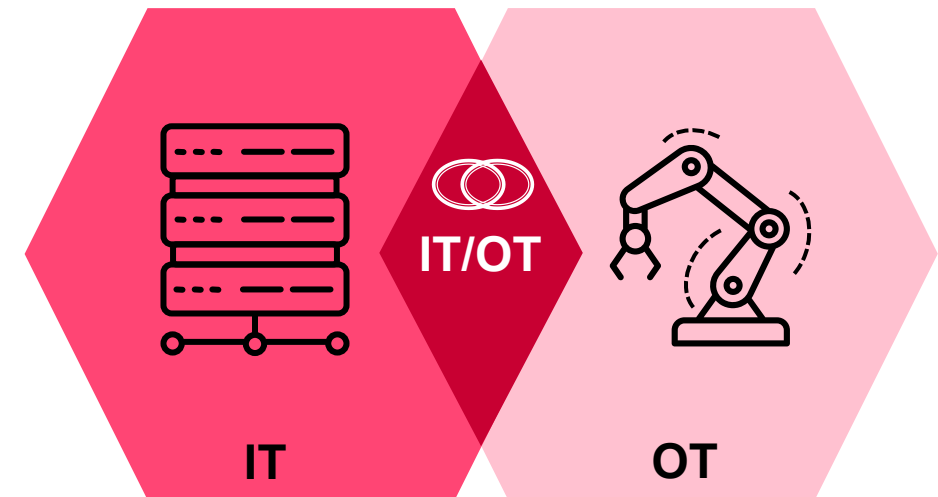
➤ **Herkömmliche Gefährdungen in der Gefährdungsbeurteilung z.B.**

- mechanische Gefährdungen
- elektrische Gefährdungen
- ergonomische Gefährdungen



➤ **Neue Gefährdungen durch Digitalisierung und Vernetzung**

- Manipulation von Signalen / Steuerungen
- unbefugter Zugriff
- Daten- oder Kommunikationsverlust
- Ausfall von Schutzfunktionen



Cyberisiken können Auslöser klassischer Gefährdungen sein.

➤ **Wo entstehen Cyberrisiken? – typische Einfallstore**

- Fernwartung
- Service-Laptop / USB-Sticks
- WLAN / VPN / Cloud-Anbindungen
- Wartungsportale

➤ **Die häufigsten Schwachstellen im Betrieb**

- Geteilte Accounts oder Standardpasswörter
- Unkontrollierte Administratorrechte
- Unzureichende Netzwerksegmentierung
- Verwendung veralteter Systeme
- Fehlende Prozesse für Softwareaktualisierungen



- **Ist Cybersecurity überhaupt ein Betreiberthema?**
 - Betreiber hat gemäß BetrSichV sichere Betriebsmittel bereitzustellen
 - Dies beinhaltet auch Cybersecurity-Belange

- **Betreiberpflichten aus der BetrSichV:**
 - Regelmäßige Durchführung der **Gefährdungsbeurteilung** und ggf. Festlegen von Schutzmaßnahmen
 - **Prüfungen** nach TRBS 1115 und TRBS 1115 Teil 1

➤ **Anforderungen an Cybersicherheitsmaßnahmen (TRBS 1115 Teil 1 Abschnitt 4.5)**



- **Ist Cybersecurity überhaupt ein Betreiberthema?**
 - Betreiber hat gemäß BetrSichV sichere Betriebsmittel bereitzustellen
 - Dies beinhaltet auch Cybersecurity-Belange

- **Betreiberpflichten aus der BetrSichV:**
 - Regelmäßige Durchführung der **Gefährdungsbeurteilung** und ggf. Festlegen von Schutzmaßnahmen
 - **Prüfungen** nach TRBS 1115 und TRBS 1115 Teil 1
 - Regelmäßige Überprüfung auf **Stand der Technik**
 - Prüfung auf „**wesentliche Änderung**“ bei Modifikationen an Maschinen

➤ Wesentliche Änderung nach Maschinenverordnung 2023/1230

MVO Art. 3 Abs. 16

„wesentliche Veränderung“ bezeichnet eine vom Hersteller nicht vorgesehene oder geplante physische oder **digitale Veränderung einer Maschine** ... nach deren bzw. dessen Inverkehrbringen oder Inbetriebnahme,...

Was sind digitale Veränderungen?

- Sicherheitsupdates
- Bugfixes
- Firmware-Updates
- Funktionsupdates
- neue Kommunikationsschnittstellen
- Änderungen der Konfiguration
- Cloud-Anbindungen
- ...

Wann gilt eine digitale Veränderung als „wesentliche Veränderung“?

➤ Was bedeutet „wesentliche Änderung“ nach CRA?

Eine „**wesentliche Änderung**“ ist eine Änderung des Produkts mit digitalen Elementen nach dessen Inverkehrbringen, die sich **auf die Konformität des Produkts mit den grundlegenden Cybersicherheitsanforderungen in Anhang I Teil I auswirkt** oder zu einer **Änderung des bestimmungsgemäßen Zwecks**, für den das Produkt geprüft wurde, führt;

Softwareänderung ist eine
„wesentliche Veränderung“



- Betrachtung als Neuprodukt
- Neues Konformitätsbewertungsverfahren nach CRA



Softwareänderung ist
keine wesentliche Veränderung



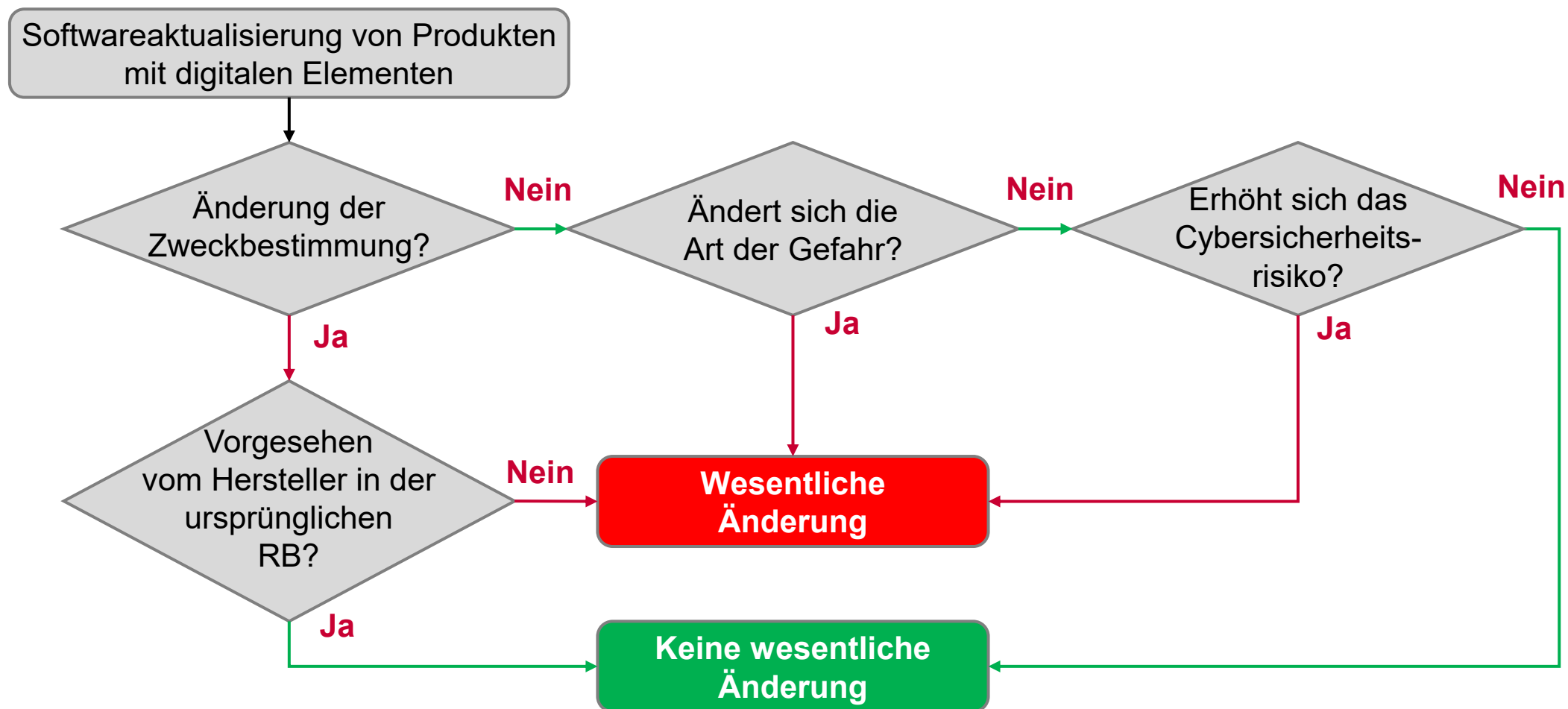
- Ggf. Aktualisierung von Betriebsanleitungen
- Aktualisierung der Dokumentation z.B. Checksummenhistorie



➤ Wesentliche Änderung in den Erwägungsgründen (39)

Ein Produkt mit digitalen Elementen gilt durch eine **Softwareänderung** als wesentlich geändert, wenn

- die Softwareaktualisierung die **Zweckbestimmung des Produkts ändert** und
 - diese Änderungen vom Hersteller **in der ursprünglichen Risikobewertung nicht vorhergesehen** wurden,
oder
 - wenn sich **die Art der Gefahr geändert** hat
oder
 - sich das **Cybersicherheitsrisiko aufgrund der Softwareaktualisierung erhöht** hat.
-



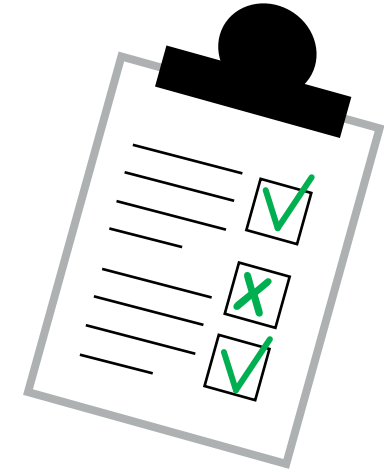
EUCHNER

More than safety.

FAZIT

➤ Zusammenfassung für Betreiber

- Cybersecurity ist Teil des sicheren Betriebs von Maschinen und Anlagen.
- Cyberbedingte Gefährdungen müssen im Rahmen der **Gefährdungsbeurteilung** betrachtet werden.
- Bei Veränderungen von Maschinen sind die Auswirkungen auf **funktionale Safety und Cybersecurity** zu prüfen.
- Nicht jede digitale Veränderung ist eine wesentliche Änderung.
- Bei einer **wesentlichen Änderung** muss die **Konformität nach CRA bzw. MVO** für die Maschine hergestellt werden.



Sie haben Fragen?

Schreiben Sie uns – das **EUCHNER-Team** hilft Ihnen gerne weiter.
Oder besuchen Sie uns hier auf der Messe – **Stand 1-445!**



EUCHNER GmbH + Co. KG

Kohlhammerstraße 16

70771 Leinfelden-Echterdingen | Germany

Tel. +49 711 7597-0 | info@euchner.de

www.euchner.com