Autor: Carsten Bokholt
November 2026



WHITEPAPER

INDUSTRIAL SECURITY

VERTRAUEN DURCH SICHERHEIT – SO SCHÜTZT HELMHOLZ DIE INDUSTRIELLE KOMMUNIKATION.

Ein Leitfaden für Hersteller und Betreiber von Maschinen
zum Umgang mit der aktuellen EU-Gesetzgebung.

www.helmholz.de

Helmholz®
COMPATIBLE WITH YOU

INHALTSVERZEICHNIS

4 **ÜBER UNS**

5 **MOTIVATION & VISION**

6 **RELEVANTE VERORDNUNGEN UND RICHTLINIEN**

- Cyber Resilience Act
- Maschinenverordnung
- NIS-2 Richtlinie

9 **GESETZLICHE VERPFLICHTUNGEN: DIE RELEVANTEN NORMEN**

- IEC 62443
- ISO 27001 / BSI IT-Grundschutz

13 **SECURITY BEI HELMHOLZ: PRAXIS STATT THEORIE**

- Security ist kein Zustand – sondern ein Prozess
- Unsere Partner

15 **CRA READY: SO BEREITET HELMHOLZ SEINE PRODUKTE VOR**

16 **CYBER RESILIENCE ACT: DIE WICHTIGSTEN FRAGEN IM ÜBERBLICK**

20 **EU-MASCHINENVERORDNUNG: WAS MASCHINENBAUER WISSEN MÜSSEN**

ÜBER UNS

Wo Maschinen kommunizieren, schafft Helmholz Vertrauen: mit Technologie, die verbindet, schützt und industrielle Kommunikation einfach sicher macht.

Seit über 35 Jahren entwickelt Helmholz Lösungen, die industrielle Netzwerke effizienter und zukunftsfähiger machen – von der Feldebene bis in die Cloud. Als Spezialist für PROFINET, Industrial Ethernet und IoT setzt Helmholz auf Qualität, Präzision und partnerschaftliches Denken.

Sichere Kommunikation – von der Komponente bis zur Anlage

Unser Ziel: Technik verständlich und Sicherheit selbstverständlich machen. Ob PROFINET, Industrial Ethernet oder IoT – Helmholz bietet die passenden Komponenten für reibungslose Kommunikation in industriellen Anlagen.

Von Switches und Gateways über Firewalls bis hin zu Remote-Access-Lösungen entstehen Systeme, die verbinden, schützen und Prozesse effizienter machen. Alle Produkte werden in Deutschland entwickelt, geprüft und nach DIN ISO 9001:2015 gefertigt – für Qualität, auf die man sich verlassen kann.

Helmholz denkt Automatisierung weiter: mit Security-by-Design, offenen Standards und Lösungen, die den steigenden Anforderungen an Industrial Security gerecht werden.



So unterstützen wir Maschinenbauer, Integratoren und Betreiber dabei, ihre Anlagen zuverlässig, skalierbar und normkonform zu vernetzen.

Helmholz – Compatible with you. Denn echte Partnerschaft ist die Basis sicherer Kommunikation.

MOTIVATION & VISION

Die Sicherheit von Maschinen und Anlagen ist entscheidend für einen stabilen und ausfallsicheren Produktionsprozess. Nur wer seine Kommunikation absichert, sorgt für dauerhaft verfügbare Anlagen.

Spätestens mit neuen Verordnungen wie dem Cyber Resilience Act (CRA) und der Europäischen Maschinenverordnung werden entsprechende Cybersecurity-Maßnahmen nun für jeden Pflicht, der Produkte oder Maschinen in den Verkehr bringt.

Motivation

Bei Helmholz wurde Security schon früh im Unternehmen und in den Produkten mitgedacht. Dieses Dokument soll einen Überblick über die Rechtslage und die relevanten Normen für Hersteller, Maschinenbauer und Endanwender erläutern und den Stand und den Ausblick der Umsetzung bei der Firma Helmholz geben.

Vision

Vertrauen durch Sicherheit! Sicherheit ist mehr als Technik – sie ist Haltung. Helmholz integriert Security by Design in jedes Produkt, um industrielle Kommunikation dauerhaft zu schützen.

Unsere Vision: Vertrauen entsteht dort, wo Sicherheit beginnt.



RELEVANTE VERORDNUNGEN UND RICHTLINIEN

Mit dem Siegeszug der Ethernet-Vernetzung in Fertigungsanlagen gewinnt auch Cybersecurity an zentraler Bedeutung, wie die aktuellen Normen und Richtlinien zeigen.

Der EU-Gesetzgeber hat zu diesem Themenkomplex verschiedene Verordnungen und Richtlinien verfasst oder aktualisiert. Vom Cyber Resilience Act (CRA) für Produkte mit digitalen Elementen über die neue Maschinenverordnung für die Sicherheit von Maschinen bis hin zur Sicherheit der Unternehmens-IT und kritischer Infrastruktur („NIS-2“) ist für jeden was dabei.

Cyber Resilience Act

Der Cyber Resilience Act betrachtet Produkte (Komponenten) mit digitalen Elementen. Das kann ein Handy sein, ein elektronisches Spielzeug mit USB, die Waschmaschine mit WLAN, IT-Produkte oder eben auch eine SPS oder ein industrieller Switch. Es geht hierbei um die Verarbeitung, Speicherung, Übertragung von digitalen Daten. Das bezieht sowohl die Hardware als auch die Software inkl. der zum Produkt zugehörige Cloudanwendung mit ein.



Der CRA wird verpflichtend für alle Produkte bei Verkauf ab Dezember 2027. Der CRA kennt aber Ausnahmen. Das sind bereits regulierte Branchen (Automotive, Medical, Aeronautic), Open Source Software als solches, reine Cloudanwendungen, Ersatzteile und Legacy Produkte. Als Besonderheit ist beim CRA die Forderung zu nennen, dass die Cybersicherheit des Produktes im Rahmen der CE-Erklärung vom Hersteller bestätigt werden muss. Die Cybersicherheit steht somit in Zukunft gleichberechtigt z.B. neben einem EMV-Test.

Der CRA betrachtet die Produkte über Ihren gesamten Lebenszyklus. Beginnend bei den ersten Konzepten über die eigentliche Entwicklung, den Verkauf bis hin zur Abkündigung und lange darüber hinaus.

Zentraler Punkt ist die dauerhafte Sicherstellung einer bestmöglichen Fehlerfreiheit in Bezug auf die Security. Täglich werden neue Erkenntnisse zu Bedrohungen bekannt. Daher ist es unabdingbar die Security auf den Stand der Technik zu halten und neue Risiken den Nutzern zu melden.

Zudem sind entsprechende Lösungen anzubieten beispielsweise in Form von Firmwareupdates, eine Anpassung der Konfiguration oder die Veränderung der Zugriffsmöglichkeiten.

Der CRA enthält auch die Verpflichtung – nach einer Produktabkündigung weiterhin für einen spezifischen Zeitraum (mindestens 5 Jahre) – Sicherheitsupdates zur Verfügung stellen zu können. Eine Abkündigung führt also zur Verpflichtung, die Verwendbarkeit des Produktes durch Sicherheitsupdates weiterhin zu ermöglichen.

Im Umfeld der industriellen Automatisierung und Kommunikation kann aus heutiger Sicht die IEC 62443, speziell der Teil 4 (Entwicklungsprozess und Produktsicherheit) herangezogen werden, um den CRA umzusetzen.

Der CRA unterteilt auch die verschiedenen Produktarten in Security Kategorien. Die meisten Produkte fallen unter die Standard-Kategorie, wie z.B. unmanaged Switche, SPSen oder Bedienterminals. Hierbei muss der Hersteller die Einhaltung des CRA mit den verfügbaren Normen selber sicherstellen und eine CE-Eigenerklärung für jedes betroffene Produkt ausstellen. Daneben gibt es Produkte der Klasse I und II (Class I / II), wie z.B. Router, Firewalls und managed Switches. Für diese Produkte muss der Hersteller die Konformität der Produkte und seine Entwicklungsprozesses durch eine notifizierte Stelle prüfen lassen. In der höchsten Kategorie liegen die kritische Produkte für den direkten Betrieb von kritischer Infrastruktur.

Maschinenverordnung

Die neu aufgelegte Maschinenverordnung betrachtet Maschinen und Teile von Maschinen. Sie richtet sich somit an den Integrator, bzw. den Maschinenbauer aber auch an den Betreiber. Bisher lag der Fokus der vorangegangenen Maschinenrichtlinie darauf, den Menschen vor der Maschine zu schützen. Safety stand im Vordergrund.



Mit der Neufassung der Maschinenrichtlinie als Maschinenverordnung (EU 2023/1230) wurde die Betrachtungsweise hinzugefügt, die Maschine vor dem Menschen zu schützen, also die Security. Wichtige Themen wie der Schutz der Maschine selbst und des Maschinennetzwerks vor Angreifern von außen wurden hinzugefügt. Es gilt die Risiken aus digitalen Technologien und der tiefen Kommunikation abzusichern.

Zur Umsetzung der Maschinenverordnung kann die IEC 62443, insbesondere der Teil 3, oder die kommende Norm EN 50742, die die relevanten Themen der IEC 62443-3 zusammenfasst, herangezogen werden.

NIS-2 Richtlinie

Die NIS-2 Richtlinie betrachtet die Security im Unternehmen selbst – also nicht um die Produkte, die das Unternehmen in Verkehr bringt. Die NIS-2 Richtlinie hat hierbei speziell Unternehmen im Bereich der Kritischen Infrastruktur im Fokus, aber – und das ist neu – auch eine Vielzahl von Unternehmen, die Zulieferer oder Dienstleister für kritische Infrastruktur sind, die sogenannten wesentlichen oder wichtigen Unternehmen.



Ziel der NIS-2 Richtlinie ist es die Informationssicherheit des Unternehmens als ganzes zu betrachten. Somit soll sichergestellt werden, dass weder eine Kritische Infrastruktur angegriffen werden kann noch Gefahren von den Dienstleistern oder Zulieferern auf die kritische Infrastruktur ausgehen können.

Zur Umsetzung von NIS-2 ist die ISO 27001 oder der BSI-Grundschutz relevant. Mit der Implementierung dieser Norm können die Anforderungen für viele Unternehmen erfüllt werden. Neben der NIS-2 Umsetzung spielt in Deutschland noch das KRITIS-Dachgesetz und das IT-Sicherheitsgesetz (2.0) eine wesentliche Rolle für Betreiber von kritischer Infrastruktur.

GESETZLICHE VERPFLICHTUNGEN: DIE RELEVANTEN NORMEN

Zur technischen Umsetzung der gesetzlichen Vorgaben existieren Normen, von denen einige bereits vor Inkrafttreten der genannten Verordnungen erstellt und daher im Vorfeld entwickelt wurden.

Die Notwendigkeit eines einheitlichen Rahmens und verlässlicher Verfahren für Industrial Security bestand bereits vor den aktuellen Verordnungen. Die Normen werden aktuell in EU-Gremien (z. B. CENELEC) an neue Vorgaben wie den CRA angepasst und bieten heute eine gute Orientierung für die Konformität von Produkten, Maschinen und Unternehmen.

IEC 62443

Als zentrale Norm im Bereich der industriellen Kommunikation befasst sich die internationale Normenreihe **IEC 62443** mit der Cybersicherheit von „Industrial Automation and Control Systems“ (IACS) und verfolgt dabei einen ganzheitlichen Ansatz für Betreiber, Integratoren und Hersteller.

Sie betrifft also alle, die an der Herstellung und dem Betrieb von Maschinen beteiligt sind. Entsprechende Verantwortlichkeiten für Maschinenbauer, Zulieferer und Endkunden werden dort definiert.

Aktuell teilt sich die **Norm in 4 Teile** auf. Während **Teil 1 Begrifflichkeiten** klärt und **generelle Konzepte** erläutert, betreffen die **Teile 2 bis 4** aus **Sicht** des **Produktherstellers**, des **Integrators/ Maschinenbauers** sowie des **Betreibers**.

Die IEC 62443 definiert die Cybersicherheit industrieller Automatisierungs- und Steuerungssysteme (IACS) mit einem ganzheitlichen Ansatz für Hersteller, Integratoren und Betreiber.

Wesentliche Bestandteile dieser Norm sowie anderer Normen für die IT oder Funkprodukte, sind der **risikobasierte Ansatz** und die Betrachtung der Security als immerwährender **Verbesserungsprozess**.

Der risikobasierte Ansatz zwingt einen Hersteller oder Anwender immer dazu, die tatsächliche Gefährdung einer Anwendung zu diskutieren und je nach Schutzbedarf angemessene Maßnahmen zu ergreifen.

Der Verbesserungsprozess fordert von allen Teilnehmern eine Disziplin, die Sicherheit der Anlage oder des Produkts fortwährend an neue Bedrohungen und Angriffsmöglichkeiten anzupassen.

Für einen Produkt- oder Maschinenhersteller fängt es mit dem Entwicklungsprozess an. In jeder Phase des Entwicklungsprozesses sind sowohl die Sicherheitsanforderungen als auch die daraus folgenden Maßnahmen zu betrachten und festzulegen.

In diesem Zusammenhang stellt sich die Frage, welchen Schutzbedarf das Produkt oder die Anlage überhaupt hat. Fragestellungen auf welche Art das Produkt oder die Maschine überhaupt eingesetzt wird und ob von der Maschine oder dem produzierten Gut eine Gefahr ausgehen kann, sind vorab zu klären.

In diesem Zusammenhang definiert die IEC 62443 den Begriff des Security Levels. Der Security Level legt fest, gegen wen wir uns absichern wollen.

Vom Gelegenheitshacker, der mal probieren will was möglich ist, bis zum gezielt eingesetzten staatlichen Akteur.



IEC 62443 SECURITY LEVELS
Industrial communication networks - Network and system security

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS Security Program Ratings	3-2	Security risk assessment and system design	4-2	Technical security requirements for ICAS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers				
		2-5	Implementation guidance for IACS asset owners				

End customer / Operator / Asset owner

Machine builder / Solution provider

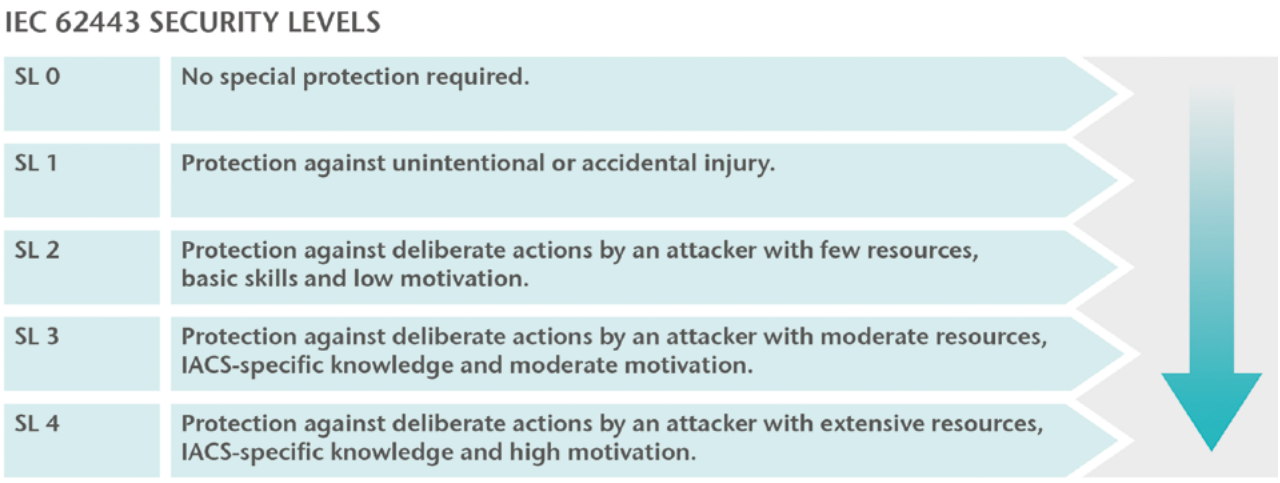
Product manufacturer

Im Anwendungsumfeld unserer Kunden sind je nach Produkt und Einsatzfall die Security Level 2 oder 3 relevant.

Speziell als Produkthersteller sind die zwei Teilbereiche der Norm 62443-4-1 und -4-2 zu betrachten. Im Teilbereich „-4-1“ geht es um den Entwicklungsprozess, die Risikobeurteilung, das Management der Sicherheitsanforderungen und die fortwährende Aufrechterhaltung der Sicherheit des Produkts. Im Teilbereich „-4-2“ geht es um die einzelnen technischen Maßnahmen, die zur Produktsicherheit funktional zu betrachten sind.

Den Entwicklungsprozess eines Herstellers kann man nach dem Teilbereich „-4-1“ zertifizieren lassen. Ein Produkt kann nach dem Teilbereich „-4-2“ zertifiziert werden. Ohne einen etablierten und zertifizierten Entwicklungsprozess gemäß „4-1“ ist eine Produktzertifizierung aber nur schwer machbar.

Derzeit wird die IEC 62443 in den europäischen Normungsgremien aktualisiert und erweitert. Ziel ist es, diese als harmonisierte Norm zur Erfüllung des CRA im industriellen Umfeld vollständig nutzten zu können.



ISO 27001 / BSI IT-Grundschutz

Die ISO 27001 Normenreihe ist bereits seit vielen Jahren eine etablierte Norm zur Implementierung und Betrieb eines ISMS (Informations-Sicherheits Management System) im Unternehmen. Der „IT-Grundschutz“ ist die vom BSI für Deutschland konkretisierte Umsetzung der Elemente des ISO 27001.

Ein ISMS soll sicherstellen, dass alle schützenswerten Informationen, Prozesse und IT-Systeme des Unternehmens dauerhaft vor Bedrohungen geschützt sind.

Mit der Implementierung eines ISMS gemäß ISO 27001 oder IT-Grundschutz sollten die wesentlichen Forderungen der NIS-2 Richtlinie erfüllt werden können.

SECURITY BEI HELMHOLZ: PRAXIS STATT THEORIE

Helmholz beschäftigt sich schon lange mit dem Thema Security. Nicht umsonst haben wir bereits seit über 10 Jahren Produkte wie die Firewall „WALL IE“ im Programm.

Was früher durch eine sicherheitsgerichtete Planung, Konzeption und PEN-Testing erreicht wurde, wird heute und in Zukunft durch einen Produktentwicklungszyklus gemäß IEC 62443-4-1 betrieben.

Security ist kein Zustand – sondern ein Prozess.

Umfassende Schulungen der Mitarbeiter, ein risikobasiertes Anforderungsmanagement für Produkt-Features und Funktionen sowie das gezielte Testen der Sicherheitsanforderungen gewährleisten die Entwicklung von sicheren Produkten.

Ein zentrales Element der IEC 62443 Norm als auch im Cyber Resilience Act, ist das Management von neuen Bedrohungen und neuen Sicherheitsrisiken. Was heute noch als sicher gilt, kann morgen schon kompromittiert sein. Als kontinuierliches Wachorgan gibt es bei Helmholz dafür das PSIRT-Team.

Das **Helmholz PSIRT-Team** besteht aus geschulten Experten im Haus, welche auf Sicherheitsmeldungen von Lieferanten, Behörden (z.B. dem BSI), Kunden oder anderen Akteuren im Sicherheitsumfeld (Schwachstellen-Melder) reagieren und alle Informationen zusammentragen, diese bewerten und Maßnahmen unverzüglich umsetzen.

Zertifizierung des Entwicklungsprozesses gemäß IEC 62443-4-1 durch den TÜV Nord.

Die Kommunikation nach außen (das Veröffentlichen von Meldungen und Advisories zu den Helmholz Produkten), betreiben wir in einer Partnerschaft mit dem CERT@VDE.

Im Gleichklang wie es auch viele andere große und kleine Marktbegleiter machen. Das CERT@VDE ist auch an der Normungsarbeit und den Verfahren zur Gesetzgebung beteiligt.

Helmholz ist Zulieferer von Netzwerkprodukten in viele Branchen, u.a. auch in den KRITIS nahen Bereich. Dadurch sind wir gemäß der **NIS-2** Richtlinie als **„wichtiges Unternehmen“** einzustufen. Die Umsetzung der hieraus resultierenden Anforderungen der NIS-2 Richtlinie sind für uns somit relevant und werden 2026 durchgeführt.

Unsere Partner zum Thema Sicherheit

Helmholz arbeitet im Bereich Industrial Security mit anerkannten Institutionen und Netzwerken zusammen, um höchste Standards in Produkt- und Informationssicherheit zu gewährleisten.

Unsere Partner unterstützen uns bei der kontinuierlichen Weiterentwicklung, Zertifizierung und im fachlichen Austausch zu aktuellen Sicherheitsanforderungen und Normen. Gemeinsam stellen wir sicher, dass unsere Lösungen den neuesten Richtlinien entsprechen und langfristig vertrauenswürdig bleiben.

Wir danken unseren Partnern für die enge Zusammenarbeit und das gemeinsame Engagement für mehr Sicherheit in der Industrie.

Unsere Partner:
Bundesamt für Sicherheit in der Informationstechnik (BSI) | VDE CERT | TeleTrusT | Secuvera | die Resilienz GmbH

Bundesamt für Sicherheit in der Informationstechnik

VDE CERT

TeleTrusT Pioneers in IT security.

secuvera: Cybersicherheit. Nachhaltig.

die RESILIENZ GmbH

CRA READY: SO BEREITET HELMHOLZ SEINE PRODUKTE VOR

Die in diesem Dokument genannten gesetzlichen Vorgaben und die hierbei relevanten Normen adressieren immer Komponenten mit „digitalen Elementen“ und einer Kommunikationsschnittstelle.

Im Produktportfolio der Firma Helmholz sind dies alle **Produkte mit einer Kommunikationsschnittstelle**, wie Ethernet, USB oder auch Funk. Insbesondere Produkte mit eingebauter Software und einer Kommunikationsmöglichkeit sind hier vorrangig zu betrachten.

Mechanische- oder elektromechanische Komponenten wie bspw. Stecker und Kabel, sind hiervon nicht betroffen. Auch Produkte, die zur Verarbeitung von digitalen oder analogen Signalen gedacht sind und keine Kommunikationsschnittstellen haben, fallen nicht unter diese Regulierungen.

Ab dem Zeitpunkt des Inkrafttretens des Cyber Resilience Act können Produkte, die bereits abgekündigt sind, auch weiterhin als **Ersatzteile** verkauft werden. Die sicherheitsrelvante Betrachtung dieser Produkte obliegt dann dem Anwender der Produkte in seiner Maschine oder Anlage. Bei Ersatzteilen sind zusätzliche Sicherheitsmaßnahmen im Maschinen- oder Netzwerkdesign notwendig.

Alle Produkte, die unter die Regulierung des CRA fallen, werden von Helmholz nach und nach gemäß den Vorgaben der Norm IEC 62443-4-2 angepasst. Der Entwicklungsprozess bei Helmholz arbeitet dabei gemäß IEC 62443-4-1.

Ziel ist es bis zum Inkrafttreten des CRAs im Dezember 2027 alle Produkte mit einer erweiterten CE-Erklärung ausstatten zu können. Eine Produktzertifizierung der meisten Helmholz Produkte bei einer notifizierten Stelle ist voraussichtlich nicht notwendig. Produkte, die im Zentrum der Security-Infrastruktur einer Anlage stehen, wie z.B. WALL IE, den Routern oder den managed Switchen, werden aber eine 62443-4-2 Zertifizierung erhalten.

CYBER RESILIENCE ACT: DIE WICHTIGSTEN FRAGEN IM ÜBERBLICK

Der Cyber Resilience Act stellt neue Anforderungen an die Cybersicherheit digitaler Produkte. Die folgenden Fragen und Antworten erläutern die wichtigsten Regelungen und Pflichten.

Was bedeutet „CRA-konform“ bei einem Produkt?
Ein CRA-konformes Produkt erfüllt die grundlegenden Cybersecurity-Anforderungen des CRA, wurde einer Cybersecurity-Risikoanalyse unterzogen und verfügt über Prozesse zur Behandlung von Schwachstellen und Sicherheitsupdates.
Nach erfolgreicher Konformitätsbewertung wird die Konformität in der EU-Konformitätserklärung dokumentiert und das Produkt entsprechend CE-gekennzeichnet.
Alle Produkte, die unter den CRA fallen und ab dem 11. Dezember 2027 in der EU in Verkehr gebracht werden (verkauft werden!), müssen den CRA einhalten.

Müssen bereits installierte Helmholz-Produkte ausgetauscht werden?
Nein! Der CRA führt grundsätzlich nicht dazu, dass bereits installierte Produkte ausgetauscht werden müssen. Produkte, die vor dem 11. Dezember 2027 verkauft wurden, unterliegen grundsätzlich nicht rückwirkend den Produktanforderungen des CRA.
Eine wesentliche Änderung am Produkt nach diesem Zeitpunkt kann jedoch eine erneute Bewertung erforderlich machen.

Werden alle Helmholz-Produkte CRA haben?
Alle vom CRA betroffenen aktuellen Helmholz-Produkte werden den CRA erfüllen.

Ab wann erfüllen Helmholz-Produkte den CRA?
Alle aktuellen Helmholz Produkte werden ab dem 11. Dezember 2027 die für sie geltenden Anforderungen des Cyber Resilience Act erfüllen.

Werden die Produkte für den CRA überarbeitet?
Ja, viele Produkte erhalten ein Redesign.
Die Produkte werden modernisiert und auf eine technisch moderne Plattform aufgesetzt. Form und Funktion werden dabei erhalten bleiben.
Die neue Plattform ermöglicht dann einen längeren Supportzeitraum.

Was passiert mit den alten Produkten?
Die Produktvarianten, die von einem Redesign betroffen sind, werden dann zeitnah abgekündigt.
Die abgekündigten Produkte erhalten aber weiterhin Sicherheitspatches und können nach Ende 2027 auch noch als Ersatzteile bezogen werden.
Der CRA enthält hierfür eine ausdrückliche Ersatzteilregelung.

Gibt es Produkte, die mit dem CRA nicht mehr verfügbar sein werden?
Es gibt einige sehr alte Produkte (z.B. MPI-Adapter oder CAN 300 PRO), die ab Ende 2027 nur noch als Ersatzteil lieferbar sein werden.
Eine Liste dieser Produkte wird zeitnah veröffentlicht.

Wie ist der Supportzeitraum für die Produkte?
Der Supportzeitraum wird im Rahmen der CRA-Konformitätsbewertung für jedes Produkt festgelegt und dokumentiert.
Aktuell streben wir einen Supportzeitraum von ca. 8-10 Jahren ab Produktrelease an.
Der Supportzeitraum wird als festes Datum dokumentiert werden, z.B. „dieses Produkt erhält Sicherheitsupdates bis 31.12.2035“.
Helmholz kann den ursprünglich festgelegten Supportzeitraum für jedes Produkte später freiwillig verlängern, z.B. bei Funktionserweiterungen.

Was passiert nach Ende des Security-Supportzeitraums?
Nach dem veröffentlichten Ende des Security-Supportzeitraums besteht keine Verpflichtung mehr seitens Helmholz zur Bereitstellung neuer Sicherheitsupdates.
Helmholz empfiehlt deshalb, das Produkt rechtzeitig durch ein weiterhin unterstütztes Nachfolge-Produkt zu ersetzen oder geeignete kompensierende Schutzmaßnahmen vorzusehen.

Wo ist die Produktsicherheit dokumentiert?
Die sichere Verwendung ist im „Security Guideline“ des Produktes dokumentiert, welches im Handbuch des Produktes oder als eigenständiges Dokument zu finden ist.
Im Security Guideline dokumentiert, unter welchen Rahmenbedingungen das Produkt sicher verwendet werden kann (Intended-use), welche Sicherheitsfähigkeiten das Produkte hat und wie diese zu konfigurieren sind.

Was muss der Kunde für einen sicheren Betrieb tun?
Der CRA betrachtet Produktsicherheit und sicheren Betrieb gemeinsam. Produkte müssen entsprechend ihrer vorgesehenen Verwendung eingesetzt, sicher konfiguriert und in eine geeignete Netzwerkarchitektur integriert werden. Hinweise hierzu enthält der jeweilige Security Guideline.

Wo finde ich Schwachstellenmeldungen zu den Produkten?
Schwachstellenmeldungen zu den Helmholz-Produkten werden über das CERT@VDE (https://cert-vde.com/de/advisories/vendor/helmholz/) als Advisory veröffentlicht.

Wo finde ich Firmwareupdates?
Die aktuellen Firmwareversionen sind auf Helmholz Webseite unter dem jeweiligen Produkt zu finden.
Helmholz unterscheidet nicht zwischen Sicherheitsupdates und Funktionsupdates.

Gibt es zu jeder Schwachstelle ein Firmwareupdate?
Eine Schwachstelle muss laut CRA nicht unbedingt durch ein Firmwareupdate gelöst werden. Je nach Schwachstelle kann das Risiko auch durch kompensatorische Maßnahmen außerhalb des Produktes gelöst werden.
Kompensatorische Maßnahmen können z.B. eine Veränderung der Konfiguration sein oder eine andere Anbindung des Produktes im Netzwerk.
Eine solche Lösung wird dann ebenfalls in einem Advisory und im Produkthandbuch dokumentiert.

Sind Security-Updates kostenpflichtig?
Sicherheitsupdates zur Behandlung von Schwachstellen werden grundsätzlich kostenfrei bereitgestellt.

Wie kann ich Schwachstellen an Helmholz melden?
Festgestellte oder vermutete Schwachstellen an Helmholz Produkten können jederzeit an das PSIRT-Team (psirt@helmholz.de, https://www.helmholz.de/service-support/service/security-psirt) gemeldet werden. Alternativ ist auch eine Meldung über das CERT@VDE möglich.

Liefert Helmholz eine SBOM zum Produkt?
Helmholz erstellt und pflegt für relevante Produkte eine Software Bill of Materials (SBOM) als Bestandteil der internen technischen Dokumentation und zur Schwachstellenüberwachung.
Eine öffentliche Bereitstellung oder standardmäßige Lieferung der SBOM an Kunden ist durch den CRA nicht vorgeschrieben und von Helmholz derzeit nicht vorgesehen.
Gegenüber zuständigen Behörden (z.B. dem BSI) wird die SBOM im Rahmen der gesetzlichen Verpflichtungen bereitgestellt.

Wie entwickelt Helmholz sicher?
Helmholz entwickelt die Produkte in einem sicherem Entwicklungsprozess gemäß IEC/EN 62443-4-1 und den darüber hinaus gehenden Anforderungen des CRA. Die Zertifizierung des Entwicklungsprozesses wird aktuell vom TÜV Nord durchgeführt.
Helmholz entwickelt die Produkte vollständig (Hardware und Software) im eigenen Haus und produziert auch in eigener Fertigung. Somit kann die Sicherheit der Produkte durch die ganze Entwicklung bis zur Fertigung sichergestellt werden.

Welche Norm gilt für die Produkte?
Alle unter den CRA fallenden Produkte werden gemäß IEC/EN 62443-4-2 entwickelt.

Welchen Security-Level haben die Produkte gemäß 62443-4?
Alle unter den CRA fallenden Produkte haben mindestens Security-Level 2 (SL-2).

Wie betrachtet man „Legacy“ Protokolle?
Alte Protokolle (z.B. ModbusTCP oder RFC1006) können aus technischen Gründen und aufgrund der Kompatibilität zu vorhandenen Kommunikationspartnern nicht „sicher“ gemacht werden.
Bei der Verwendung diese Protokolle müssen die Netzwerke durch den Maschinenplaner oder den

Kunden abgesichert werden, z.B. durch eine Firewall und strikte Zugriffsbeschränkungen auf die betroffenen Geräte.

Wie sicher ist Helmholz als Unternehmen?
Helmholz ist „Wichtiges Unternehmen“ nach NIS-2. Eine entsprechende ISO 27001 Zertifizierung ist für 2027 vorgesehen.

EU-MASCHINENVERORDNUNG: WAS MASCHINENBAUER WISSEN MÜSSEN

Die neue EU-Maschinenverordnung rückt die Cybersicherheit von Maschinen stärker in den Fokus. Die folgenden Fragen und Antworten geben einen Überblick über die wichtigsten Anforderungen.

Was hat die neue Maschinenverordnung mit Cybersecurity zu tun?
Manipulationen oder unbeabsichtigte Veränderungen von Hardware, Software oder Netzwerkkommunikation dürfen nicht dazu führen, dass Sicherheitsfunktionen einer Maschine beeinträchtigt werden.
Die Maschinenverordnung betrachtet Cybersecurity also insbesondere dort, wo ein Cyberangriff Auswirkungen auf die funktionale Sicherheit haben kann.

Was ist der Unterschied zwischen CRA und Maschinenverordnung?
Der CRA adressiert die Cybersecurity eines Produkts mit digitalen Elementen über seinen Lebenszyklus.
Die Maschinenverordnung adressiert dagegen die Sicherheit der Maschine.
Cybersecurity wird dort relevant, wenn Manipulationen die Sicherheit der Maschine beeinträchtigen können.
Beide Rechtsakte können daher gleichzeitig relevant sein.

Wenn ein Helmholz-Produkt CRA-konform ist, ist dann automatisch auch die Maschine konform mit der Maschinenverordnung?
Nein. Ein CRA-konformes Kommunikationsprodukt kann einen Beitrag zur sicheren Maschine leisten, ersetzt aber nicht die Risikobeurteilung und Konformitätsbewertung der Gesamtmaschine.

Welche Verantwortung hat der Maschinenbauer beim Einsatz eines Routers, Switches oder einer Firewall?
Der Maschinenbauer muss im Rahmen seiner Risikobeurteilung bewerten, ob eine Manipulation des Kommunikationssystems Auswirkungen auf Sicherheitsfunktionen oder andere sicherheitsrelevante Funktionen der Maschine haben kann.
Die sicheren Produkte von Helmholz ermöglichen dies durch umfangreiche Sicherheitsfunktionen und eine entsprechende Dokumentation.

Muss jede Netzwerkkomponente einer Maschine besondere Security-Funktionen besitzen?
Nicht zwangsläufig. Entscheidend ist die Funktion innerhalb der Maschine und das daraus resultierende Risiko.
Eine einfache Netzwerkkomponente kann beispielsweise durch Netzwerksegmentierung, Firewalling oder andere organisatorische und technische Maßnahmen abgesichert werden.

Sind PROFINET, Modbus TCP oder andere unverschlüsselte Industrieprotokolle nach der Maschinenverordnung noch zulässig?
Grundsätzlich ja. Die Maschinenverordnung verbietet solche Protokolle nicht. Der Maschinenhersteller muss aber berücksichtigen, welche Risiken durch Manipulation oder unberechtigten Zugriff entstehen können, und gegebenenfalls geeignete Schutzmaßnahmen vorsehen.

Muss eine Maschine künftig eine Firewall besitzen?
Nein, die Verordnung schreibt keine bestimmte Technologie vor.
Je nach Risikobeurteilung sind eine Firewall, die Netzwerksegmentierung oder Zugriffskontrolle aber sehr geeignete Schutzmaßnahmen.

Welche Rolle spielen Security Guidelines von Helmholz bei der Maschinenkonformität?
Die Security Guideline kann dem Maschinenbauer Informationen zur sicheren Integration und Konfiguration liefern. Die Verantwortung für die Risikobeurteilung der Maschine verbleibt jedoch beim Maschinenhersteller.

Was bedeutet eine „wesentliche Veränderung" einer Maschine?
Die neue Verordnung definiert ausdrücklich die „substantial modification".
Eine nicht vom ursprünglichen Hersteller vorgesehene physische oder digitale Änderung kann wesentlich sein, wenn sie ein neues Sicherheitsrisiko erzeugt oder ein bestehendes Risiko erhöht und dadurch neue wesentliche Schutzmaßnahmen erforderlich werden, zum Beispiel die Aktivierung eines Übertragungsprotokolls.
Derjenige, der eine solche Änderung durchführt, kann dadurch selbst zum Hersteller im Sinne der Maschinenverordnung werden.

Kann auch ein Firmware- oder Softwareupdate eine wesentliche Veränderung einer Maschine darstellen?
Ja, grundsätzlich können auch digitale Veränderungen relevant sein. Entscheidend ist, ob dadurch die Sicherheit der Maschine beeinflusst wird.
Ein normales Security-Update ist deshalb nicht automatisch eine wesentliche Veränderung.
Die Beurteilung hängt von den weiteren Änderungen an der Firmware und von deren Auswirkungen auf die Maschine ab.

Führt ein Firmwareupdate eines Helmholz-Gerätes dazu, dass die gesamte Maschine neu CE-bewertet werden muss?
Normalerweise nicht allein aufgrund des Updates. Der Maschinenbetreiber bzw. Maschinenhersteller muss jedoch bewerten, ob die Änderung in der Firmware Auswirkungen auf die Sicherheit der Maschine hat.
Insbesondere reine Wartungs- oder Reparaturmaßnahmen, welche die Einhaltung der Sicherheitsanforderungen nicht beeinflussen, gelten nicht automatisch als wesentliche Veränderung.

Wer trägt die Verantwortung, wenn der Betreiber eine Maschine nachträglich verändert?
Führt ein Unternehmen eine wesentliche Veränderung durch, kann es für die betroffene Maschine die Herstellerpflichten übernehmen und muss gegebenenfalls eine neue Konformitätsbewertung durchführen.

Welche Bedeutung haben Fernzugänge für die Maschinenverordnung?
Remote-Zugänge sollten so ausgelegt und betrieben werden, dass unberechtigte Zugriffe oder Manipulationen keine sicherheitsrelevanten Funktionen beeinträchtigen können.
Gerade bei Routern und Fernwartungslösungen sind Authentifizierung, Zugriffsbeschränkung und sichere Konfiguration deshalb relevante Maßnahmen.
Die Helmholz Produkte stellen alle erforderlichen Funktionen für einen sicheren Fernwartungsbetreib zur Verfügung.

Muss der Maschinenbauer Security-Updates von Komponenten installieren?
Es gibt keine einfache pauschale Pflicht, jedes Update unmittelbar einzuspielen. Der Betreiber bzw. Hersteller muss jedoch sicherstellen, dass die Maschine weiterhin sicher betrieben wird.
Ein bekanntes Cybersecurity-Problem mit möglicher Auswirkung auf die Maschinensicherheit muss daher in der Risikobetrachtung berücksichtigt werden. Daraus kann abgeleitet werden, ob die Sicherheit der Maschine überhaupt betroffen ist und mit welcher Dringlichkeit Maßnahmen, wie z.B. ein Firmwareupdate ergriffen werden muss.

Was passiert, wenn eine bekannte Schwachstelle in einer Komponente nicht behoben werden kann?
Wenn daraus ein relevantes Risiko für die Maschinensicherheit entsteht, können technische oder organisatorische Maßnahmen erforderlich sein – beispielsweise eine neue Netzwerksegmentierung, Zugriffsbeschränkung oder der Austausch der Komponente.

Welche Informationen stellt Helmholz dem Maschinenbauer für seine Risikobeurteilung zur Verfügung?
Die sichere Verwendung und Konfiguration der Produkte ist im jeweiligen Security Guideline der Helmholz-Produkte dokumentiert.
Sicherheits-Advisories zu den Produkten sind beim CERT@VDE (https://certvde.com/de/advisories/vendor/helmholz/) zu finden.
Aktuelle Firmware-Updates können jederzeit kostenfrei auf der Helmholz-Produktseite des jeweiligen Produktes heruntergeladen werden.

Welche Rolle spielt IEC 62443 bei der Maschinenverordnung?
IEC 62443 kann als technischer Rahmen für Industrial Cybersecurity und insbesondere für Defense-in-Depth, sichere Komponenten und sichere Systemarchitekturen dienen.
Insbesondere der Teil 3 der IEC 62443 dient zur Orientierung für den Maschinenbauer. Sie ersetzt aber nicht automatisch die Konformitätsbewertung nach der Maschinenverordnung.

Helmholz GmbH & Co. KG | Hannberger Weg 2 | 91091 Großenseebach | Germany
Phone +49 9135 7380-0 | Fax +49 9135 7380-110 | info@helmholz.de | www.helmholz.de

Änderungen und Irrtümer vorbehalten. 11-2026