OVE
Österreichischer Verband für Elektrotechnik

10. Oktober 2023,
Haus der Ingenieure

100 years of passion for technology and innovation

Welcome

zur Tagung

Cybersicherheit industrieller Automatisierungssysteme

PHOENIX CONTACT

Cyber Resilience Act - Critical Class I/II

(CRA)

Zu Deutsch, das „Cyber-Resilienz-Gesetz“

(Cyber – Cyberkriminalität - Angriffe auf Informations- und Kommunikationstechnik)

(Resilienz - Widerstandskraft oder Fähigkeit auf schwierige Situationen zu reagieren)

(Gesetz /Verordnung - verbindlicher Rechtsakt, den alle EU-Länder umsetzen müssen)

EUROPÄISCHE KOMMISSION

Die Europäische Kommission veröffentlichte

am 15. September 2022 den

Cyber Resilience Act – Entwurf.

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

und zur Änderung der Verordnung (EU) 2019/1020

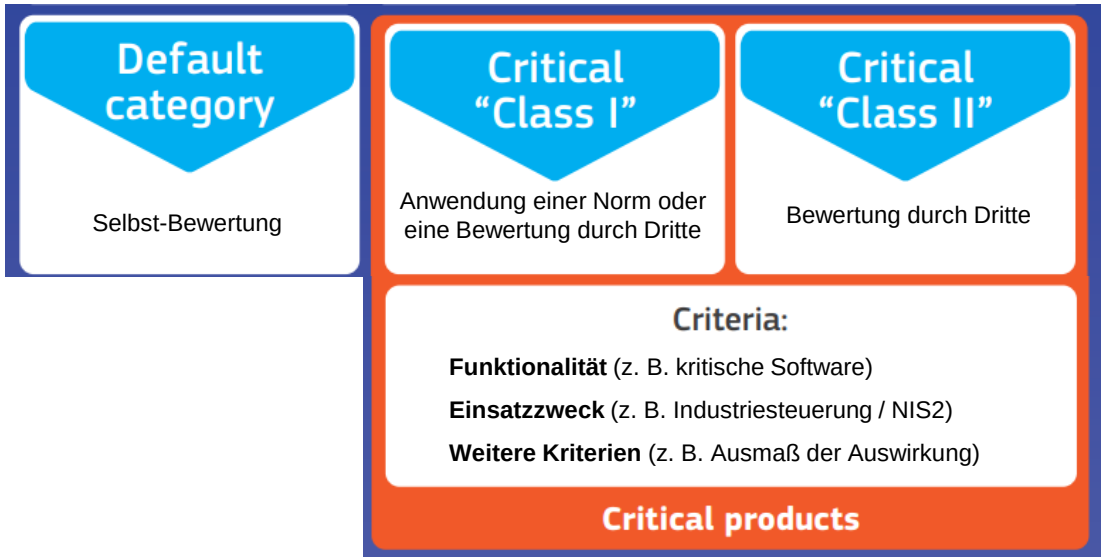
PHOENIX CONTACT

Cyber Resilience Act - Critical Class I/II

Der CRA bezieht sich auf

„Produkte mit digitalen Elementen, deren beabsichtigte oder vernünftigerweise vorhersehbare Verwendung in einer direkten oder indirekten logischen und/oder physischen Verbindung zu einem Gerät oder Netzwerk umfasst“

Dabei handelt es sich um die Cyberkriminalitäts-Beständigkeit sämtlicher Software-, sowie Hardwareprodukte mit Datenkommunikations-Möglichkeiten.



Cyber Resilience Act - Critical Class I/II

Der CRA-E fordert

„die Schaffung der Bedingungen für die Entwicklung sicherer Produkte mit digitalen Elementen, damit Hardware- und Softwareprodukte mit weniger Schwachstellen in Verkehr gebracht werden und damit die Hersteller sich während des gesamten Lebenszyklus eines Produkts ernsthaft um die Sicherheit kümmern“.

Des Weiteren wird,

„es den Nutzern ermöglichen, bei der Auswahl und Verwendung von Produkten mit digitalen Elementen die Cybersicherheit zu berücksichtigen“.

Wie entsteht ein solches Gesetz das Normen für ein Konformitätsbewertungsverfahren zur CE-Kennzeichnung harmonisiert (hENs)

Nach Aufforderung der EU-Kommission an die europäischen Normungs-Organisationen der CEN / CENELEC entsenden nationale Normungsorganisationen, wie ÖVE und ASI - Austrian Standards International, bzw. Deutschland DIN und DKE sogenannte “Experten”. Ich wurde von den Österreichischen Gremium der ASI als ISO-Expert an die WG 9 "Special Working Group on Cyber Resilience Act" entsandt, da ich unter anderem auch in der ÖVE als IEC-Expert tätig bin und an der ISA/IEC 62443 Norm mitarbeite.

Wir als SWG Cyber Resilience Act arbeitet nun an den „Draft Standardization Request“ (SReq) der in 3 Teile gefasst ist:

Teil 1: Die Einleitung des Cyber Resilience Act Entwurfs, was sich die Kommission von der Erarbeitung von Normen oder die Revision existierender Normen von CEN / CENELEC erwartet.

Teil 2: Im Anhang I, werden detailliert die Inhalte der zu erstellenden / revidierenden Normen aufgelistet.

I. **Produktübergreifende Security Anforderungen** (12 Horizontale = Generic / bis 05/2025)

II. **Produktspezifische Security Anforderungen** (33 Vertikale = Products, wie SPS/PLC, Firewall, IoT / bis 05/2026)

III. **Anforderungen an ein Schwachstellen Management** (bis 05/2025)

Teil 3: Der Anhang II enthält formale und inhaltliche Anforderungen, die die entwickelten / revidierten Normen erfüllen müssen. Das sind durchaus sehr konkrete inhaltliche Vorgaben — etwa die Notwendigkeit, Anforderungen für sichere **Softwareentwicklung und SBOMs** zu definieren.

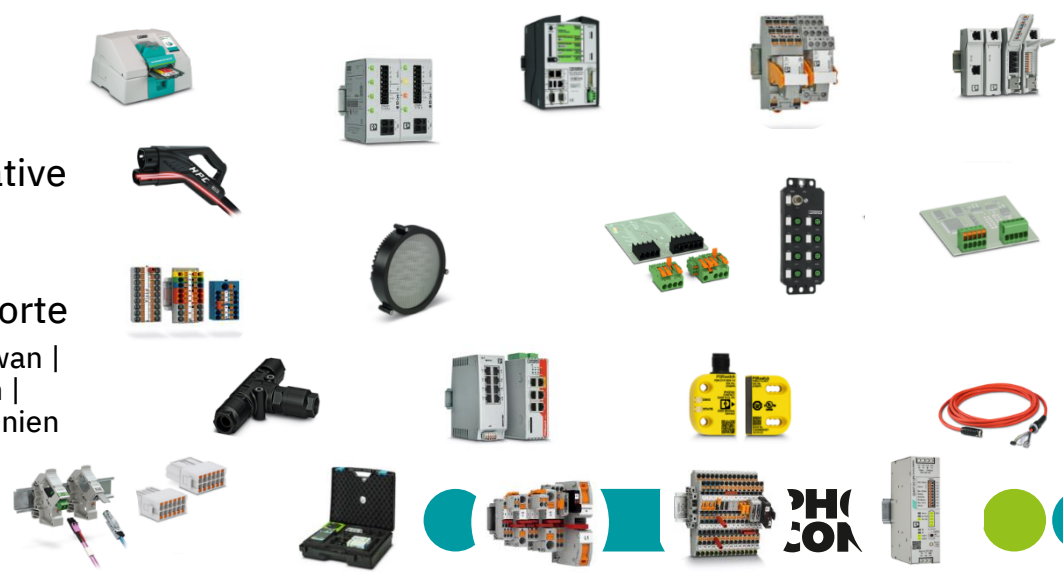
Phoenix Contact Österreich

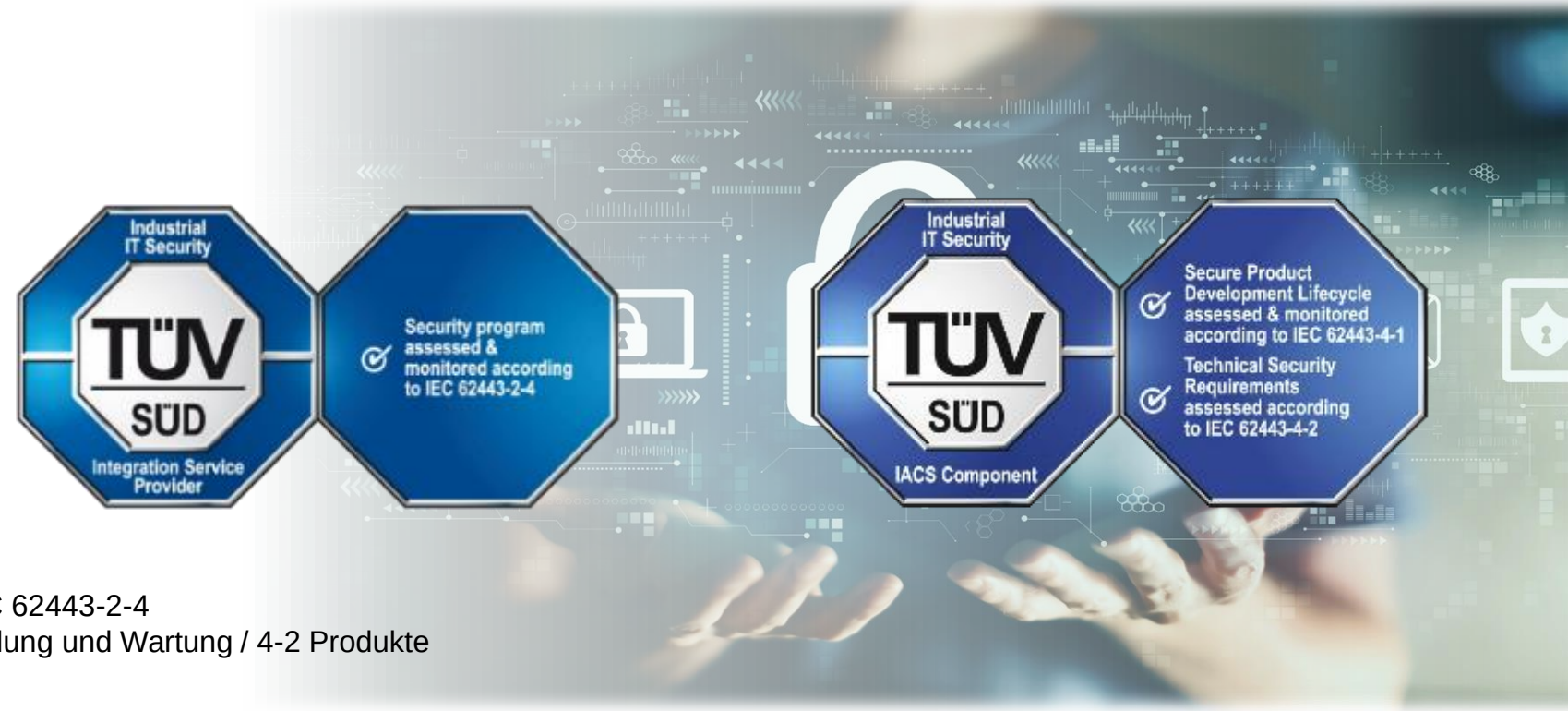
Wir sind ein Familienunternehmen mit Stammsitz in Deutschland und weltweit Marktführer und Innovationsträger für Elektrifizierung, Vernetzung und Automatisierung auf dem Weg in eine smarte Welt.

Über **100.000** innovative Produkte

11 Produktionsstandorte

Deutschland | China | Taiwan | Indien | Polen | Schweden | Schweiz | Türkei | Argentinien Griechenland | USA





Phoenix Contact Österreich

TÜV zertifizierter OT-Security Dienstleister gemäß IEC 62443-2-4
International zertifiziert gemäß IEC 62443-4-1 Entwicklung und Wartung / 4-2 Produkte

Organisationen:

ASI - Austrian Standards International

ISO-Expert der AG 001.27 Information Security, Cybersecurity and Privacy Protection
CEN/CLC/JTC 13 - Cybersecurity and Data Protection
JTC 13/WG 9 "Special Working Group on Cyber Resilience Act"

OVE - Österreichischer Verband für Elektrotechnik

IEC-Expert TSK MR65 Industrielle Prozess-, Mess-, Regelungs- u. Steuerungstechnik
Stellv. Vorsitzender OVE AG MR65 Industrial Automation & Control Systems Security (z.B. IEC 62443)

Supply-Chain-Attacks

Ist ein Cyberangriff, der auf eine Schwachstelle in der Lieferkette (Supply Chain) abzielt. Dabei nutzen die Angreifer das Vertrauen aus, das ein Unternehmen einem Drittanbietern entgegen bringt. Es ist eine Art Insel-Hopping-Attacke um das Ziel über einen schlecht abgesicherten Lieferanten oder Produkten zu erreichen.

Kaseya

Einer der größten Hackerangriffe der vergangenen Jahre beeinträchtigte IT-Systeme zahlreicher Unternehmen. Weltweit seien über 1500 Unternehmen betroffen gewesen.

Zuerst waren dies überwiegend amerikanischen Unternehmensnetzwerke, wirkte sich aber auch bald in Europa aus.

Die VSA-Software von Kaseyas dient der Fernüberwachung und -steuerung, Patch-Management, Netzwerküberwachung, Prozessautomatisierung, Backup und mehr.

Eine Hackergruppe erlangte damals über eine ungepatchte Zero-Day-Schwachstelle Zugriff auf deren Server. Nachdem sie Zugang hatten, erstellten die Angreifer ein gefälschtes, bösartiges automatisches Update mit dem Namen **“Kaseya VSA Agent Hot-fix”** und spielten es auf den Servern der Kunden ein.

Die EU-Kommission begründet nun unter anderem auch wegen des Kaseya-Vorfalls die Notwendigkeit eines
Cyber Sicherheitsgesetz Gesetzes, um Lieferanten in die Pflicht zu nehmen.

PHOENIX CONTACT

EUROPÄISCHE
KOMMISSION

Hardware- und Softwareprodukte sind zunehmend Gegenstand erfolgreicher Cyberangriffe, was bis 2021 zu geschätzten jährlichen **Kosten der Cyberkriminalität in Höhe von 5,5 Milliarden EUR** führt.

Diese Produkte leiden unter zwei großen Problemen, die den Nutzern und der Gesellschaft Kosten verursachen:

1. ein niedriges Cybersicherheitsniveau, …..
2. unzureichendes Verständnis und unzureichenden Zugang zu Informationen für die Nutzer, ….

https://digital-strategy.ec.europa.eu/de/library/cyber-resilience-act

NIS-2 Richtlinie - mindestmaßnahmen für ein Risikomanagement:

- Konzept Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- **Sicherheit der Lieferkette**
- **Sicherheitsmaßnahmen bei Erwerb/Entwicklung/Wartung von IKT**
  (Informations- und Kommunikationstechnologie)
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
- Cyberhygiene und Schulungen zur Cybersicherheit
- Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle
- Multi-Faktor-Authentifizierung

PHOENIX CONTACT

https://www.wko.at/service/innovation-technologie-digitalisierung/nis2-uebersicht.html

Welche Maßnahmen können die Sicherheit der Lieferkette und von Produkten nachweisen?

- **Zertifizierungen relevanter Standards/Normen:**
  Unternehmen können Zertifizierungen gemäß international anerkannten Standards wie **ISO/IEC 27001** (Informationssicherheits-management) und/oder **IEC 62443** (IT-Sicherheit industrieller Automatisierung und Steuerungssysteme) durchführen. Diese Zertifizierungen bestätigen die Einhaltung von Security Standards und können als Nachweis für die Sicherheit in der Lieferkette dienen.

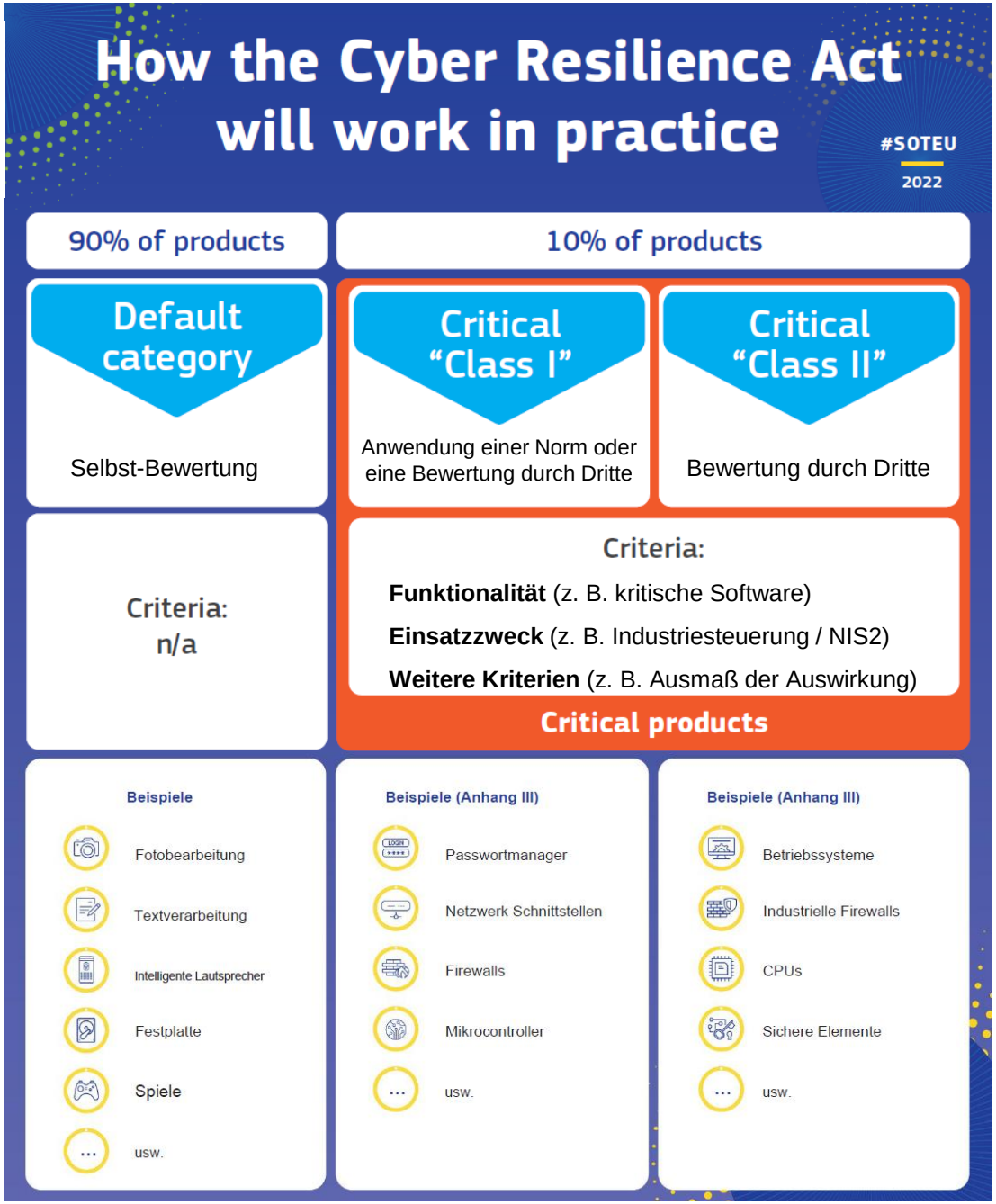
- **Ratings und Bewertungen:**
  Cyber Risk Ratings, wie das KSÖ (Kompetenzzentrum Sicheres Österreich) Cyber Risk Rating, bewerten die Security Maßnahmen von Unternehmen anhand verschiedener Faktoren. Diese Bewertungen können als Indikator für die Sicherheit der Lieferkette dienen und potenziellen Partnern oder Kunden vermitteln, wie sicher Ihr Unternehmen und Ihre Lieferanten sind.

- **Eigene Audits und Prüfungen:**
  Regelmäßige Security Audits und Prüfungen können durchgeführt werden, um die **Security Maßnahmen von Lieferanten zu überprüfen**. Diese Audits können von internen oder externen Fachleuten durchgeführt werden, um die Einhaltung der **Security Anforderungen zu verifizieren**.

- **Externen Prüfungsorganisationen:**
  Die Zusammenarbeit mit unabhängigen Dritten, wie Security Beratern oder **Prüfungsgesellschaften**, kann dazu beitragen, die Sicherheit der Lieferkette zu bewerten und zu gewährleisten. Diese externen Fachleute können unvoreingenommene Einschätzungen abgeben.

Empfehlungen für Lieferantenbeziehungen / Verträge:
Implementieren Sie Security Anforderungen in **Lieferantenverträgen. Verlangen Sie von Lieferanten Nachweise derer Security Maßnahmen und Compliance nach relevanten Industrie Security Standards/Normen**.

EUROPÄISCHE KOMMISSION



Pflichten des Herstellers nach CRA (Wunsch der Kommission)

Cybersicherheit wird in **der Planungs-, Design-, Entwicklungs-, Produktions-, Liefer-** und **Wartungsphase** berücksichtigt.

Alle **Cybersicherheitsrisiken** werden dokumentiert.

Hersteller müssen **aktiv ausgenutzte Schwachstellen und Vorfälle melden.**

Nach dem Verkauf müssen Hersteller sicherstellen, dass Schwachstellen während der **erwarteten Produktlebensdauer** oder für einen Zeitraum von fünf Jahren (je nachdem, welcher Zeitraum kürzer ist) **effektiv behandelt werden.**

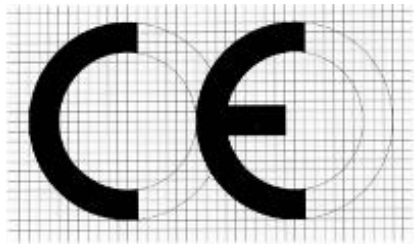
Klare und verständliche Anleitungen zur Nutzung von Produkten mit digitalen Elementen.

Sicherheitsupdates müssen **für mindestens fünf Jahre verfügbar** sein .

Harmonisierte Regeln zur Sorgfaltspflicht für den gesamten Lebenszyklus von Produkten mit digitalen Elementen.

https://digital-strategy.ec.europa.eu/de/library/cyber-resilience-act

CE-Kennzeichnung als Abkürzung für “Conformité Européenne”



Mit der Anbringung der CE-Kennzeichnung wird erklärt, dass das Produkt allen anzuwendenden Vorschriften der Europäischen Union entspricht und die entsprechenden **Konformitätsbewertungsverfahren** durchgeführt wurden.

- Maschinenrichtlinie 2006/42/EG / Maschinenverordnung (EU) 2023/1230
- Verordnung (EU) Nr. 2016/426 über Geräte zur Verbrennung gasförmiger Brennstoffe (Gasgeräte)
- Aufzüge-Sicherheitsverordnung 2015 – ASV 2015
- Sportbooteverordnung 2015 – SpBV 2015
- **Verordnung (EU) Nr. 2016/425 über persönliche Schutzausrüstungen (PSA)**

Alle Sonnenbrillen tragen ein CE-Kennzeichen.

Die aktuelle EU-PSA-Verordnung (**EU 2016/425**) harmonisierter Standard für Sonnenbrillen ist die Version EN **ISO 12312-1**:2013/A1:2015.

Nach dieser Norm wird ein **Konformitätsbewertungsverfahren** durchgeführt.

Zukünftig gilt dies für „**Produkte mit digitalen Elementen, deren beabsichtigte oder vernünftigerweise vorhersehbare Verwendung eine direkte oder indirekte logische oder physische Verbindung zu einem Gerät oder Netzwerk umfasst**“ ebenfalls.

Vertikale Themen – IACS Normen (10% - Kritische Klasse I/II)

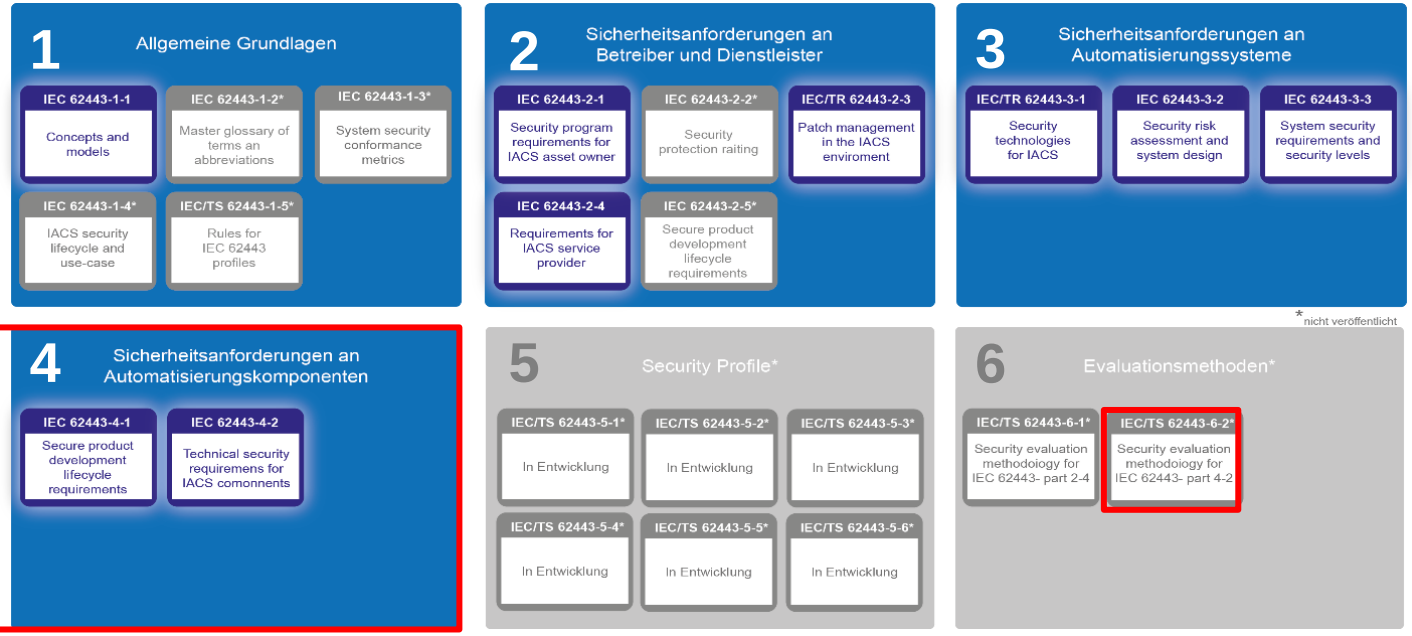
International Electrotechnical Commission

IEC 62443 ist ein internationaler Cybersicherheitsstandard für industrielle Automatisierungs- und Steuerungssysteme.

International Society of Automation

- **Betreiber**
  (Industrie Anlagen, Energie-, Verkehrstechnik,..)
- **OT-Systemintegrator**
  (Industrie Dienstleister zur Integration und Wartung)
- **Produkt Hersteller**
  (Industrie Netzwerke, Hardware und Software)

IEC 62443 Dokumenten-Struktur



Vertikale Themen – IACS Normen (10% - Kritische Klasse I/II)

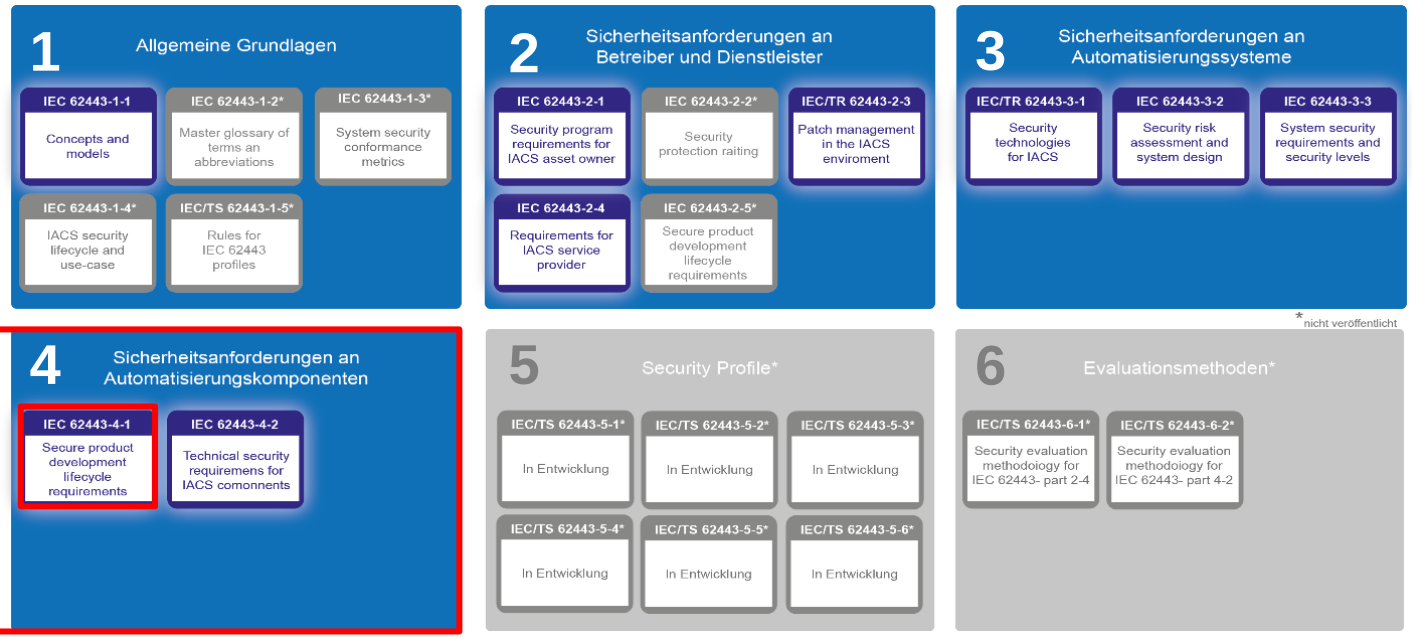
International Electrotechnical Commission

IEC 62443 ist ein internationaler Cybersicherheitsstandard für industrielle Automatisierungs- und Steuerungssysteme.

International Society of Automation

- **Betreiber**
  (Industrie Anlagen, Energie-, Verkehrstechnik,..)
- **OT-Systemintegrator**
  (Industrie Dienstleister zur Integration und Wartung)
- **Produkt Hersteller**
  (Industrie Netzwerke, Hardware und Software)

IEC 62443 Dokumenten-Struktur



IEC 62443-4

Sicherheitsanforderungen an Automatisierungskomponenten

IEC 62443 Kapitel 4 Absatz 1:

Anforderungen an den Entwicklungsprozess von Produkten, die in diese Systeme eingebaut werden sollen. Unter "Produkt" wird dabei verstanden: z.B. ein eingebettetes Gerät, das in eine zu automatisierende Umgebung eingebettet ist, eine SPS, - ein Host-Gerät, eine Bedienstation, eine Netzwerkkomponente, welche zur Netzwerkinfrastruktur gehört, wie z. B. ein Router und eine "Anwendung„.

Produktmängelbehandlung, die die Mängel in der IT-Sicherheit behandelt, die nach dem Einsatz des Produktes offenbar werden. Patch-Management, das der Hersteller für die Anwender eines Produktes betreibt.

Zertifizierte Entwicklungs- und Supportprozesse für Secure-by-Design-Produkte.

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. IITS1 029429 0016 Rev. 01

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Site(s):
PHOENIX CONTACT Electronics GmbH Industry Management and Automation Business Unit Automation Systems
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

PHOENIX CONTACT Electronics GmbH Industry Management and Automation Business Unit Automation Infrastructure
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

Certification Mark:

Type: Secure Product Development Lifecycle

Scope of Certificate: **Product creation process of the Phoenix Contact Group Master Development Guideline**

Applied Standard(s): IEC 62443-4-1:2018
PPP 15002B:2021 (IEC 62443-4-1 Full ML2 Process Profile)

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report.
See http://www.tuvsud.com/ps-cert for details.

Report No.: 18CR01S007

Valid until: 2024-09-30

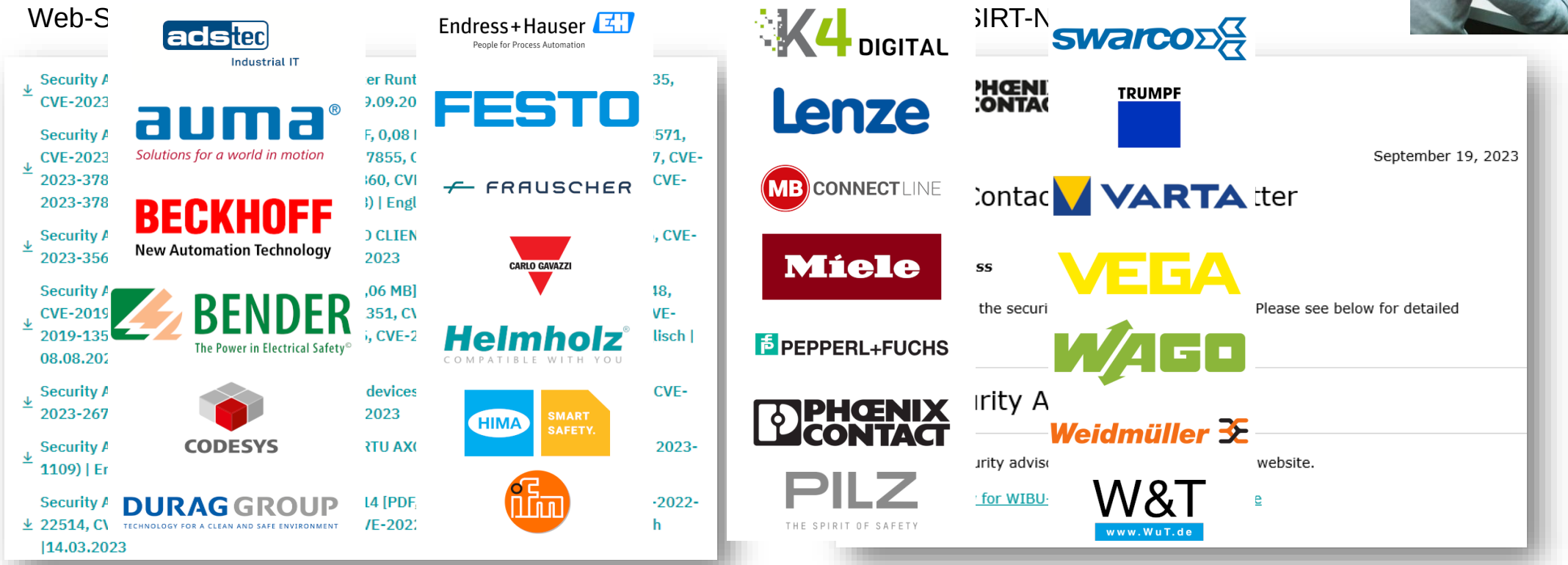
Date, 2021-11-18 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

Product Security Incident Response Team

ist bei Security-Incidents (Sicherheits-Vorfällen) die zentrale Kontaktstelle für Betreiber, Integratoren oder Security Spezialisten, die zu den PRODUKTEN des jeweiligen Herstellers Fragen haben. Das Hersteller PSIRT analysiert, klassifiziert und bearbeitet gemeldete Schwachstellen und Incidents, zu deren Produkten.

Das PSIRT von Phoenix Contact informiert mit einem Security Advisory über bekanntgewordene Security Schwachstellen und Update Möglichkeiten oder mit einem empfohlenen Workaround.



Vertikale Themen – IACS Normen (10% - Kritische Klasse I/II)

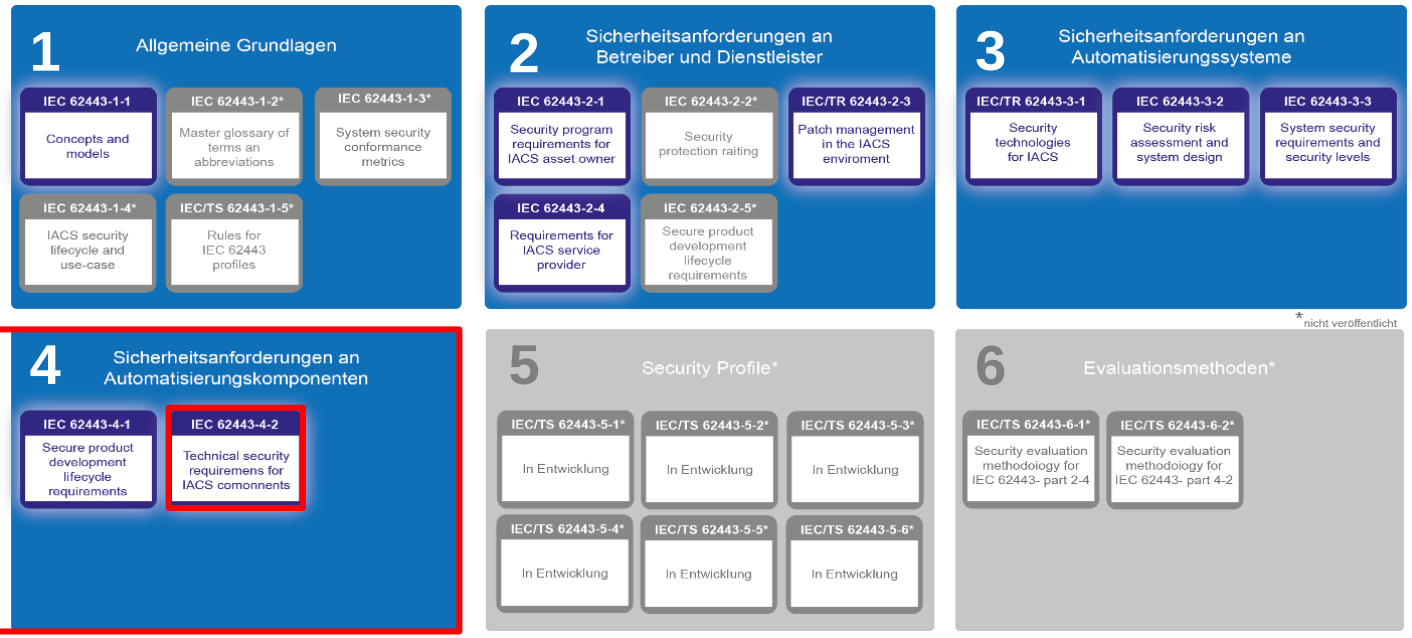
International Electrotechnical Commission

IEC 62443 ist ein internationaler Cybersicherheitsstandard für industrielle Automatisierungs- und Steuerungssysteme.

International Society of Automation

- **Betreiber**
  (Industrie Anlagen, Energie-, Verkehrstechnik,..)
- **OT-Systemintegrator**
  (Industrie Dienstleister zur Integration und Wartung)
- **Produkt Hersteller**
  (Industrie Netzwerke, Hardware und Software)

IEC 62443 Dokumenten-Struktur



IEC 62443-4

Sicherheitsanforderungen an Automatisierungskomponenten

IEC 62443 Kapitel 4 Absatz 2:

Enthält detaillierte **technische Anforderungen an die Komponenten** von Steuerungssystemen (CRs) im Zusammenhang mit den sieben (neu zwölf) grundlegenden Anforderungen (FRs), die in IEC TS 62443-1-1 beschrieben sind, einschließlich der Definition der Anforderungen für die **Security Level (1/2/3/4)** der Steuerungssystem-fähigkeit und ihrer Komponenten, SL-C (Komponente).

Die erste Industrie-Steuerung (SPS / PLC) mit TÜV SÜD Zertifizierung nach IEC 62443

PLCnext Technology
Designed by Phoenix Contact

Industrial Cyber Security Certification according to

IEC 62443-4-1 ML3 & IEC 62443-4-2 SL2

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service

CERTIFICATE

No. IITS2 029429 0027 Rev. 00

Holder of Certificate: PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: IACS components

Model(s): PLCnext Control
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: IEC 62443-4-1:2018
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S047
Valid until: 2024-10-20

Date, 2021-11-19 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

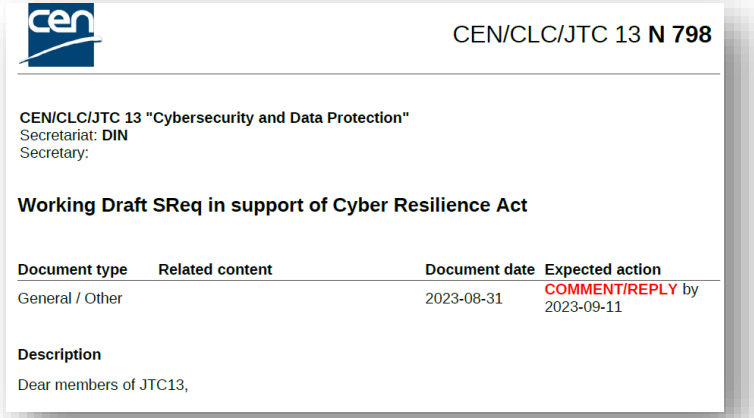
SBOM- und CSAF Format

Anforderungen an ein Schwachstellen Management

Europäische Kommission

Um die Schwachstellenanalyse zu erleichtern, müssen Hersteller die in deren Produkten enthaltenen Komponenten mit digitalen Elementen identifizieren und dokumentieren, unter anderem durch Erstellung von Software-Stücklisten (SBOMs).

„Software-Stückliste“ (SBOM / Software Bill of Materials) bezeichnet eine formelle Aufzeichnung mit Details und Lieferketten- beziehungen von Komponenten, die in den Softwareelementen von allen Produkt mit digitalen Elementen enthalten sind.



CEN/CLC/JTC 13 **N 798**

CEN/CLC/JTC 13 "Cybersecurity and Data Protection"
Secretariat: **DIN**
Secretary:

Working Draft SReq in support of Cyber Resilience Act

Document type	Related content	Document date	Expected action
General / Other		2023-08-31	COMMENT/REPLY by 2023-09-11

Description

Dear members of JTC13,

Vorteile für den Betreiber / Maschinenbau:

1. **Risikobewertung:** Durch die Analyse der SBOM kann der Käufer/Betreiber potenzielle Schwachstellen in den verwendeten Komponenten erkennen und das Sicherheitsrisiko für das gesamte Produkt bewerten.

2. **Maßnahmen ableiten**: Durch die Kenntnis der genauen Komponenten kann der Käufer/Betreiber leichter auf Sicherheitslücken reagieren und Komponenten auf dem neuesten Stand bringen, isolieren, oder abschalten, um Schwachstellen zu minimieren.

3. **Lizenzmanagement:** Die SBOM hilft bei der Überwachung der Lizenzen, die mit den verwendeten Komponenten verbunden sind, um sicherzustellen, dass keine Lizenzverletzungen auftreten.

SBOM- und CSAF Format

Anforderungen an ein Schwachstellen Management

Common Security Advisory Framework
(Gemeinsames Sicherheitsberatungs-Framework)

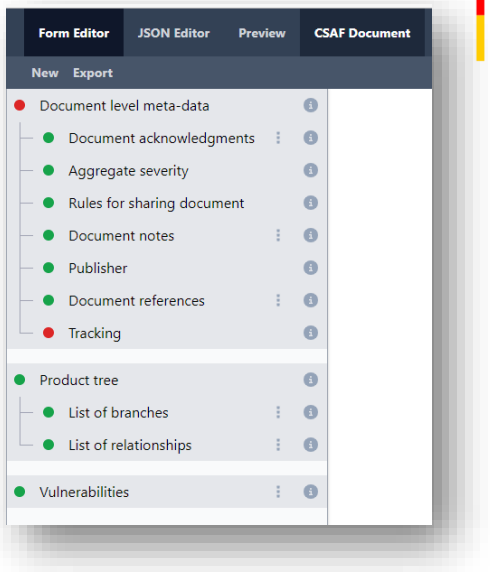
Die Verwendung einer einfachen Tabelle zur Verwaltung einer SBOM kann jedoch einige Einschränkungen haben, insbesondere wenn es um automatisierte Prozesse, Aktualisierungen und Integrationen in andere Systeme geht.

Ein zentrales Repository / Framework für SBOMs, kann von Herstellern „Security Advisories“ automatisiert abrufen und mit der eigenen Inventardatenbank abgeglichen werden.

Bundesamt
für Sicherheit in der
Informationstechnik

CSAF ermöglicht Automatisierung

Zusammen mit nationalen und internationalen Partnern arbeitet das BSI an einer Lösung, Anwendern das Auffinden sowie die Bewertung und Umsetzung von Security Advisories zu erleichtern. Das maschinenverarbeitbare Format für Security Advisories, das sogenannte Common Security Advisory Framework (CSAF) 2.0, wird einen entscheidenden Beitrag dazu leisten, dass Unternehmen den Überblick behalten und ihre Anlagen absichern können.
Die Security Advisories können dabei automatisiert von den Herstellern abgerufen und mit der eigenen Inventardatenbank abgeglichen werden. Das erste Tool zum Erstellen von CSAF-Dokumenten (Secvisogram) hat das BSI bereits auf seiner GitHub-Seite veröffentlicht.
Das BSI trägt mit diesen Aktivitäten dazu bei, die Informationssicherheit in den Unternehmen zu erhöhen und die Digitalisierung in Deutschland erfolgreich zu gestalten.



Good Practices for Supply Chain Cybersecurity

Published: June 13, 2023

Download
PDF document, 2.63 MB

Der Bericht bietet einen Überblick über die aktuellen Cybersicherheitspraktiken in der Lieferkette, die von wesentlichen und wichtigen Einrichtungen in der EU angewendet werden, und basiert auf den Ergebnissen einer ENISA-Studie aus dem Jahr 2022, die sich auf Investitionen in Cybersicherheitsbudgets bei Organisationen in der EU konzentrierte.

https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity/@@download/fullReport

Cyber Security Seminar mit TÜV Rheinland Prüfung

Phoenix Contact Cyber Security GmbH ist anerkannter Kursanbieter für Cyber Security im international etablierten „TÜV Rheinland Functional Safety (FS) & Cyber Security (CySec) Training Program"

Das 4-Tages-Vorbereitungsseminar **„Fundamentals of Cyber Security"** mit schriftlicher Prüfung findet erstmalig bei Phoenix Contact Österreich statt. Ziel ist es, im Rahmen des TÜV Rheinland Cyber Security Training Program das erforderliche Grundlagenwissen auf dem Weg zum **„CySec Specialist (TÜV Rheinland)"** zu erlangen.

Industrial OT- Security IEC 62443 (4 Tage mit Prüfung)

Datum	Dauer	Ort	Location	Preis*
13.03. – 16.03.2023	4 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 2.550,-
17.04. – 20.04.2023	4 Tage	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 2.550,-
24.04. – 27.04.2023	4 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 2.550,-
08.05. – 11.05.2023	4 Tage	Dornbirn	Hotel Vienna House Martinspark Mozartstraße 2, 6850 Dornbirn	€ 2.550,-
25.09. – 28.09.2023	4 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 2.550,-
16.10. – 19.10.2023	4 Tage	Linz	PHOENIX CONTACT GmbH Flachenauergutstraße 10, 4020 Linz	€ 2.550,-
06.11. – 09.11.2023	4 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 2.550,-
13.11. – 16.11.2023	4 Tage	Dornbirn	Hotel Vienna House Martinspark Mozartstraße 2, 6850 Dornbirn	€ 2.550,-

* exkl. MwSt., inkl. Prüfung je Teilnehmer

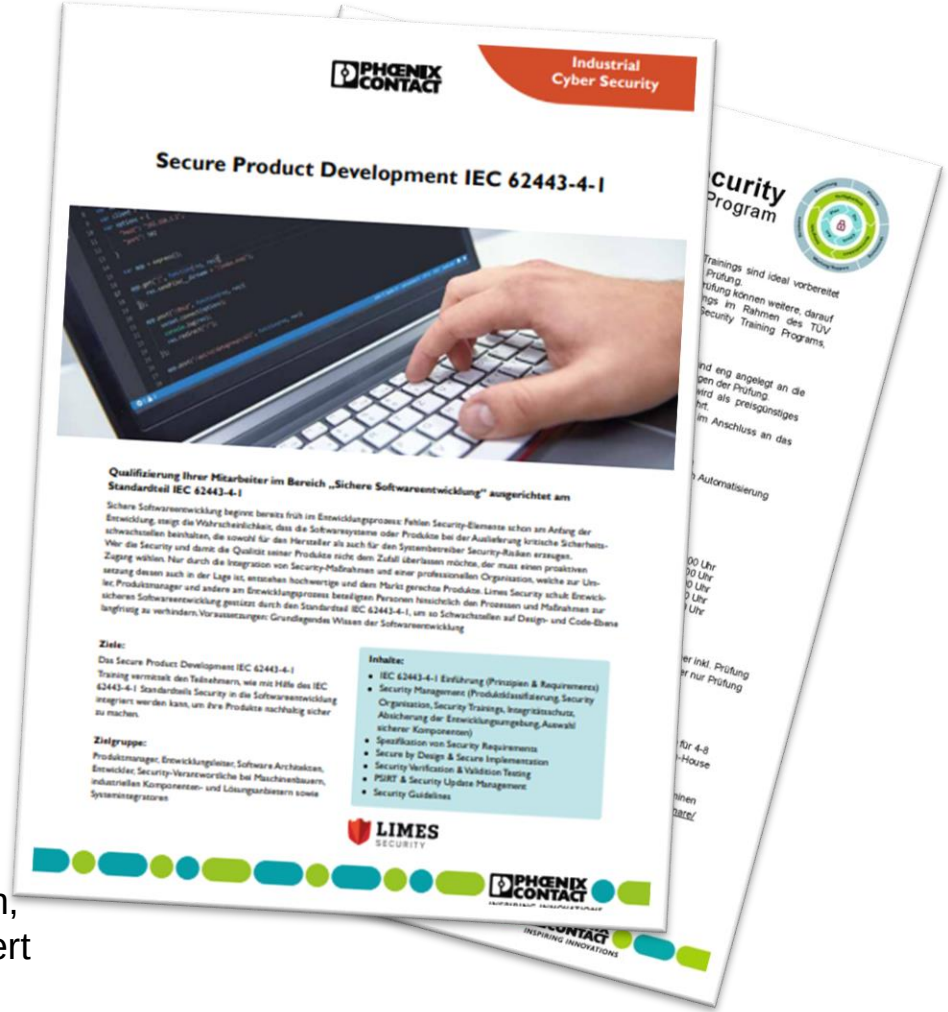
TÜVRheinland®

Das Seminar vermittelt Grundlagen zur Analyse von potenziellen Cyber Security Schwachstellen wie auch Referenzmodelle, **IEC 62443** zur Umsetzung von sicheren Netzen in der industriellen Automatisierungs- und Steuerungstechnik.

PHOENIX CONTACT

Secure Product Development IEC 62443-4-1

Sichere Softwareentwicklung beginnt bereits früh im Entwicklungsprozess: Fehlen Security-Elemente schon am Anfang der Entwicklung, steigt die Wahrscheinlichkeit, dass die Softwaresysteme oder Produkte bei der Auslieferung kritische Sicherheitsschwachstellen beinhalten, die sowohl für den Hersteller als auch für den Systembetreiber Security-Risiken erzeugen.



Secure Product Development IEC 62443-4-1				
Datum	Dauer	Ort	Location	Preis*
30.05. – 31.05.2023	2 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 1.576,-
13.06. – 14.06.2023	2 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 1.576,-
12.09. – 13.09.2023	2 Tage	Wien	PHOENIX CONTACT GmbH Ada-Christen-Gasse 4, 1100 Wien	€ 1.576,-
26.09. – 27.09.2023	2 Tage	Graz	PHOENIX CONTACT GmbH Gasometerweg 47, 8055 Graz	€ 1.576,-

* exkl. MwSt.

Das Secure Product Development with IEC 62443-4-1 Training vermittelt den Teilnehmern, wie mit Hilfe des IEC 62443-4-1 Standardteils Security in die Softwareentwicklung integriert werden kann, um ihre Produkte nachhaltig sicher zu machen.

Incident Handling für OT-Umgebungen

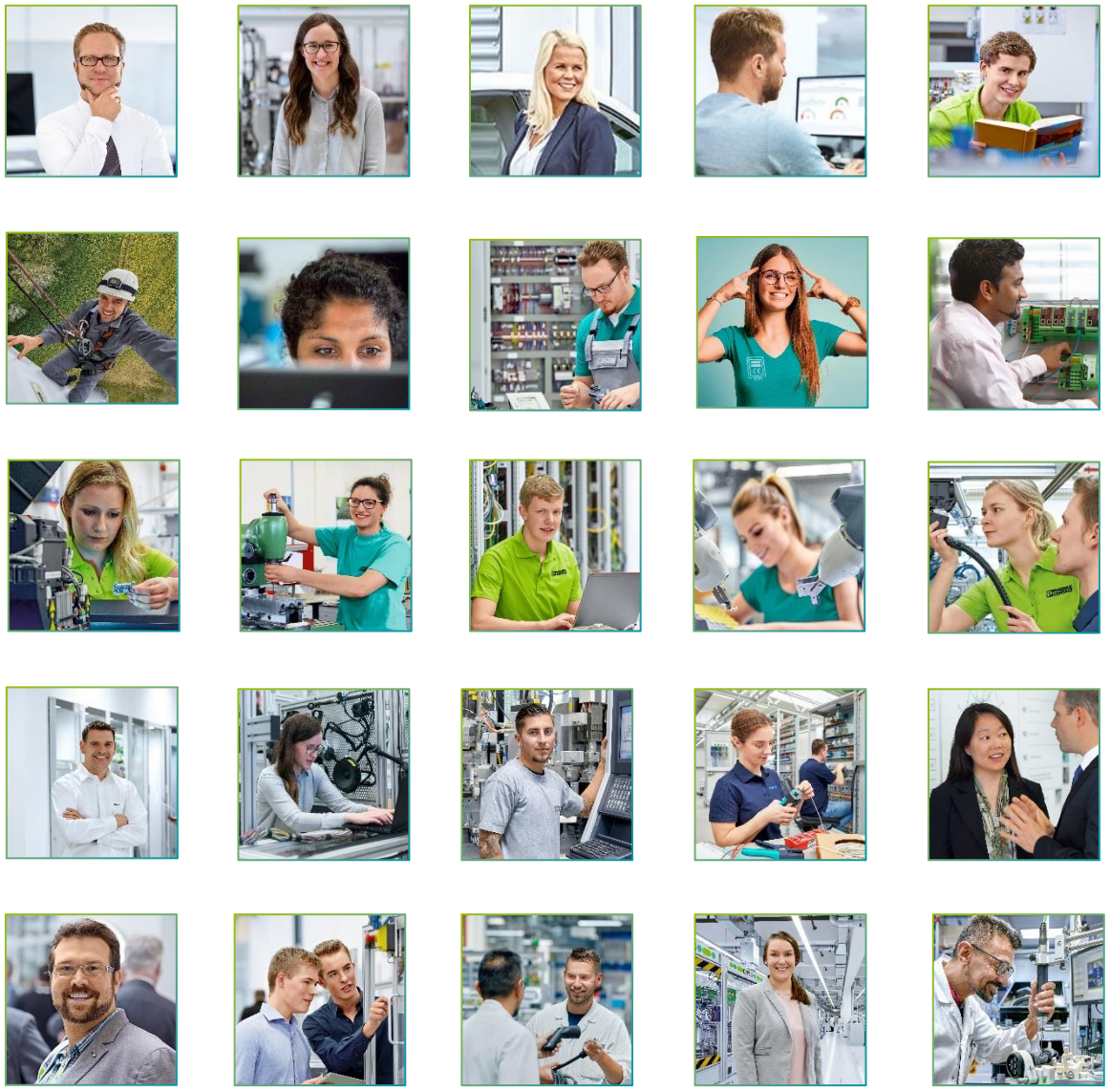
Vernetzte IT-Systeme sind fast ständig Angriffen aus dem Internet ausgesetzt. Dies gilt zunehmend auch für industrielle Kontrollsysteme, wie zahlreiche Beispiele in der Vergangenheit gezeigt haben. Im Falle eines Cyber-Angriffs ist die richtige Vorbereitung essentiell, um richtig auf einen Angriff reagieren zu können. In diesem Training wird neben den technischen und organisatorischen Maßnahmen auch ein konkretes Angriffsszenario praktisch in der AIT Cyber Range simuliert. Eine Cyber Range ist eine Simulationsumgebung, die es Teilnehmern von Schulungen und Trainings ermöglicht, Aufgaben in einer möglichst realistischen Umgebung bewältigen und die notwendigen Prozesse erlernen zu können.

Incident Handling für OT-Umgebungen

Datum	Dauer	Ort	Location	Preis*
28.03. – 29.03.2023	1,5 Tage	Wien	AIT Austrian Institute of Technology GmbH Giefinggasse 4, 1210 Wien	€ 1.040,-
10.10. – 11.10.2023	1,5 Tage	Wien	AIT Austrian Institute of Technology GmbH Giefinggasse 4, 1210 Wien	€ 1.040,-

* exkl. MwSt.

Kennenlernen typischer Bedrohungen von OT-Systemen, Verständnis entwickeln für die Rolle eines Security, Operations Center (SOC) bei der Behandlung von Sicherheitsvorfällen
In einer praktischen Übung auf der AIT Cyber Range die richtige Vorgehensweise bei Sicherheitsvorfällen exerzieren



Dankeschön!

…für Ihre Zeit und Ihr Interesse