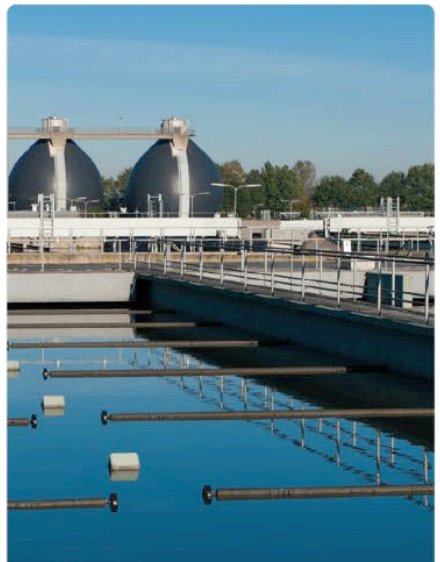
INDUSTRIAL AUTOMATION

NIS 2.0

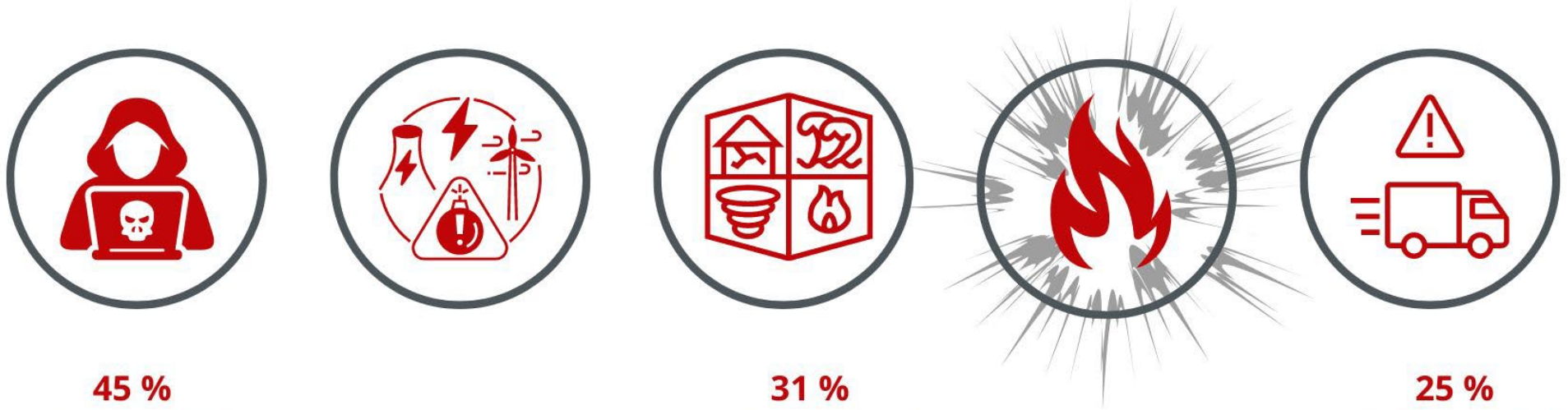
und seine Herausforderungen



INDUSTRIAL AUTOMATION

NIS 2.0

Meist gefürchteten Gründe für Betriebsunterbrechungen



45 %
Cybervorfälle

35 %
Energiekrise

31 %
Naturkatastrophen

30 %
Feuer, Explosion

25 %
Lieferausfall

Quelle: Allianz

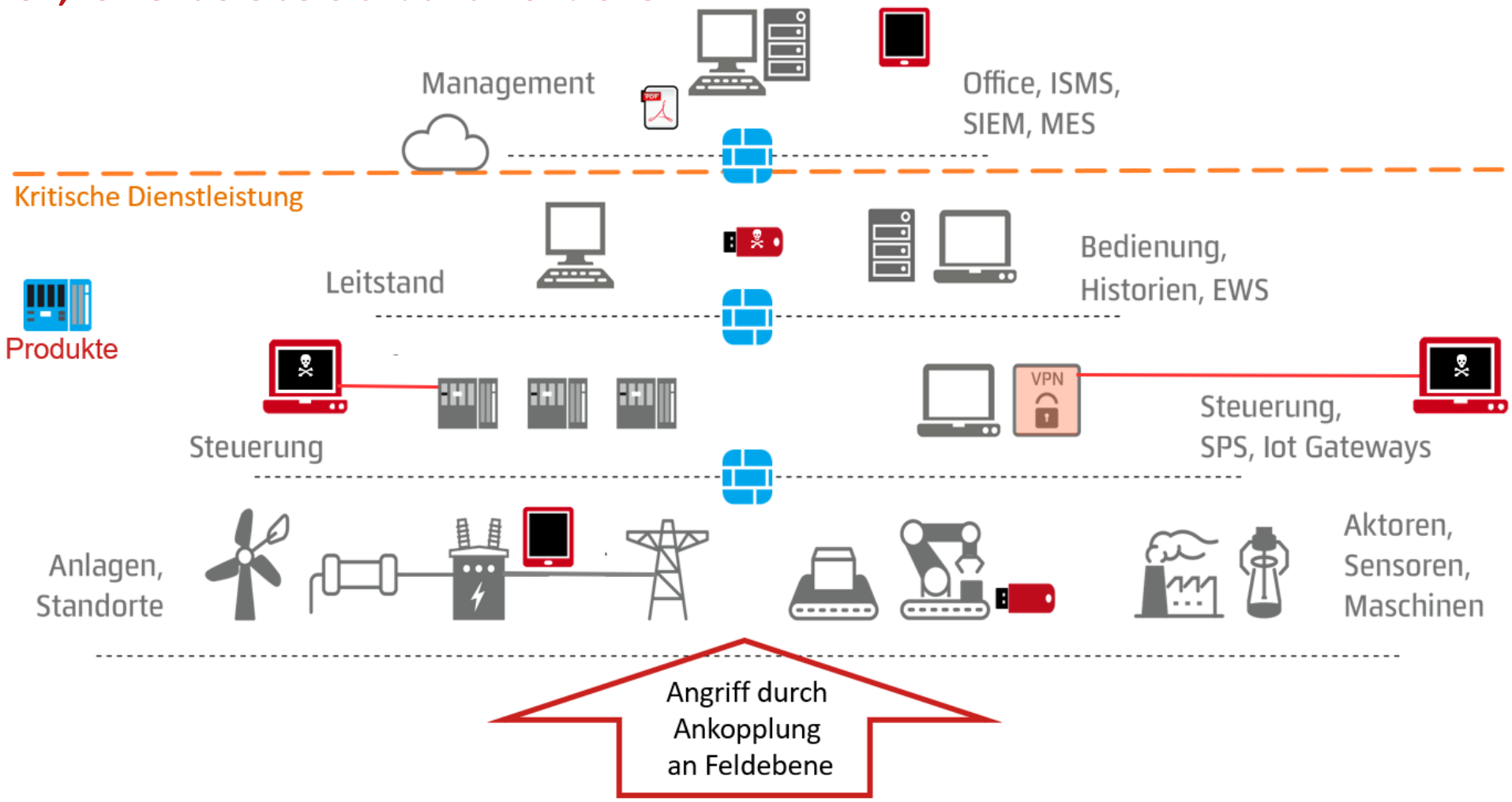
NIS 2.0

Mythen:

- Wir sind nicht mit dem Internet verbunden
- Unsere Systeme sind durch eine Firewall geschützt
- Hacker verstehen keine Automatisierung und Steuerungen
- Unsere Firma ist kein Ziel
- Unser Sicherheitssystem beschützt uns

NIS 2.0

Schwachstellen, fehlende Übersicht und Kontrolle



NIS 2.0

Von der Risiko Analyse zur kontinuierlichen Sicherheit

Protokollierung – Detektion - Reaktion

Analysieren

- Assets automatisch identifizieren
- Verwalten: z.B. Owner, Standort, Gruppen
- Verbindungen beurteilen, zB.: Treshold setzen
- Validieren

Risiko Management

- Schwachstellen
- Bedrohungen
- Risiken
- Maßnahmen
- Reports

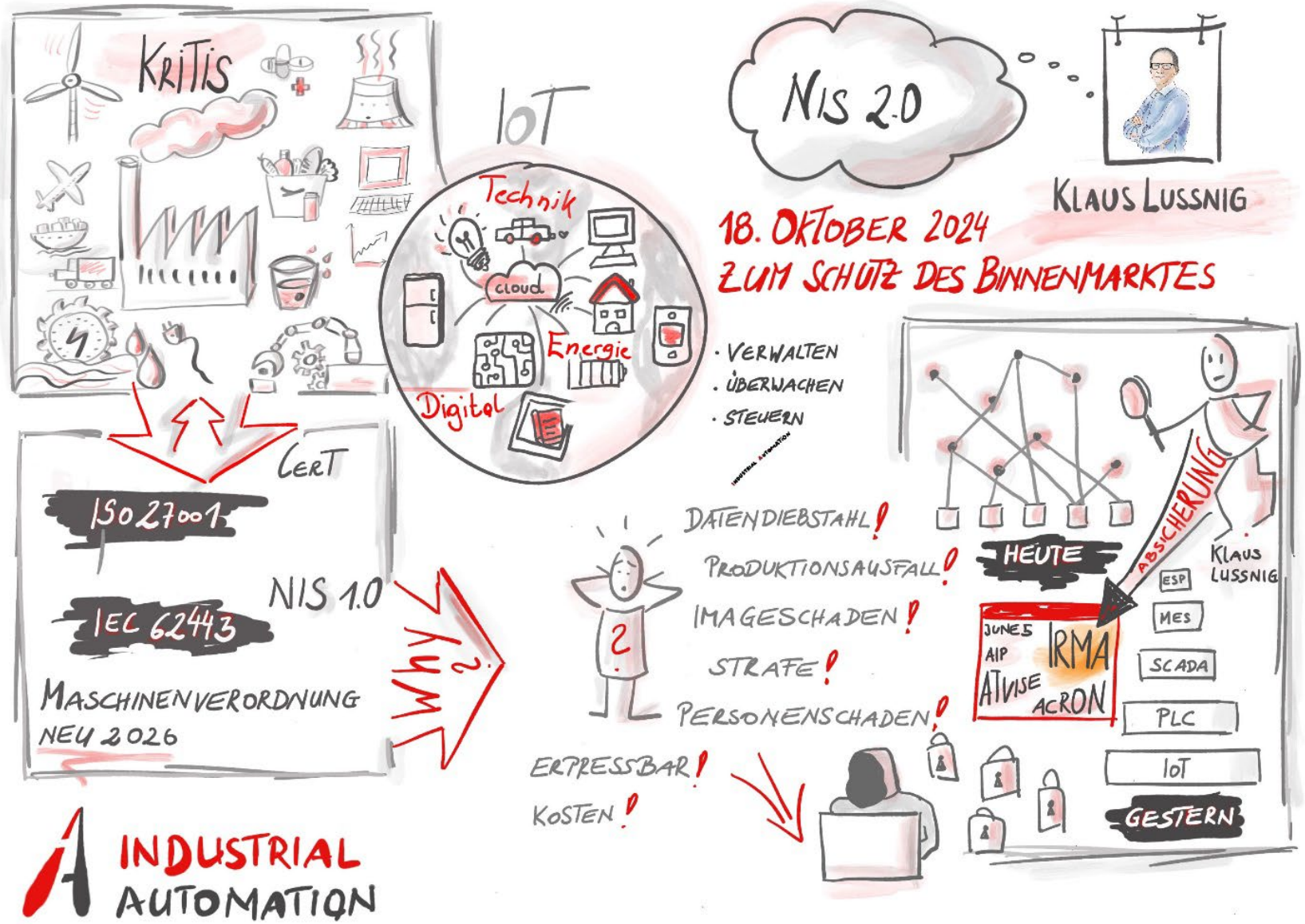
Anomalien

- Assets
- Verbindungen
- Daten
- Attacken / Schwachstellen
- Kontrolle

Kontinuität

- Status Quo prüfen
- Soll / Ist Abgleich
- Attacken / Schwachstellen
- Alarme
- KPI Bedrohungslevel

NIS 2.0


KRITIS
IOT
Technik
cloud
Energie
Digital
NIS 2.0
KLAUS LUSSNIG
18. OKTOBER 2024
ZUM SCHUTZ DES BINNENMARKTES
· VERWALTEN
· ÜBERWACHEN
· STEUERN
CERT
ISO27001
IEC 62443
NIS 1.0
MASCHINENVERORDNUNG
NEU 2026
Why ?
DATENDIEBSTAHL!
PRODUKTIONSAUSFALL!
IMAGESCHADEN!
STRAFE!
PERSONENSCHADEN!
ERPRESSBAR!
KOSTEN!
HEUTE
ABSICHERUNG
KLAUS LUSSNIG
ESP
MES
SCADA
PLC
IOT
GESTERN
INDUSTRIAL AUTOMATION

NIS 2.0

Es geht um:

- ein Funktionieren am Binnenmarkt – daher die vielen Differenzierungen
- eine EU-weite horizontale Gesetzgebung (ersetzt NIS 1)

- eine Modernisierung des Rechtsrahmens durch:
    - Zunehmende Digitalisierung
    - Entwicklung der Bedrohungslandschaft
    - Defizite von NIS 1

- **Wirksam mit 18.10. 2024**

NIS 2.0

Hauptziele von NIS2

Größeren Teil der Wirtschaft und Gesellschaft abdecken (**mehr Sektoren**)	Systematische Konzentration auf **größere, mittlere und kritische Akteure**	**Angleichung der Sicherheitsanforderungen**
Straffung der Berichtspflichten	Angleichung der **Aufsicht und Durchsetzung**	**Mehr operative Zusammenarbeit,** inkl. EU-Cyber-Krisenmanagement

INDUSTRIAL AUTOMATION

NIS 2.0

10 Jahre NIS (Sicherheit von Netz- und Informationssystemen)

NIS 2.0

Die 3 Säulen von NIS2

Für Unternehmen besonders relevant

Fähigkeiten der Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
Computer-Notfallteams (CERTs/CSIRTs)	CSIRTs-Netzwerk	Schulungen für Top-Management
Cyber-Krisenmanagement	EU-Cyberkrisennetzwerk (CyCLONe)	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	ENISA Cybersecurity Reports	Sicherheitsmaßnahmen
Rahmen für CVD (Coordinated Vulnerability Disclosure)	Europäisches Schwachstellenregister	Berichtspflichten

Rot = Neuerungen gegenüber NIS1

INDUSTRIAL AUTOMATION

Anwendungsbereich:

wird durch Größenschwellwerte (size cap rule) bestimmt nach:

- mittleren und große Unternehmen
- Kleinunternehmen (nur in bestimmten Ausnahmefällen)
- Level-Playing-Field
- Öffentliche und Private Einrichtungen
- Arten der Einrichtungen nach Spalte 3 von Anhang I & II

NIS 2.0

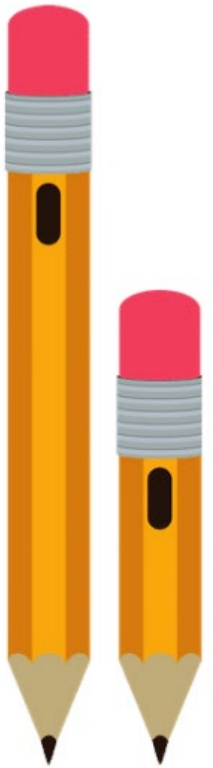
Prüfschema:

- Erbringt das Unternehmen seine Dienstleistungen in der EU oder übt seine Tätigkeiten in der EU aus
- Entspricht das Unternehmen einer in Spalte 3 von Anhang I und Anhang II genannten Art
- Ist das Unternehmen größer als ein Kleinunternehmen
    - Ausnahmen und Sonderregeln: Kleinunternehmen insb. im Sektor digitale Infrastruktur erfasst und wenn sie als „kritisch“ eingestuft werden (!)
- Ist das Unternehmen eine wesentliche oder wichtige Einrichtung

INDUSTRIAL AUTOMATION

Ist das Unternehmen größer als ein Kleinunternehmen?

- Empfehlung 2003/361/EG der EU-Kommission
  - **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
  - **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
  - **Großunternehmen**: Alle Unternehmen, sofern kein KMU.
- Benutzerleitfaden der EU-Kommission zur Definition von KMU



NIS 2.0

Betroffene Sektoren

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produken und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Rot = Neuerungen gegenüber NIS1

INDUSTRIAL AUTOMATION

NIS 2.0

Grundregel Anwendungsbereich Anhang I

Sektoren	Große Unternehmen	Mittlere Unternehmen	Klein-unternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktsaufsicht / Gesundheitswesen / Trinkwasser / Abwasser / Verwaltung von IKT-Diensten / Weltraum	Wesentlich	wichtig	

- Große Unternehmen: wesentlich
- Mittlere Unternehmen: wichtig
- Kleinunternehmen: nicht im Anwendungsbereich

INDUSTRIAL AUTOMATION

NIS 2.0

Grundregel Anwendungsbereich Anhang II

Sektoren	Große Unternehmen	Mittlere Unternehmen	Klein-unternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / verarbeitendes Gewerbe bzw. Herstellung von Waren / Anbieter digitaler Dienste	wichtig	wichtig	

- Große Unternehmen: wichtig
- Mittlere Unternehmen: wichtig
- Kleinunternehmen: nicht im Anwendungsbereich

INDUSTRIAL AUTOMATION

NIS 2.0

Entspricht das Unternehmen einer in Spalte 3 von Anhang 1 & 2 genannten Art?

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944[1], die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944

- Anhang I: 53 Arten
- Anhang II: 14 Arten

INDUSTRIAL AUTOMATION

NIS 2.0

Ist das Unternehmen eine wesentliche oder wichtige Einrichtung?

- **Wesentliche Einrichtungen**
  - Alle im Anhang I angeführten Arten von Unternehmen, die groß sind.
- **Wichtige Einrichtungen**
  - Alle anderen Einrichtungen.
- **Sonderregeln:**
  - Sektor Digitale Infrastruktur

NIS 2.0

Kernpflichten für Unternehmen

Governance:

- Verantwortung des Top-Managements
- Schulungen für das Top-Management

Risikomanagementmaßnahmen:

- Unternehmen müssen Maßnahmen ergreifen, um die Risiken für die Sicherheit ihrer Netz- und Informationssysteme zu beherrschen und die Auswirkung von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten

NIS 2.0

Risikomanagementmaßnahmen:

- **All-Gefahren-Ansatz**

- **Risikobasierter Ansatz:**
  - Angemessene und verhältnismäßige technische, operative und organisatorische Maßnahmen
  - Berücksichtigung des Stands der Technik und der Kosten der Umsetzung
  - Berücksichtigung des Ausmaßes der Risikoexposition und der Größe des Unternehmens
  - Berücksichtigung der Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere (inkl. Gesellschaftlichen und wirtschaftlichen Auswirkungen)

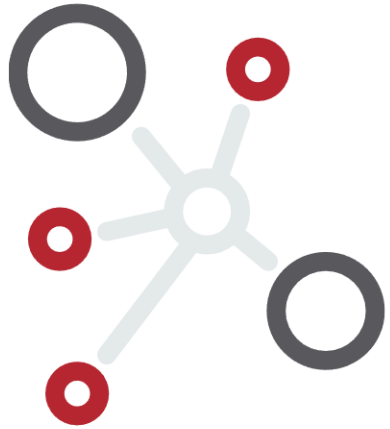
Risikomanagementmaßnahmen:

- Konzepte in Bezug auf **Risikoanalyse** und Sicherheit für Informationssysteme
- **Bewältigung** von Sicherheitsvorfällen
- **Lieferkettensicherheit**
- Sicherheitsmaßnahmen bei **Erwerb**, Entwicklung und Wartung von
- IKT (Informations- und Kommunikationstechnologie)
- Grundlegende Praktiken der **Cyberhygiene** und **Schulungen** zur Cybersicherheit
- Sicherheit des **Personals**, Konzepte für **Zugriffskontrolle, MFA** (Multifaktorauthentifizierung)
- … uvm.

NIS 2.0

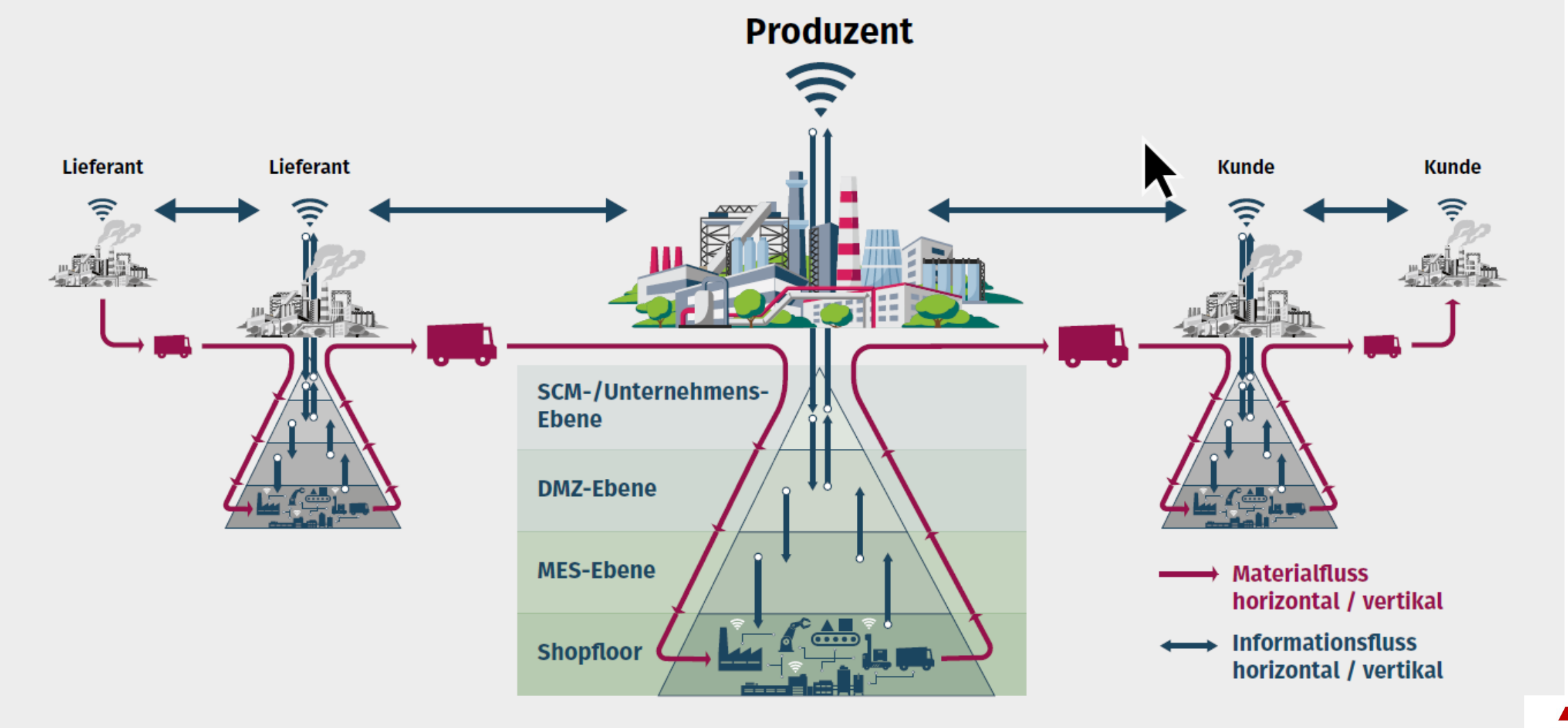
Es ist genau spezifiziert, was technisch notwendig ist. Unternehmen müssen künftig mindestens die folgenden Cybersecurity-Maßnahmen umsetzen, um IT-Infrastruktur und Netzwerke ihrer kritischen Dienstleistungen zu schützen:

- **Policies:** Richtlinien für Risiken und Informationssicherheit
- **Incident Management:** Prävention, Detektion und Bewältigung von Sicherheitsvorfällen
- **Business Continuity:** Backup-Management, Desaster Recovery, Krisenmanagement
- **Supply Chain:** Sicherheit in der Lieferkette
- **Einkauf:** Sicherheit in der Beschaffung von IT und Netzwerk-Systemen
- **Effektivität:** Vorgaben zur Messung von Cyber- und Risikomaßnahmen
- **Kryptographie:** Verschlüsselung wo immer möglich
- **Zugangskontrolle:** Einsatz von Multi-Faktor-Authentifizierung und Single Sign-on
- **Kommunikation:** Einsatz sicherer Sprach-, Video- und Text-Kommunikation



INDUSTRIAL AUTOMATION

OT/ICS – Security



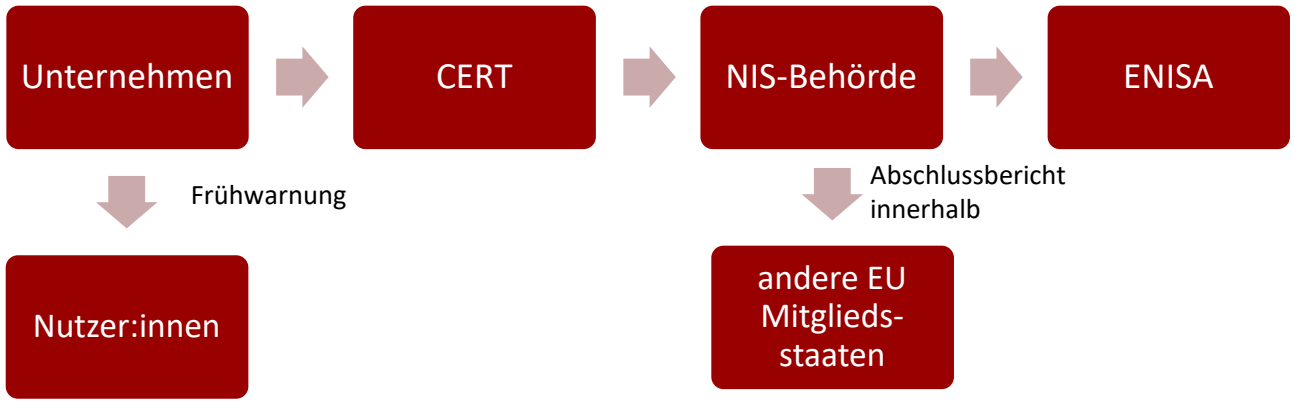
NIS 2.0

Berichtspflichten:

Unternehmen müssen erhebliche Sicherheitsvorfälle unverzüglich an das Computer-Notfallteam (CERT/CSIRT) melden

Unternehmen müssen gegebenenfalls Empfänger ihrer Dienste über erhebliche Sicherheitsvorfälle und Bedrohungen informieren

Meldeweg:



NIS 2.0

Frühwarnung

Frist: unverzüglich bis max. 24 h nach Kenntnisnahme	**Inhalt:** Verdacht, ob Sicherheitsvorfall auf rechtswidriger oder böswilliger Handlung beruht oder grenzüberschreitend ist

Meldung

Frist: unverzüglich bis max. 72 h nach Kenntnisnahme	**Inhalt:** Erste Bewertung des Sicherheitsvorfalls (inkl. Schweregrad, Auswirkungen, ggf. Kompromittierungsindikatoren)

Abschlussmeldung

Frist: 1 Monat nach Meldung	**Inhalt:** Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen, Abhilfemaßnahmen

INDUSTRIAL AUTOMATION

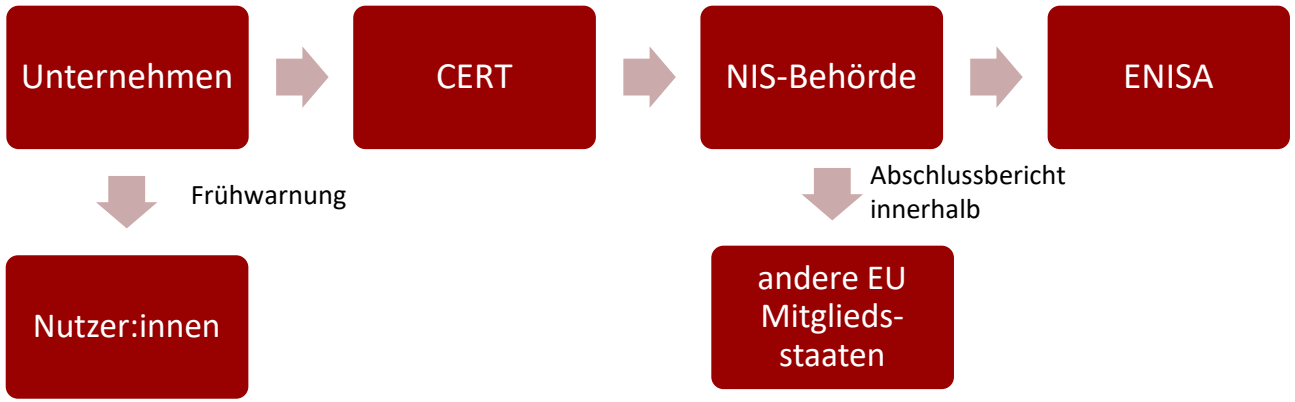
NIS 2.0

Berichtspflichten:

Unternehmen müssen erhebliche Sicherheitsvorfälle unverzüglich an das Computer-Notfallteam (CERT/CSIRT) melden

Unternehmen müssen gegebenenfalls Empfänger ihrer Dienste über erhebliche Sicherheitsvorfälle und Bedrohungen informieren

Meldeweg:



NIS 2 - Konsequenzen

Betroffene Unternehmen müssen ab sofort Cybersicherheit als eigenständiges Thema und als Chefsache betrachten

Folgen wesentlicher Sektor

- Vor-Ort-Kontrollen, Ad-hoc-Prüfungen, Verlangen von Nachweisen
- öffentliche Bekanntgabe der Verstöße
- Aussetzung von Zertifizierungen
- Verbot der Wahrnehmung von Leitungsaufgaben natürlicher Personen auf Geschäftsführung- und Vorstandsebene
- Geldbußen von bis zu 10 Mio. EUR oder 2% des Jahresumsatzes
- persönliche Haftung der Führungskräfte

Folgen wichtiger Sektor

- Vor-Ort-Kontrollen, gezielte Sicherheitsprüfungen, Verlangen von Nachweisen, Sicherheitsscans
- öffentliche Bekanntmachung der Verstöße
- Geldbußen von bis zu 7 Mio. EUR oder 1,4% des weltweiten Jahresumsatzes
- persönliche Haftung der Führungskräfte

NIS 2 erfüllt

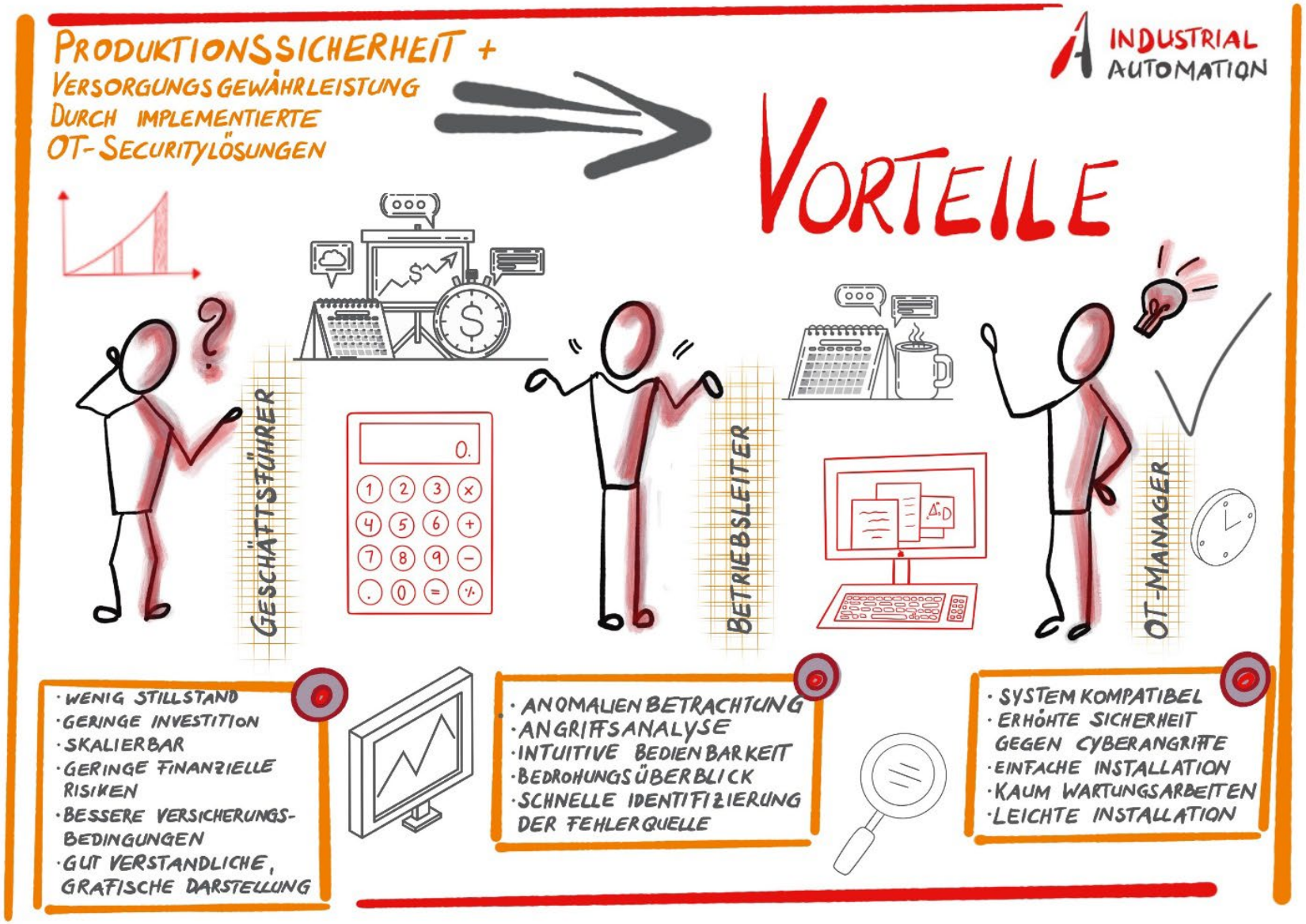
- Regelmäßger Review und laufende Anpassung der Maßnahmen

Liste nicht vollständig

NIS 2.0


Ist die NIS2-Richtlinie für mich relevant?
Mein Unternehmen hat mind. 50 Mitarbeiter und Jahresumsatz von mind. 10 Mio. EUR bzw. Jahresbilanzsumme von mind. 10 Mio. EUR
Mein Unternehmen ist einem **wesentlichen oder wichtigen Sektor** zugehörig.
Mein Unternehmen wird **unabhängig von der Größe** reguliert.
NIS2
Mein Unternehmen ist Teil der **Lieferkette** eines NIS2 betroffenen Unternehmens.
Mein Unternehmen ist Teil der **Lieferkette** eines NIS2 betroffenen Unternehmens.
Anforderungen
• Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
• Risikomanagement für Cybersicherheit
• Backup-Management
• Krisenmanagement
• Schwachstellenmanagement
• Schulungen für Cybersicherheit
• gesicherte Sprach-, Video- und Textkommunikation
• Reporting innert 24 Std. bei erheblichen Sicherheitsvorfällen an Cybersicherheits-behörde und Kunden
nicht NIS2 relevant
mittelbar betroffen; NIS2 fordert Cybersicherheit in der Lieferkette
mittelbar betroffen; NIS2 fordert Cybersicherheit in der Lieferkette
nicht NIS2 relevant
Liste nicht vollständig

NIS 2.0



INDUSTRIAL AUTOMATION

Vielen Dank!

Weitere Informationen im Internet | **www.SCADA.online**

Industrial Automation GmbH
AT-6020 Innsbruck
Technikerstraße 1 - 3

Tel.: +43 512 27 22 71-00
office@automation.team

Industrial Automation Suisse GmbH
CH-8808 Pfäffikon SZ
Churerstraße 16

Tel.: +41 55 56 002-00
office@automation.team

Büro Italien
IT-39032 Campo Tures
Via Unterwalburgen 15B

Tel.: +41 0474 86 93-00
office@automation.team

www.scada.online