

# CySeReS-KMU Abschlussveranstaltung

15.04.2026

# Agenda

---

- Kurze Vorstellung CySeReS-KMU
- Exklusive Werksführung im Saalachkraftwerk Bad Reichenhall [Christoph Mexis, DB Energie GmbH]
- Kaffeepause & Networking
- Cyber-Security in Lieferketten
- Umsetzbare Bausteine in fünf Kernbereichen für KMU
- Q&A mit Expertinnen und Experten
- Networking & Austausch bei Buffet

# Team CySeReS-KMU



**Dr. Michael Plasch, BA MA**  
FH Oberösterreich, Logistikum

Assistenzprofessor  
+43 5 0804 33257  
[michael.plasch@fh-steyr.at](mailto:michael.plasch@fh-steyr.at)



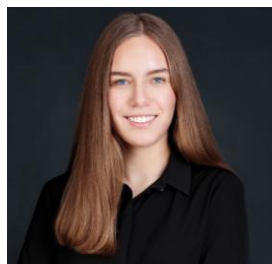
**Prof. Dr. Stefan Katzenbeisser**  
Universität Passau

Professor  
[stefan.katzenbeisser@uni-passau.de](mailto:stefan.katzenbeisser@uni-passau.de)



**Stefan Anthuber, M. Eng.**  
TH Deggendorf

Operative Leitung des Technologie  
Campus Vilshofen  
[stefan.anthuber@th-deg.de](mailto:stefan.anthuber@th-deg.de)



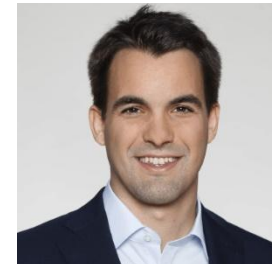
**Amelie Gutbrod, BA**  
FH Oberösterreich, Logistikum

Wissenschaftliche Mitarbeiterin  
[amelie.gutbrod@fh-steyr.at](mailto:amelie.gutbrod@fh-steyr.at)



**Dr. Amar Almaini**  
TH Deggendorf

Wissenschaftlicher Mitarbeiter  
[amar.almaini@th-deg.de](mailto:amar.almaini@th-deg.de)



**Ass.-Prof. Dipl.-Ing. Clemens  
Sauerwein, PHD**  
Universität Innsbruck

Assistenz-Professor  
[cyseres@uibk.ac.at](mailto:cyseres@uibk.ac.at)



**Nico Mexis, M. Sc.**  
Universität Passau

Wissenschaftlicher Mitarbeiter  
[nico.mexis@uni-passau.de](mailto:nico.mexis@uni-passau.de)



**Prof. Dr. Martin Schramm**  
TH Deggendorf

Wissenschaftlicher Leiter  
[martin.schramm@th-deg.de](mailto:martin.schramm@th-deg.de)



**Alexander Zeisler, B.A., M.A**  
FH Salzburg


Senior Lecturer  
[alexander.zeisler@fh-salzburg.ac.at](mailto:alexander.zeisler@fh-salzburg.ac.at)

# Was ist CySeReS-KMU?



## Cyber Security und Resilienz in Supply Chains mit Fokus auf KMUs

**Juni 2026**

 Januar 2023 – Dezember 2025

**Projektziel:**

Unterstützung von kleinen und mittleren Unternehmen bei der IT-Sicherheit, Cyber-Security und Resilienz mit dem Fokus auf die Supply Chain im Interreg Programmraum.

CySeReS-KMU

# Kraftwerksführung

---

*Christoph Mexis wird Sie nun durch das Saalachkraftwerk Bad Reichenhall führen.  
Bitte folgen Sie seinen Anweisungen.*



# Kaffeepause & Networking

---

*Sie können die Zeit bis 15:30 gerne „networken“ und eine kleine Kaffeepause genießen.*

# Danksagungen



Fördergeber: Interreg  
Bayern-Österreich



COC AG



KMU Forschung Austria



Bayern Innovativ



WKO Österreich Sst.  
Krisenmanagement und  
Sicherheitsvorsorge



b-plus technologies  
GmbH



IHK für München und  
Oberbayern



Easylogix.de – Schindler  
und Schill GmbH



WKO Oberösterreich



MonLog GmbH



IT-sicherheitscluster.de



Digital Innovation Hub  
West



WKO Tirol

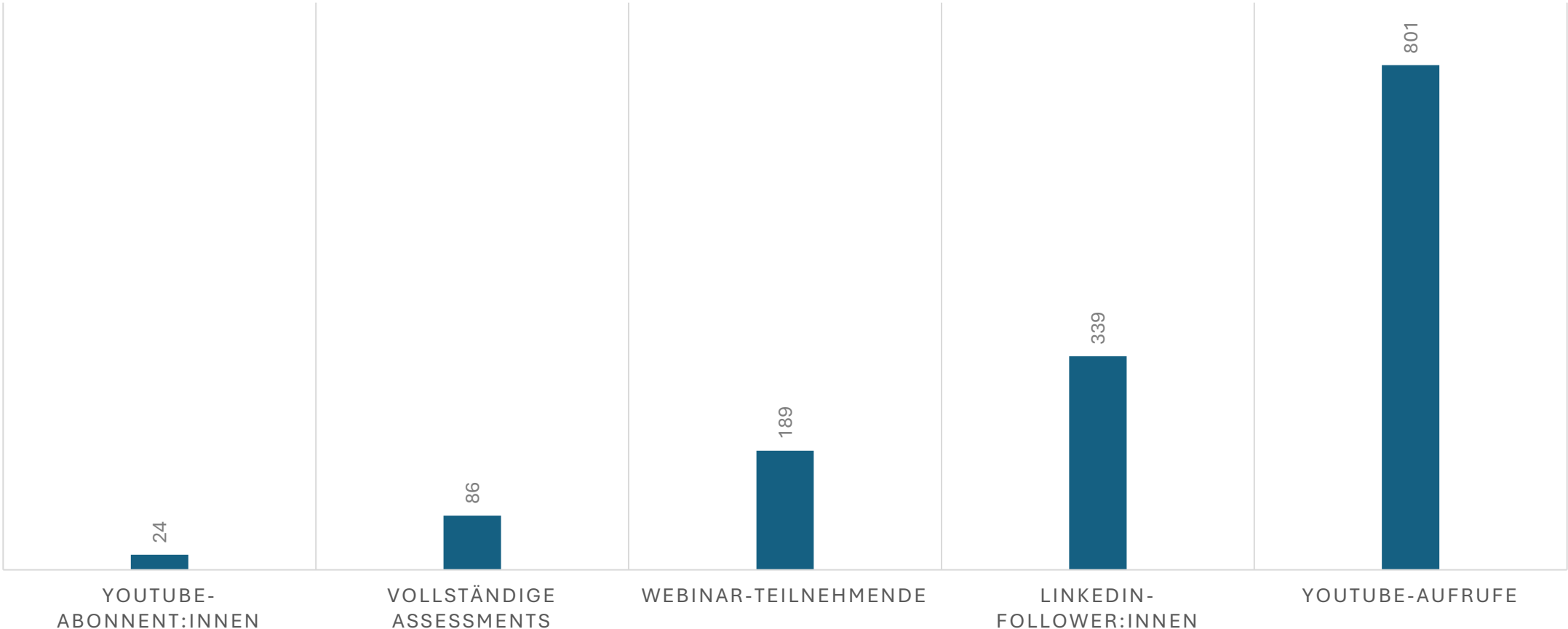


Biz Up



VNL – Verein Netzwerk  
Logistik

# Rückblick auf 3,5 Jahre CySeReS-KMU



# Webinare

8 Webinare + 1 Workshop auf YouTube verfügbar!



**CySeReS-KMU**  
@CySeReS-KMU · 24 Abonnenten · 9 Videos  
CySeReS-KMU ist ein ausgeschriebenes Forschungsprojekt von Interreg Österreich-Bayern ...mehr  
cyseres-kmu.eu und 2 weitere Links  
Abonniert

Übersicht Videos Playlists

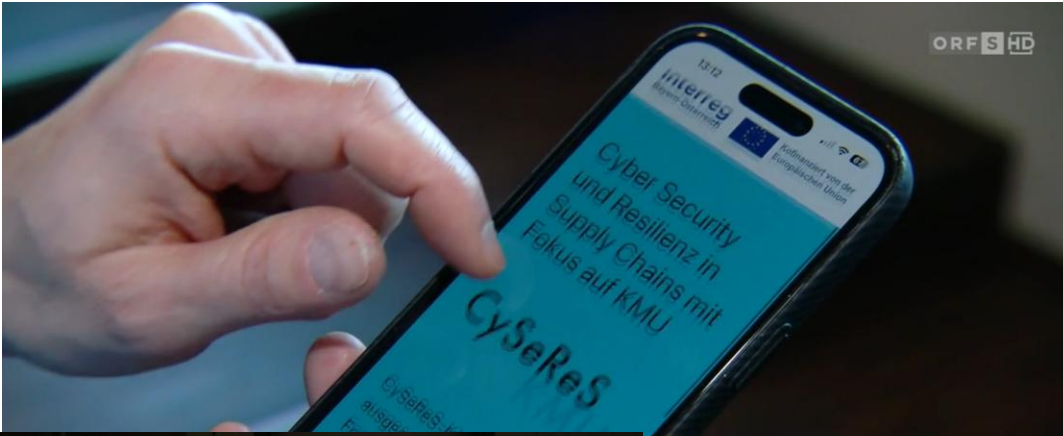
Neueste Beliebt Älteste

- Webinar**  
Infotermin: Wie Sie als KMU von CySeReS-KMU und CYSSME profitieren können  
Projektteam CySeReS-KMU  
CYSSME  
43:46  
CySeReS-KMU: Webinar "Wie Sie als KMU von CySeReS-KMU und CYSSME profitiere...  
86 Aufrufe · vor 1 Jahr
- Webinar**  
Künstliche Intelligenz verstehen: Grundlagen, Anwendungen und Sicherheitsaspekte  
Projektteam CySeReS-KMU  
Experten Referents  
Hilob Foltz M.Sc.  
1:10:29  
CySeReS-KMU: Webinar "KI verstehen: Grundlagen, Anwendungen und...  
57 Aufrufe · vor 1 Jahr
- Webinar**  
Cybersecurity heute und morgen: Sicherheitskonzepte für die nächste Generation von Cyber-Bedrohungen  
Projektteam CySeReS-KMU  
Experten Referents  
Axi Kravitz, MSc (Blue Shield Security GmbH)  
51:16  
CySeReS-KMU: Webinar "Cybersecurity heute und morgen: Sicherheitskonzepte" a...  
113 Aufrufe · vor 1 Jahr
- Webinar**  
IT-Sicherheitsstrategien für KMU  
Projektteam CySeReS-KMU  
Experten Referents  
Ass.-Prof. Dipl.-Ing. Clemens Sauerwein, PhD  
46:27  
CySeReS-KMU: Webinar "IT-Sicherheitsstrategien für KMU" am...  
154 Aufrufe · vor 2 Jahren

# Webinare

<p>Online-Workshop</p> <ul style="list-style-type: none"> <li>• Lieferkettensicherheit</li> <li>• Limes-Security</li> </ul> <p>Video</p>	<p>Webinar 09/23</p> <ul style="list-style-type: none"> <li>• Lieferkettensicherheit</li> <li>• Projektteam</li> </ul> <p>Video</p>	<p>Webinar 10/23</p> <ul style="list-style-type: none"> <li>• Lieferkettensicherheit</li> <li>• Projektteam</li> </ul> <p>Video</p>	<p>Webinar 11/23</p> <ul style="list-style-type: none"> <li>• Penetrationstests</li> <li>• Zentrale Ansprechstelle Cybercrime (ZAC)</li> </ul>
<p>Webinar 12/23</p> <ul style="list-style-type: none"> <li>• Grundschutz</li> <li>• Cyber Trust Austria</li> </ul> <p>Video</p>	<p>Webinar 01/24</p> <ul style="list-style-type: none"> <li>• Penetrationstests</li> <li>• ProtectIT</li> </ul> <p>Video</p>	<p>Webinar 03/24</p> <ul style="list-style-type: none"> <li>• IT-Sicherheitsstrategien</li> <li>• Universität Innsbruck</li> </ul> <p>Video</p>	<p>Webinar 04/24</p> <ul style="list-style-type: none"> <li>• Sicherheitskonzepte</li> <li>• Blue Shield Security</li> </ul> <p>Video</p>
<p>Webinar 07/24</p> <ul style="list-style-type: none"> <li>• OT-Security</li> <li>• Verbund AG</li> </ul> <p>Folien</p>	<p>Webinar 09/24</p> <ul style="list-style-type: none"> <li>• KI in KMU</li> <li>• ProtectIT</li> </ul> <p>Video</p>	<p>Webinar 11/24</p> <ul style="list-style-type: none"> <li>• Assessments und Lösungen</li> <li>• CySeReS-KMU &amp; CYSSME</li> </ul> <p>Video</p>	

# Nennenswerte Auftritte „außerhalb“



# Unser Reifegradmodell

## Neuartiges Cyber-Security Assessment spezifisch für KMU auf Website verfügbar!

*Details später...*

### A: Themenbereich Grundschutz

1. Zugriffskontrolle: Der Zugriff auf Daten, Netzwerke und Systeme ist durch Zugriffskontrollmechanismen wie Passwörter, Zwei-Faktor-Authentifizierung und Verschlüsselung gesichert. Dies gilt insbesondere für Remote- und administrative Accounts. \*

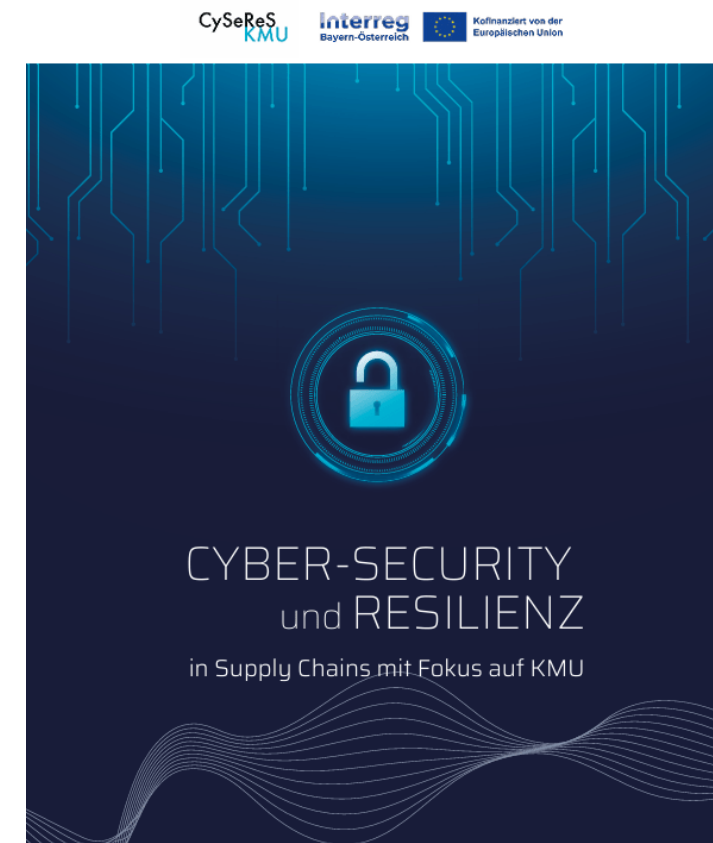
- Nicht umgesetzt
- Geplant
- In Umsetzung
- Teilweise umgesetzt
- Weitgehend umgesetzt
- Vollständig umgesetzt

2. Sicherung des Unternehmensumfeldes: Nur autorisierte Personen und Geräte haben Zugang zu Netzwerken und sensiblen Daten. Digitale und physische Sicherheitsmaßnahmen wie Firewalls, VPNs, WLAN-Schutz und Zugangskontrollen verhindern unbefugten Zugriff. \*

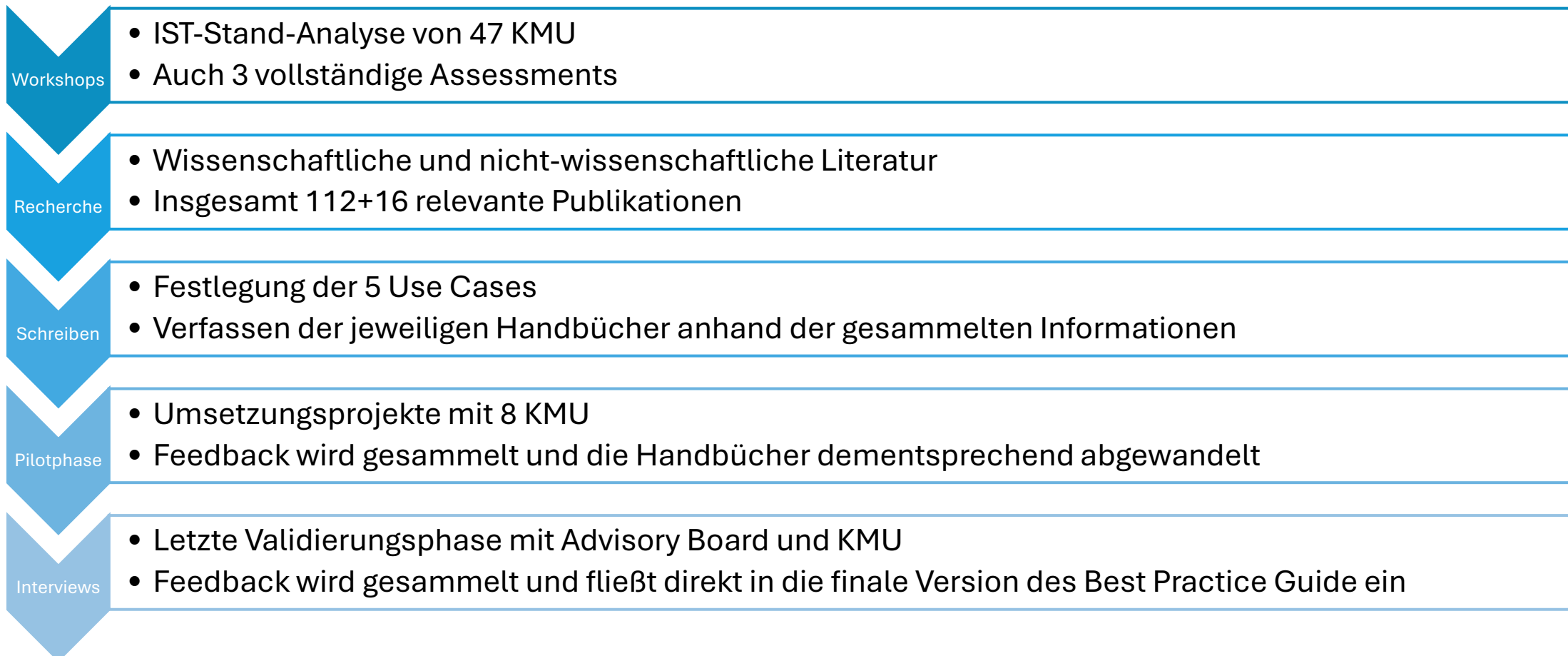
- Nicht umgesetzt
- Geplant
- In Umsetzung
- Teilweise umgesetzt
- Weitgehend umgesetzt
- Vollständig umgesetzt

# Unser Best Practice Guide

Finale Version unserer früheren Handbücher  
– jetzt auch für jedermann auf der Webseite  
verfügbar!



# Die Basis



# Unser Best Practice Guide

Grundschutz  
für KMU

Awareness &  
Kultur

Supply Chain  
Cybersecurity

Notfallkonzept  
für KMU

OT-Security  
für KMU

# Unser Best Practice Guide

- 5 Use Cases
- So kompakt wie möglich
- Handmarken für bessere Navigation
- Glossar und weiterführende Literatur
- Zusätzliche Anhänge wie Gantt-Charts

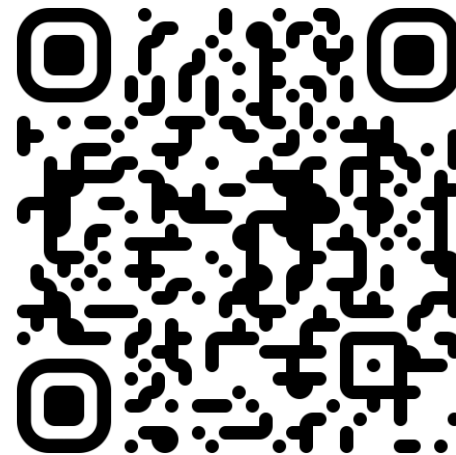
# Ihr Unser Best Practice Guide

---

*Wenn Sie ein gedrucktes Exemplar des Best Practice Guides haben wollen, bekommen Sie gerne eins!*

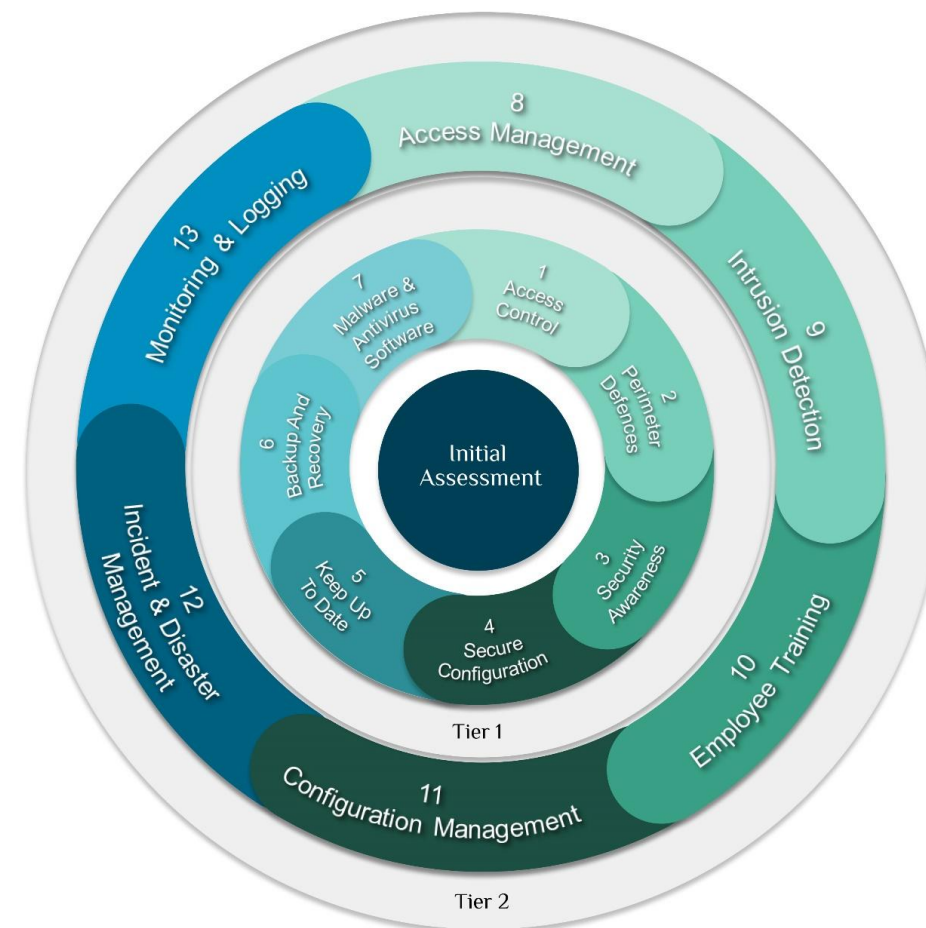
*Sie können auch mehrere mitnehmen.*

*Eine PDF-Version befindet sich hier:*



# Grundschutz für KMU

Aufgeteilt in 2 Tiers  
 ... 15 Hauptmaßnahmen  
 ... und 44 konkrete  
 Handlungsempfehlungen



# Projektvorbereitung

---

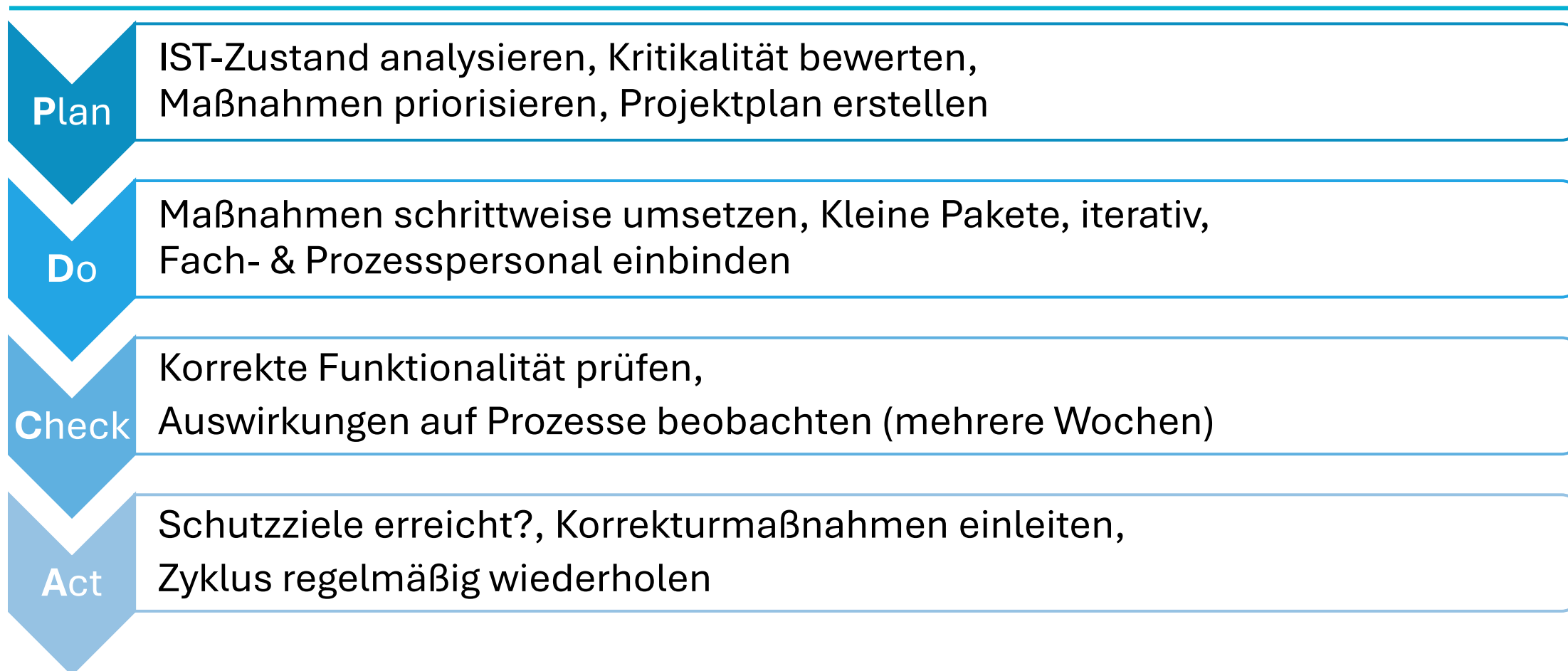
## IST-Zustand erfassen:

- Informationen & Daten
- Hardware & Software (Inventarisierung)
- Prozesse & Datenflüsse
- Wissenstand/Expertise
- Bereits umgesetzte Maßnahmen
- Kritische Prozesse & Assets

## Projektplanung:

- Zielsetzung festlegen  
*Schutzziele, Normen, Ressourcen*
- Verantwortlichkeiten?  
*1-2 dedizierte Ansprechpartner benennen*
- Priorisierung & Zeitplan  
*Gantt-Chart als anpassbare Vorlage verfügbar*

# Vorgehensweise: Der PDCA-Zyklus



# Unsere Grundschutz-Maßnahmen

Zugangskontrolle	Sicherung des Unternehmensumfelds	Sicherheitsbewusstsein	Sichere Konfiguration	Patches & Updates
Datensicherung & Wiederherstellung	Malware & Antivirus	Zugangsmanagement	Angriffserkennung	Mitarbeiterschulungen
Konfigurationsmanagement	Reaktion auf Zwischen- und Notfälle	Logging & Monitoring	Cyber-Versicherung	Lieferkette & OT

# Ausgewählte Schlüsselmaßnahmen

## Zugangskontrolle

*Benutzerauthentifizierung*

*Least-Privilege-Prinzip*

*Passwortrichtlinie*

*Verschlüsselung*

## Sicherung des Unternehmensumfelds

*Kontrolle von Hardware*

*WLAN sichern*

*Physische Zugangskontrolle*

## Datensicherung

*Automatisierung*

*Segmentierung*

*Verschlüsselung*

*Testen der Kopien*

## Sichere Konfiguration

*Authentifizierung einrichten*

*Protokollierung*

*Deaktivierung von Funktionen*

# Kontinuierliche Verbesserung & Frameworks



## Cybersecurity als fortlaufender Prozess

- *Bedrohungen entwickeln sich ständig weiter*
- *PDCA-Zyklus muss regelmäßig wiederholt werden*
- *Maßnahmen müssen aktualisiert werden*
- *Neue Risiken müssen bewertet werden*

BSI IT-Grundschutz / KMU Leitfaden

*Bundesamt für Sicherheit (DE)*

ENISA Cybersecurity Guide for SMEs

*EU Agency for Cybersecurity*

NIST CSF 2.0 – Small Business Guide

*National Institute of Standards (US)*

CIS Critical Security Controls v8.1

*Center for Internet Security*

ISO 27001/27002

*Für zertifizierungswillige Unternehmen*

# Take-Aways

IST-Analyse zuerst:  
Inventarisierung von Assets, Prozessen & Daten

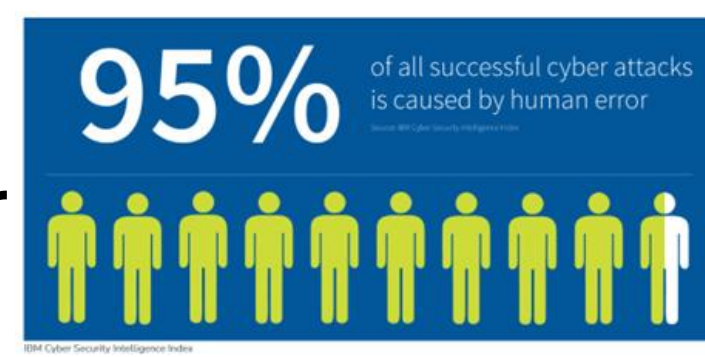
Schrittweise vorgehen: PDCA-Zyklus ermöglicht  
inkrementelle, kontrollierbare Verbesserungen

Mensch im Mittelpunkt: Mitarbeiterschulungen, klare  
Sicherheitsrichtlinien und Prozesse sind entscheidend

Kein Endpunkt: Cybersecurity ist ein  
kontinuierlicher Prozess – nichts Einmaliges

Werkzeuge nutzen: Inventarlisten, Gantt-Chart und  
etablierte Frameworks als Starthilfe

# Cyber-Security Awareness & Kultur



Safety First

Zero Trust



**ZERO TRUST**

Skillset

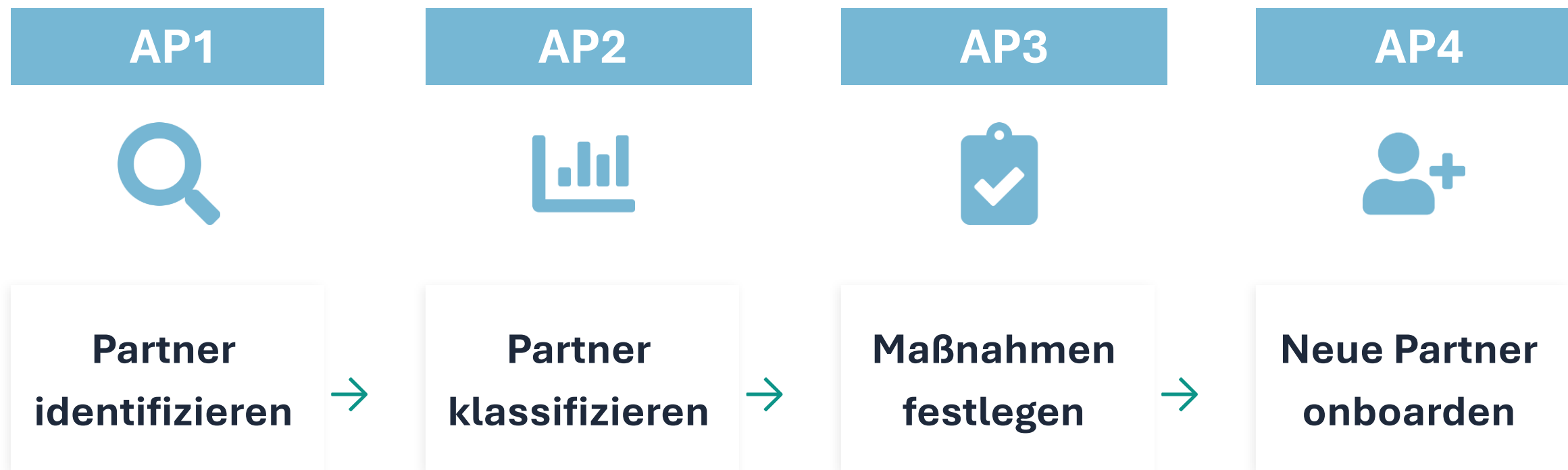
Mindset

Toolset

# Warum Supply Chain Cyber-Security?



# Vorgehensweise in 4 Arbeitspaketen



# SC-Partner identifizieren



## Kreditoren- & Debitorenliste

- Export aus ERP-System
- Mit Fachabteilung prüfen: Hat der Partner Zugriff auf IT/OT-Systeme oder Assets?



## Assets als Ausgangsbasis

- Kritische Assets identifizieren (IT, OT, Daten, Logistik)
- Zuordnen, welche SC-Partner darauf Zugriff haben



## Kombinierter Ansatz

Beide Methoden verbinden:

- Assets identifizieren
- Mit Kreditoren/Debitorenliste abgleichen und ergänzen

# SC-Partner klassifizieren mit Excel-Tool



# Risikobasierte Maßnahmen festlegen

## Unternehmensinterne Maßnahmen



Kompetenzen aufbauen  
Interne Kapazitäten und Backups schaffen



Mehrlieferantenstrategie  
Abhängigkeiten durch multiple Quellen  
reduzieren



Need-to-Know Prinzip  
Zugriff auf das Notwendigste beschränken

## Maßnahmen mit SC-Partnern



Verantwortliche benennen  
Ansprechpartner für Cyber-Security festlegen

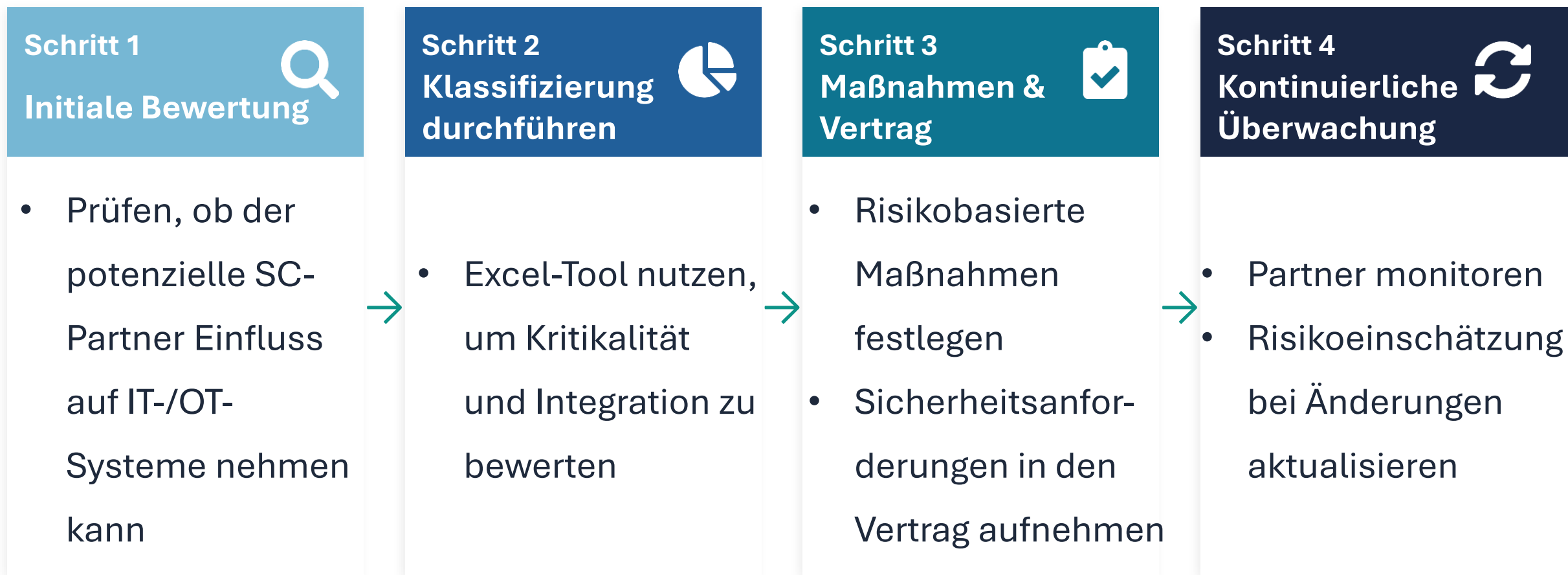


Fragebögen & Zertifizierungen  
Sicherheitspraktiken abfragen (ISO 27001,  
TISAX)



Verträge anpassen  
Sicherheitsanforderungen vertraglich  
verankern

# Prozess für neue SC-Partner



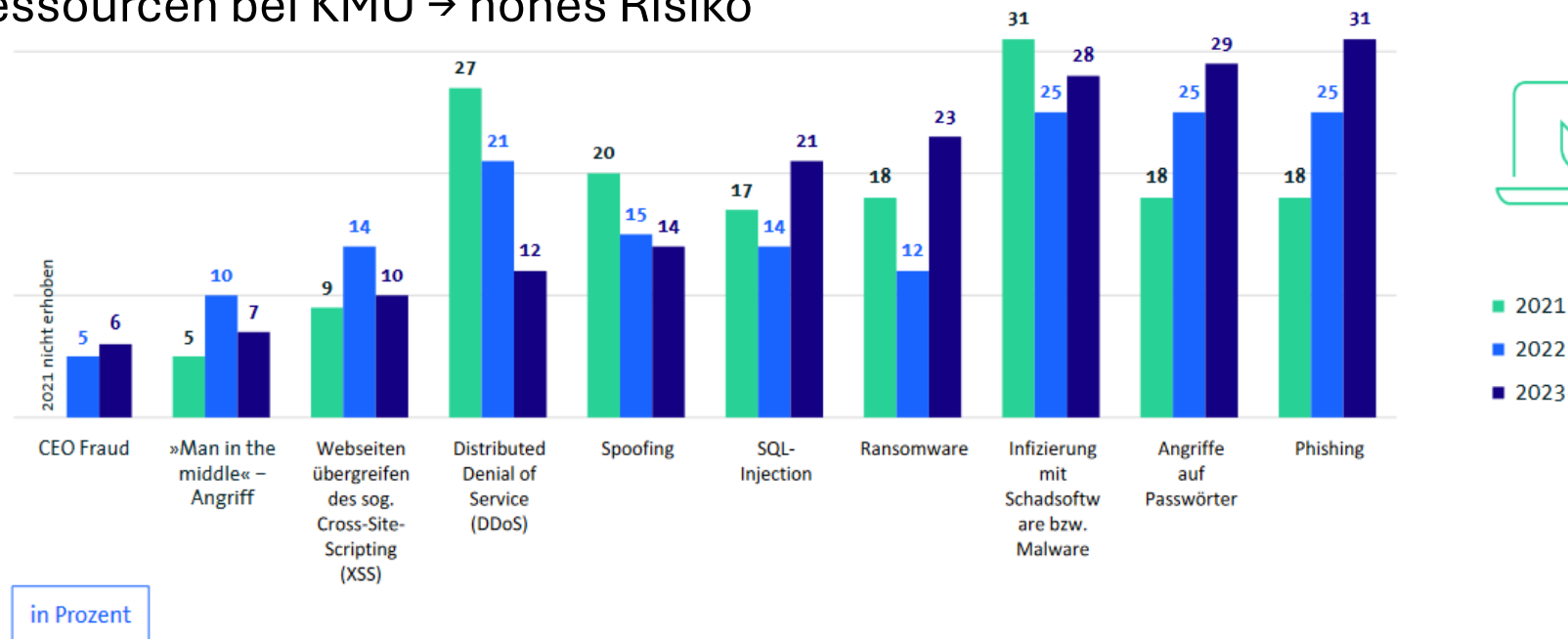
# Take-Aways

---

- 1 Nicht nur IT-Lieferanten sind relevant**
- 2 Klassifizierung schafft Fokus**
- 3 Maßnahmen skalieren mit dem Risiko**
- 4 Neue Partner von Anfang an einbinden**
- 5 Cybersicherheit ist ein fortlaufender Prozess**

# Warum ein Cyber-Notfallkonzept?

- Existenzbedrohende Schäden
- Gesetzliche Meldepflichten (DSGVO)
- Mangelnde Ressourcen bei KMU → hohes Risiko



Basis: Alle Unternehmen (n=1.002) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2023

# Das 4-Phasen-Modell

## Vorbereitung

- Risikoanalyse
- Notfallplan
- Business Continuity Plan (BCP)

## Bereitschaft

- Notfallteam aufstellen
- Kontaktliste + Kommunikationswege
- Schulungen & technische Schutzmaßnahmen

## Bewältigung

- Incident erkennen
- Eindämmung und Sofortmaßnahmen
- Kommunikation & Wiederherstellung

## Nachbereitung

- Lessons Learned
- Konzept überarbeiten
- Monitoring verbessern

# Phase 1 – Vorbereitung auf den Ernstfall

## Risikoanalyse & Bewertung

- Identifikation kritischer Systeme und Daten
- Bewertung von Bedrohungen und Schwachstellen
- Ermittlung potenzieller Auswirkungen
- Vorlage für Risikomatrix in Best Practice Guide

## Notfallplan mit Eskalationsstufen

- Festlegung von Eskalationsstufen
- Definition von Alarmierungswegen
- Dokumentation von Wiederherstellungsverfahren

## Business Continuity Plan (BCP)

- Analyse kritischer Geschäftsprozesse
- Festlegung maximaler Ausfallzeiten (RTO/RPO)
- Entwicklung von Notfallbetriebsverfahren

# Phase 2 – Bereitschaft

## Organisation & Team

Aufbau eines Cyber-Notfallmanagementteams

Zuweisung klarer Rollen (z. B. IT, Datenschutz, extern)

Regelmäßige Kontaktpflege & Erreichbarkeit sicherstellen

Einrichtung sicherer Kommunikationskanäle (z. B. Threema, Signal)

## Technische Prävention

Regelmäßige Backups (intern & extern)

Multi-Faktor-Authentifizierung (MFA) aktivieren

Sicherheitsupdates und Patches stets aktuell halten

Netzwerksegmentierung + Firewall-Management

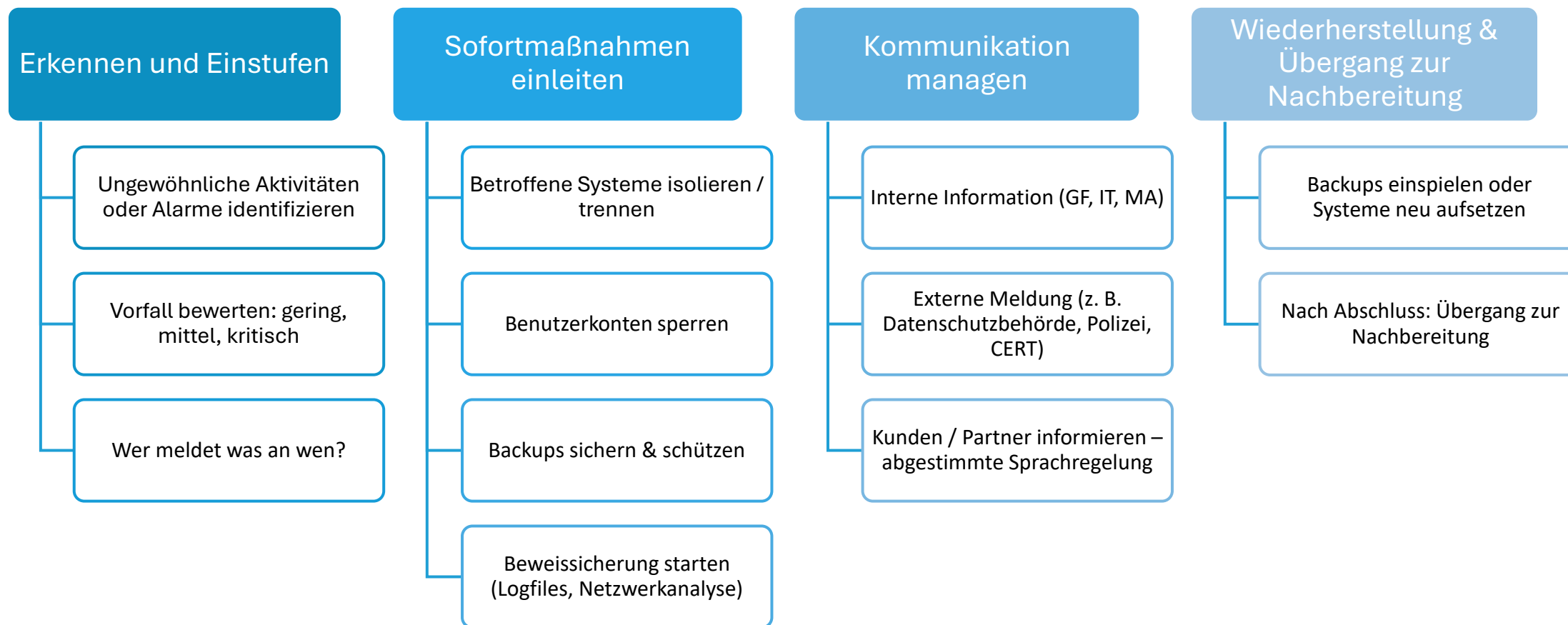
## Schulung & Übung

Sensibilisierung der Mitarbeitenden (Phishing, Passwortregeln etc.)

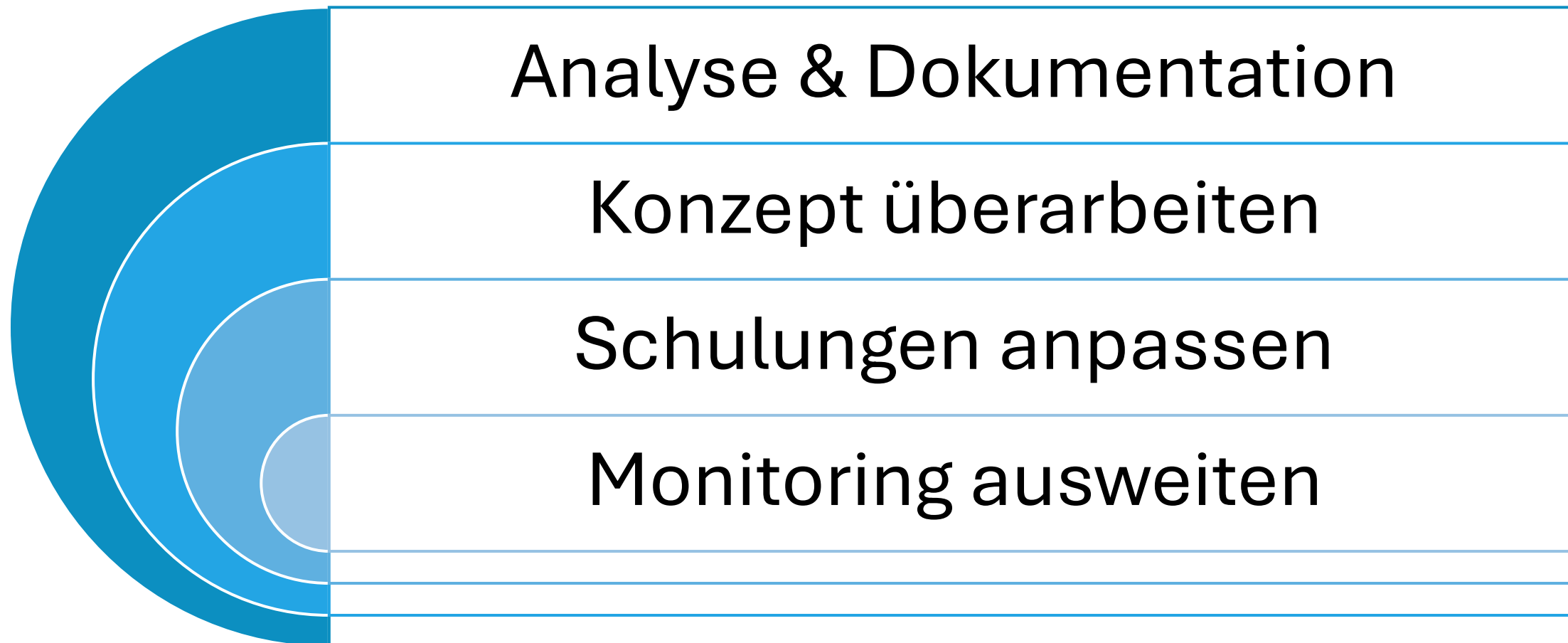
Durchführen von Planspielen und Szenarioübungen

Testen des Notfallplans unter realistischen Bedingungen

# Phase 3 – Reaktion (Incident Response)



# Phase 4 – Lessons Learned

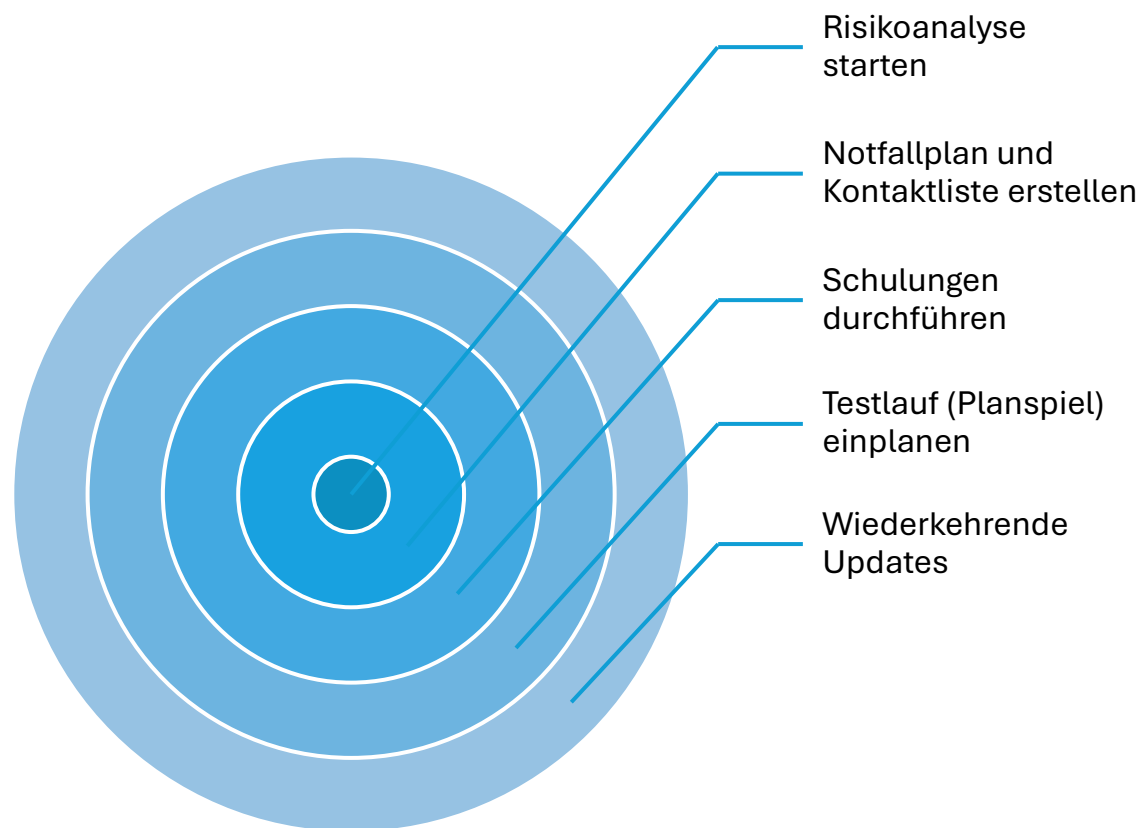


# Im Ernstfall: Schnell und strukturiert reagieren

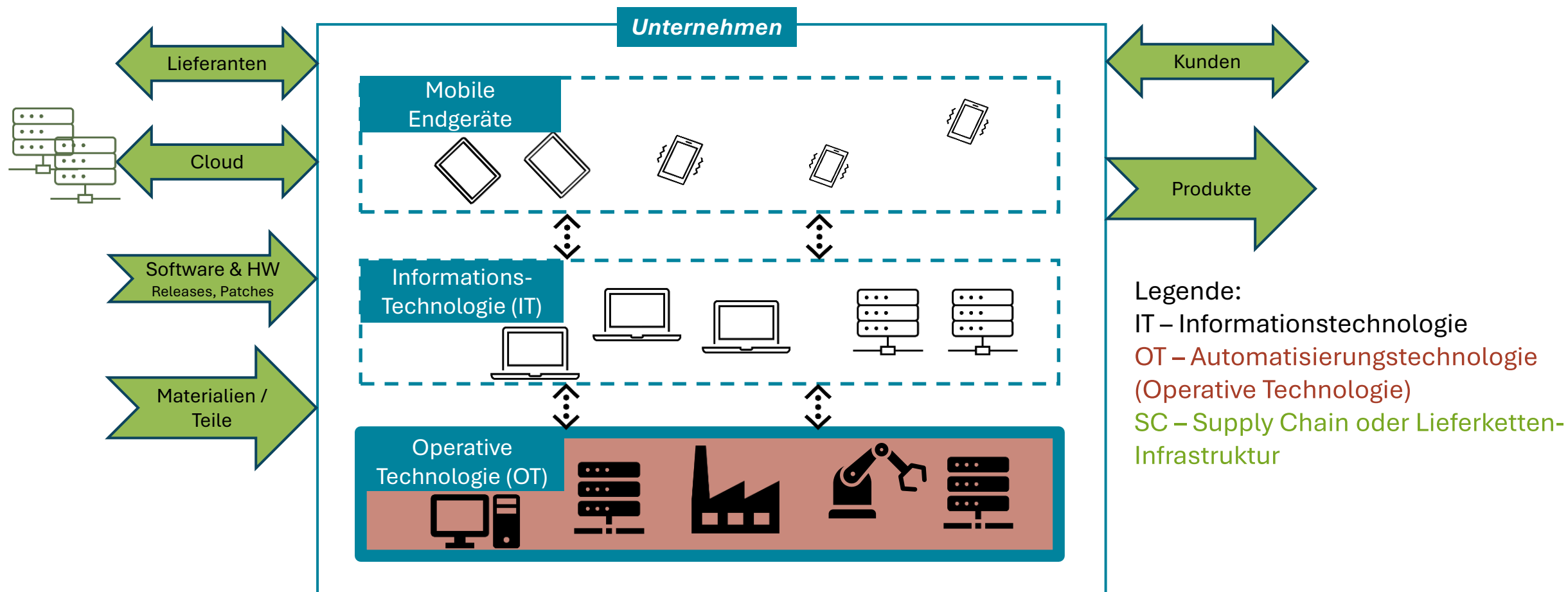
---

- 🚨 Vorfall erkennen & korrekt einstufen
- 🚨 Betroffene Systeme sofort trennen
- 🚨 IT-Team oder Dienstleister aktivieren
- 🚨 Beweissicherung starten
- 🚨 Datenschutzbehörde / Polizei informieren (bei Bedarf)
- 🚨 Kunden & Partner aktiv informieren
- 🚨 Alle Maßnahmen dokumentieren
- 🚨 Nach dem Vorfall: Lessons Learned & Schulung anpassen

# Take-Aways – Was Sie jetzt tun sollten



# Wie ist ein KMU aufgebaut?



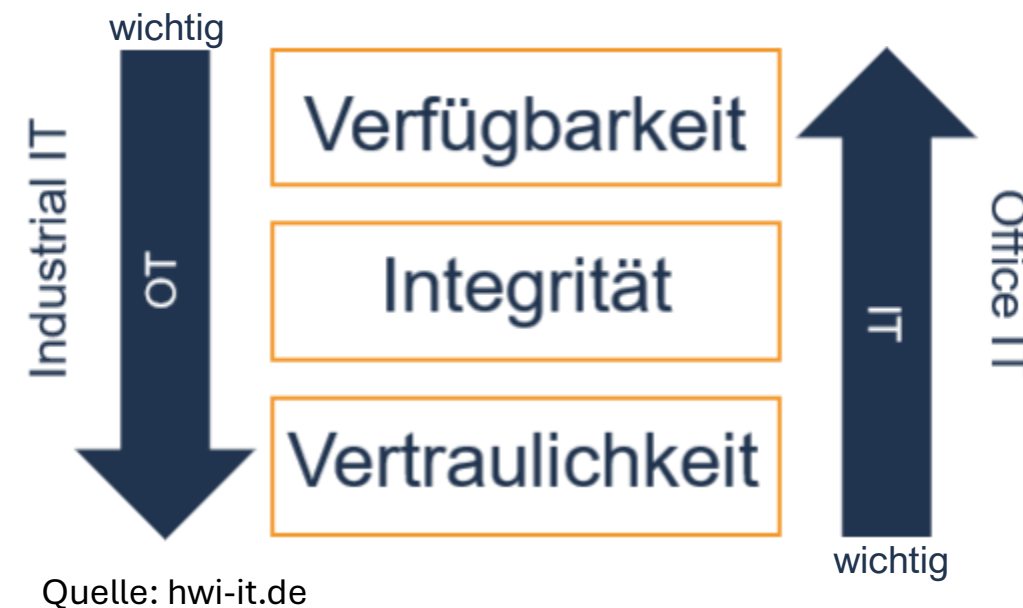
# Was gehört alles zur OT?

---

- ICS (Industrial Control System): überwacht und steuert Betrieb von Maschinen und zugehörigen Geräten
- SCADA (Supervisory Control and Data Acquisition): das Computersystem/die Software eines ICS
- DCS, RTU, PLC, BMS, BAS, CNC, SPS, Energieüberwachung, Verkehrssysteme

# Unterschiede: IT- vs. OT-Sicherheit

- In IT: Vertraulichkeit am wichtigsten  
In OT: Verfügbarkeit am wichtigsten
- In IT: Antivirus-Software  
In OT: schwer/nicht möglich
- In IT: Regelmäßige Updates  
In OT: Updates schwer möglich
- In IT: Lebenszyklus „eher kurz“  
In OT: Lebenszyklus sehr lang



# Warum ist OT-Security wichtig?

DDoS-Angriffe leicht durchzuführen

↔ Verfügbarkeit ↔

Keine Antivirensoftware

↔ Schadsoftware leicht einzuschleusen ↔

Updates schwer möglich

↔ mehr bekannte Sicherheitslücken ↔

# Open-Source Assessment: LARS-ICS

**Network Design & Management**

Nicht relevant

**Netzplan**

- Die Struktur des Netzes muss in einem physischen und einem logischen Netzplan dokumentiert werden.
- Der physische Plan zeigt die Orte und Infrastruktur des ICS, z. B. Kabel, Gebäude, Funkverbindungen. Der Plan muss dem aktuellen Stand der Technik berücksichtigen und mindestens Folgendes enthalten:
  - IP-Netzadressen und Netzmasken (z. B. 192.168.1.0/24),
  - IP-Adressen aller angeschlossenen Netzinterfaces (z. B. 192.168.1.54)
  - MAC-Adressen,
  - Computernamen und Funktionalität der Systeme,
  - (falls vorhanden) DNS-Name,
  - (falls vorhanden) FQDN (FullyQualifiedDomainName) und
  - Die technische Dokumentation muss im gesamten Lebenszyklus aktualisiert und gepflegt werden (beginnend bei den Vorgaben an Lieferanten und Planer).
- Der logische Netzplan ignoriert die physischen Gegebenheiten und fokussiert auf die logische Sicht und Sicherheitszonen.

umgesetzt  teilweise umgesetzt  nicht umgesetzt  nicht relevant

**Netzsegmentierung**

- Ein ICS-Netz muss aus mehreren Netzsegmenten mit individuellen Schutzbedarfen bestehen.
- Der Datenverkehr zwischen den Netzen muss durch eine Datenflusskontrolle, z. B. Firewall, auf das betriebliche notwendige Maß reglementiert werden.
- Bei entsprechend hohem Schutzbedarf muss zwischen der Unternehmensebene und der Leitebene eine Demilitarisierte Zone (DMZ) eingefügt werden.
- Proxy-Dienste mit Filtermöglichkeiten bis hin zum Layer 7 müssen den Datenverkehr steuern und kontrollieren.
- Neben der Trennung von Netzen mit unterschiedlichen Funktionalitäten müssen auch standortübergreifende Netze oder allgemein organisatorisch unabhängige Maschinen/Anlagen untereinander segmentiert werden (vertikale Trennung)
- Der Verbindungsaufbau muss immer aus dem Netzsegment mit dem höheren Schutzbedarf in das Netzsegment mit dem niedrigeren Schutzbedarf aufgebaut werden.
- Eine Umgehung der Netztrennung durch undokumentierte Verbindungen darf nicht stattfinden.
- Insbesondere dürfen keine unkontrollierten Verbindungen zu Netzsegmenten mit niedrigerem Schutzbedarf zugelassen werden.

umgesetzt  teilweise umgesetzt  nicht umgesetzt  nicht relevant

Vorige Nächste Zurück Weiter

ICS gesamt->Übergeordnet->Network Design & Management

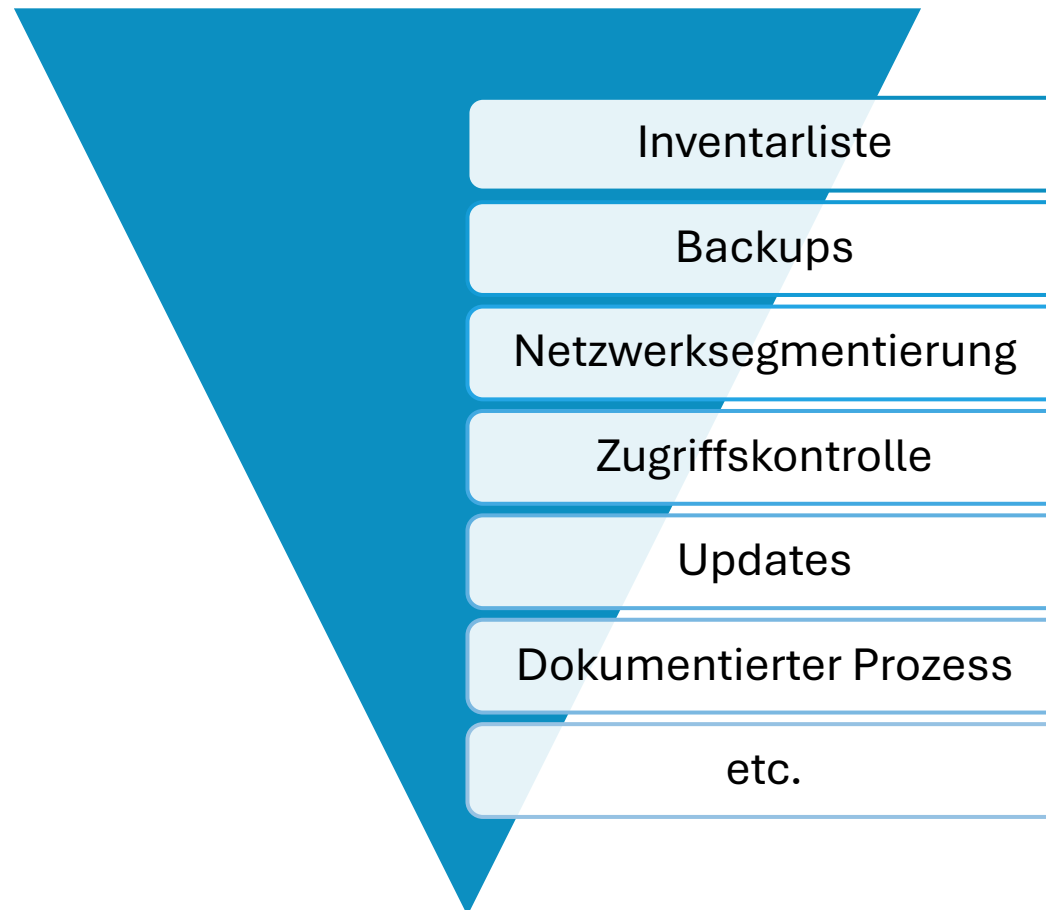


# Open-Source Assessment: CSET

The screenshot displays the CSET web application interface. The top navigation bar includes 'File', 'Edit', 'View', and 'Window'. Below this is a dark blue header with the CSET logo, 'Tools', 'Resource Library', 'Help', and a user profile 'nicom'. The main content area is divided into three tabs: 'Prepare', 'Assessment' (active), and 'Results'. A left sidebar contains a navigation menu with sections for 'Prepare', 'Assessment', and 'Results'. Under 'Assessment', 'Standard Requirements' is selected. The main content area shows 'Requirements Mode' with a progress indicator '2/185' and an 'Auto-load Guidance' checkbox. The title 'Standard Requirements' is followed by the instruction: 'Select the applicable answer for each of the following questions. Unanswered questions are calculated as a 'No' response.' The current question is 'Access Control - SP800-82 R3' with the sub-heading 'Access Control Policy and Procedures' and a 'Requires Review' checkbox. The question text is: 'AC-1 OT Discussion: The policy specifically addresses the unique properties and requirements of OT and the relationship to non-OT systems. OT access by vendors and maintenance staff can occur over a large facility footprint or geographic area and into unobserved spaces, such as mechanical or electrical rooms, ceilings, floors, field substations, switch and valve vaults, and pump stations.' Below the text are five response buttons: 'Yes' (green), 'No' (red), 'N/A' (blue), 'Alt' (yellow), and a flag icon. A sub-question 'a. Develop, document, and disseminate to [Assignment organization-defined personnel or roles]:' is followed by a numbered list: '1. [Selection (one or more): Organization-level; Mission/business process-level; System level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and'.



# Best Practices



# Best Practice: Inventarliste

## Vollständigkeit

Sind alle Geräte erfasst?

## Richtigkeit

Regelmäßige (bspw. halbjährliche) Aktualisierung  
Am besten: dokumentierter Prozess

## Nutzbarkeit

Wikis, Datenbanken, Tabellen,  
dedizierte Inventarisierungs-Software

## Sicherheit

Passwortschutz, Erreichbarkeit im Notfall, Backups

- Interne\_ID\_des\_Geräts\_1 (Gerätename 1):
  - Hersteller mit Kontaktdaten: XX
  - Instandhalter mit Kontaktdaten: XX
  - Notfallkontaktdaten: XX
  - SLAs:
    - XX
    - YY
  - Modellnummer: XX
  - Seriennummer: XX
  - Installationsdatum: XX.XX.XXXX
  - EOL-Datum: XX.XX.XXXX
  - Standort: XX
  - [...]
- Interne\_ID\_des\_Geräts\_2 (Gerätename 2):
  - [...]

# Best Practice: Netzwerksegmentierung

## Makrosegmentierung

- Geräte von außen nicht mehr erreichbar

## Mikrosegmentierung

- Kommunikation der OT-Geräte untereinander einschränken

# Take-Aways

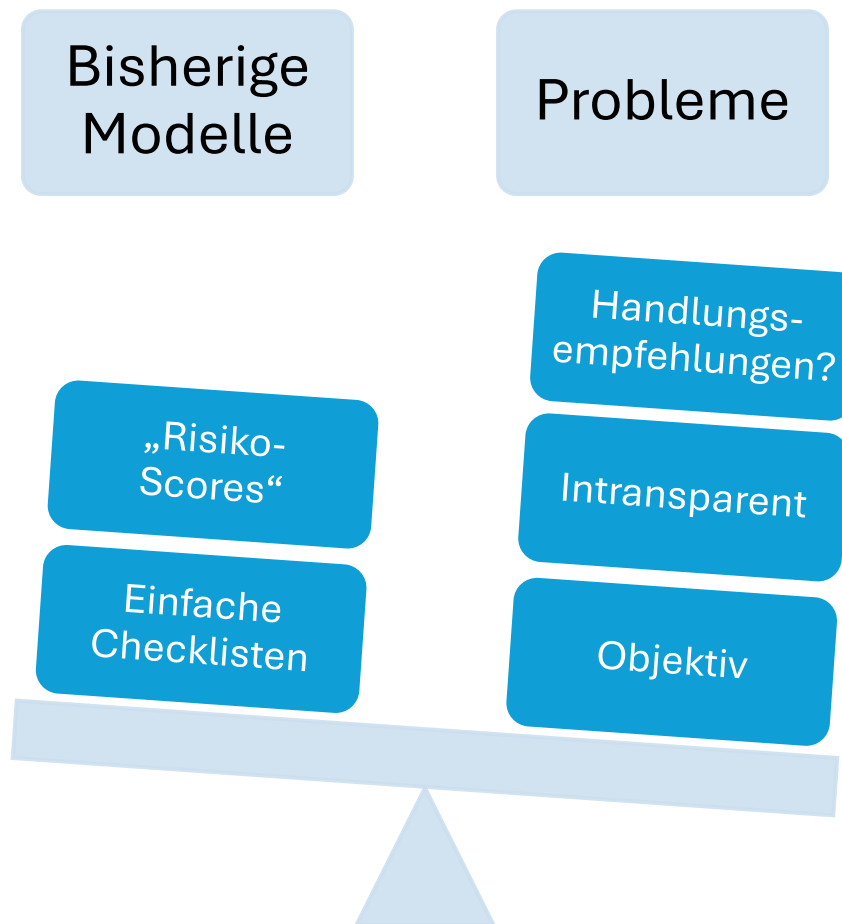
Inventarliste anlegen oder aktualisieren

Netzwerkstruktur untersuchen und segmentieren

Backups einrichten, testen und einen regelmäßigen Prozess definieren

Audits in Prozess integrieren

# Der Status Quo



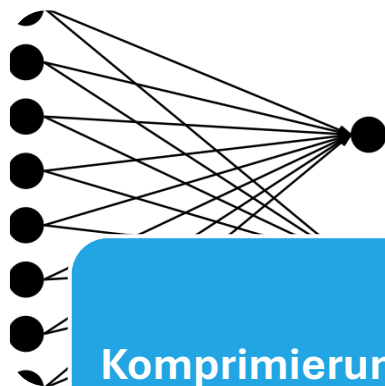
# Unser Reifegradmodell

## ← Themenbereich Grundschutz

1. Zugriffskontrolle: Der Zugriff auf Daten, Netzwerke und Systeme ist durch Zugriffskontrollmechanismen wie Passwörter, Zwei-Faktor-Authentifizierung und Verschlüsselung gesichert. Dies gilt insbesondere für Remote- und administrative Accounts.\*
- Nicht umgesetzt
  - Geplant
  - In Umsetzung
  - Teilweise umgesetzt
  - Weitgehend umgesetzt
  - Vollständig umgesetzt

2. Sicherung des Unternehmensumfeldes: Nur autorisierte Personen und Geräte haben Zugang zu Netzwerken und IT-Systemen.
- Nicht umge
  - Geplant
  - In Umsetzu
  - Teilweise u
  - Weitgehen
  - Vollständig

**Assessment**  
KMU füllen Fragebogen aus



**Komprimierung**  
Daten werden komprimiert



**Untersuchung**  
KMU werden verglichen und Anhäufungen identifiziert



**Interpretation**  
Ihre Position im Feld zeigt Ihre Ähnlichkeit zu anderen KMU (nah - Das 'x' in der Mitte zeigt Ihr Unternehmen - jeder Punkt ist ein and Die unterschiedlichen Farben trennen Anhäufungen von KMU. Ihre Bewertung hängt von dieser Farbe ab.

**Ihr Ergebnis im Detail**  
Ihr Unternehmen befindet sich in folgender Anhäufung:  
*"Die bewussten Einsteiger: Gute Basis, schwache Reaktion"*

Sie haben somit einen Risiko-Score von 5.  
Je niedriger dieser Score, desto besser. Er befindet sich immer zw

Sie haben ein gutes Fundament im Grundschutz und eine sensiblen Fokus

**Rückmeldung**  
KMU erhalten Ergebnis basierend auf ihrer Position im Gesamtbild

# Unser Reifegradmodell – Assessment

Grundschutz

13 Fragen

OT-Security

5 Fragen

Notfallkonzept

3 Fragen

Lieferkette

5 Fragen

Awareness &  
Kultur

2 Fragen

Demographie

4 Fragen

# Unser Reifegradmodell – Statistik

## Komprimierung

28 Fragen werden  
auf 2 Dimensionen  
reduziert

Ähnliche  
Antworten bleiben  
nah beieinander

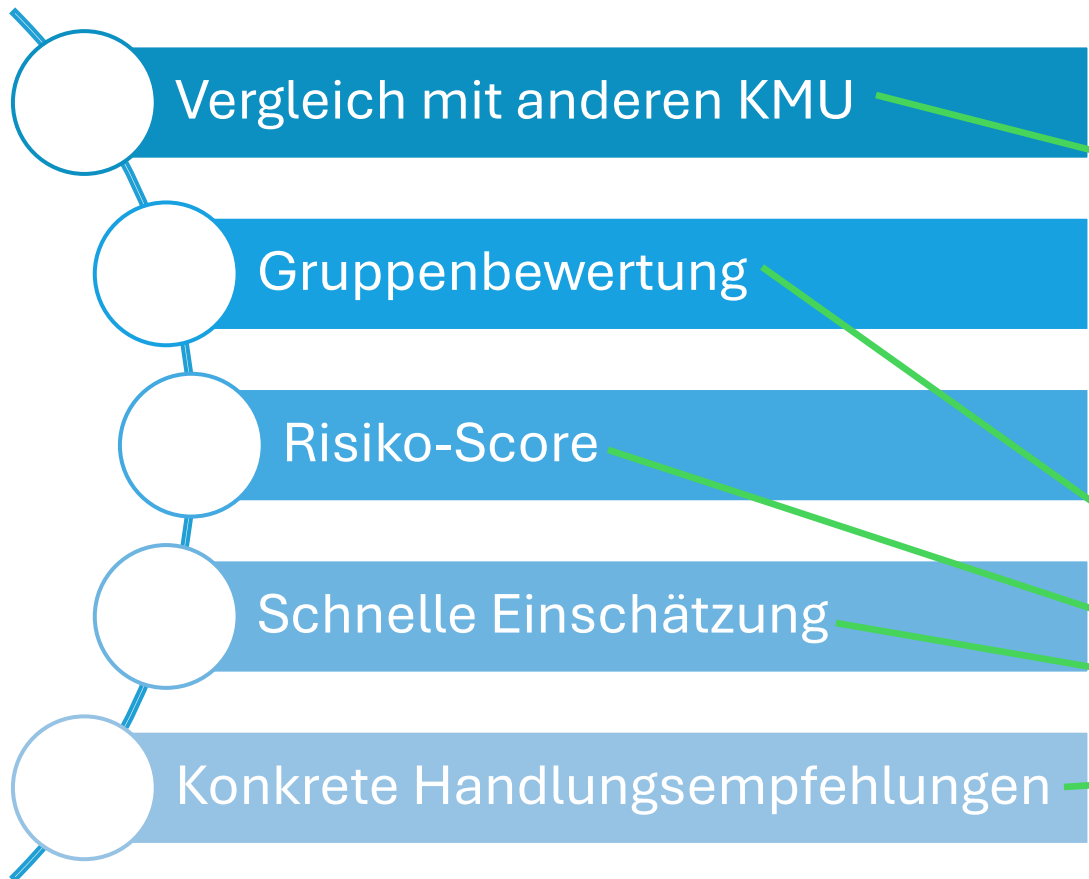
## Untersuchung

Anhäufungen  
werden gesucht  
KMU werden in  
Gruppen eingeteilt

## Identifikation

Gruppen werden  
interpretiert und  
bewertet  
KMU erhalten ihr  
Assessment

# Unser Reifegradmodell – Rückmeldung

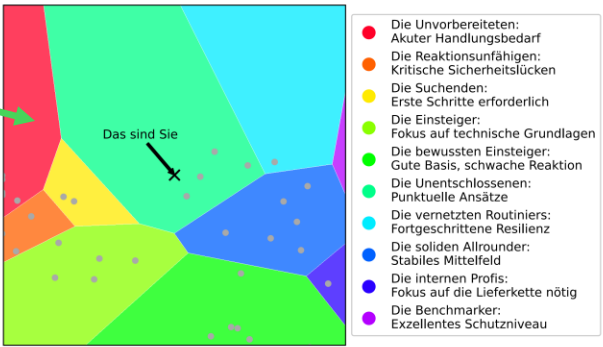


**CySeReS-KMU Reifegradmodell Bericht**



Vom: 17.02.2026, 16:06  
Company Name | Risiko-Score: 4/8

**Wo stehe ich im Vergleich zu anderen KMU?**



**Interpretation**

Ihre Position im Feld zeigt Ihre Ähnlichkeit zu anderen KMU (nah = ähnlich). Das 'x' in der Mitte zeigt Ihr Unternehmen - jeder Punkt ist ein anderes KMU. Die unterschiedlichen Farben trennen Anhäufungen von KMU. Ihre Bewertung hängt von dieser Farbe ab.

**Ihr Ergebnis im Detail**

Ihr Unternehmen befindet sich in folgender Anhäufung: *"Die Unentschlossenen: Punktuelle Ansätze"*  
 Sie haben somit einen Risiko-Score von 4. Je niedriger dieser Score, desto besser. Er befindet sich immer zwischen 1 und 8.  
 Sie haben in einigen Bereichen bereits gute Ansätze, aber das Gesamtbild ist sehr ungleichmäßig. Es scheint, als würden Maßnahmen eher zufällig als nach einem strategischen Plan umgesetzt. Fokus: Harmonisierung der Maßnahmen und Schließung der größten Lücken.

→ Auf der nächsten Seite geht es weiter!

**Die nächsten Schritte für Ihr Unternehmen**

Aufgrund Ihres Assessment haben wir drei konkrete Empfehlungen für Ihre Cybersicherheit. Unserer Analyse stellen diese die zielführendste Variante dar, um die Cybersicherheit Ihres Unternehmens nachhaltig zu stärken.

**Maßnahmen und Abläufe im Alltag**

Identifizieren und wenden Sie im Arbeitsalltag einen ganzheitlichen Ansatz zum Schutz vor digitalen Risiken, wie Hackerangriffe, Schadsoftware etc. mit klaren Maßnahmen und Abläufen an. Details hierzu finden Sie in unserem Handbuch "Cyber Security Awareness & Kultur".

**Sicherheitsbewusstsein**

Informieren Sie Ihre Mitarbeitenden über aktuelle Sicherheitsbedrohungen und Ihre aktuellen Maßnahmen in der Cybersicherheit auf. Ein Newsletter kann hierbei sehr hilfreich sein. Details hierzu finden Sie in unseren Handbüchern "Cyber Security Awareness & Kultur" und "Security Grundschutz für KMU".

**Arbeiterschulungen**

Integrieren Sie regelmäßige Schulungen und Sicherheitsübungen ein, um die Awareness der Mitarbeitenden nachhaltig zu verbessern. Details hierzu finden Sie in unseren Handbüchern "Cyber Security Awareness & Kultur" und "Security Grundschutz für KMU".

**Die mehr möglichen Verbesserungen**

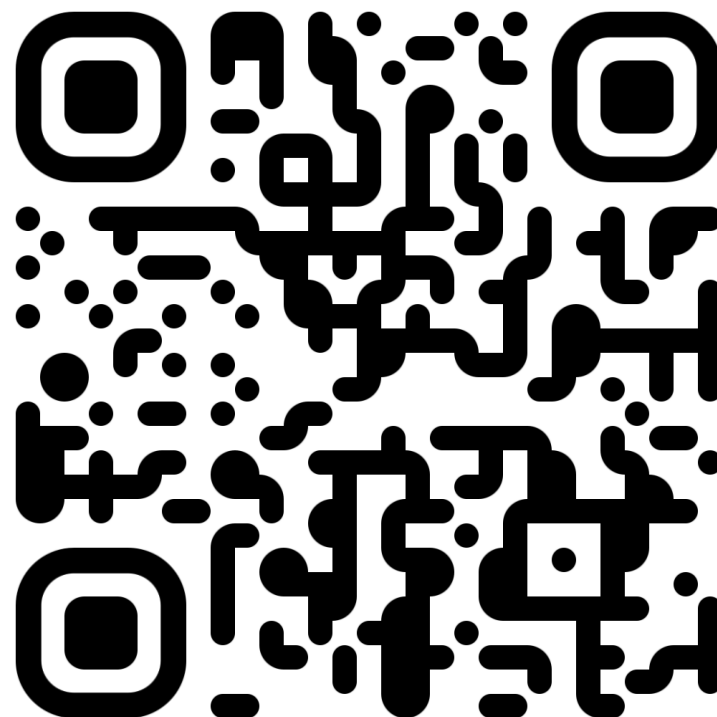
Implementieren Sie OT-Sicherheitsmaßnahmen, Konfigurationsmanagement, OT-Netzwerksegmentierung, Identifizierung und Protokollierung, Stakeholderbindung im Notfall, Datensicherung und -wiederherstellung, Feststellen von Angriffen, Standards für das Notfallkonzept, OT-Standards, Updates, Sicherheit von Partnern in der Lieferkette, Malware- und Antivirus-Schutz, Listen von Partnern in der Lieferkette, Sicherung des Unternehmensumfeldes, Supply Chain-Security, Zugriffskontrolle, Supply Chain-Security Verträge

Wenn Sie mehr Unterstützung erhalten Sie unsere Handbücher hier:

[/cyseres-kmu.eu/handbuecher/](https://cyseres-kmu.eu/handbuecher/)  
 Sie Fragen zu Ihrer Auswertung haben, können Sie uns gerne per E-Mail kontaktieren: [lexis@uni-passau.de](mailto:lexis@uni-passau.de)

# Unser Reifegradmodell ausprobieren

Verfügbar unter: <https://cyseres-kmu.eu/reifegradmodell/>



# Q&A mit Expertinnen und Experten

---

*Sie haben Fragen?  
Wir haben Antworten.*

# Buffet

---

*Vielen Dank für Ihre Aufmerksamkeit!*

*Das Buffet ist mittlerweile angerichtet.  
Bedienen Sie sich!*