Die digitale Hausbesetzung
Cybersicherheit in der technischen Gebäudeausrüstung (TGA)

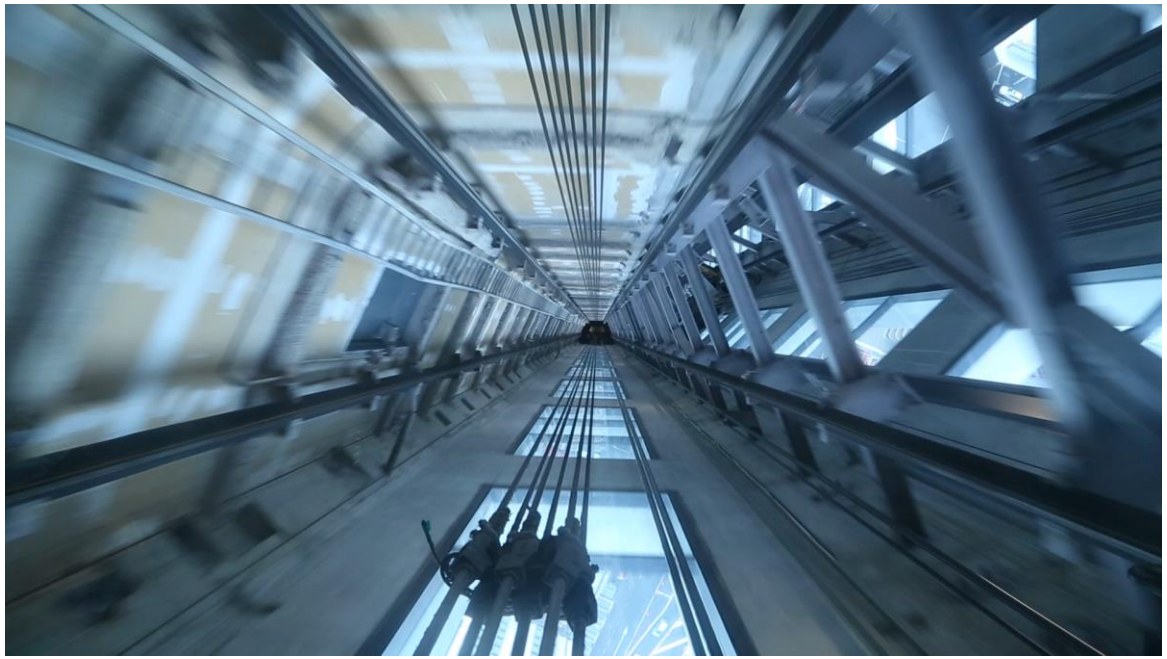
Ralf Schmitt
TÜV Rheinland Industrie Service GmbH

TÜVRheinland®
Genau. Richtig.

Wenn Sie so etwas auf dem Monitor sehen:

TÜVRheinland®
Genau. Richtig.

Welche Anlagen sind betroffen?

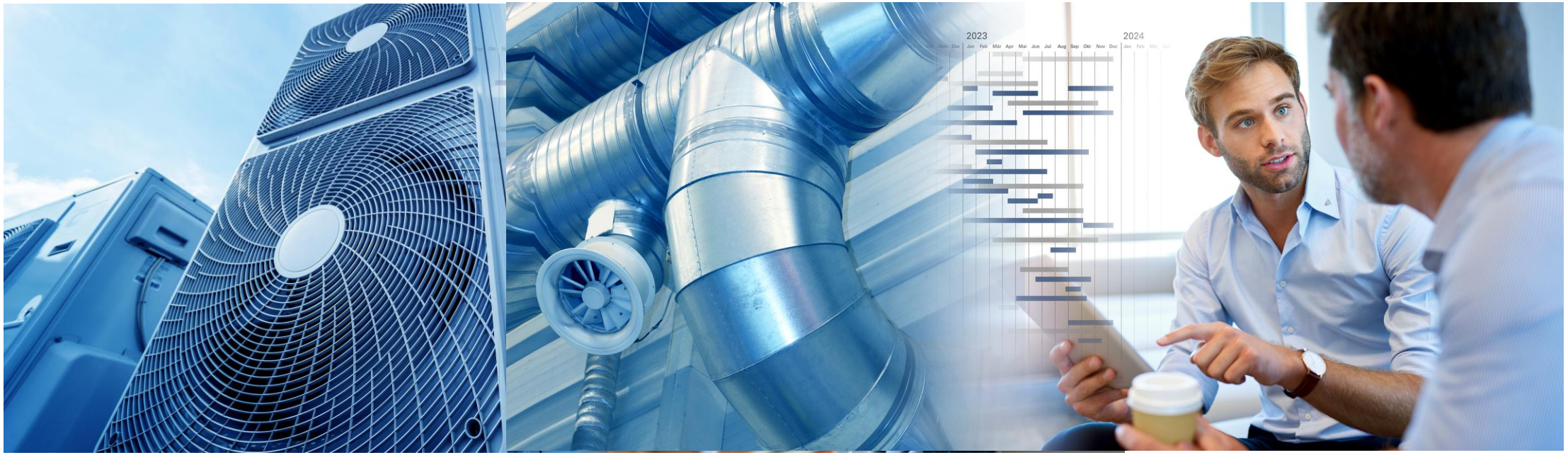


- **Aufzugsanlagen**

  Müssen entsprechend TRBS 1115-1 heute schon hinsichtlich der Cybersicherheit betrachtet werden.

TÜVRheinland®
Genau. Richtig.

Welche Anlagen sind betroffen?

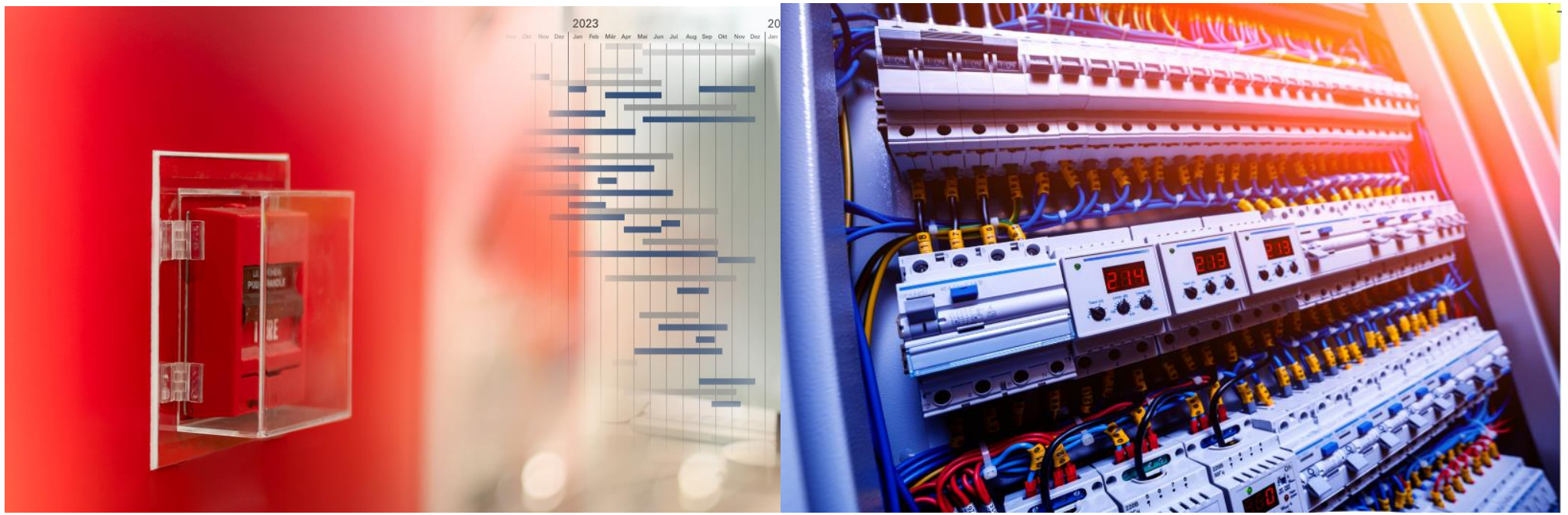


- **Klima-/Lüftungsanlagen**
  Regelung in ArbStättV § 4 Abs. 3 sicherheitsrelevanter gebäudetechnischer Anlagen.

- **Kälteanlagen (besondere Druckanlagen)**
  Müssen entsprechend TRBS 1115-1 heute schon hinsichtlich der Cybersicherheit betrachtet werden

TÜVRheinland®
Genau. Richtig.

Welche Anlagen sind betroffen?

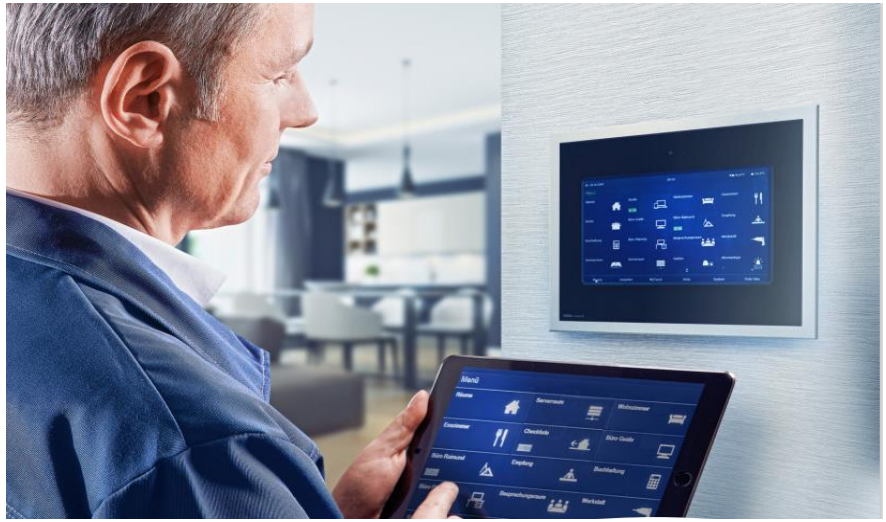


- **Brandmeldeanlagen**
  Regelung in ArbStättV § 4 Abs. 3 sicherheitsrelevanter gebäudetechnischer Anlagen.

- **Löschanlagen**
  Regelung in ArbStättV § 4 Abs. 3 sicherheitsrelevanter gebäudetechnischer Anlagen

TÜVRheinland®
Genau. Richtig.

Welche Anlagen sind betroffen?



- **Gebäudeleittechnik**
  Verfügbarkeit der gebäudetechnischen Anlagenteile und deren Komponenten

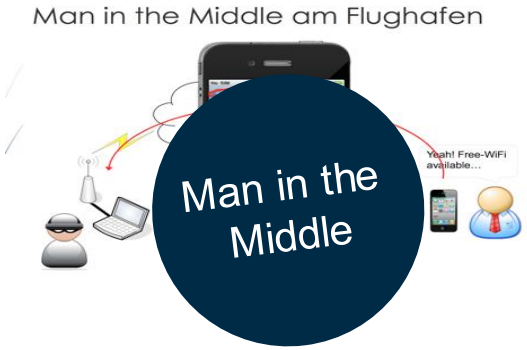
.

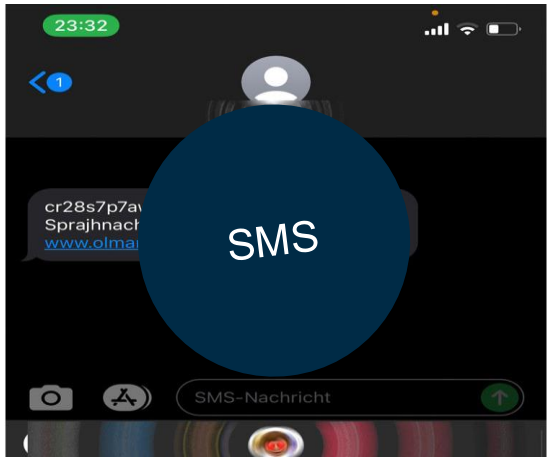
- **Beleuchtungsanlagen**
  Regelung in ArbStättV § 4 Abs. 3 sicherheitsrelevanter gebäudetechnischer Anlagen.

TÜVRheinland®
Genau. Richtig.

Was sind Cyberbedrohungen?

Zugriffsmöglichkeiten

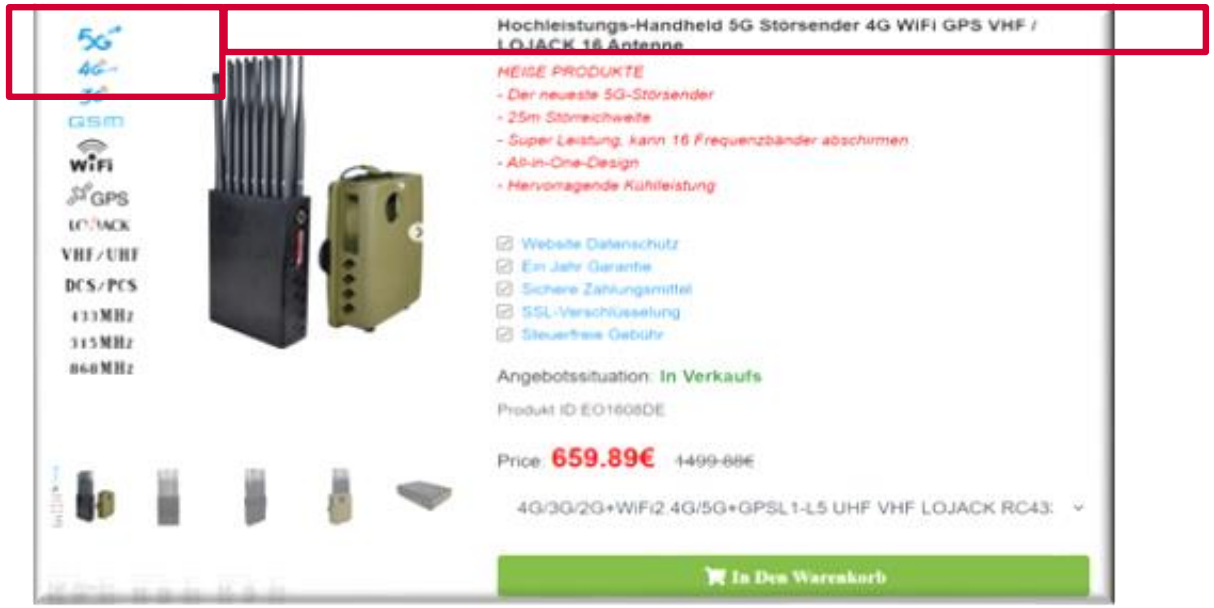




USB-Stick

TÜVRheinland®
Genau. Richtig.

Die kleinen Helfer für die Angreifer

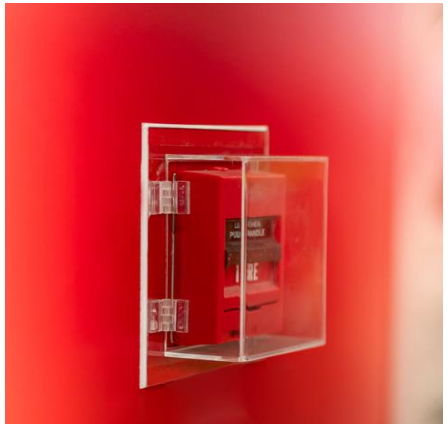


ALIExpress.com

Amazon.de

TÜVRheinland®
Genau. Richtig.

Szenarien, was ist möglich?



- **Zusammenspiel von Fluchttüren, Brandmeldeanlage und Zutrittsmanagement**
  auf der einen Seite müssen im Brandfall die Türen geöffnet werden, auf der anderen Seiten dürfen die Fluchttüren nicht unberechtigt geöffnet werden.

  Bei einer manipulierten Steuerung öffnen sich die Türen im Notfall ggf. nicht oder sie können unberechtigt geöffnet werden.

- **Fehlerhaft konfigurierte Klimatisierung,**
  die zu einer Überhitzung und Ausfall von IT-Systemen führen kann.

- **Nicht abgestimmt konfigurierte Systeme der Gebäudetechnik,**
  die zu Personen- und Systemschäden führen kann, wenn beispielsweise Strom- und Löschanlagen nicht koordiniert betrieben werden.

- **Manipulierte Lüftungsanlagen**
  in Sicherheitslaboren

TÜVRheinland®
Genau. Richtig.

Gefährdungen in der Gebäudeautomation

		Schweregrad			
		Akzeptabel Wenig oder keine Auswirkung durch den Zwischenfall	Tolerierbar Spürbare Auswirkung, aber nicht kritisch für das Ergebnis	Unerwünscht Schwere Auswirkung auf den Verlauf des Bereichs oder das Ergebnis	Nicht tolerierbar Könnte zu einer Katastrophe führen
Wahrscheinlichkeit	Unwahrscheinlich Es ist unwahrscheinlich, dass das Risiko auftritt	GERING – 1 –	MITTEL – 4 –	MITTEL – 6 –	HOCH – 10 –
	Möglich Das Risiko wird wahrscheinlich auftreten	GERING – 2 –	MITTEL – 5 –	HOCH – 8 –	EXTREME – 11 –
	Wahrscheinlich Das Risiko wird auftreten	MITTEL – 3 –	HOCH – 7 –	HOCH – 9 –	EXTREME – 12 –

Risikomatrix aus der IEC 62443-3

Die wesentlichen Gefährdungen der Gebäudeautomatisierung sind:

1. eine unzureichende Planung,
2. fehlende ganzheitliche Risikobetrachtung
3. fehlende Integration der TGA,
4. Nutzung unsicherer Systeme und Protokolle,
5. fehlerhafte Konfiguration der Gebäudeautomation,
6. Manipulation der Schnittstellen,
7. unzureichend geschützte Zugänge,
8. unzureichend abgesicherte Bedienelemente,
9. unzureichend abgesicherte Mobilfunk-Anschlüsse

TÜVRheinland®
Genau. Richtig.

Problemstellung

- Für das Errichten, Warten und Betreiben der Systeme sind meist externe Unternehmen verantwortlich, welche über die erforderlichen fachspezifischen Qualifikationen verfügen.

- Im Informationssicherheitsmanagement (ISMS) der Unternehmen sind die Komponenten und Anlagen der Gebäudeautomatisierung und der technischen Gebäudeausstattung oft nicht oder nur eingeschränkt im einer Organisation berücksichtigt.

Dies betrifft insbesondere die folgenden Aspekte:

- Vorgaben zur IT/OT-Sicherheit beim Planen, Errichten, Betrieb und Warten,
- Risikoanalyse unter Beachtung der Abhängigkeiten kritischer Geschäftsprozesse von Gebäudefunktionen,
- Sicherheitskonzepte für die GA und die einzelnen TGA-Gewerke,
- Festlegungen für Überprüfungen von technischen und organisatorischen Cybermaßnahmen.

TÜVRheinland®
Genau. Richtig.

Wie schätzt das BSI die Lage ein?

CSW-Nr. 2023-222993-1031, Version 1.0, 04.04.2023

Das BSI stellt fest:

Das Gebäudemanagement und deren eingesetzte Gebäudeautomation und TGA stellen essentiell wichtige Funktionen für das Funktionieren einer Organisation bereit.
Störungen reichen von Komforteinschränkungen, wenn Beleuchtung oder Klimatisierung der Büros beeinträchtigt ist, bis hin zu gefährlichen Situationen, die Menschenleben gefährden können.

TÜVRheinland®
Genau. Richtig.

Rechtsgrundlagen Technische Regeln

Konkretisierungen

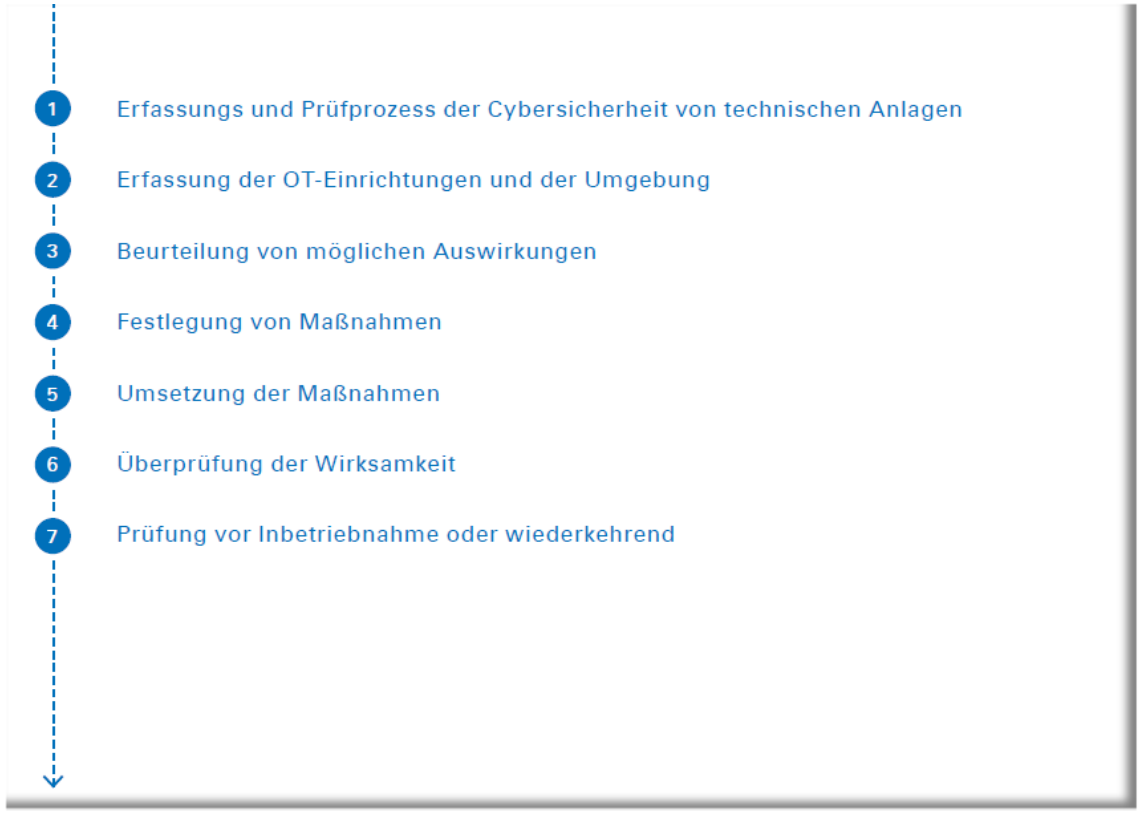
- TRBS 1115-1 — Cybersicherheit für sicherheitsrelevante Mess-, Steuer- und Regeleinrichtungen (betrifft insbesondere Kälteanlagen und Aufzüge)
- KAS 51 — Leitfaden Maßnahmen gegen Eingriffe Unbefugter

- EN 62443 — IT-Sicherheit für industrielle Automatisierungssysteme
- BSI INF 13 — Technisches Gebäudemanagement
- BSI INF 14 — Gebäudeautomation

TÜVRheinland®
Genau. Richtig.

Einführung der Cybersicherheit in das Gebäudemanagement

TGA und Gebäudeautomation



In einem Schutzkonzept der Cybersicherheit sind die erforderlichen Maßnahmen der Cybersicherheit für die TGA und GA zu beschreiben.
Basierend auf dem Schutzkonzept sind Anforderungen an die Komponenten der TGA und GA und erforderlich an die IT/OT-Umgebung in einer Spezifikation der Cybersicherheit festzulegen.

TÜVRheinland®
Genau. Richtig.

„Cybersicherheit ist der Brandschutz des 21. Jahrhunderts.“

Vielen Dank für Ihre Aufmerksamkeit!

Ralf Schmitt

Fachgebietsleiter

0171-9918823

ralf.schmitt@de.tuv.com

LEGAL DISCLAIMER

Dieses Dokument ist Eigentum von TÜV Rheinland. Es dient nur zu vertraulichen Informationszwecken für den Empfänger. Weder dieses Dokument noch irgendwelche Informationen oder Daten, die darin enthalten sind, dürfen ohne vorherige schriftliche Zustimmung von TÜV Rheinland zu anderen Zwecken verwendet oder vervielfältigt oder ganz oder teilweise an Dritte weitergegeben werden. Dieses Dokument ist nicht ohne eine mündliche Erklärung (Präsentation) des Inhalts vollständig.

TÜV Rheinland AG

TÜVRheinland®
Genau. Richtig.