



Reliable and Energy Efficient Data Center Design

## Opening Solutions Day

10. Mai 2023  
Hilton Vienna Park in Wien

**ASSA ABLOY**  
Opening Solutions

## NISG – gesetzliche Verpflichtung zum Zutrittsschutz & physischer Sicherheit

Dipl.-Ing. Georg Meixner, MBA  
Senior Data Center Consultant /  
Architektur & Sicherheit  
Frauscher Consulting GmbH

# Analogie “The Power of Ten”:

Dokumentarfilm, Charles & Ray Eames, 1977: eine Reise durch die Dimensionen

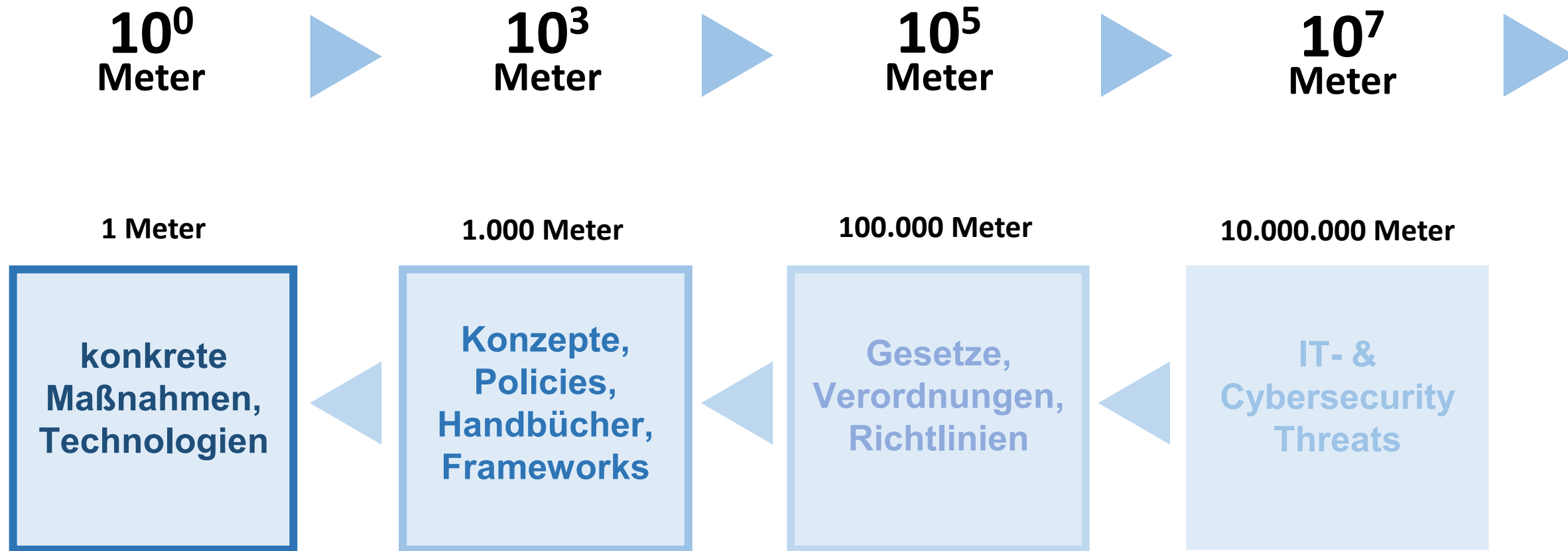




Foto: Foto Weiwurm

## Georg Meixner

- Dipl.-Ing. Arch. > IT-Konzern
- MBA WBS, Bauträger
- 23 Jahre Erfahrung in RZ-Planung & -Bau
- 10 Jahre CEE & MEA
- Uptime Institute ATD & TSI.Professional
- FCG: Architektur & physische Sicherheit

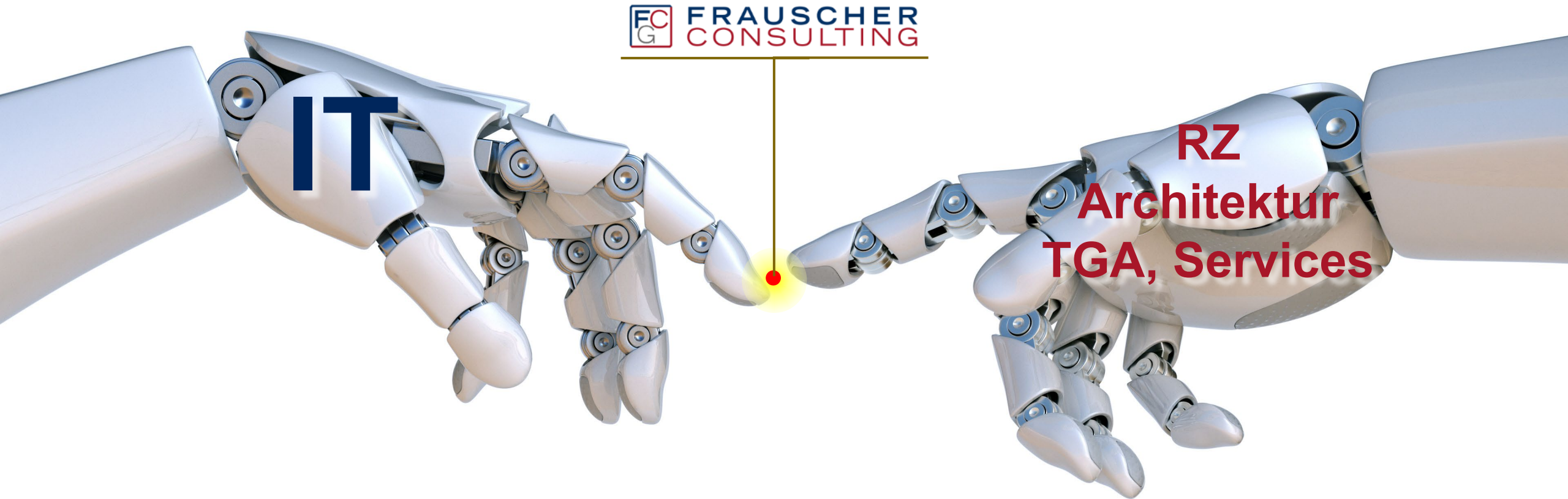


**FRAUSCHER  
CONSULTING**



DI Georg Meixner, MBA

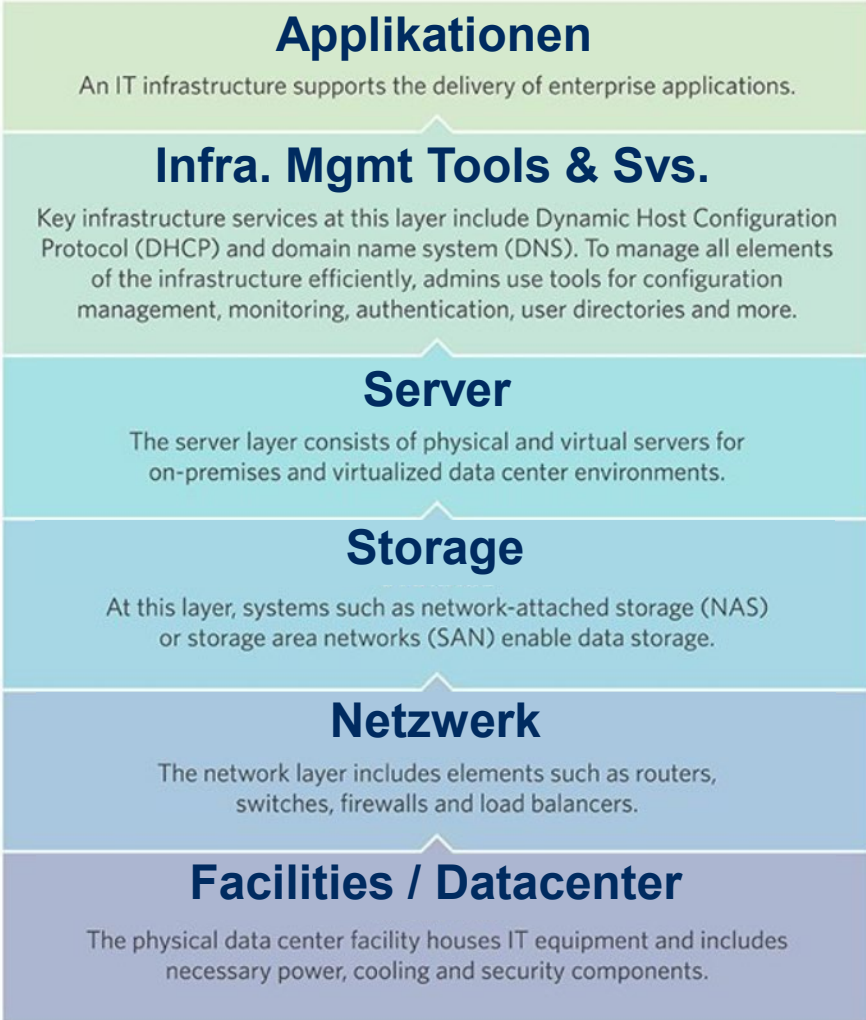
+43 (0)676 884 855 210  
georg.meixner@frauscher.consulting  
Frauscher Consulting GmbH  
Bergmillergasse 8/2/2, 1140 Wien  
Hamerlingstraße 5/1, 4020 Linz







Quelle: Layer IT-Infrastruktur:  
[www.techtarget.com/searchdatacenter/definition/infrastructure](http://www.techtarget.com/searchdatacenter/definition/infrastructure)

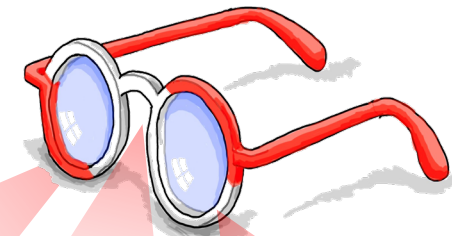


**Business-Strategie**

**IT-Strategie**

**DC-Strategie**

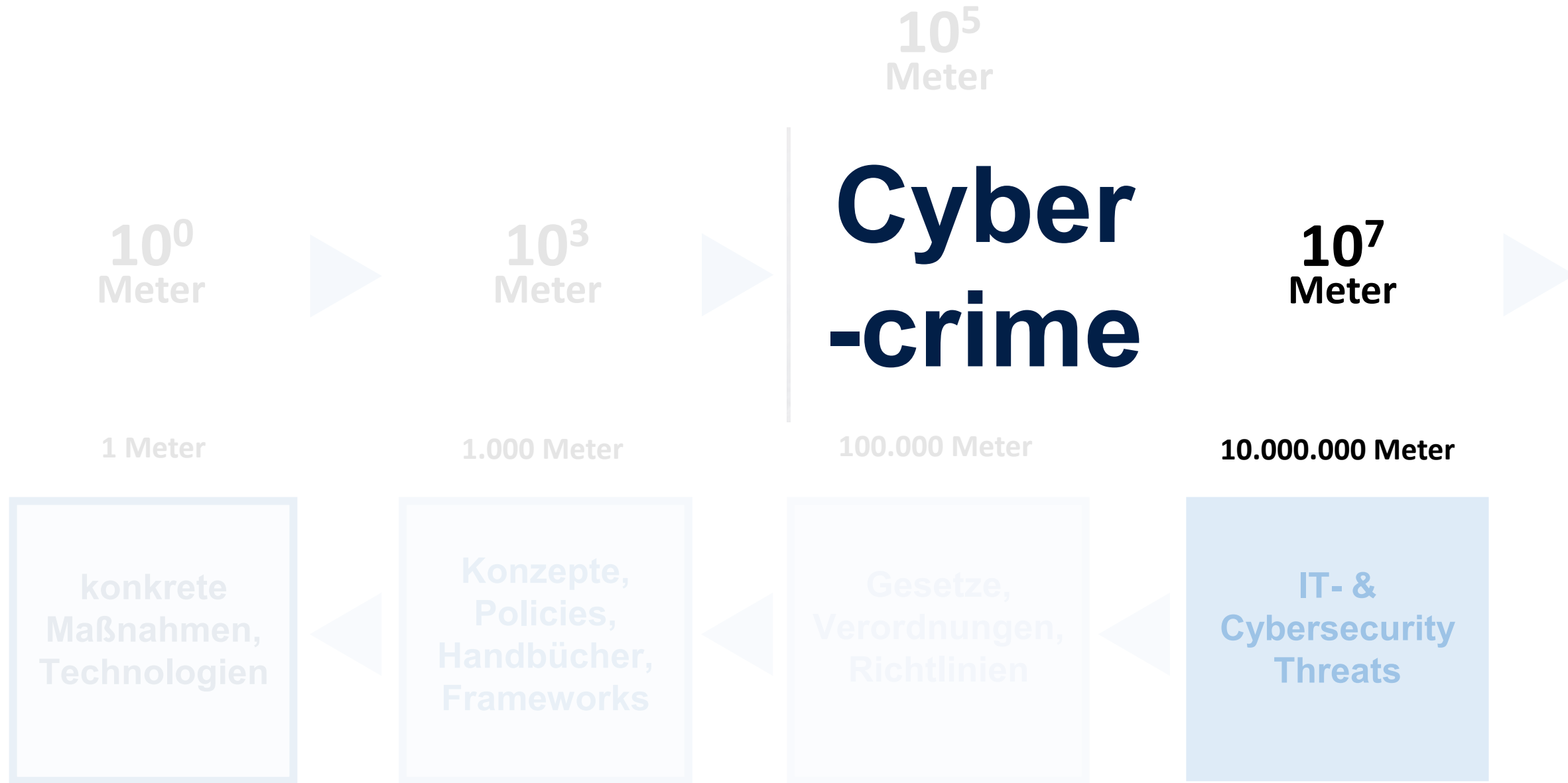
- Konzeption, Planung
- Realisierung
- Betrieb



**Praxis**

**Normen**

**Gesetze**



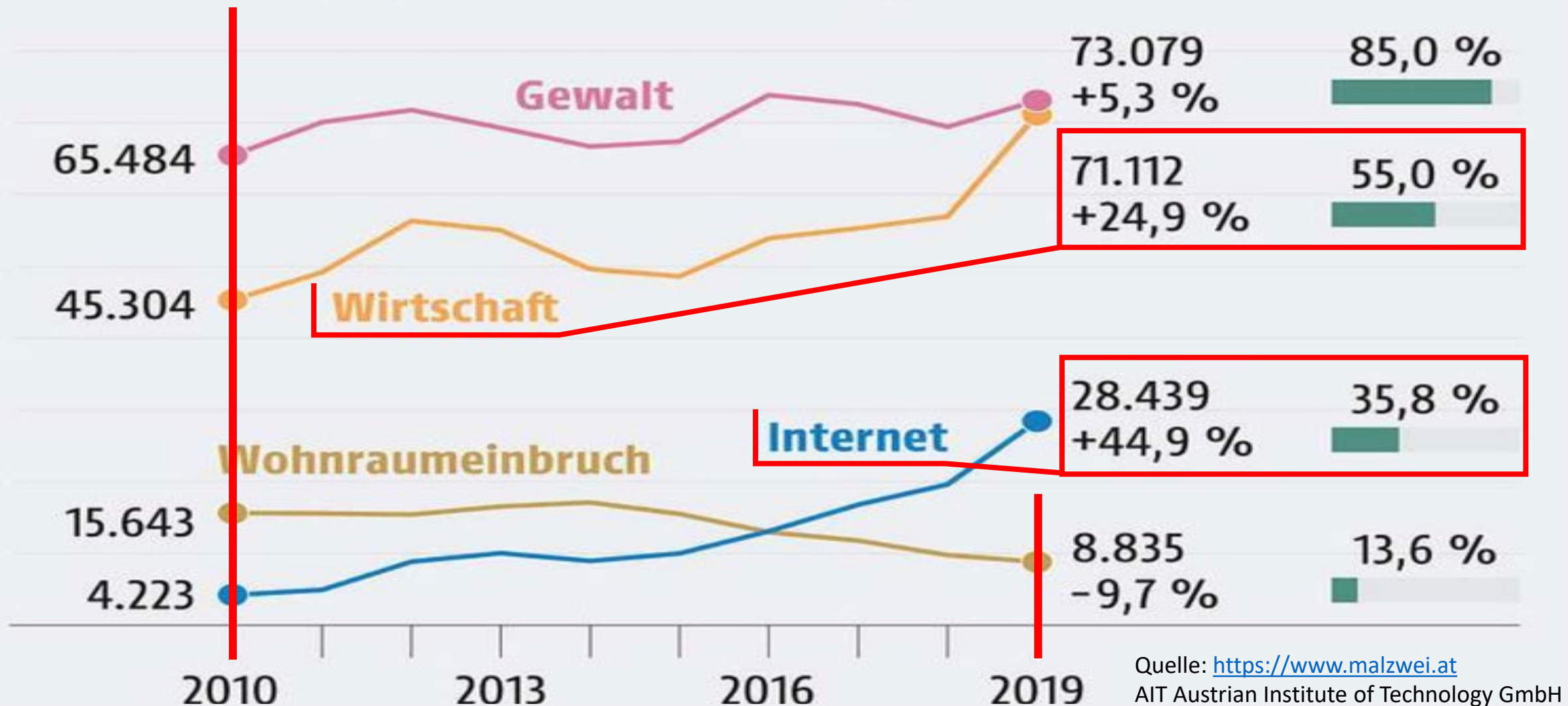
- **IT-Systeme haben zentrale Rolle in Gesellschaft**
  - IT / OT, Betrieb & Dienste
- **Verlässlichkeit & Sicherheit entscheidend:**
  - Wirtschaft
    - Funktionieren des Binnenmarktes
  - Gesellschaft



## Nach Deliktgruppen (Auswahl)

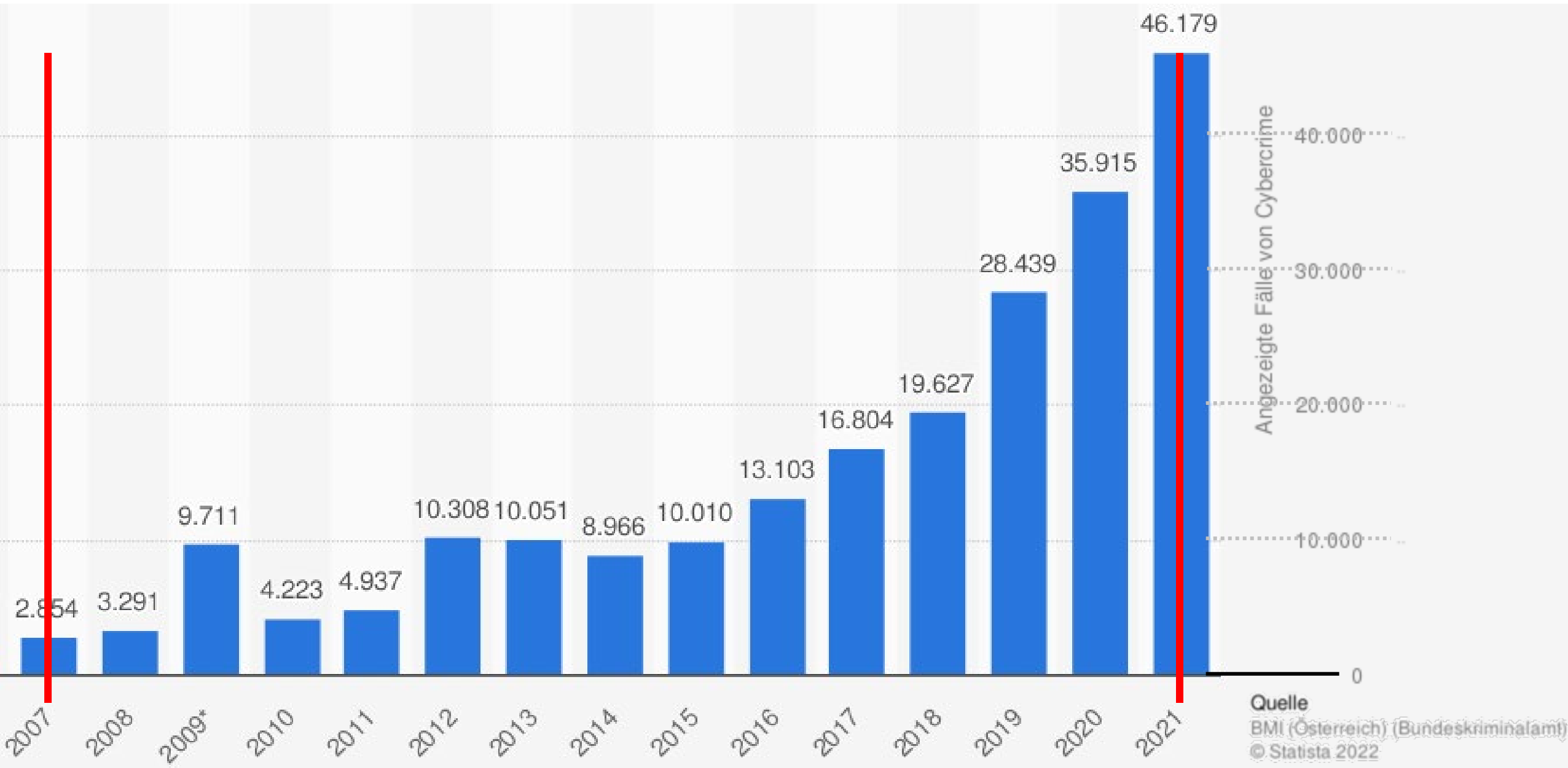
Zahl der Anzeigen, Veränderung zum Vorjahr

Aufklärungsquote



Quelle: <https://www.malzwei.at>  
AIT Austrian Institute of Technology GmbH

# angezeigter Cybercrime 2007-2021



10<sup>3</sup>  
Meter

10<sup>0</sup>  
Meter

# NISG

10<sup>5</sup>  
Meter

10<sup>7</sup>  
Meter

## Netz- und Informationssystem- Sicherheits- Gesetz

1 Meter

100.000 Meter

10.000.000 Meter

konkrete  
Maßnahmen,  
Technologien

Handbücher,  
Frameworks

Gesetze,  
Verordnungen,  
Richtlinien

IT- &  
Cybersecurity  
Threats



## NISG 1.0

- **Zusammenarbeit** - nicht versperren davor
  - **Eigenverantwortung** - nicht darauf setzen, dass jemand ein Problem für uns löst
  - **Wo IT eingesetzt wird – muss IT-Sicherheit mitgedacht & mitgelebt werden**
    - breiter Regulierungsversuch
    - allgemein formuliert
    - im Vollzug unterschiedlich
- Alle Mitgliedsstaaten:**
- Cyber-Sich.gesetze & -strategien
  - Behörden und krit. Infrastrukturen geschützt

NISG



NISV

**BwD:** per Bescheid festgelegt



**Verpflichtung** für den BwD  
(Betreiber eines  
wesentlichen Dienstes)

**Nachweis** alle 3 Jahre:

Erfüllung / Umsetzung der  
Sicherheitsvorkehrungen

**NISV Sicherheitsmaßnahmen:**

(gem. NISG)

- aufgrund Risikoanalysen einzuführen
- Mittels kontinuierlichem Verbesserungsprozess auf dem neuesten Stand der Technik zu halten
- inhaltlich >80% deckungsgleich mit ISO 27001 (Informationssicherheit)

**BwD:** Definitionen in NISV

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastruktur
- Gesundheitswesen
- Trinkwasserversorgung
- Betreiber digitaler Infrastruktur

## BwD-Verantwortung

### BwD-Verantwortung:

- organisatorische & technische Abgrenzung „**wesentlicher Dienst**“
  - **nur für diese** Organisationen & techn. Systeme Nachweis

### Anwendungsbereiches des NISG

- Komplexe **Systeme, Abhängigkeiten, Schnittstellen**
- **Identifikation** aller relevanten **Dienstleister** (für Betrieb des wB)
- ganze oder teilweise Auslagerung des Betriebes an Dienstleister:
  - **auch alle DL** mit Betriebsverantwortung im Anwendungsbereich des NISG
  - aber **BwD behält Nachweis-Verantwortung** gegenüber Behörde
- **Art & Umfang** des wD bestimmt Umfang der Prüfung



## NIS Fact-Sheet

### NIS Fact Sheet:

- **detaillierte Beschreibung der Sicherheitsmaßnahmen**, Anlage 1 NISV
  - In ihrer Gesamtheit: Sicherheitsvorkehrungen
  - **Unterstützung BwD** bei Umsetzung Vorgaben aus NISG & NISV
  - **gem. europäischen Empfehlungen** für Sicherheitsvorkehrungen
  - berücksichtigt **nationale Besonderheiten**
  - berücksichtigt Erfahrungen aus Sektorengesprächen
- Bei **Umsetzung auf angemessenes Verhältnis** zu achten
  - zwischen feststellbarem **Ausmaß einer Bedrohung**
  - und der **wirtschaftlichen Belastung**
- **Abweichungen bei Umsetzung** der Sicherheitsmaßnahmen teilweise **möglich**
  - aus **technischen oder betrieblichen** Gründen
  - dadurch bedingten Abweichungen bei Umsetzung durch **risikominimierende u/o. kompensierende** Maßnahmen auszugleichen
  - **in Nachweisen** (Aufstellung, Prüfbericht) darzustellen und glaubhaft zu begründen

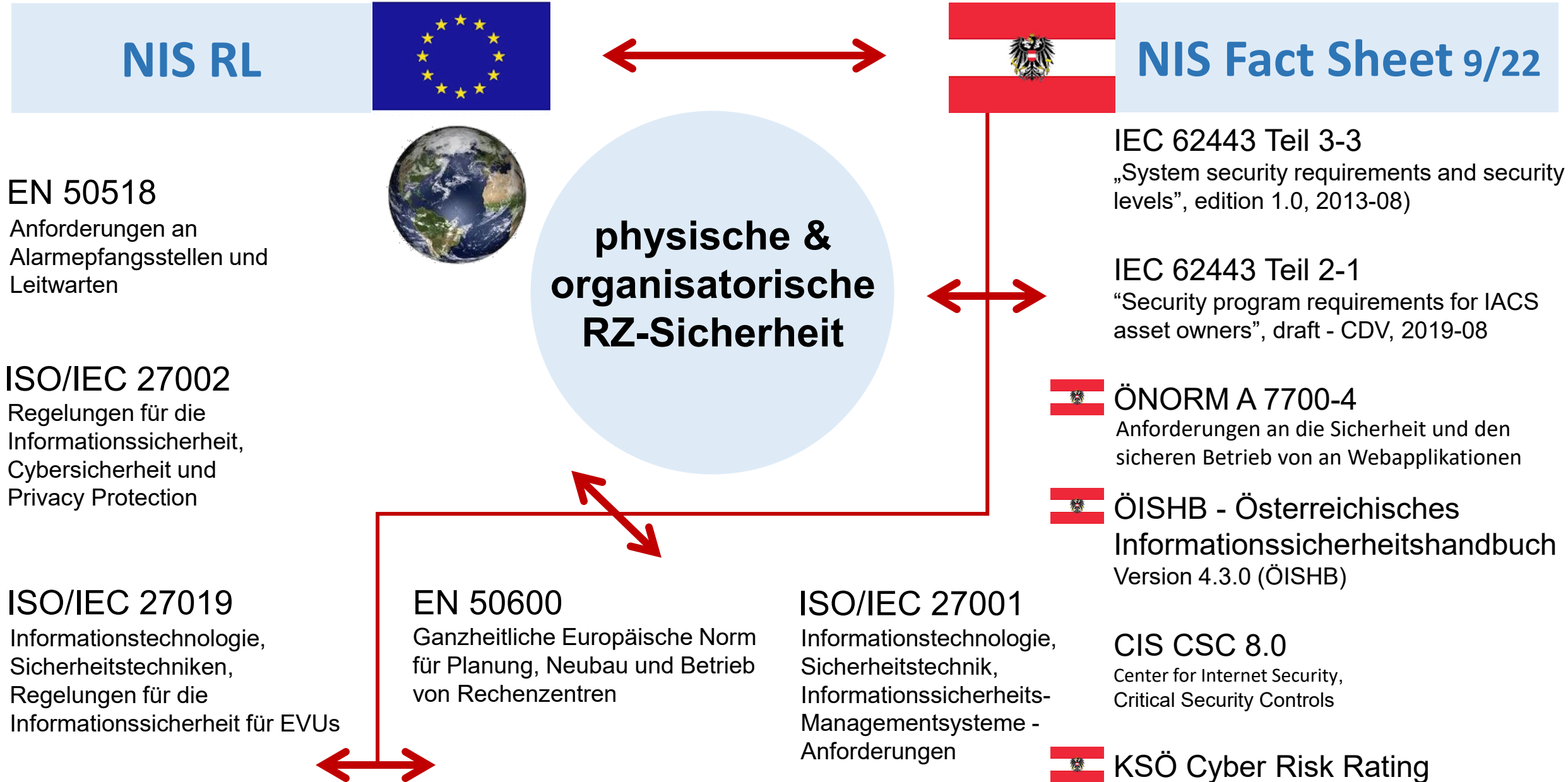
## NIS Richtlinie

### Für die Umsetzung:

- Anwendung **europä. und internat.** anerkannter Normen und Spezifikationen zu fördern
- i.S.e. **einheitlichen Anwendung** der RL
  - Workstream „Sicherheitsmaßnahmen für BwD“:
    - **Grundlage für ein Mapping**
    - ergänzt um **nationale Informationssicherheitsstandards** & Best Practices

### ausdrücklich:

- **beispielhafte** Gegenüberstellung **national >< international**
- zur Orientierung & Unterstützung bei Umsetzung & Evaluierung
- § 17 NISG:
  - **Implementierung & Überprüfung** von Sicherheitsvorkehrungen bzw. –maßnahmen
    - **dem Risiko angepasst**
    - **wirtschaftlich**

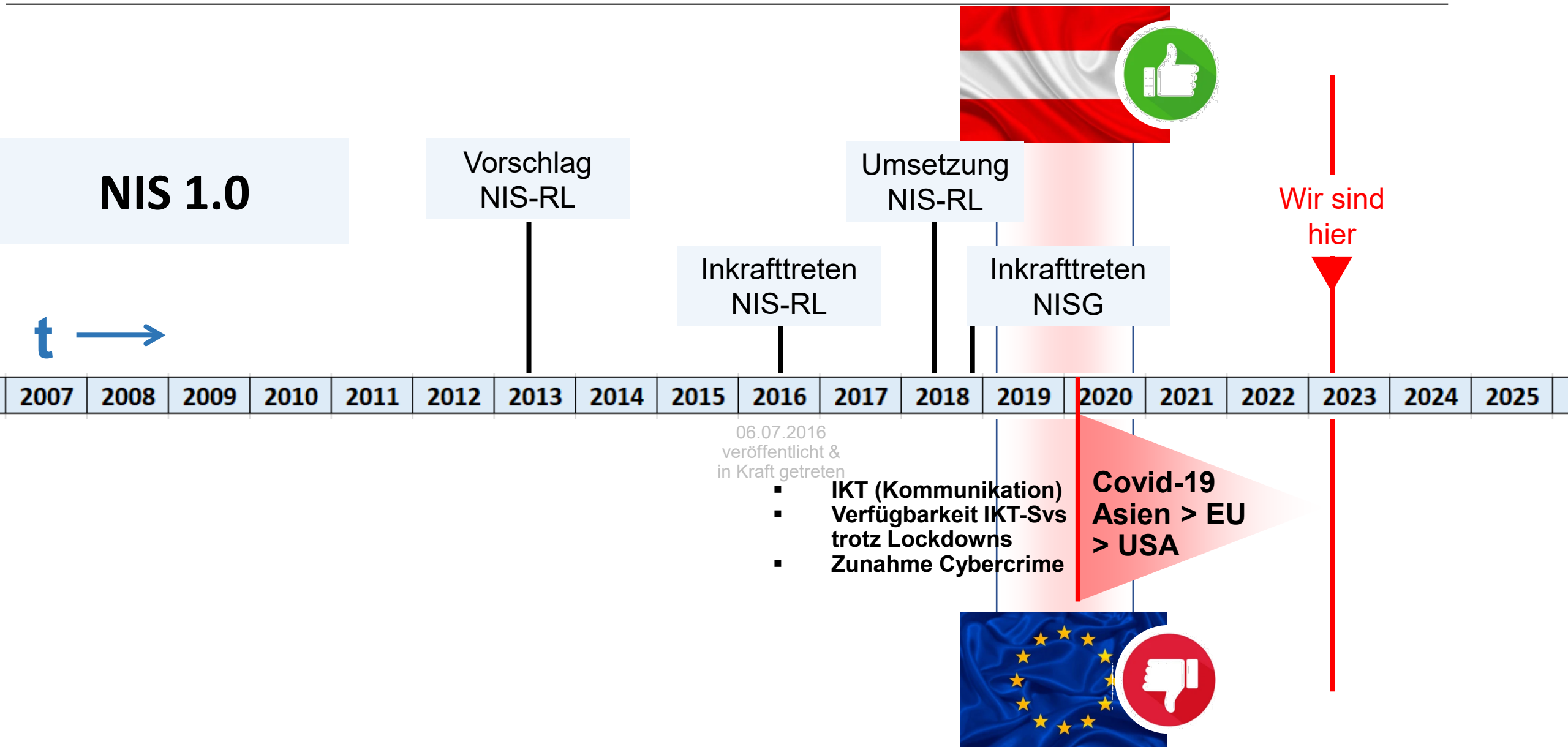


## NIS Kooperationsgruppe

### NIS Kooperationsgruppe:

- **Austausch** zwischen EU-Mitgliedsstaaten im Bereich N- & I.
- **strategische** Zusammenarbeit
- Grundsätze europäischer Zusammenarbeit bei **Cyberkrisen**
- Vertreter: Mitgliedstaaten, EU Kommission, EU Agentur für Cybersicherheit (ENISA)
- **Workstreams:**
  - Leitlinien
  - Referenzdokumente
  - z.B. „Sicherheitsmaßnahmen für BwD“
    - **Grundlage zur Absicherung wD**
    - **freiwillige Anwendung**





**NIS 1.0**



**Anwendung:**

- nicht alle kritische Sektoren
- untersch. Anwendungsbereiche

in AT per Bescheid:

- 15 Bund
- 25 Digit. DL
- 100 BwD
- weitere

**Wirkungskreis:**

exkl. Hauptbetroffene

**systematische  
Konzentration:**

große Akteure

**Sicherheits-  
anforderungen:**

- untersch. Resilienz bei
- Mitgl.staaten & Sektoren

**Berichtspflichten:**

unterschiedlich

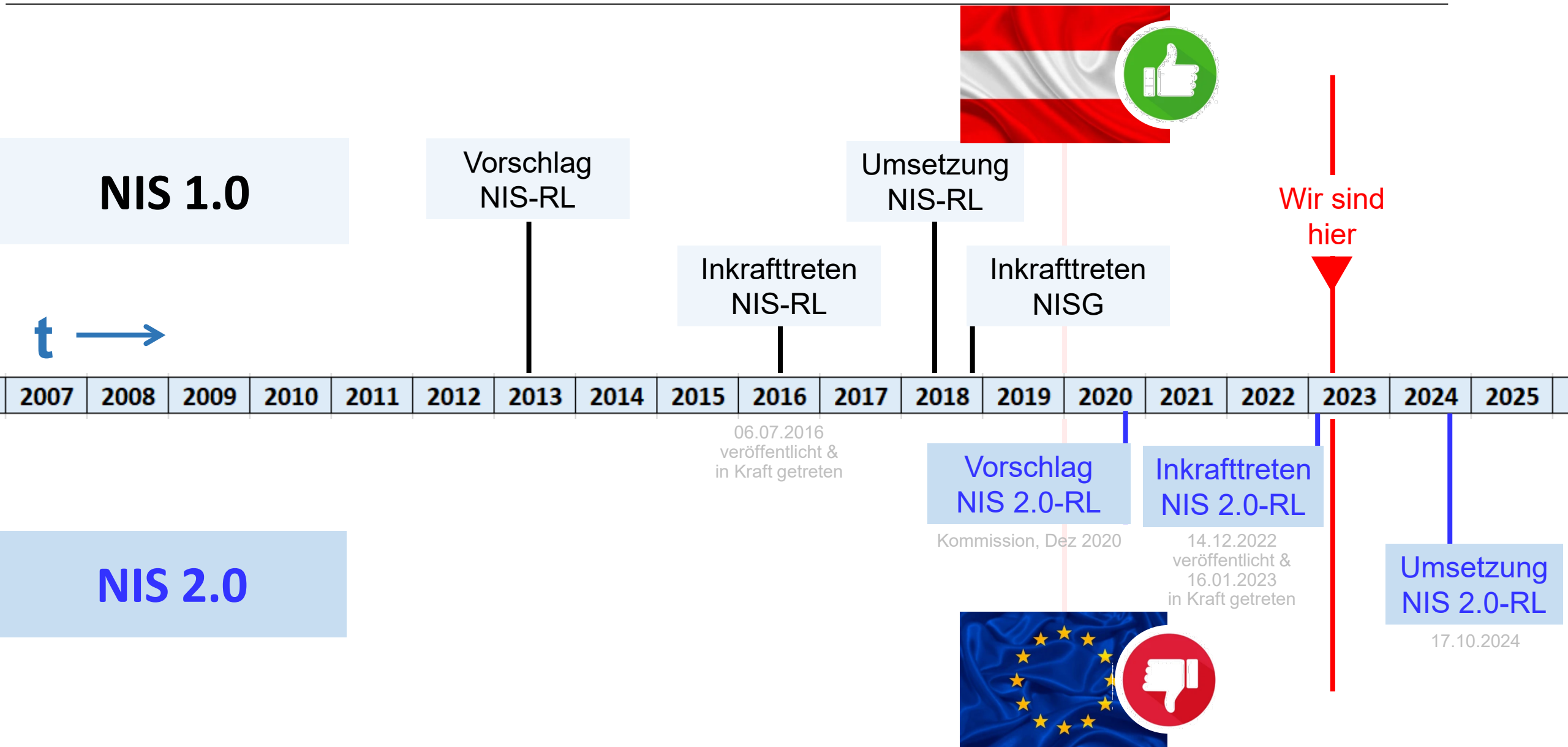
**Aufsicht &  
Durchsetzung:**

ineffektiv

**Zusammenarbeit  
EU-Ebene:**

- schwach ausgeprägt
- mangelnde EU  
Cyber-Krisenreaktionen





	NIS 1.0	ersetzt NIS 1.0 	NIS 2.0
<b>Anwendung:</b>	<ul style="list-style-type: none"> <li>▪ manche krit. Sektoren</li> <li>▪ untersch. Anwendungen</li> </ul>		<p><b>viele Sektoren</b>, in Breite: großer Teil Wirtschaft &amp; Gesellschaft</p>
<b>Wirkungskreis:</b>	exkl. Hauptbetroffene		<b>+ Lieferanten, Zulieferer</b>
<b>systematische Konzentration:</b>	große Akteure		<b>größere &amp; mittlere Akteure</b>
<b>Sicherheitsanforderungen:</b>	<ul style="list-style-type: none"> <li>▪ untersch. Resilienz bei</li> <li>▪ Mitgl.staaten &amp; Sektoren</li> </ul>	} deutlich höhere Vorgaben	<b>Angleichung</b>
<b>Berichtspflichten:</b>	unterschiedlich		<b>Straffung</b>
<b>Aufsicht &amp; Durchsetzung:</b>	ineffektiv		<b>Angleichung, Harmonisierung</b>
<b>Zusammenarbeit EU-Ebene:</b>	<ul style="list-style-type: none"> <li>▪ schwach ausgeprägt</li> <li>▪ mangelnde EU Cyber-Krisenreaktionen</li> </ul>		<b>verstärkt operativ, inkl. EU-Cyber-Krisenmanagement</b>

**Fähigkeiten der Mitgliedstaaten**  
(Behörden, Staat)

**EU Kooperation und Informationsaustausch**

(strat., operat., techn., lessons learnt, Indikatoren)

**Risiko-Management**

**nationale Behörden**

**NIS-Kooperationsgruppe**  
**Peer-Review**

**Verantwortung**  
**Top-Management**

**Computer-Notfallteams**  
(CERTs / CSIRTs)

**CSIRTs-Netzwerk**

**Schulungen für**  
**Top-Management**

**Cyber-Krisenmanagement**

**EU-Cyberkrisennetzwerk**  
(CyCLONe)

**Unterscheidung wesentliche**  
**/ wichtige Einrichtungen**

**nationale Strategien**

**ENISA**  
**Cybersecurity Reports**

**Sicherheitsmaßnahmen**

**Rahmen für CVD**  
(Coordinated Vulnerability Disclosure)

**Europäisches**  
**Schwachstellenregister**

**Berichtspflichten**

schon in NIS 1.0, nun genauer

## Risiko- Management

Verantwortlichkeit  
Top-Management

Schulungen für  
Top-Management

Unterscheidung wesentliche  
/ wichtige Einrichtungen

Sicherheitsmaßnahmen

Berichtspflichten  
(Melden von Vorfällen)

1

**Risiko-  
Management-  
Maßnahmen**  
(Cybersicherheit)

### Governance:

- Genehmigen
- Überwachen
- Verantwortung

### Schulungen:

- Fähigkeiten
- Kenntnisse
- Risikobewertungen

### Maßnahmen:

- NIS-Risiken beherrschen
- Auswirkungen S-Vorfälle verhindern / minimieren

## Risiko- Management

Verantwortlichkeit  
Top-Management

Schulungen für  
Top-Management

Unterscheidung wesentliche  
/ wichtige Einrichtungen

Sicherheitsmaßnahmen

Berichtspflichten  
(Melden von Vorfällen)

### 1 Risiko- Management- Maßnahmen (Cybersicherheit)

#### All-Gefahren-Ansatz:

- logisch (IT)
- **physisch (versorgende Infrastr., Umgebung, etc.)**

#### risikobasierter Ansatz:

- techn./ operat./ organisator.
- Angemessenheit
- Verhältnismäßigkeit
- Stand der Technik
- Kosten der Umsetzung (wsl.)
- Ausmaß der Risikoexposition
- Unternehmensgröße
- Wahrscheinlichkeit. vs. Schwere von Vorfällen (gesellsch. & wirtsch. Auswirkungen)

**angeführte Maßnahmen** (expliz.)

### Risiko- Management

Verantwortlichkeit  
Top-Management

Schulungen für  
Top-Management

Unterscheidung wesentliche  
/ wichtige Einrichtungen

Sicherheitsmaßnahmen

Berichtspflichten  
(Melden von Vorfällen)

2

#### Frühwarnung

unverzüglich bis max.  
**24h** nach  
Kenntnis

Verdacht, ob

- rechtswidrig, od.
- böswillig, ob
- grenzüberschreitend

#### Meldung

unverzüglich bis max.  
**72h** nach  
Kenntnis

erste Bewertung

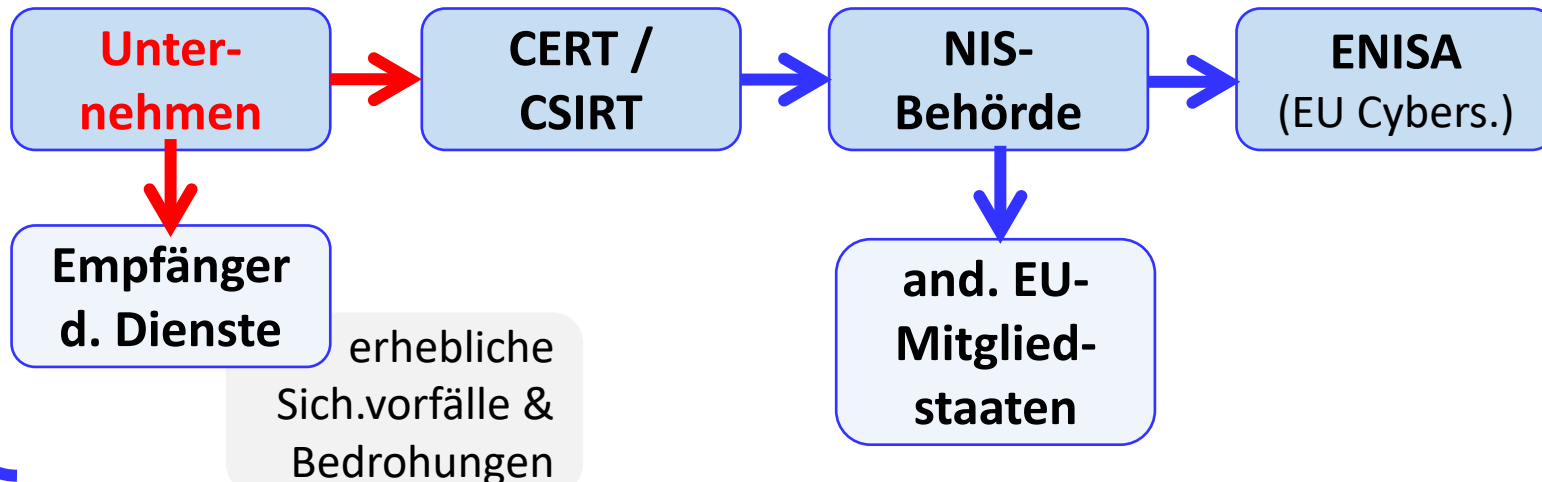
- Schweregrad
- Auswirkungen, ggf.
- Komprom.indikatoren

#### Abschluss- meldung

**1 Mo** nach  
Kenntnis

ausführl. Beschreib.

- Art der Bedrohung
- Ursachen
- Abhilfemaßnahmen





## NIS 2.0

### Nennung in NIS-RL, Spalte 3 von

- Anhang I –
  - Sektoren **hoher Kritikalität**
  - 53 Arten
- Anhang II –
  - **sonstige kritische** Sektoren
  - 14 Arten

### Prüfschema:

- öffentlich & privat
- DL oder Tätigkeit in der EU ausgeübt?
- wesentliche oder wichtige Einrichtung?
- *Ausnahmen Kleinunternehmen*

**Sektor**  
1.Energie

**Teilsektor**  
a) Elektrizität

**Art der Einrichtung**  
Verteilernetzbetreiber  
im Sinne des Art. 2  
Nummer 29 der  
RL (EU) 2019/944

**Größen-  
Schwellwert**  
(size cap rule)

+

**Nennung  
NIS-RL**

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, <b>Fernwärme/Kälte</b> , Öl, Gas und <b>Wasserstoff</b> )	<b>Post- und Kurierdienste</b>
Verkehr (Luft, Schiene, Schifffahrt, Straße)	<b>Abfallbewirtschaftung</b>
Bankwesen	<b>Chemie (Herstellung und Handel)</b>
Finanzmarktinfrastrukturen	<b>Lebensmittel (Produktion, Verarbeitung, Vertrieb)</b>
Gesundheitswesen (Gesundheitsdienstleister, <b>EU-Referenzlaboratorien</b> , <b>Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte</b> )	<b>Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)</b>
Trinkwasser	<b>Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)</b>
<b>Abwasser</b>	<b>Forschung</b>
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, <b>Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste</b> )	
<b>Verwaltung von IKT-Diensten (B2B)</b> Managed Svs Prov./ Managed Security Svs Prov.	
<b>Öffentliche Verwaltung</b>	
<b>Weltraum</b>	<b>Rot = Neuerungen gegenüber NIS1</b>

Quelle:

NIS2 Die neue Cybersicherheits-Richtlinie WKÖ Live-Webinar Mag. Vinzenz Heußler, LL.M. Bundeskanzleramt, Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) Leiter NIS-Büro Wien, 21. Februar 2023

## Größen-Schwellwert

- Empfehlung 2003/361/EG der EU-Kommission
- Benutzerleitfaden der EU-Kommission zur Def. „KMU“
  
- **Großunternehmen**
  - alle Unternehmen  $\neq$  KMU
  
- **mittleres Unternehmen**
  - < 250 Pers. beschäftigt
  - **und:** - Jahresumsatz max. € 50 Mio, **oder**  
- Jahresbilanzsumme max. € 43 Mio
  
- **Kleinunternehmen**
  - < 50 Pers. beschäftigt
  - **und:** - Jahresumsatz bzw.  
- Jahresbilanz max. € 10 Mio

wesentlich  
/ wichtig

## NIS 2.0

### Prüfschema:


- öffentlich & privat
- DL oder Tätigkeit in der EU ausgeübt?
- wesentliche oder wichtige Einrichtung?
- *Ausnahmen Kleinunternehmen*

**Größen-  
Schwellwert**  
(size cap rule)

+

**Nennung  
NIS-RL**

\*) KU-Ausnahme: insbes. > im Sektor digitale Infrastruktur  
> + mit hoher Kritikalität


	NIS 2.0 
Anwendung:	viele Sektoren
Wirkungskreis:	+ Lieferanten
systematische Konzentration:	größere & mittlere Akteure
Sicherheitsanforderungen:	Angleichung
Berichtspflichten:	Straffung
<b>Aufsicht &amp; Durchsetzung:</b>	<b>Angleichung, Harmonisierung</b>
Zusammenarbeit EU-Ebene:	verstärkt operativ

## Aufsichtsmaßnahmen & Befugnisse

- Mindestliste an **Aufsichtsmaßnahmen**
  - Regelm. & gezielte Audits
  - vor-Ort- & off-Site-Kontrollen
  - Sicherheitsscans
- **Mittel** zur Verfügung
  - Ersuchen um Information
  - Zugang zu Beweismitteln

## 2 Aufsichtssysteme

- **Vollwertige** Aufsicht
  - **wesentliche** Einrichtungen
  - ex ante & ex post
- **abgeschwächte** Aufsicht
  - **wichtige** Einrichtungen
  - ex post
  - „systemat. Dokument.-Aufwand ist zu **vermeiden & reduzieren** (im Vergleich)

	NIS 2.0 
Anwendung:	viele Sektoren
Wirkungskreis:	+ Lieferanten
systematische Konzentration:	größere & mittlere Akteure
Sicherheitsanforderungen:	Angleichung
Berichtspflichten:	Straffung
Aufsicht & Durchsetzung:	Angleichung, Harmonisierung
Zusammenarbeit EU-Ebene:	verstärkt operativ

## Verwaltungsrecht

- Mindestliste an **Verwaltungssanktionen**, jedenfalls vorzusehen, z.B.
  - verbindliche Anweisungen
  - bescheidliche Anordnungen
  - Verwaltungsstrafen

## maximale Bußgelder

- **wesentliche** Einrichtungen
  - max. **€ 10 Mio**, oder
  - **2% ww** Jahresumsatz (vorige G.-Jahr)
- **wichtige** Einrichtungen
  - max. **€ 7 Mio**, oder
  - **1,4% ww** Jahresumsatz (vorige G.-Jahr)

## natürliche Personen haftbar

- leitende Angestellte (Top-Mgmt.) können für Pflichtverletzungen haftbar gemacht werden

## Wesentliche / wichtige Unternehmen

Selben Verpflichtungen – unterschiedliche Aufsicht & Durchsetzung

Sektoren		Großunternehmen	mittleres Untern.	Kleinunternehmen
Anhang I		wesentlich	wichtig	n/a
Anhang II		wichtig		
Digitale Infrastruktur	TLD-Namensregister *)	wesentlich	wesentlich	n/a
	DNS Dienstleister **)			
	Qualif. Vertrauensdienste			
	Anb. öffentl. Elektron. Komm.-netze od. -dienste	wesentlich		wichtig
	Anb. Vertrauensdienste		wichtig	
	Betreiber Internetknoten	wesentlich	wichtig	n/a
	Anb. Cloud-Computing			
	Anb. Rechenzentrums-DL			
	Betreiber CDN ***)			

\*) Top Level Domains

\*\*\*) Ausnahme: Betreiber Root-Nameserver

\*\*\*) CDN Content Delivery Networks

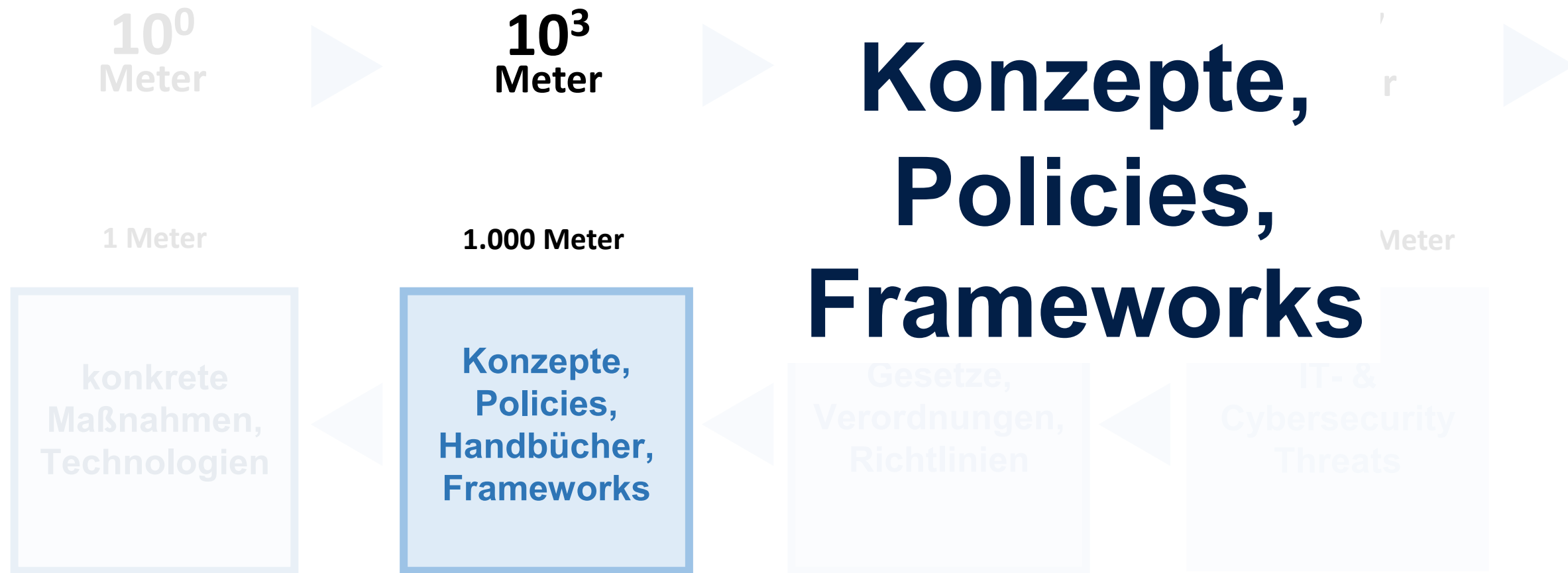


## NIS 1.0-Ziel

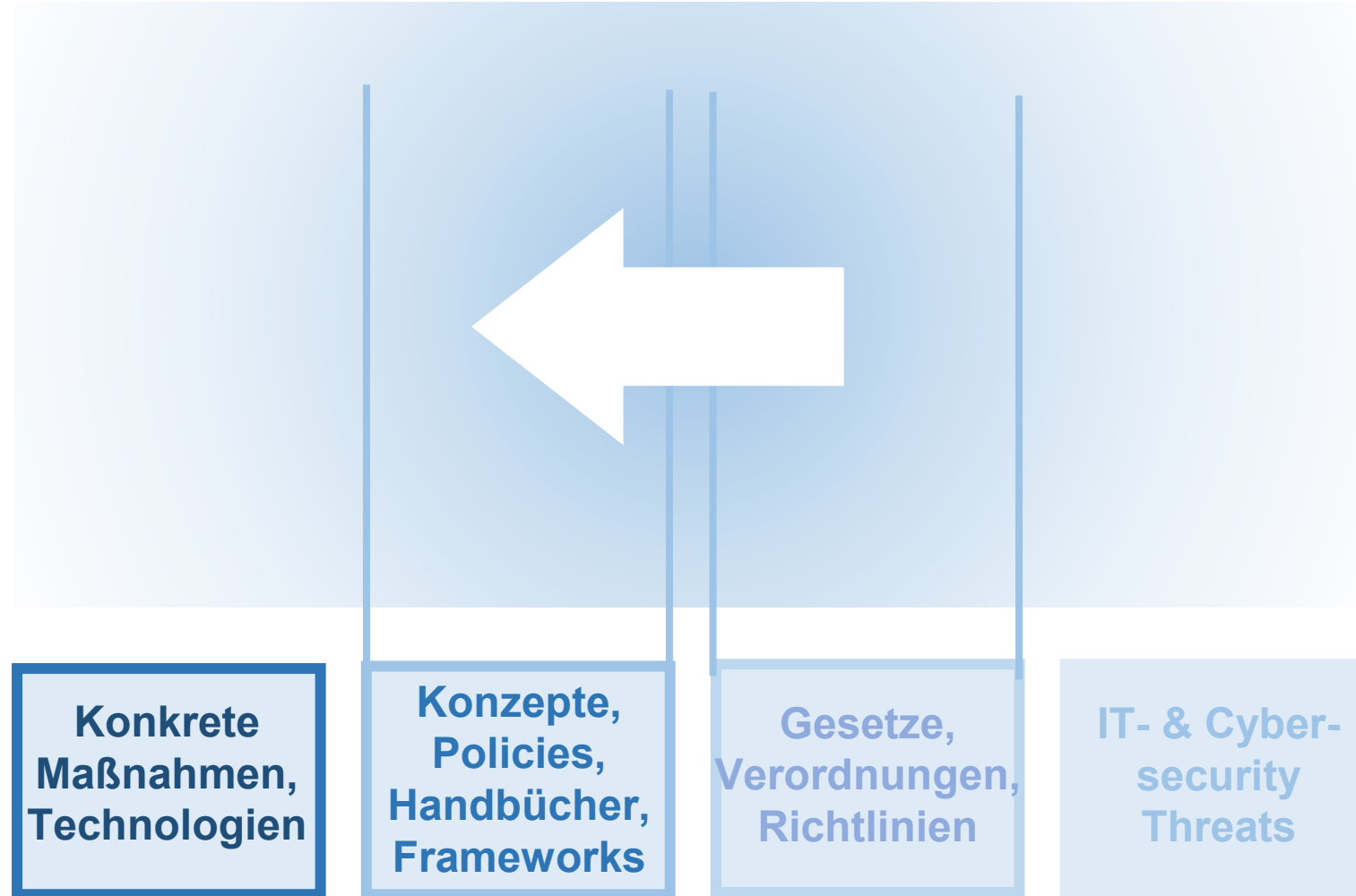
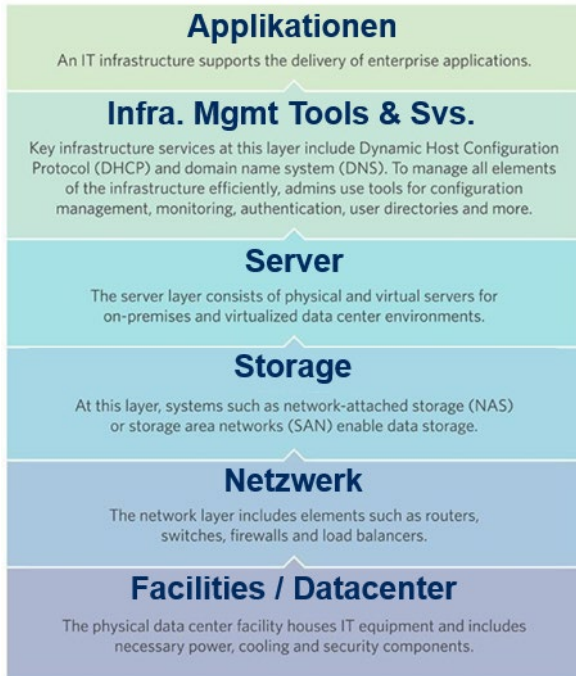
- Kapazität Cybersicherheit erhöhen
- Zuständige Behörden ernennen & Notfallteams
- Übernationale Kooperationsgruppe
- Kernstück: Regelungen für BwD: Sicherheitsvorkehrungen & Meldepflichten
- NIS RL. Sektoren genannt
- Mitgliedstaaten bestimmen wer konkret BwD

## NIS 2.0-Ziel

- **Verwaltungsaufwand abbauen**
- Weitere Sektoren ergänzt (Abwasser, öff. Verwaltung, Weltraum,...)
- **Schwellwerte für wesentliche & wichtige Dienste nun aus der RL** (nicht mehr von Mitgliedern)
- Nationale **Behörden verstärkt Überwachung & Durchsetzung**: Maßnahmen & Befugniskatalog hierzu
- **Bußgeldregelungen** für Unternehmen
- **Maßnahmen** für Betreiber nun **detaillierter**
- Verschärfung der gesetzlichen Pflichten & stärkere EU-weite Harmonisierung



## IT-Layermodell



Quelle: Layer IT-Infrastruktur:  
[www.techtarget.com/searchdatacenter/definition/infrastructure](http://www.techtarget.com/searchdatacenter/definition/infrastructure)

## Kategorien und Sicherheitsmaßnahmen der NISV .....6

1. Governance und Risikomanagement .....	6
2. Umgang mit Dienstleistern, Lieferanten und Dritten .....	10
3. Sicherheitsarchitektur .....	12
4. Systemadministration .....	16
5. Identitäts- und Zugriffsmanagement .....	18
6. Systemwartung und Betrieb.....	20
7. Physische Sicherheit .....	22
8. Erkennung von Vorfällen .....	23
9. Bewältigung von Vorfällen .....	25
10. Betriebskontinuität.....	27
11. Krisenmanagement .....	28



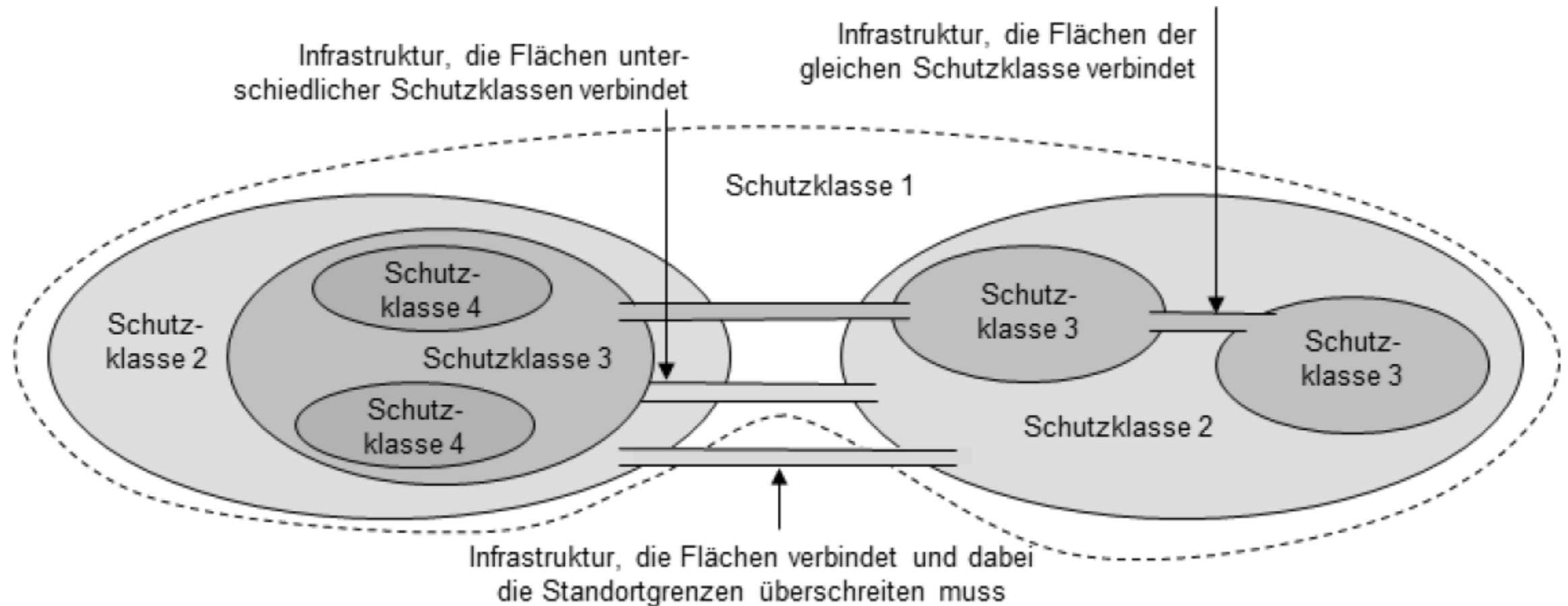


mit Zutritts- & Schließsystem-  
Herstellern abzustimmen

## Inhalte Sicherheitskonzept

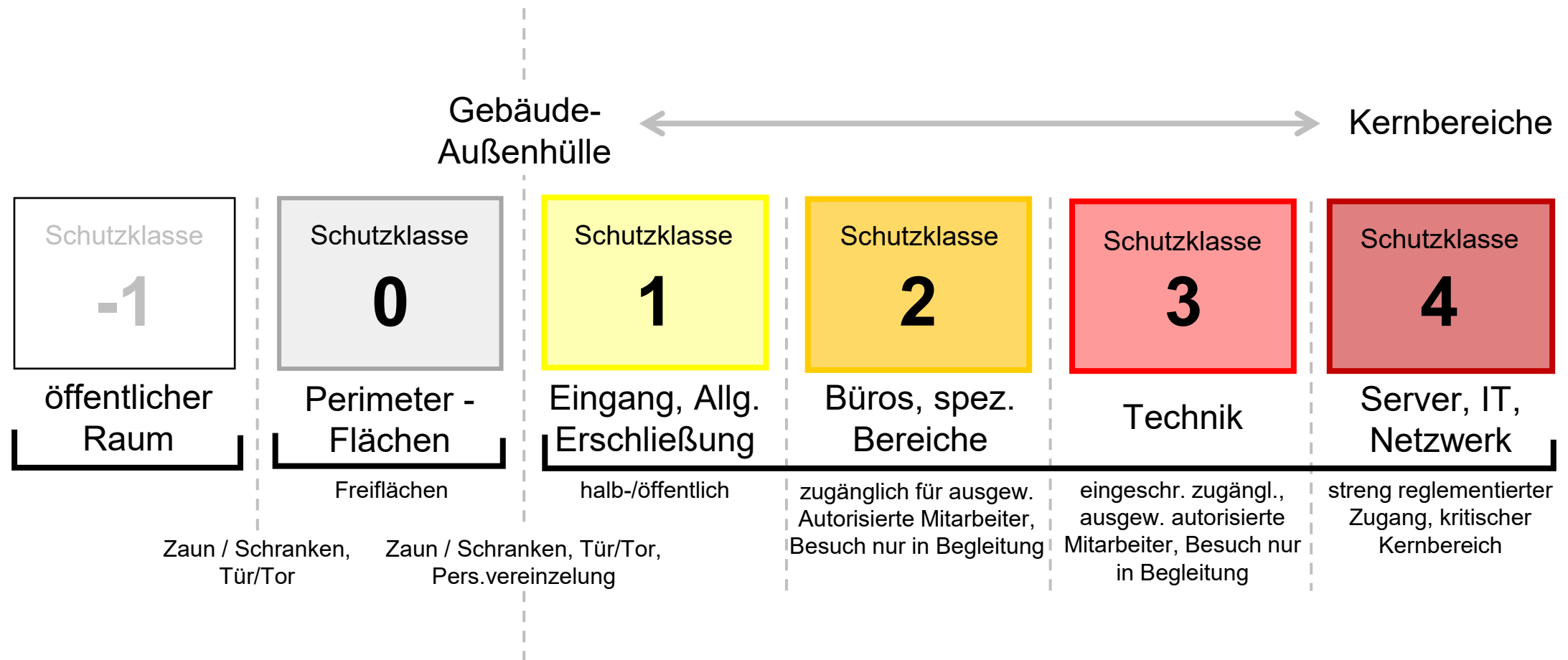
- Grundlagen Sicherheitskonzept
- Mindeststandards
- **organisatorisch-planerische Sicherheit**
  - Schutzklassen & Sicherheitszonen
  - Sicherheitszonenpläne
  - Schutzklassen & Widerstandsklassen
- **Sicherheitssysteme**
  - Einbruchmeldeanlage
  - Zutrittskontrolle
  - Videoüberwachung
  - Sicherheitsmanagementsystem
  - Brandschutz (BMA, BFE, GLA)
  - spezieller Gefahrenschutz
- **baulich-physische Sicherheit**
  - Türspezifikationen
  - RC-Vergitterungen
  - Perimeterschutz
  - baulicher Gefahrenschutz

„Zwiebelschalenprinzip“ – Hierarchie von Schutzklassen, Empfehlung gem. ÖVE EN 50600



**Bild 5 – Verbindungen zwischen Inseln von Schutzklassen**









<https://www.assaabloy.com/at/de/solutions/topics>



## CLIQ elektr. Schließanlagen

CLIQ Schließanlagen bieten für jede Anforderung eine passende Lösung.

[Mehr Infos](#) →



## Mechanische Schließanlagen

Mechanische Schließanlagen sind ausgezeichnet für den Einsatz in komplexen Schließanlagen für viele Einsatzmöglichkeiten.

[Mehr Infos](#) →



## Türschließer

Komfort, Sicherheit, Brandschutz und Design – die Ansprüche an Türschließer erfordern situationsbedingte Lösungen. Wir bieten dafür die passenden Lösungen.

[Mehr Infos](#) →



## Rettungswegtechnik

Das Dilemma bei Fluchtwegtüren ist die Gefahr der unberechtigten Nutzung. Der Fluchtweg muss frei sein - aber kontrolliert!

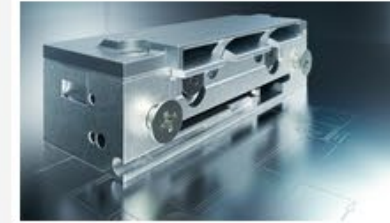
[Mehr Infos](#) →



## Zutrittskontrolle

Zutrittskontrollanlagen schützen und kontrollieren Gebäude, einzelne Räume oder andere sicherheitsrelevante Bereiche.

[Mehr Infos](#) →



## Türöffner

Seit der Gründung im Jahr 1936 hat sich das Unternehmen effeff zum Marktführer im Bereich Türöffner entwickelt.

[Mehr Infos](#) →



## MEDIATOR

Mit der MEDIATOR Schließlösung ist die Haustür immer verriegelt und gleichzeitig von innen als Fluchtweg frei nutzbar.

[Mehr Infos](#) →



## Schlosser

Flexible Schloss-Lösungen: vom Standard-Schloss im Objektbereich bis zur Hochsicherheitslösung für 2-flügelige Türen.

[Mehr Infos!](#) →



## Planet

Design trifft Funktion – Absenkdichtungen und Fingerschutz für Glastüren

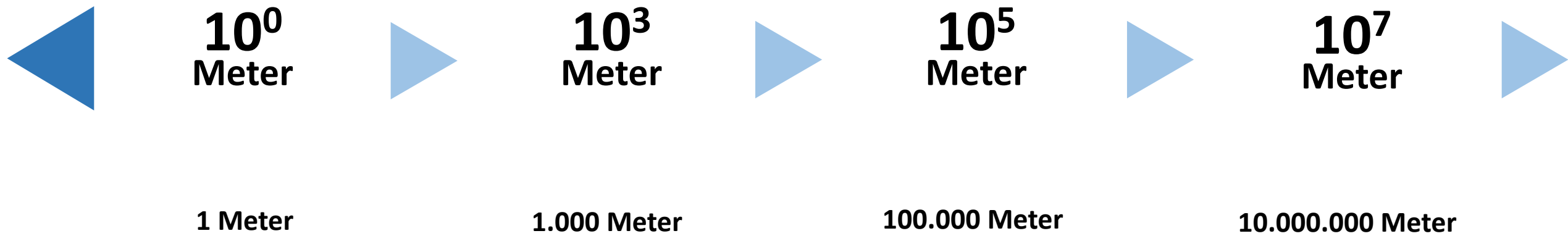
[Mehr Infos](#) →



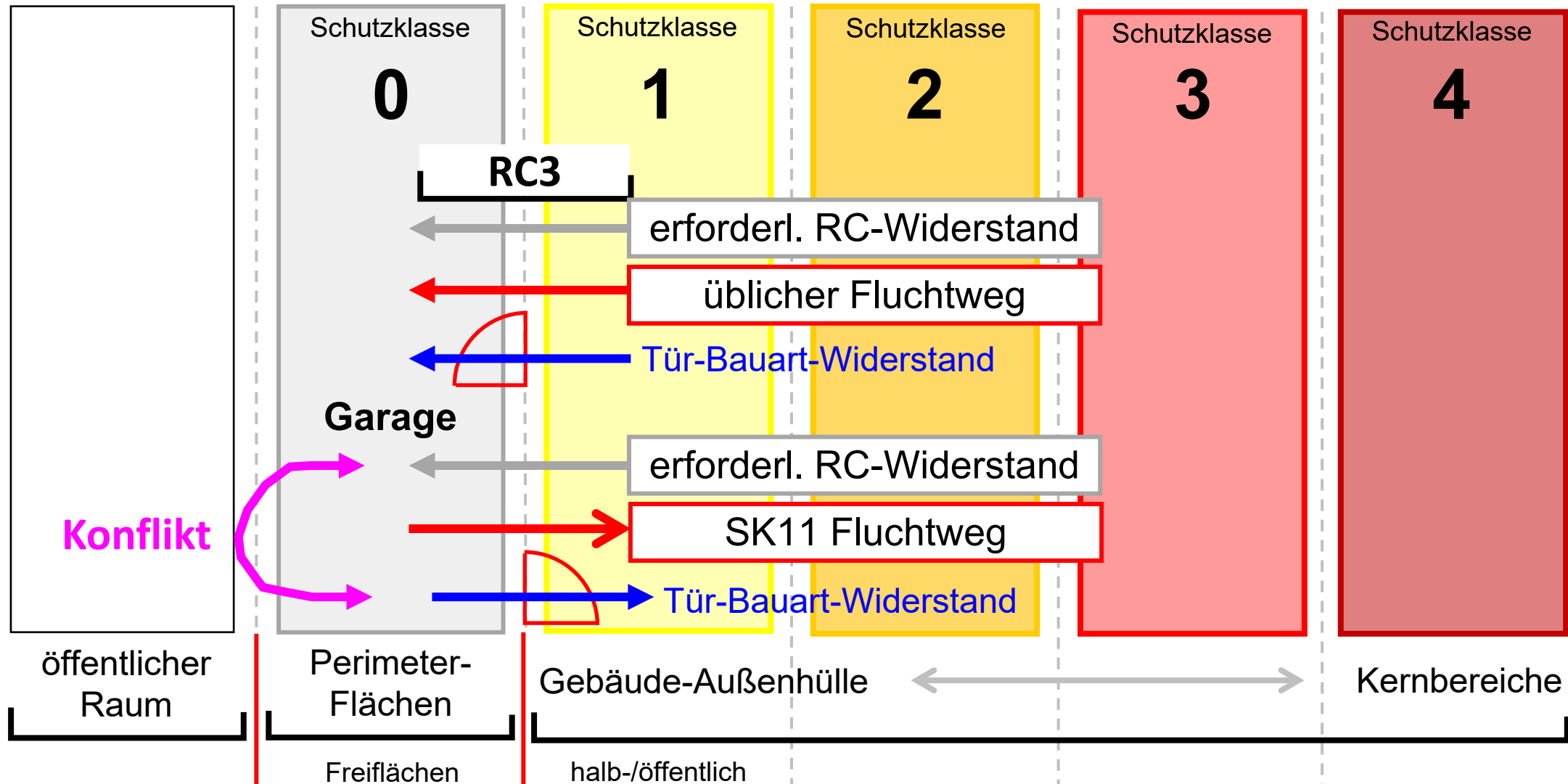
## Kindergarten

Die Kindergartentür abschließen, damit kein Kind unbeaufsichtigt auf der Straße steht? Oder für den Fluchtfall unverschlossen lassen?

[Mehr Infos](#) →



## Widerstandsklassen, für Rechenzentren





---

# Zurück am Boden.

[www.frauscher.consulting](http://www.frauscher.consulting)

# Vielen Dank!

[www.frauscher.consulting](http://www.frauscher.consulting)



Foto: Foto Weiwurm

 **FRAUSCHER  
CONSULTING**   

DI **Georg Meixner**, MBA

+43 (0)676 884 855 210  
georg.meixner@frauscher.consulting  
Frauscher Consulting GmbH  
Bergmillergasse 8/2/2, 1140 Wien  
Hamerlingstraße 5/1, 4020 Linz