

Kritische Infrastruktur im Wandel

Sicherheit als Entscheidung - Von Vorsorge zu Resilienz

20. November 2025

WIENER STADTWERKE GRUPPE

WIENER LINIEN | WIEN ENERGIE | WIENER NETZE | WIENER LOKALBAHNEN | WIPARK | WIEN IT | BESTATTUNG WIEN | FRIEDHÖFE WIEN | IMMOH! | GWSG

Die Wiener Stadtwerke

Die **Wiener Stadtwerke Gruppe** ist Österreichs größter kommunaler Infrastrukturdienstleister und unverzichtbarer Teil der Daseinsvorsorge für mehr als 2 Millionen Menschen in der Metropolregion Wien. Als integrierter Konzern deckt die Gruppe essenzielle Bereiche von Energieversorgung über Mobilität bis zu kommunalen Dienstleistungen ab.


Wiener Linien
Öffentlicher Verkehr


Wiener Lokalbahnen
Öffentlicher Verkehr


Wien Energie
Energieversorgung


Wiener Netze
Netzbetrieb


WienIT
IT-Services


Bestattung Wien
Bestattungswesen


Friedhöfe Wien
Friedhofsverwaltung


Wipark
Parkräume


GWSG
Immobiliensector


immOH!
Gebäudemanagement

18.000+
Mitarbeiter*innen

€ 6 Mrd.
Jahresumsatz

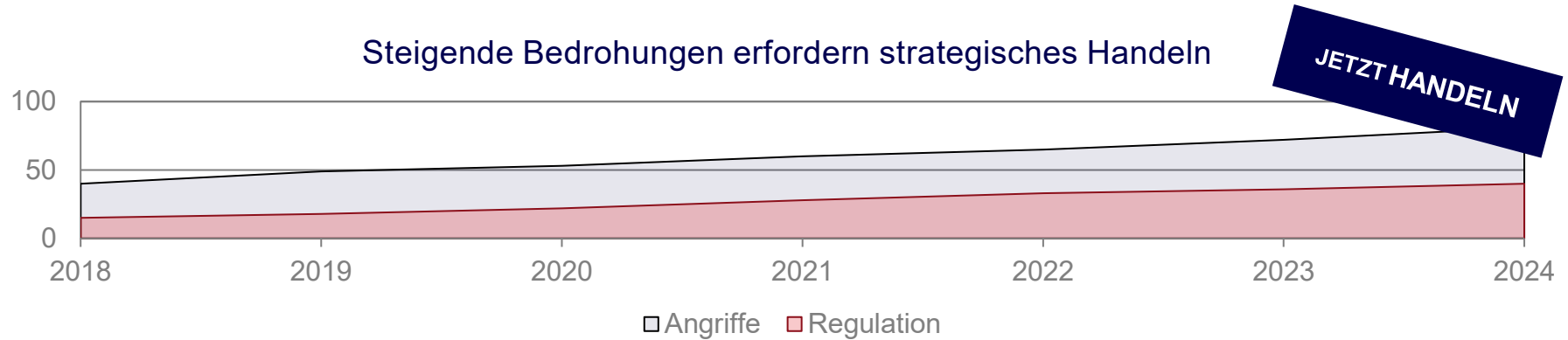
2 Mio+
Versorgte Einwohner*innen

10
Geschäftsbereiche

Sicherheitsstrategie: Die diversifizierte Struktur der Wiener Stadtwerke mit Schwerpunkt auf kritischer Infrastruktur erfordert einen mehrdimensionalen Sicherheitsansatz, der spezifische Anforderungen jedes Sektors berücksichtigt und dennoch eine einheitliche Governance gewährleistet.

Sicherheit im Wandel: Warum jetzt?

Steigende Bedrohungen erfordern strategisches Handeln



Geopolitische Spannungen

Zunehmende Bedrohungen durch Staatshacker und hybride Kriegsführung gegen kritische Infrastruktur



Digitale Transformation

Vernetzte Systeme erhöhen Angriffsfläche und Komplexität der Schutzmechanismen



Regulatorische Anforderungen

NIS2, KRITIS-Verordnung und steigende Compliance-Anforderungen erfordern strukturiertes Vorgehen

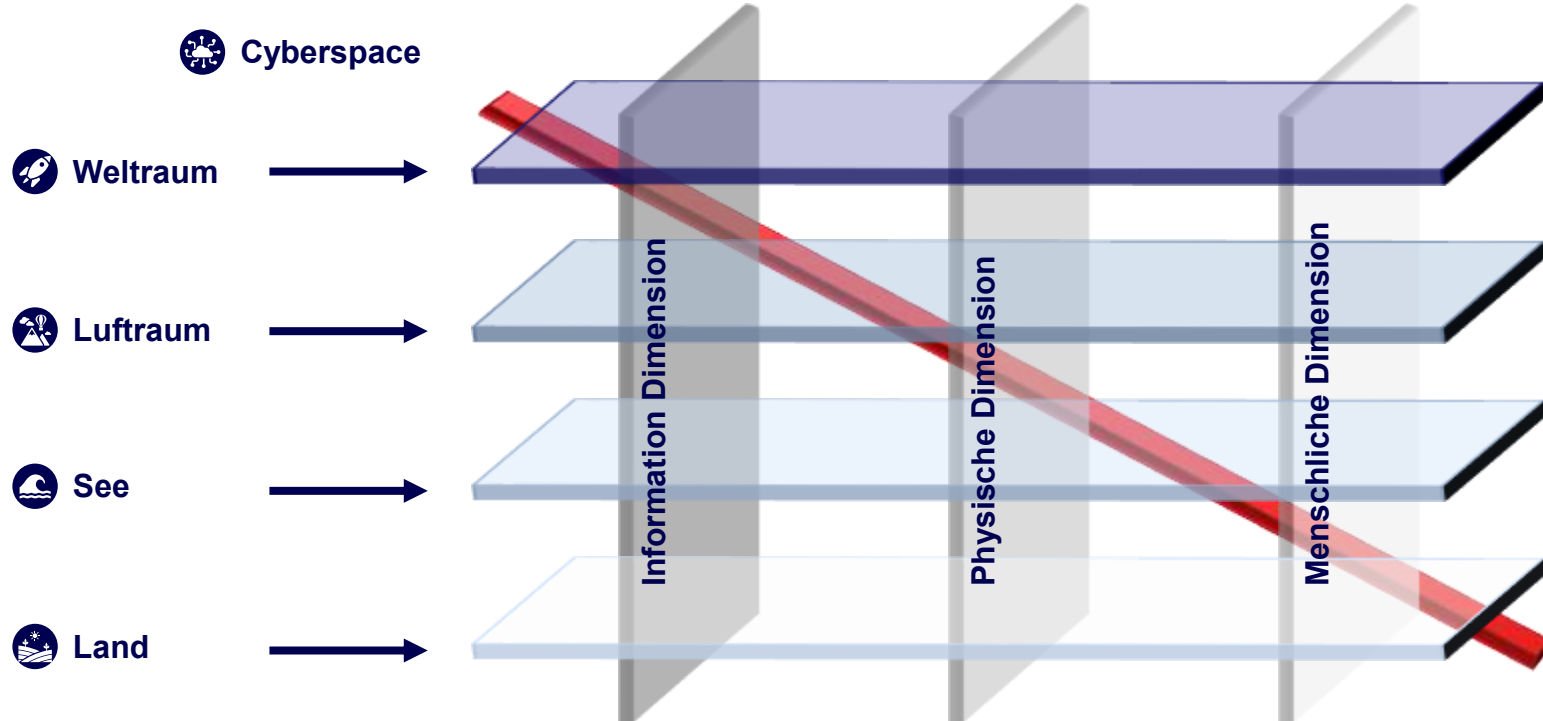


Hohe Folgekosten

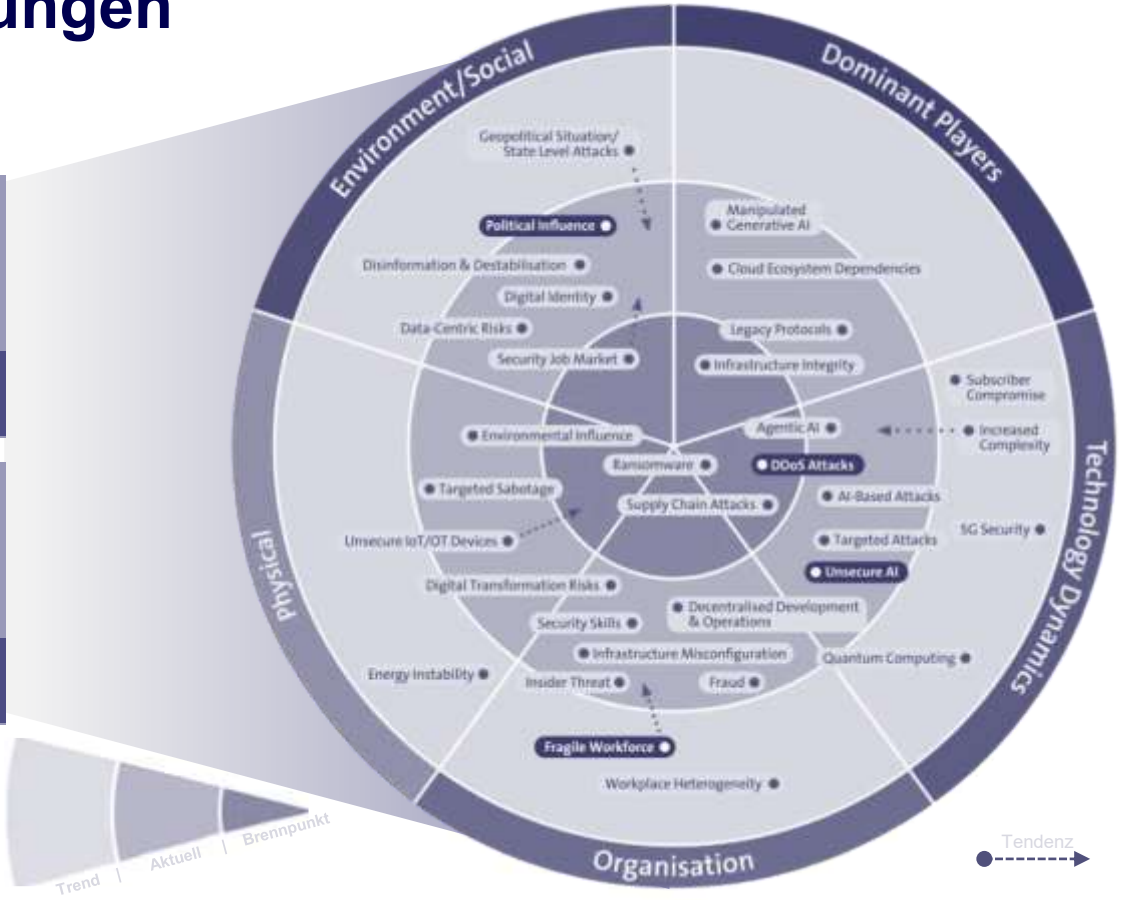
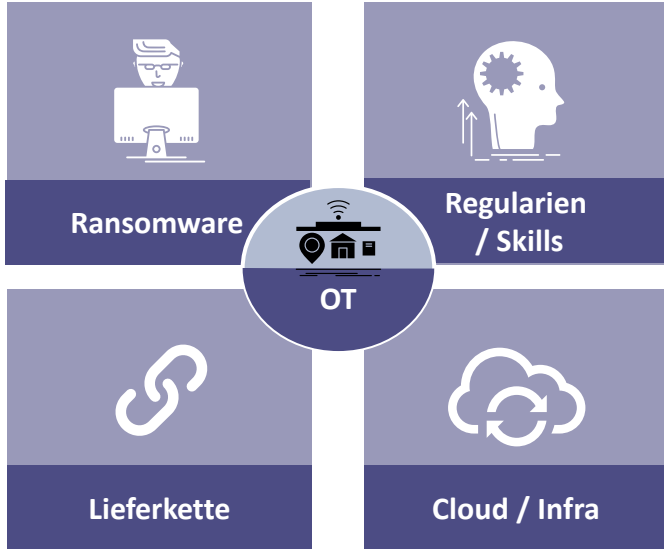
Durchschnittlich 5 Mio. € pro Sicherheitsvorfall bei kritischen Infrastrukturen in Europa

Prävention und strategisches Handeln sind kostengünstiger als Reaktion

Vielschichtige Angriffsvektoren



Wachsende Bedrohungslage & aktuelle Herausforderungen

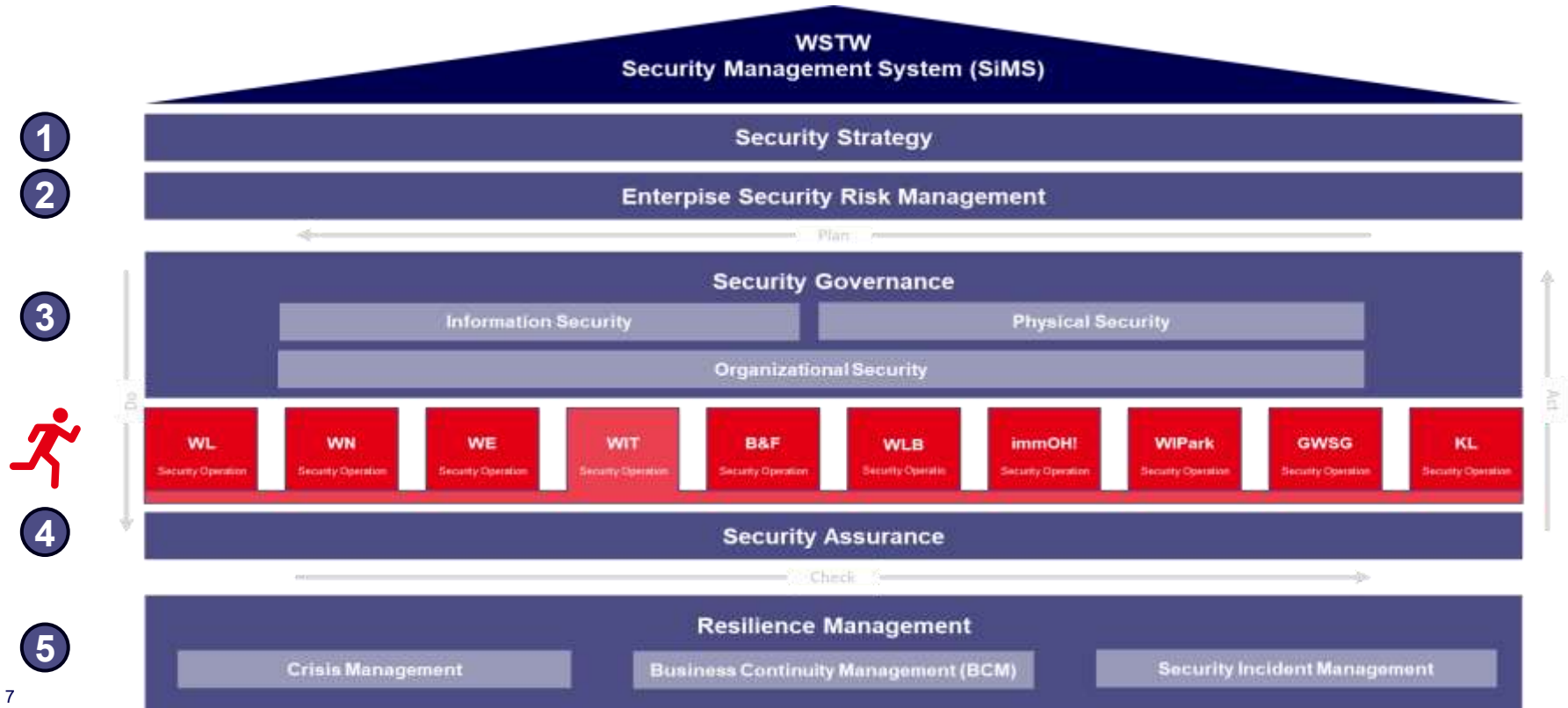


Sicherheit ist kein Sprint

Ganzheitliche Security & Resilienz als Marathon-Training

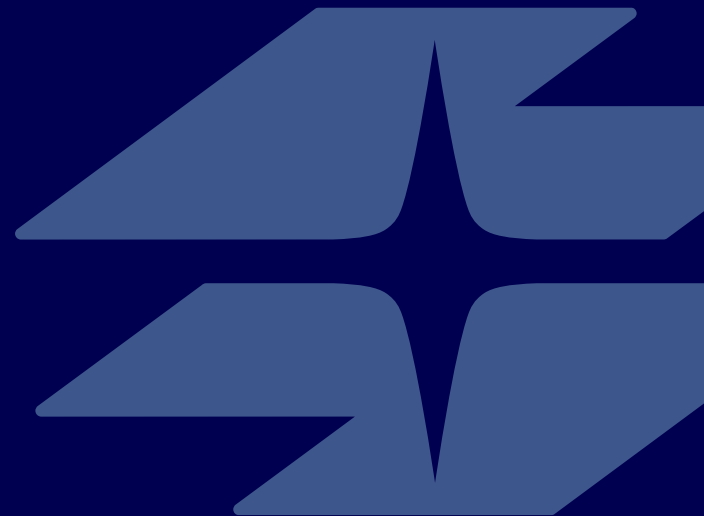


Ganzheitlicher Sicherheits- und Resilienz-Ansatz



1. Strategie - das Trainingsziel

Das "Warum" - Unser Zielbild





**Wir garantieren die
Versorgungssicherheit Wiens.**

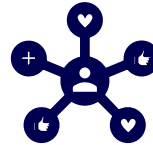
**„Die Wiener Stadtwerke-Gruppe
gestaltet Wien zur sichersten
und resilientesten
Metropolregion Europas.“**

Wiener Stadtwerke CSO-Governance

Wir laufen nicht los, weil's alle tun - sondern weil wir wissen, wo das Ziel ist.



Regulatorik + Bedrohungslage = Wettkampfkalender



Die Regulatorik (Die "Pflicht-Rennen")

EU Crisis Hub (2027), NIS 2 Gesetz (2026), RKEG (2025), European Democracy Shield (2025), Cyber Solidarity Act (2025), Cybersecurity Act (2025), ProtectEU (2025), A new European Defence Industrial Strategy (2024), EU-Konzept für kritische Infrastruktur (2024), Network Code on Cybersecurity (2024), Cyber Resilience Act (2024), EU Artificial Intelligence Act (2024), ...

Die Bedrohungslage (Die "Pop-Up-Wettkämpfe")

Ransomware, Supply Chain Attacks, IoT/OT Devices, Infrastructure Misconfiguration, Insider Threat, Disinformation & Destabilisation, DDoS Attacks, Targeted Attacks, AI-Attacks, Legacy Protocols, Cloud Services, Infrastructure Integrity, Security Skills Gap, Energy Instability, Targeted Sabotage, Environmental Influence, Quantum, Generative AI, Blackout,...

Unser Wettkampfkalender (Die agile Roadmap)

mit dem wir sowohl die Pflicht (Gesetze) als auch die Kür (akute Bedrohungen) meistern.

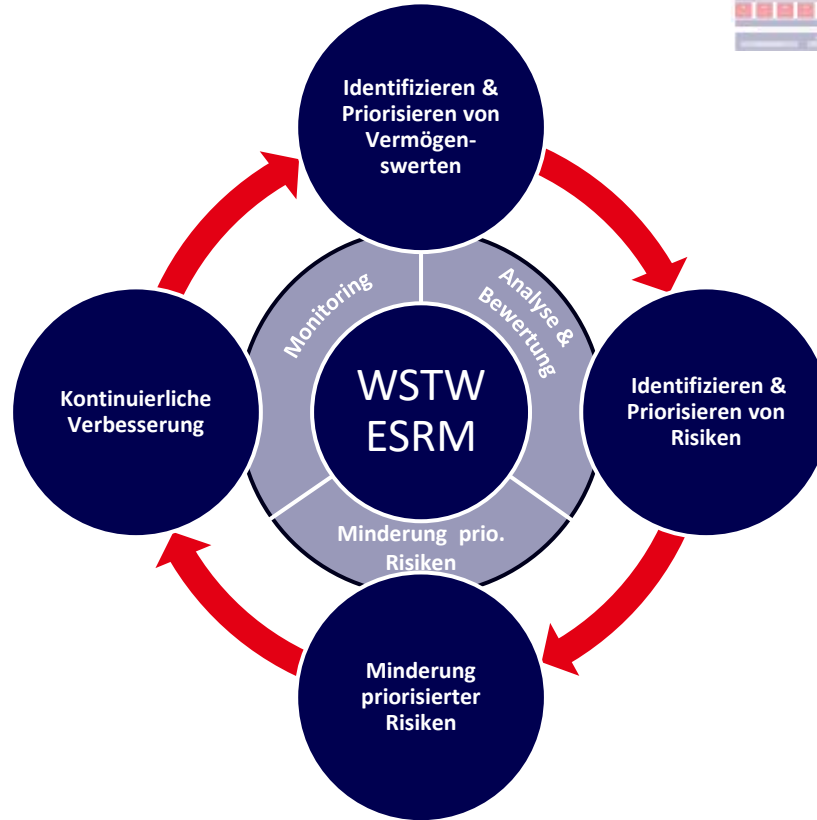
2. Risikomanagement - das Terrain kennen

**Streckenprofil: Steigungen, Engstellen,
Wetter. Risiken verstehen, Kräfte einteilen.**



ESRM

- Organisierte Kriminalität
 - Blackout
 - Desinformation
 - Migration
 - Epidemien
 - Pandemien
 - Extremismus
 - Terrorismus
 - Energiekrise
 - Rohstoffmangel
 - Naturgefahren
 - Cybergefahren
 - Spionage / Sabotage
 - Protestbewegungen
- All-Gefahren-Ansatz**



3. Governance - der Trainingsplan

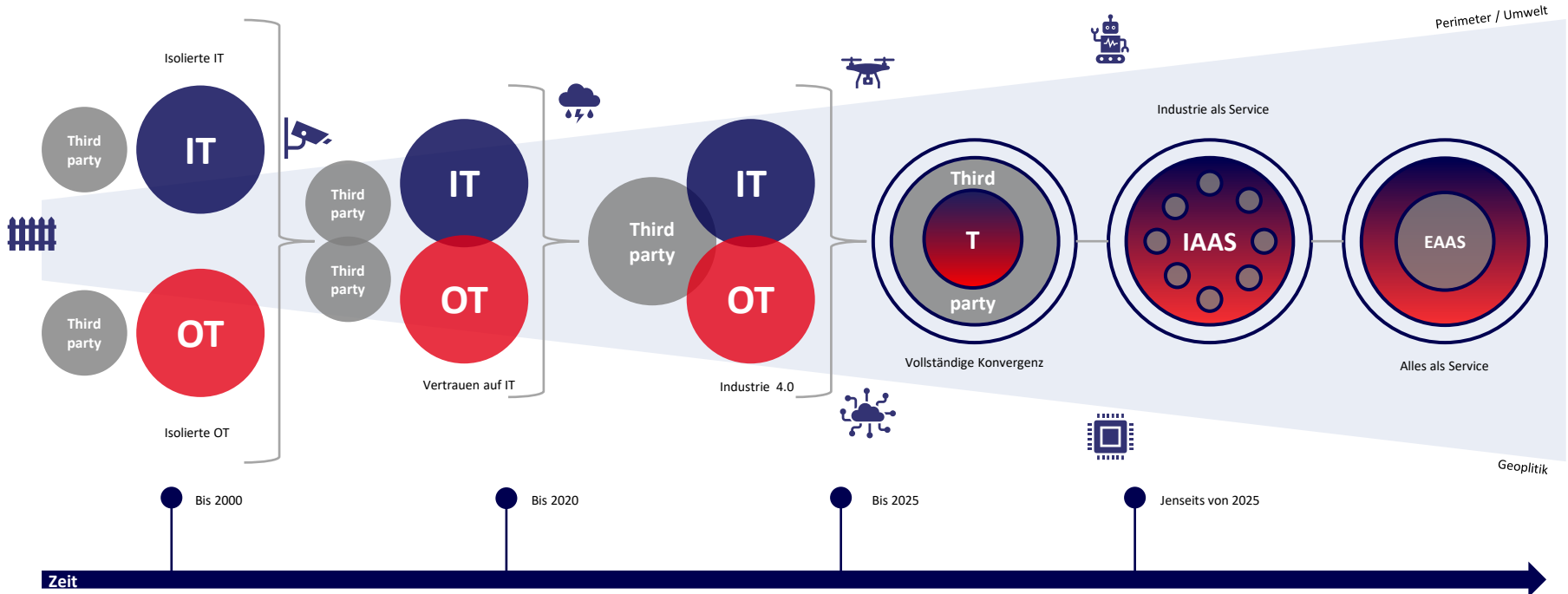
**System, das Leistung reproduzierbar macht.
Klare Rollen, Regeln & Anweisungen.**





Zunehmende Komplexität verlangt zunehmende Expertise

Die Zukunft der Sicherheit liegt im Zusammenspiel, nicht im Silodenken.





Trainer-Stab: Drei Säulen der Security



Information Security

Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Schutz der digitalen Assets, Systeme und Netzwerke vor unbefugtem Zugriff und Manipulation.



Physical Security

Schutz von Standorten, Anlagen und physischen Assets. Zutrittskontrolle, Überwachung und Sicherung der materiellen Infrastruktur.



Organizational Security

Rollen, Prozesse und Kommunikation. Governance-Strukturen, Richtlinien und Verantwortlichkeiten für ein ganzh. Sicherheitsmanagement.



Integriertes Security-Management-Framework



Keiner dieser Trainer deckt alle Fähigkeiten ab. Aber **gemeinsam**, als **integrierter Trainer-Stab**, machen sie unseren Athleten - die Wiener Stadtwerke - **fit, robust und sicher** für jedes Rennen.



Wissen bringt dich bis zur Startlinie. Tun bringt dich ins Ziel.

4. Audit - Der Leistungstest

Messen, lernen, besser werden.





Standards & Nachweise



ISO 27001 (ISMS)

- ✓ Modularer Standard für IT- und Organisationsicherheit
- ✓ Basis für Audits, Zertifizierungen, Nachweise
- ✓ Anschlussfähig für NIS2, RKEG, KRITIS



NIS2-Gesetz

- ✓ Cybersecurity-Governance & Risiko-Management
- ✓ Vorstandsbeteiligung & Risikoaufsicht
- ✓ Meldestrategie & Schutz kritischer Assets



RKEG

- ✓ Fokus auf physische & operative Resilienz
- ✓ Pflicht zu BCM, Meldewesen, Schutzplänen
- ✓ Ergänzt ISMS um sektorspezifische Tiefe



Kontroll-Mapping & Redundanzvermeidung

- ✓ Einheitliche Controls für mehrere Gesetze
- ✓ Weniger Aufwand, mehr Wirkung
- ✓ Vermeidung von Doppelstrukturen - Synergien heben

+ Sektorspezifische Anforderungen, internationale Normen und Standards

+ Physische & technische Tests

5. Resilienz

**Weiterlaufen trotz Krise. Stabil bleiben.
Schnell zurückkommen.**



Integriertes Krisenmanagement, BCM & Incident Response

Krisenmanagement



**Hitting the Wall -
Kilometer 35 kommt!**

Krisenmanagement heißt: Stabilität sichern, wenn alles in Bewegung ist.

Klare Rollen, schnelle Entscheidungen und geübte Abläufe schaffen Vertrauen - intern wie extern. So bleibt Führung auch in der Krise handlungsfähig.

BCM



BCM ist kein Sprint - sondern die Fähigkeit, das Ziel trotz Rückschlägen zu erreichen.

Unsere Resilienz beruht auf Ausdauer und Vorbereitung. BCM sichert kritische Prozesse, gewährleistet Wiederanlauf und minimiert Unterbrechungen - in alle Geschäftsbereiche integriert.

Incident Response



Wer hier zögert, verliert Meter - und Vertrauen.

Reagieren, bevor der Schaden eskaliert: Schnelle Identifikation, strukturierte Analyse und sofortige Maßnahmen.

Resilienz ist der eingeeübte Reflex, wenn der Plan zerreißt.



REEN



**Der schwerste Schritt ist der Erste -
alles danach ist Bewegung...**

Gemeinsam für eine sichere Zukunft!



**Unser
Einsatz!
Eure
Sicherheit!**



Kontakt

Marcel Lehner, BSc. MSc. MBA (CSO / Leiter Konzernsicherheit)
Seit 25+ Jahren: **Gemeinsam für eine sichere Zukunft!**

