Digitale Souveränität bei kritischen Infrastrukturen

– Resilienz, Sicherheit und strategische Handlungsfähigkeit im Energie-, Mobilitäts- und Versorgungssektor

AGEO Forum · 6. Oktober 2026

Mag. Dr. Georg Scheiber

TLP:CLEAR

VISION UND MISSION

Sicherheit für ein versorgtes Wien

Kritische Infrastruktur schützen. Energie und Mobilität zuverlässig bereitstellen. Digitale und physische Räume absichern.

Wiener Stadtwerke Sicherheitsstrategie

©mRGB - stock.adobe.com

Mehrdimensionaler Sicherheitsansatz

Wiener Linien
Öffentlicher Verkehr

Wiener Lokalbahnen
Regionalverkehr und Bahn

Wien Energie
Energieversorgung

Wiener Netze
Netzbetrieb

WienIT
IT-Services

Bestattung Wien
Bestattungswesen

Friedhöfe Wien
Friedhofsverwaltung

Wipark
Parkräume

GWSG
Immobiliensektor

immOH!
Gebäudemanagement

Sektorbezogene Umsetzung, gemeinsame Governance

Die Unternehmen haben unterschiedliche Risiken. Die Sicherheitsstrategie verbindet die Perspektiven im Konzern.

Vier Risikofelder fordern die Versorgung

01 BEDROHUNGEN

Cyber und hybride Angriffe

Angriffe auf Netze, Steuerung und Kommunikation können sich mit Sabotage verbinden.

02 UMWELT UND ANLAGEN

Klima und Infrastruktur

Extremwetter und alternde Anlagen erhöhen die Anforderungen an Vorsorge und Wiederanlauf.

03 TECHNOLOGIE

Komplexität und Daten

KI, vernetzte Systeme und Datenschutz verlangen klare Sicherheitsregeln und Zuständigkeiten.

04 BETRIEB

Versorgung aufrechterhalten

Redundanz und Ersatzverfahren müssen auch bei kombinierten Störungen funktionieren.

Risikobild: Digitale und physische Störungen können sich gegenseitig verstärken.

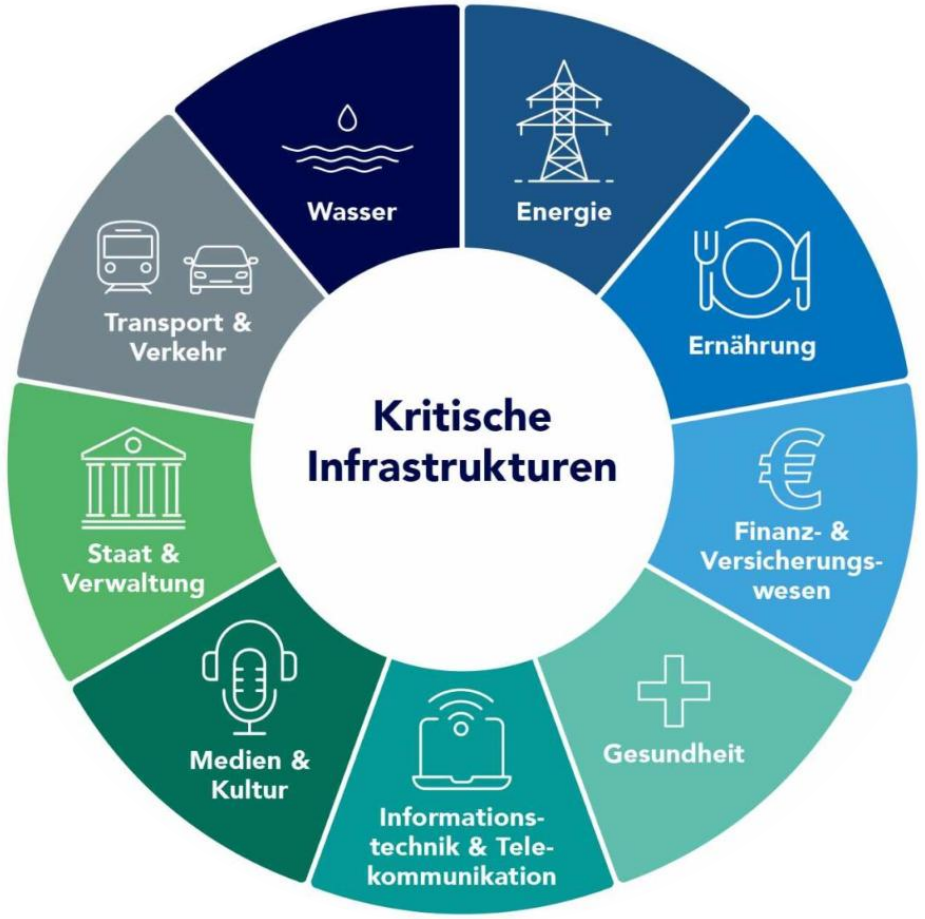
Wiener Stadtwerke als kritische Infrastruktur

Das KRITIS-Bild ist breit. Für diese Präsentation stehen drei miteinander verbundene Bereiche im Mittelpunkt.

Energie
Erzeugung, Wärme und Netze

Mobilität
Öffentlicher Verkehr und Disposition

Digitale Basis
IT, Kommunikation, Identitäten und Daten



Quelle: DKE, 2026

Vier Perspektiven auf denselben Versorgungsauftrag

Wien Energie

Energie und Fernwärme

Erzeugung und Versorgung

Wiener Netze

Netzinfrastruktur

Verteilung und Entstörung

Wiener Linien

Öffentlicher Verkehr

Betrieb und Fahrgastinformation

WienIT

Digitale Grundlage

Konzernweite IT-Services

Souveränität muss über Konzern- und Systemgrenzen hinweg funktionieren.

TLP:CLEAR

SAFE CITY

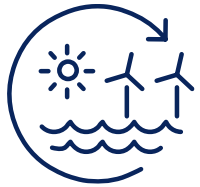
Digitale Souveränität für ein versorgtes Wien

Strom, Wärme und öffentlicher Verkehr sind im Stadtraum unmittelbar spürbar. Ihre digitalen Abhängigkeiten gehören deshalb zur Sicherheitsvorsorge.

Bild: © mRGB – stock.adobe.com | WSTW Safe City 2025

Drei Leistungen, gemeinsame digitale Abhängigkeiten

Aus der WSTW-Konzern-Perspektive wird sichtbar, weshalb Ausfälle selten an einer Unternehmensgrenze enden.

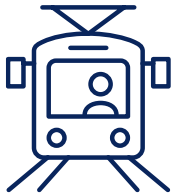


WIEN ENERGIE

WIENER NETZE

Energie

Strom und Wärme brauchen steuerbare Anlagen und Netze.



WIENER LINIEN

WIENER LOKALBAHNEN

WIPARK

Mobilität

Betrieb und Information hängen von verfügbaren Diensten ab.

WIEN IT

Digitale Infrastruktur

Identitäten, Daten und Kommunikation verbinden die Leistungen.

Souveränität entsteht erst, wenn Abhängigkeiten konzernweit bekannt und beherrschbar sind.

ILLUSTRATIVES STÖRUNGSSZENARIO

Ein digitaler Ausfall kann mehrere Betriebe treffen

Beispiel: Ein zentraler Identitätsdienst ist vorübergehend nicht verfügbar.

01

Digitaler Dienst

Anmeldung und Zugriff gestört

02

Anwendungen

Arbeitsabläufe eingeschränkt

03

Einsatz und Disposition

Alternative Verfahren nötig

04

Versorgung

Betrieb stabil halten

Die Frage lautet: Wer kann entscheiden, umschalten und den Betrieb weiterführen?

BEGRIFF

Digitale Souveränität hält Leistungen steuerbar

01

Wahlfreiheit

Welche Alternative hält Betrieb und Entstörung arbeitsfähig?

02

Transparenz

Welche Anbieter, Daten, Zugriffe und Schnittstellen sind kritisch?

03

Wiederanlauf

Sind Notbetrieb, Wechsel und Wiederherstellung geübt?

Nicht vollständige Autarkie, sondern belastbare Handlungsoptionen je Dienst.

RISIKOBILD

Kritische Infrastruktur braucht einen All-Gefahren-Blick

Cyber
Angriffe auf IT und Steuerung

Physisch
Sabotage und Anlagenschäden

Natur
Sturm, Hochwasser und Hitze

Technik
Ausfall und Fehlfunktion

Lieferkette
Komponenten und Herstellerdienste

Personal
Ausfälle und fehlende Fähigkeiten

Eine kombinierte Lage kann digitale und physische Abhängigkeiten zugleich treffen.

ESRM übersetzt Gefahren in priorisierte Maßnahmen

Enterprise Security Risk Management verbindet das All-Gefahren-Bild mit Entscheidungen im Konzern.

01 SICHTBARKEIT

Werte und Dienste erfassen

Welche Anlagen, Systeme und Leistungen sind für Wien wesentlich?

02 BEWERTUNG

Risiken priorisieren

Auswirkungen und Kaskaden über Unternehmensgrenzen hinweg beurteilen.

03 UMSETZUNG

Risiken mindern

Maßnahmen, Verantwortliche und Ressourcen für die wichtigsten Risiken festlegen.

04 LERNEN

Wirksamkeit prüfen

Lagebild und Annahmen aktualisieren, Maßnahmen nachschärfen.

Der Kreislauf schafft Transparenz über Risiken und die Wirkung der Maßnahmen.

RESILIENZ

Versorgungssicherheit über den Störfall hinaus

01

Vorsorgen

Risikoanalysen, Redundanzen und Abhängigkeiten kennen

02

Weiterbetreiben

Notbetrieb, Entscheidungswege und Kommunikation aktivieren

03

Wiederherstellen

Systeme prüfen, hochfahren und Erfahrungen einarbeiten

Maßstab: Wie zuverlässig bleiben Strom, Wärme und Mobilität verfügbar?

ZIELBILD

Kritikalität bestimmt Architektur und Ausweichfähigkeit

Vier Fragen gehören für jeden wesentlichen digitalen Dienst zusammen.

Dienst

Was muss auch im Störfall funktionieren?

Daten und Assets

Wo liegen sie und wer hat Zugriff?

Betriebsmodell

Welche Abhängigkeit wird bewusst akzeptiert?

Rückfall

Wie wird ein Wechsel oder Notbetrieb getestet?

Kritische Betriebsführung anders behandeln als weniger kritische Anwendungen.

Sicherheitsbausteine zu einer Steuerung verbinden

1	**NIS2 und RKEG-Governance**		Verantwortung, Risiken und Meldungen
2	**Zero Trust**		Identitäten, Geräte und Zugriffe
3	**Zentrales 24/7 SOC**	WIEN IT	Erkennen und Reagieren
4	**GRC-System und ISMS**	crisam	Risiken transparent steuern
5	**Cloud- und KI-Governance**		Nutzung risikobasiert freigeben

Der nächste Schritt ist die Kopplung an Dienstkritikalität und Lieferantensteuerung.

NISG 2026 und RKEG gemeinsam umsetzen

NISG 2026

Cybersicherheit von Netz- und Informationssystemen: Risiko, Maßnahmen, Vorfälle und Verantwortung.

RKEG

Resilienz kritischer Einrichtungen: Risikoanalyse, physischer Schutz, Vorsorge und Meldung.

Für betroffene Konzernunternehmen müssen digitale und physische Risiken zusammen gedacht werden.

Aktueller Rechtsstand: RKEG seit 01.03.2026, NISG 2026 seit 01.10.2026.

ABHÄNGIGKEITEN

Ein Vertrag allein schafft noch keine Wechseloption

Cloud und Plattform

Datenexport, Schnittstellen und Ersatzbetrieb

OT-Hersteller

Updates, Wartung und Ersatzteile

Identitätsdienste

Kontrollrechte und Notzugang

Geopolitik und Recht

Verfügbarkeit, Sanktionen und Zugriffe

Souverän ist eine Option erst dann, wenn sie technisch und organisatorisch funktioniert.

VORGEHEN

Vom Lieferantenausfall zur getesteten Maßnahme

Illustratives Szenario: Eine zentrale Anbieterkomponente fällt länger aus.

1 Dienst bestimmen

Welche WSTW-Leistung ist betroffen?

2 Abhängigkeit erfassen

System, Vertrag, Daten und Personal

3 Auswirkung bewerten

Dauer, Reichweite und Kaskaden

4 Option planen

Notbetrieb, Ersatz, Trennung

5 Umsetzen

Technik, Vertrag und Zuständigkeit

6 Üben

Wechsel und Wiederanlauf testen

Das Ergebnis ist eine betriebsfähige Option, keine ungeprüfte Annahme.

MANAGEMENTENTSCHEIDUNG

Drei Entscheidungen für die Wiener Stadtwerke

1	**Kritische Dienste je KU erfassen**	Energie, Netze, Mobilität und digitale Basis gemeinsam betrachten.
2	**Mindestfähigkeit festlegen**	Notbetrieb, Zugriffe, Wiederanlauf und Lieferantenoption je Dienst.
3	**Optionen finanzieren und testen**	Übungen, Exit-Tests, Ersatzteile und Kompetenzen einplanen.

Digital souverän wird die Gruppe durch klare Verantwortung und erprobte Optionen.

TLP:CLEAR

Digital souverän heißt: Versorgung steuern, auch wenn digitale Abhängigkeiten unter Druck geraten.

Resilienz, Sicherheit und strategische Handlungsfähigkeit
für Energie, Mobilität und Versorgung in Wien.

Danke für Ihre Aufmerksamkeit

Bild: © mRGB – stock.adobe.com | WSTW Safe City 2025