

NGAI White Paper

Navigieren in der neuen CER-Ära: Ein Whitepaper zur Resilienz kritischer Einrichtungen am Standort Wien

Prepared By

Andrei I. Cursaru

Jun 29, 2026

Zusammenfassung

Am 23. Juni 2026 versammelten sich führende Akteure der nationalen Sicherheit, darunter Vertreter der Nexus Group AI, zum hochkarätig besetzten KSÖ-Rechts- und Technologiedialog. Flankiert vom Bundesministerium für Inneres (BMI) und der Direktion Staatsschutz und Nachrichtendienst (DSN) stand ein sicherheitspolitischer Meilenstein im Fokus des Diskurses: die vollständige Implementierung der Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) in der Republik Österreich (1). Mit dem offiziellen Inkrafttreten des österreichischen Resilienz kritischer Einrichtungen-Gesetzes (RKEG) am 1. März 2026 sowie der präzisierenden Resilienz kritischer Einrichtungen-Verordnung (RKEV) am 15. April 2026 hat sich die Sicherheitsarchitektur des Landes fundamental gewandelt (2).

Ende der Freiwilligkeit: Die Überführung der EU-CER-Richtlinie in das österreichische RKEG markiert für KRITIS-Betreiber das definitive Ende unverbindlicher Empfehlungen. Sanktionsbewehrtes Pflichtenregime: Unternehmen werden rechtlich dazu verpflichtet, strikte physische, personelle und organisatorische Schutzmaßnahmen umzusetzen. Ganzheitliche Risikosysteme: Zur Bewältigung kaskadierender Risikoszenarien ist eine nahtlose Integration von Cyber- und physischen Sicherheitsarchitekturen sowie der Einsatz moderner Technologien erforderlich.



CRITICAL ENTITIES RESILIENCE DIRECTIVE

Der Paradigmenwechsel: Vom APCIP zum RKEG und die Abgrenzung zum NISG 2026

Historisch basierte der Schutz kritischer Infrastrukturen in Österreich primär auf dem "Austrian Program for Critical Infrastructure Protection" (APCIP), dessen Masterplan aus dem Jahr 2014 im Wesentlichen auf freiwilliger Kooperation, Sensibilisierung und dem informellen Austausch zwischen Staat und Privatwirtschaft fußte. Angesichts der zunehmenden systemischen Vernetzung, wachsender geopolitischer Spannungen und der Entstehung hybrider Bedrohungslagen erwies sich dieses Paradigma der Freiwilligkeit als unzureichend (6). Das RKEG löst den APCIP-Masterplan offiziell ab und etabliert einen rechtsverbindlichen, harmonisierten europäischen Rahmen (7).

Der konzeptionelle Kern dieses neuen Rahmens ist der sogenannte "All-Hazards-Approach" (All-Gefahren-Ansatz). Während frühere, oftmals fragmentierte Konzepte isolierte Bedrohungen wie Cyberangriffe oder Naturkatastrophen in separaten Silos betrachteten, zwingt das RKEG kritische Organisationen nun zu einem holistischen Risikomanagement. Betreiber müssen sich rechtsverbindlich auf sämtliche natürliche, technische, anthropogene und intentionale Bedrohungen vorbereiten (5). Dies inkludiert Extremwetterereignisse, Pandemien, physische Sabotage, Spionage, bewaffnete Konflikte sowie systemische Lieferkettenausfälle, deren Interdependenzen eine neue Dimension der Gefahrenabwehr darstellen.

Ebenso entscheidend wie der Inhalt des RKEG ist seine systematische Abgrenzung zu parallel laufenden Legislativakten, insbesondere dem Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026), welches am 1. Oktober 2026 in Kraft tritt und die NIS2-Richtlinie umsetzt (11). Während das RKEG die physische, operative und organisatorische Resilienz im Sinne der CER-Richtlinie reguliert, fokussiert sich das NISG 2026 als eigenständiges Regelwerk auf die Cybersicherheit und das IT-Vorfallsmanagement (11). Diese rechtliche Trennung bedeutet jedoch keine operative Isolation: Gemäß § 24 Abs 1 Z 1 lit f NISG

2026 gilt jede Einrichtung, die unter dem RKEG formell als "kritisch" eingestuft wird, automatisch auch als "wesentliche Einrichtung" unter dem NISG 2026 (11). Für Unternehmensführungen bedeutet diese Schnittstelle, dass integrierte Governance-Strukturen geschaffen werden müssen, um Doppelgleisigkeiten zu vermeiden und simultan die Konformität in der physischen und digitalen Domäne sicherzustellen (4).

Die erfassten Sektoren und die urbane Dimension

Wiens

Das RKEG identifiziert elf essenzielle Sektoren, deren Ausfall oder signifikante Störung gravierende Auswirkungen auf das gesellschaftliche Leben, die öffentliche Gesundheit oder die nationale Wirtschaft hätte. Bundesweit rechnet das Innenministerium mit der Erfassung von rund 500 bis 600 Einrichtungen, die für die staatliche Grundversorgung unverzichtbar sind (4). Die nachfolgende Tabelle strukturiert die abgedeckten Sektoren und illustriert die weitreichende Durchdringung des Gesetzes in alle Bereiche der Daseinsvorsorge:

RKEG-Sektor Relevanz und kritische Teilbereiche Energie Stromerzeugung, Übertragungs- und Verteilernetze, Gasversorgung, Fernwärmenetze, Öllagerung. Verkehr Schienennetzbetreiber, Zivilluftfahrt, Flughäfen, öffentlicher Personennahverkehr (ÖPNV), Binnenhäfen. Bankwesen Kreditinstitute mit systemischer Relevanz für den Finanzkreislauf. Finanzmarktinфраstruktur Handelsplätze, zentrale Gegenparteien, Clearingstellen. Gesundheit Krankenhäuser, Großlabore, Forschungseinrichtungen, pharmazeutische Produktionsstätten und Logistikzentren. Trinkwasser Kommunale und überregionale Wasserversorgung, Aufbereitungsanlagen, Hochquellenleitungen. Abwasser Kläranlagen, Pumpwerke, kritische Kanalnetzbetreiber. Digitale Infrastruktur Rechenzentren, Telekommunikationsanbieter, Cloud-Dienste, Internet-Knotenpunkte. Öffentliche Verwaltung Zentralstaatliche Ministerien, Sicherheitsbehörden, Parlamentsgebäude, systemrelevante Dienststellen. Weltraum Bodeninfrastrukturen zur Satellitensteuerung, Kommunikation und Navigation. Lebensmittel Großhandel, Logistikzentren, systemrelevante Lebensmittelproduktion und -distribution. Tabelle 1: Vom RKEG erfasste kritische Sektoren gemäß EU CER-Richtlinie 2022/2557 (2).

Wien stellt als Metropolregion ein hochgradig vernetztes, sozio-technisches Ökosystem dar, in dem kaskadierende Effekte (Cascading Failures) verheerende Ausmaße annehmen können. Wissenschaftliche Studien zu Smart-City-Infrastrukturen belegen, dass die Resilienz in solchen Umgebungen nicht durch das isolierte Betrachten einzelner Anlagen gewährleistet werden kann (15). Die Wiener Stadtwerke (WSW) fungieren mit ihren Konzerntöchtern – Wien Energie, Wiener Netze, Wiener Linien, Wiener Lokalbahnen und WienIT – als das absolute Rückgrat der städtischen Daseinsvorsorge (13).

Die Komplexität der urbanen Resilienz wird im Falle eines Blackout-Szenarios evident. Ein flächendeckender Stromausfall erfordert das präzise, sektorübergreifende Ineinandergreifen diverser Akteure (17). Die Wiener Netze müssen die Netzstabilität durch Inselfahrweise managen, während Wien Energie die Fernwärmeversorgung durch thermische Kraftwerke und Schwarzstartfähigkeit aufrechterhält (17). Simultan steuert die Leitstelle der Wiener Linien die geordnete Evakuierung und Stilllegung des Verkehrsnetzes, gestützt auf vom öffentlichen Netz unabhängige Notstromversorgungen und autarke Kommunikationswege (17).

Eng verknüpft mit der Energie- und Mobilitätswende ist die öffentliche Verwaltung der Stadt Wien, insbesondere die Magistratsabteilung 31 (Wiener Wasser) und die Magistratsabteilung 68 (Feuerwehr und Katastrophenschutz). Die MA 31 versorgt rund 1,8 Millionen Menschen über ein Leitungsnetz von 3.000 Kilometern und 350 Kilometern Hochquellenleitungen (18). Ein durch Sabotage oder Systemausfälle bedingter Druckabfall im Wassernetz würde nicht nur die Trinkwasserversorgung kollabieren lassen, sondern zeitgleich die Löschwasserversorgung der MA 68 gefährden. Als älteste Berufsfeuerwehr der Welt (gegründet 1686) bewältigt die MA 68 mit über 1.600 Einsatzbediensteten jährlich rund 43.000 Einsätze (19). Die RKEG-Bewältigung erfordert eine lückenlose Schnittstellenkoordination zwischen den Krisenstäben der kritischen Einrichtungen und den Einsatzleitern der Berufsfeuerwehr, um bei kaskadierenden Katastrophen die Handlungsfähigkeit der Stadt aufrechtzuerhalten.

Darüber hinaus wird die "Digitale Souveränität" zu einem imperativen Resilienzfaktor für Betreiber (21). Der zunehmende Einsatz von Cyber-Physical Systems (CPS) und dem Industrial Internet of Things (IIoT) bedeutet, dass physische Prozesse massiv von Cloud-Diensten und Datenverarbeitung abhängen (16). Die strategische Position der Wiener Stadtwerke unterstreicht die Notwendigkeit von Datenlokalität, Interoperabilität und der Förderung europäischer Cloud-Infrastrukturen (22). Wenn Cyber- und physische Domänen verschmelzen, kann eine Software-Verwundbarkeit in einer vermeintlich sicheren Cloud-Plattform physische Zerstörungen an Pumpstationen oder Umspannwerken nach sich ziehen, was die Forderung nach Reversibilität und Herstellerunabhängigkeit zu einer Frage der nationalen Sicherheit macht (15).

Nationaler Risiko- und Strategierahmen (ÖSRKE & NRA 2026)

Um den Betreibern eine makroskopische Orientierung zu geben und die Basis für die unternehmensinternen Analysen zu schaffen, veröffentlichte das BMI im Januar 2026 zwei fundamentale Dokumente: die Österreichische Strategie für die Resilienz kritischer Einrichtungen (ÖSRKE 2026) und die Nationale Risikoanalyse (NRA 2026) (10). Österreich nahm mit der fristgerechten Veröffentlichung dieser Dokumente eine Vorreiterrolle in Europa ein, da vielen anderen Staaten die staatliche Makrogrundlage zu diesem Zeitpunkt noch fehlte (24). Die ÖSRKE 2026 formuliert die übergeordneten nationalen Ziele. Sie verdeutlicht auf strategischer Ebene, dass Resilienz nicht nur die robuste Widerstandsfähigkeit gegen Erstschläge bedeutet (Robust Design), sondern vor allem die Fähigkeit zur raschen Absorption, Anpassung und Wiederherstellung wesentlicher Dienste (Bounce-back-Fähigkeit) nach einem Schockereignis (25).

Dieser Paradigmenwechsel wird durch die NRA 2026 methodisch fundiert. Die Erstellung der NRA erfolgte unter strenger Beachtung internationaler Standards, insbesondere der ISO 31000 ("Risk management – Guidelines") und der darauf aufbauenden, österreichspezifischen ÖNORM D 4900-Reihe (27). Die ÖNORM D 4900 fungiert als essenzielle Brücke zwischen der internationalen Norm und der praktischen Umsetzung im heimischen Markt. Sie fordert ein integratives Risikomanagementsystem, das systemische Ansätze verbindet: Eine "Top-down"-Perspektive, bei der die strategische Steuerung durch die Unternehmensführung erfolgt, und eine "Bottom-up"-Perspektive zur operativen Risikoerfassung an der Basis (28). Durch standardisierte Handlungsanleitungen ermöglicht sie Organisationen, durch Business Impact Analysen (BIA) priorisierte Ziele zu setzen und das Notfall-, Krisen- und Kontinuitätsmanagement (verankert in der ÖNORM D 4902-3) effektiv zu steuern (14).

Die NRA 2026 wendet diese Methodik auf gesamtstaatlicher Ebene an und liefert alarmierende, datengestützte Erkenntnisse über das aktuelle Bedrohungsumfeld. Der Bericht bewertet Risiken in einer detaillierten Matrix nach Eintrittswahrscheinlichkeit und Schadensausmaß (24). Von den 113 identifizierten Hauptrisiken entfallen 37 auf intentionale (mutwillige) Gefahren wie physische Sabotage, hybride Angriffe oder gezielte Spionage (24). Damit überwiegen die absichtlichen Angriffe die rein technischen Gefahren (23 Risikoeinträge) und Naturgefahren (19 Risikoeinträge) deutlich (24). Diese Verteilung ist ein direktes Abbild der geopolitischen Lageeinschätzung und markiert laut dem Bundesministerium für Landesverteidigung (BMLV) das "Ende der Ordnung" und den Übergang zu einem konfrontativen, multipolaren System (6). Für kritische Einrichtungen bedeutet dies operativ, dass die Modellierung von Täterprofilen und gezielten Sabotageakten nun ein zwingender Bestandteil der eigenen, nach RKEG vorgeschriebenen Risikoanalyse sein muss (14).

Zusätzlich analysiert die NRA intensiv die Beziehungsgeflechte zwischen Bedrohungen. Sie unterscheidet zwischen auslösenden Beziehungen (ein Ereignis verursacht mehrere Gefährdungen), verstärkenden Beziehungen (Klimawandel erhöht die Wahrscheinlichkeit von Folgegefahren) und kumulativen Beziehungen (kombinierte Auswirkungen sind größer als die Summe der Einzelereignisse) (24). Der Bericht plädiert unmissverständlich für sektorübergreifende Ansätze als wirksamste Antwort auf Multigefährdungsszenarien (24).

Das Pflichtenregime nach § 11 RKEG: Bescheide und Fristen

Ein zentrales Merkmal der österreichischen CER-Umsetzung ist, dass der Status als "Kritische Einrichtung" (kE) nicht automatisch durch die reine Zugehörigkeit zu einer Branche oder das Überschreiten gewisser Unternehmensgrößen entsteht (anders als bei NIS2). Stattdessen wird die Eigenschaft als kE ausschließlich durch einen rechtsgestaltenden, konstitutiven Bescheid des Bundesministers für Inneres festgestellt (9).

Die Ermittlung erfolgt gemäß § 11 Abs. 1 RKEG anhand von vier kumulativen Kriterien: Die Einrichtung muss im Inland (Österreich) tätig sein. Die kritische Infrastruktur (Objekte, Anlagen, Systeme) muss sich im Inland befinden. Es muss ein wesentlicher Dienst gemäß § 3 Z 6 RKEG erbracht werden. Bei der Erbringung dieses Dienstes muss die Möglichkeit bestehen, dass ein Sicherheitsvorfall eintritt (9).

Sobald dieser behördliche Bescheid rechtskräftig zugestellt wird (erste Bescheide werden ab Mitte bis Ende 2026 erwartet), unterliegt die Einrichtung einem streng strukturierten Fristenregime. Die nachfolgende Tabelle fasst die kritischen Meilensteine zusammen, die ab dem Zeitpunkt der Bescheidezustellung rechtlich bindend sind:

Frist ab Einstufungsbescheid Verpflichtende operative Maßnahme gemäß RKEG Innerhalb von 4 Wochen
Benennung einer Kontaktstelle (§ 4.1): Die kritische Einrichtung muss eine zentrale Kontaktstelle und mindestens eine konkrete Ansprechperson an die Behörde melden. Die ständige Erreichbarkeit dieser Stelle muss während der Betriebszeiten des wesentlichen Dienstes zwingend garantiert sein. Änderungen sind unverzüglich, spätestens binnen zwei Wochen, zu melden. Ausländische Einrichtungen ohne Inlandsniederlassung müssen einen verantwortlichen Beauftragten bestellen (9). Innerhalb von 9 Monaten
Risikoanalyse (§ 4.2 / § 14): Durchführung, Dokumentation und Vorhaltung einer vollumfänglichen, internen Risikoanalyse, die sich inhaltlich und methodisch an der NRA 2026 orientiert. Diese muss den

All-Gefahren-Ansatz strikt abdecken und Lieferketten, kritische Prozesse sowie technische Abhängigkeiten bewerten. Eine Aktualisierung hat anlassbezogen, längstens jedoch alle vier Jahre, zu erfolgen (9). Innerhalb von 10 Monaten Resilienzplan und Maßnahmen (§ 4.3 / § 15): Erstellung, Dokumentation und vollständige Implementierung eines umfassenden Resilienzplans. Dieser Plan dokumentiert die Umsetzung verhältnismäßiger technischer, organisatorischer und personeller Schutzmaßnahmen zur Sicherstellung der Governance und operativen Widerstandsfähigkeit (9).

5.1. Meldepflichten und Vorfallsmanagement Ab dem Zeitpunkt, an dem die 10-Monats-Frist zur Umsetzung der Resilienzmaßnahmen abgelaufen ist, greift ein scharfes Regime zur Meldung von Vorfällen (4). Ein "Sicherheitsvorfall" ist im RKEG äußerst weit gefasst definiert: Es umfasst nicht nur IT-bezogene Störungen, sondern jegliches Ereignis (inklusive Beinahe-Vorfälle), das die Erbringung eines wesentlichen Dienstes erheblich stört oder stören könnte (11).

Die RKEV (§ 2) konkretisiert diese abstrakte Definition durch messbare Schwellenwerte. Um eine erhebliche Störung quantifizieren zu können, verwendet die Verordnung sektorspezifische Parameter wie "Nutzerstunden" (Dauer des Ausfalls multipliziert mit der Anzahl der betroffenen Nutzer) oder "Zählpunktstunden" im Energiebereich (11).

Wird ein solcher Schwellenwert überschritten, muss die Einrichtung das BMI unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung, formell benachrichtigen (11). Dieses extrem enge Zeitfenster erfordert hochautomatisierte Detektions- und Meldekette innerhalb der Organisation. Dem initialen Alert muss zwingend innerhalb eines Monats ein detaillierter Folgebericht (Folgemeldung) nachgereicht werden. Dieser Bericht muss eine tiefgehende faktische Aufarbeitung des Vorfalls, die Ursachenanalyse sowie die Dokumentation der zur Schadensbegrenzung gesetzten Maßnahmen beinhalten (11).

Gesetzliche Ausnahmen (§ 18 Abs. 3 RKEG)

Eine wichtige Sonderregelung betrifft kritische Einrichtungen, die den Sektoren Digitale Infrastruktur, Bankwesen und Finanzmarktinфраstruktur angehören. Gemäß § 18 Abs. 3 RKEG sind diese Sektoren von den spezifischen Verpflichtungen zur Erstellung eigener Risikoanalysen, Resilienzpläne und den RKEG-spezifischen Meldepflichten ausgenommen (11). Der Gesetzgeber trägt hiermit dem Umstand Rechnung, dass diese Industrien bereits durch hochspezifische und extrem strenge europäische Regulierungen (wie die DORA-Verordnung für den Finanzsektor oder das NISG 2026 für digitale Dienste) erfasst sind. Diese Ausnahme reduziert den administrativen Overhead für betroffene Organisationen signifikant, entbindet sie jedoch nicht von der allgemeinen Einstufung als wesentliche Instanzen der nationalen Sicherheit (11).

Das RKEG beschreibt die Pflichten zur Resilienzstärkung abstrakt. Um zu verhindern, dass die vorgeschriebenen Resilienzpläne zu rein formalen Papiertigern mutieren, hat die Direktion Staatsschutz und Nachrichtendienst (DSN) am 18. Juni 2026 praxisnahe Leitfäden veröffentlicht (24). Diese "Soft Law"-Dokumente strukturieren die gesetzlichen Anforderungen entlang von Zieldimensionen (Z0 bis Z6) und dienen als Benchmark, an dem sich Betreiber und Auditoren orientieren müssen (9).

Z0 – Allgemeine Grundlagen und Anwendungen: Dieser Basisleitfaden definiert den juristischen und konzeptionellen Rahmen. Er erläutert die Maßstäbe der "Geeignetheit" und "Verhältnismäßigkeit" von Maßnahmen. Eine 100-prozentige Sicherheit ist in komplexen Systemen eine Illusion; Z0 fordert vielmehr einen risikobasierten Ansatz, bei dem Investitionen in den Schutz in direkter Relation zur Kritikalität des Dienstes und der Wahrscheinlichkeit des Risikos stehen (9). Zudem wird das Normenverhältnis zu

bestehenden Managementsystemen (wie ISO 27001 oder ISO 22301) geklärt und die Konformitätsvermutung definiert.

Z1 – Verhinderung von Sicherheitsvorfällen (Prävention): Die erste operative Dimension fokussiert sich auf die proaktive Vermeidung von Vorfällen, bevor diese manifest werden. Dies umfasst die anlagentechnische Wartung, die betriebliche Arbeitssicherheit und die strukturelle Härtung von Gebäuden (9). Da die NRA 2026 den Klimawandel als signifikanten Risikomultiplikator identifiziert, verlangt Z1 explizit langfristige Strategien zur Katastrophenvorsorge und Klimawandelanpassung. Für Infrastrukturbetreiber bedeutet dies oft signifikante CAPEX-Investitionen, beispielsweise um Umspannwerke vor prognostizierten Jahrhunderthochwassern zu schützen oder Kühlsysteme an längere Hitzewellen anzupassen.

Z2 – Physischer Schutz: Diese Dimension adressiert die klassische Perimetersicherheit. Die Anforderungen zielen auf den angemessenen Schutz von Räumlichkeiten und Anlagen durch ein Schichtenmodell ab (Defense-in-Depth). Dies inkludiert mechanische Barrieren (Zäune, Poller), bauliche Härtung (sprengwirkungshemmende Verglasung) sowie den flächendeckenden Einsatz moderner elektronischer Verteidigungssysteme wie biometrische Zutrittskontrollen, Einbruchmeldeanlagen und KI-gestützte Videoanalytik (9). Ein besonderes Augenmerk liegt auf der physischen Resilienz sogenannter Single Points of Failure (SPOFs) – Knotenpunkte, deren Zerstörung das gesamte Netzwerk eines Unternehmens lahmlegen würde.

Z3 – Abwehr und Bewältigung von Sicherheitsvorfällen: Im Krisenfall muss eine Organisation unter extremem Druck reaktions- und führungsfähig bleiben. Z3 fordert den Aufbau einer klar definierten Krisenmanagementstruktur mit eindeutigen Befehlsketten. Essentiell sind redundante Kommunikationsprotokolle, die auch bei einem totalen Ausfall der öffentlichen Mobilfunk- oder Datennetze (Blackout) funktionieren (9). Zudem verlangt Z3 konkrete prozessuale Maßnahmen zur Wirkungsminimierung (Containment) und Ressourcensteuerung, um zu verhindern, dass ein lokaler Vorfall auf das gesamte System übergreift. Die Etablierung einer 24-Stunden-Meldekette mit klaren Vertretungs- und Eskalationsmechanismen ist hier das zentrale operative Element (11).

Z4 – Fortführung und Wiederaufnahme (Business Continuity): Dieser Punkt verankert das Business Continuity Management (BCM) als gesetzliche Notwendigkeit. Kritische Prozesse müssen auch bei Teilausfällen fortgeführt werden können. Z4 verlangt detaillierte Wiederanlaufplanungen (Disaster Recovery Plans), die Definition akzeptabler Ausfallzeiten (Recovery Time Objectives, RTO) und die Vorhaltung technischer Redundanzen wie Notstromaggregate, Back-up-Leitstellen oder physischer Ersatzteile (9). Angesichts der komplexen Logistiknetze fordert Z4 auch die Etablierung alternativer Lieferketten, um die Supply Chain Resilienz zu gewährleisten (5).

Z5 – Personelle Sicherheitsvorkehrungen: Der Faktor Mensch wird sowohl als stärkste Verteidigungslinie als auch als maßgebliches Risiko identifiziert. Organisationen müssen kritische personelle Funktionen benennen und spezifische Zugangs- und Qualifikationsbenchmarks festlegen (9). Dies betrifft nicht nur das eigene Stammpersonal, sondern schließt externe Dienstleister, Wartungstechniker und Reinigungskräfte zwingend ein, da Lieferkettenangriffe durch kompromittiertes Fremdpersonal (Insider Threats) ein rasant wachsender Bedrohungsvektor sind. Z5 regelt auch die organisatorischen Vorbereitungen für die im RKEG vorgesehenen Zuverlässigkeitsüberprüfungen.

Z6 – Sensibilisierung und Schulung: Sämtliche technischen und prozessualen Investitionen der Stufen Z1 bis Z5 laufen ins Leere, wenn das Personal nicht entsprechend ausgebildet ist, um Alarme richtig zu interpretieren und Protokolle fehlerfrei auszuführen. Z6 verlangt fortlaufende Schulungen, regelmäßige

Krisenübungen (Stresstests) und die aktive Entwicklung einer sicherheitsbewussten Organisationskultur (Security Awareness) über alle Hierarchieebenen hinweg (13).

Spezifische Sicherheitsprotokolle und urbane Bedrohungsvektoren

Während die DSN-Leitfäden das strategische Fundament legen, erfordert die urbane Realität Wiens die Implementierung hochspezifischer, taktischer Sofortmaßnahmen für akute Bedrohungslagen.

Zuverlässigkeitsüberprüfungen gemäß § 16 RKEG

Die Zunahme von Insider-Bedrohungen, Industriespionage und Radikalisierungstendenzen zwingt Unternehmen, präventive Personalmaßnahmen zu ergreifen. Gemäß § 16 RKEG haben kritische Einrichtungen die Möglichkeit, das BMI offiziell um tiefgehende Zuverlässigkeitsüberprüfungen für internes und externes Personal zu ersuchen (4). Dies betrifft primär Personen, die unbegleiteten Zugang zu kritischen Infrastrukturen, hochsensiblen Informationen oder kritischen Steuerungssystemen (SCADA/ICS) haben.

Die behördliche Überprüfung ist umfassend: Sie inkludiert den Abgleich mit Strafregistern, die Prüfung von Waffenverboten und die Konsultation nachrichtendienstlicher Erkenntnisse über Verbindungen zu extremistischen oder terroristischen Gruppierungen. Die Kosten für diese Überprüfungen trägt die anfragende Einrichtung. Von zentraler juristischer Bedeutung ist, dass das BMI lediglich die aufbereiteten Daten liefert; die finale, arbeitsrechtliche Entscheidung über die Zuverlässigkeit einer Person und die Erteilung von Zugangsberechtigungen verbleibt bei der kritischen Einrichtung (9). Dies erfordert von den Human Resources- und Corporate Security-Abteilungen die Etablierung diskreter, revisionssicherer und datenschutzkonformer Bewertungsprozesse.

7.2. Operatives Protokoll bei Bombendrohungen

Intentionale Störungen, insbesondere anonyme Drohungen, erfordern ein Höchstmaß an standardisierter Reaktion, um Panik zu vermeiden und eine fundierte polizeiliche Gefahreneinschätzung zu ermöglichen. Im Falle einer telefonischen Bombendrohung muss das Empfangspersonal oder die Leitstelle strikte operative Protokolle befolgen. Der Anrufer darf keinesfalls unterbrochen oder provoziert werden. Stattdessen ist sofort ein Kollege per Handzeichen zu alarmieren, um parallel die Polizei über den Notruf 133 zu verständigen. Der annehmende Mitarbeiter muss umfassende Notizen anfertigen, die sich auf forensisch verwertbare Details konzentrieren: Dialekt, Stimmlage, Sprachrhythmus (z. B. abgelesen oder spontan), spezifische Hintergrundgeräusche (Straßenlärm, Maschinengeräusche) und die exakte Wortwahl. Diese Erstinformationen sind oft das einzige Puzzleteil, das entscheidet, ob eine Drohung als Scherzanruf klassifiziert wird oder ob eine sofortige Evakuierung der kritischen Anlage eingeleitet werden muss.

7.3. Asymmetrische Bedrohungen: Drohnenabwehr im urbanen Raum

Ein rasant wachsendes Risiko, das im RKEG zwar als organisatorische Schutzmaßnahme impliziert, aber nicht explizit in einem eigenen Paragraphen ausformuliert ist, stellt die asymmetrische Bedrohung durch

unbemannte Luftfahrzeuge (UAVs/Drohnen) dar (31). Die nationale Risikoanalyse identifiziert Drohnenangriffe ausdrücklich als konkrete, intentionale Bedrohung für kritische Infrastrukturen (24).

In Wien ist der Luftraum durch das permanente Flugbeschränkungsgebiet LO R 15 weitgehend reguliert. Ausnahmen gelten lediglich für Kleinstdrohnen unter 250 Gramm, die nicht höher als 30 Meter über Grund fliegen (32). Für alle anderen Flüge ist eine strenge Betriebsbewilligung der Austro Control erforderlich (32). Diese administrativen Hürden täuschen jedoch nicht darüber hinweg, dass böswillige Akteure sich nicht an Flugverbotszonen halten. Kritische Freiluftanlagen (wie Umspannwerke, chemische Lager oder Wasseraufbereitungsbecken) sind massiv durch Ausspähung oder den Abwurf von Spreng-/Brandmitteln gefährdet (32). Betreiber fordern daher dringend klare gesetzliche Vorgaben und praxistaugliche Abwehrtechnologien (32). Um diesem Risiko im Rahmen des Z2-Physischen Schutzes zu begegnen, müssen Einrichtungen den Einsatz von Multi-Sensor-Detektionssystemen (Radar, RF-Scanner, optische/thermische Kameras) in Betracht ziehen. Diese Command & Control-Systeme sind essenziell, um eine koordinierte und verzugslose Steuerung der Drohnenabwehr in enger Abstimmung mit der Polizei und dem Bundesheer (welche über die rechtliche Befugnis zur Neutralisation verfügen) sicherzustellen (32).

Kaskadierende Risiken und die Komplexität der Interdependenz

Die wahre Herausforderung der CER-Ära offenbart sich nicht auf der Ebene isolierter Unternehmensprozesse, sondern in der enormen Komplexität interagierender Systeme (Critical Infrastructure Interdependency) (15). Wissenschaftliche Untersuchungen im Bereich des Systems Engineering belegen eindrücklich, dass kritische Infrastrukturen keine isolierten Anlagen sind, sondern ein eng verwobenes sozio-technisches Netz bilden (15). Der Ausfall eines scheinbar isolierten Subsystems – beispielsweise ein lokaler Telekommunikationsknoten – führt zu sofortigen kaskadierenden Ausfällen (Cascading Failures) über geografische, physische und organisatorische Grenzen hinweg und beeinträchtigt unweigerlich die Sektoren Verkehr, Energie und Gesundheit (15). In solchen Umgebungen ist die Wiederherstellung nach einem Vorfall (Post-Incident Recovery) niemals eine einfache, lineare Checklisten-Übung. Eine Isolationsentscheidung, die für ein Subsystem (z.B. Abschaltung eines IT-Netzes zur Eindämmung von Malware) getroffen wird, kann die Verfügbarkeit eines anderen Systems (z.B. Fernsteuerung von Wasserpumpen) drastisch verringern, operative Sicherheitsbeschränkungen verletzen oder die Wiederherstellung einer für die Öffentlichkeit wesentlich wichtigeren Dienstleistung verzögern (15). Die Wissenschaft spricht hierbei von der Notwendigkeit einer Transition vom bloßen "Robust Design" (Mauern bauen) hin zu einem echten "Resilience Design", das sich auf Vorbereitung, schnelle Reaktion und agile Wiederherstellung konzentriert (25). Eine Infrastruktur gilt heute nur dann als resilient, wenn sie die Fähigkeit besitzt, (i) sich Bedrohungen vorzustellen (imagine), (ii) ihnen zu widerstehen (protect), (iii) die negativen Effekte zu absorbieren (absorb) und (iv) sich an neue Bedingungen anzupassen (adapt) (25).

Dieser akademische Diskurs hat massive praktische Relevanz für die Erstellung der Risikoanalysen und Resilienzpläne nach RKEG, da Betreiber explizit grenz- und sektorübergreifende Abhängigkeiten nachweisen müssen.

1. Aufsicht, Unterstützung und Durchsetzung: "Dialog statt Strafen"

Die Implementierung des RKEG in die unternehmerische Praxis wird durch ein duales System der Behörden gesteuert, das auf einer Balance zwischen kooperativer Unterstützung und stringenter Sanktionierung beruht. Das Bundesministerium für Inneres (BMI) agiert hierbei als primäre Aufsichts- und Durchsetzungsbehörde (5).

Behördliche Unterstützung: Um die immense administrative und konzeptionelle Last, die insbesondere auf mittelständische Betreiber zukommt, abzufedern, bietet das BMI weitreichenden Support an. Die primäre regulatorische Haltung der Behörde folgt dem Paradigma "Dialog statt Strafen!". Zu den Unterstützungsleistungen zählen die Bereitstellung der erwähnten DSN-Leitfäden ("Soft Law"), standardisierte Templates für Risikoberichte, Schulungsmodule zur Sensibilisierung sowie ein staatliches Frühwarnsystem für geopolitische oder physische Bedrohungslagen (35). Ziel ist es, Unternehmen zu befähigen, ihre Widerstandsfähigkeit proaktiv und organisch zu steigern, anstatt sie durch reine Compliance-Bürokratie zu lähmen.

Aufsicht und Audits: Trotz dieses kooperativen Ansatzes stattet der Gesetzgeber das BMI mit weitreichenden und robusten Durchsetzungsbefugnissen aus. Die Behörde kann jederzeit und ohne besonderen Verdacht die Vorlage der aktuellen Risikoanalysen und Resilienzpläne verlangen (5). Zudem ist sie berechtigt, unangekündigte Vor-Ort-Kontrollen durchzuführen, um die physischen Maßnahmen (Z1 und Z2) in der Realität zu überprüfen (5). Bei festgestellten Mängeln ordnet die Behörde per Bescheid die Behebung binnen einer fixen Frist an (5). Um die Qualität der Maßnahmen zu verifizieren, kann das BMI formelle Audits durch zertifizierte, unabhängige "Resilienzauditoren" anordnen, deren Kosten vollständig von der kritischen Einrichtung zu tragen sind (4).

Sanktionen: Wenn der kooperative Pfad von Seiten der Betreiber verweigert wird, grobe Fahrlässigkeit vorliegt oder gesetzliche Vorgaben beharrlich ignoriert werden, greift ein scharfes Sanktionsregime. Das RKEG sieht empfindliche Verwaltungsstrafen vor, die eine massive abschreckende Wirkung entfalten sollen:

Bis zu 50.000 Euro drohen bei formalen Pflichtverletzungen oder administrativen Versäumnissen, wie beispielsweise der unterlassenen oder verspäteten Durchführung einer Risikoanalyse, der unzureichenden Dokumentation von Maßnahmen oder der verspäteten Benennung der Kontaktstellen (5). Bis zu 500.000 Euro können bei schwerwiegenden, existenziellen Verstößen verhängt werden. Hierzu zählen die völlige Nicht-Umsetzung behördlich angeordneter physischer und baulicher Schutzmaßnahmen, die hartnäckige Ignoranz von Bescheiden oder die grobe Verletzung der unverzüglichen 24-Stunden-Meldepflicht bei kritischen Sicherheitsvorfällen (5). Für öffentliche Stellen droht neben den finanziellen Konsequenzen zudem die öffentliche Bekanntmachung (Naming and Shaming) der Nichteinhaltung, was mit einem massiven Reputationsverlust einhergeht (5).

Dieses Pönal-Niveau stellt endgültig sicher, dass das Thema Resilienz keine nachrangige, delegierbare operative Aufgabe für mittlere Managementebenen bleibt, sondern direkt auf Vorstandsebene (C-Level) als zentraler Bestandteil der Corporate Governance verantwortet werden muss (4).

Technologische Bewältigung der CER-Ära: Die IRIS-Plattform

Die regulatorische Wucht des RKEG und die unbedingte Forderung, kaskadierende Interdependenzen nach dem All-Gefahren-Ansatz zu bewerten, stellen Betreiber vor nahezu unlösbare manuelle Herausforderungen. Der Versuch, die hochkomplexen Wechselwirkungen zwischen physischer Sicherheit, Cybersecurity, Personalverfügbarkeit und globalen Lieferketten mit traditionellen, isolierten (siloed) Softwarelösungen oder gar statischen Tabellenkalkulationen zu modellieren, ist zum Scheitern verurteilt. Solche fragmentierten Herangehensweisen sind nicht nur ineffizient, sondern hinterlassen gefährliche blinde Flecken, die im Ernstfall zu den gefürchteten Kaskadeneffekten führen.

Wissenschaftliche Analysen zur IT-Sicherheit und Systemresilienz zeigen, dass der Einsatz von Artificial Intelligence (AI) und Large Language Models (LLMs) einen Paradigmenwechsel in der Risikobewertung ermöglicht. Architekturen wie Retrieval-Augmented Generation (RAG) und Multi-Agenten-Systeme sind prädestiniert dafür, riesige Mengen heterogener Daten zu klassifizieren, komplexe Abhängigkeiten zu erkennen und mehrstufige Krisenpläne in Echtzeit zu generieren (15).

An dieser technologischen Schnittstelle setzt die Nexus Group AI mit der Entwicklung von IRIS (All-Hazard Risk Intelligence Platform) an. Das System adressiert präzise die administrativen und analytischen Engpässe, die durch die RKEG-Pflichten entstehen, und transformiert isolierte Datenpunkte in ganzheitliche, entscheidungsorientierte Resilienzstrategien (36).

IRIS bietet drei entscheidende Kernfunktionen für Betreiber kritischer Infrastrukturen:

Automated Intelligence: Die Plattform aggregiert und quantifiziert hochvolumige, unstrukturierte Datenströme – insbesondere aus Open-Source Intelligence (OSINT) sowie von physischen und digitalen Sensoren – in strukturierte, entscheidungsrelevante Metriken. Bedrohungen wie lokale Extremwetterwarnungen, geopolitische Spannungen in Zulieferermärkten oder aufkommende Cyberkampagnen werden in Echtzeit analysiert und in die Unternehmensrisikomatrix eingespeist. **Unified Vision:** IRIS liefert ein "Single Pane of Glass" – eine einheitliche, hochgradig visuelle Echtzeit-Übersicht, die speziell für C-Level-Führungskräfte und Krisenmanager konzipiert ist. Die Plattform durchbricht historische Silos und verschmilzt digitale Cyber-Risikodaten nahtlos mit physischen Sensordaten. So wird beispielsweise sofort ersichtlich, wenn ein Cyberangriff auf ein Zutrittskontrollsystem (digital) die physische Integrität einer Wasseraufbereitungsanlage (physisch) gefährdet. **Measurable Impact:** Die messbaren operativen Effekte einer solchen KI-gestützten Resilienzplattform sind signifikant. Indem IRIS verborgene Interdependenzen und Kaskadeneffekte automatisiert aufdeckt und modelliert, können Betreiber ihre Planungsfehler bei Z4-Wiederanlaufplänen um nachweislich 30 % reduzieren. Im akuten Krisenfall ermöglicht die automatisierte Triage und die sofortige Zuordnung von Z3-Reaktionsmaßnahmen eine 80 % schnellere Incident-Response-Rate. Dies ist der entscheidende Faktor, um die strikte 24-Stunden-Meldepflicht an das BMI rechtssicher und inhaltlich fundiert zu erfüllen.

Der Einsatz moderner Risiko-Intelligenz-Systeme wie IRIS erlaubt es Betreibern, den Fokus von der reinen, ressourcenfressenden formularbasierten Compliance hin zu einer echten, prädiktiven und dynamischen Resilienzsteuerung zu verschieben.

Fazit und strategischer Ausblick

Die vollständige Implementierung der CER-Richtlinie durch das Resilienz kritischer Einrichtungen-Gesetz (RKEG) und die zugehörige Verordnung (RKEV) leitet eine neue sicherheitspolitische Epoche in der Republik Österreich ein. Der unumkehrbare Übergang von freiwilliger Kooperation hin zu einem

sanktionsbewehrten Pflichtenregime reflektiert das massiv gestiegene Risikobewusstsein des Gesetzgebers. Angesichts hybrider Bedrohungen, geopolitischer Instabilitäten, extremer Wetterereignisse und hochkomplexer, globaler Lieferketten ist die Resilienz der Daseinsvorsorge zu einer Frage der nationalen Sicherheit avanciert.

Für Vorstände und Geschäftsführungen kritischer Infrastrukturen bedeutet dies einen radikalen Perspektivenwechsel: Physische und organisatorische Resilienz darf nicht länger als unproduktiver Kostenfaktor (Cost Center) betrachtet werden, sondern muss als integraler Bestandteil der Corporate Governance und als strategischer Wettbewerbs- und Überlebensvorteil verstanden werden. Die Pflicht zur Erstellung tiefgreifender Risikoanalysen innerhalb von neun Monaten und die Implementierung umfassender Resilienzpläne (Z1–Z6) innerhalb von zehn Monaten nach Erhalt des Bescheids setzt Organisationen unter immensen administrativen und operativen Zeitdruck.

Die wahre Bewährungsprobe liegt jedoch in der Vermeidung von Kaskadeneffekten. Metropolregionen wie Wien zeigen exemplarisch, wie stark vernetzt die Lebensadern einer modernen Gesellschaft sind. Das nahtlose Ineinandergreifen von Energieversorgern (Wiener Netze), Wasserwerken (MA 31) und Blaulichtorganisationen (MA 68) im Krisenfall verzeiht keine konzeptionellen Fehler oder isolierten Silodenkweisen. Um den Stresstest der neuen CER-Ära zu bestehen, bedarf es weit mehr als nur der Abarbeitung behördlicher Checklisten. Es erfordert einen tiefgreifenden kulturellen Wandel in der Belegschaft, die Harmonisierung von physischer (RKEG) und digitaler (NISG 2026) Sicherheit in integrierten Managementsystemen und den zwingenden Einsatz modernster KI-gestützter Analysetechnologien, um verborgene systemische Abhängigkeiten beherrschbar zu machen. Nur durch diesen ganzheitlichen Ansatz kann die Widerstandsfähigkeit der kritischen Infrastrukturen kontinuierlich und agil an ein sich rapide wandelndes globales Risikobild angepasst werden.

Quellenverzeichnis

1. Rechts- und Technologiedialog: Resilienz kritischer Einrichtungen, <https://kompetenzzentrum-sicheres-oesterreich.at/2026/07/21/rechts-und-technologiedialog-resilienz-kritischer-einrichtungen-gesetz/>
2. Resilienz kritischer Einrichtungen-Gesetz (RKEG) - WKO, <https://www.wko.at/noe/wirtschaft/resilienz-kritischer-einrichtungen-gesetz-rkeg-richtlinie>
3. richtlinie (eu) 2022/2557 des europäischen parlaments und des rates, <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2557>
4. RKEG im Überblick » Resilienz kritischer Einrichtungen - EY, https://www.ey.com/de_at/insights/cybersecurity/rkeg
5. RKEG 2026 Österreich: Umsetzung & Audit - Devoteam, <https://www.devoteam.com/at/rke-resilienz-kritischer-einrichtungen-oesterreich/>
6. Bundesheer - Aktuell - Risikobild 2026 präsentiert, <https://www.bmlv.gv.at/cms/artikel.php?ID=12167>
7. Directive 2022/2557 on the resilience of critical entities – Policies - IEA, <https://www.iea.org/policies/26916-directive-20222557-on-the-resilience-of-critical-entities>
8. Critical Entities Resilience Directive – What It Brings And How To, <https://www.deloitte.com/cz-sk/en/services/consulting/services/critical-entity-resilience-directive-cer.html>
9. RKEG in Österreich - KPMG International, <https://kpmg.com/at/de/insights/2026/08/rkeg-in-oesterreich.html>
10. Umsetzung der Risikoanalyse anhand RKEG - BC Consulting, <https://www.bc-consulting.at/umsetzung-der-risikoanalyse-anhand-rkeg/>

11. Österreich: Das RKEG und die RKEV im Reality-Check, <https://www.schoenherr.eu/content/oesterreich-das-rkeg-und-die-rkev-im-reality-check-pflichten-systematik-und-abgrenzung-zum-nisg-2026>
12. Bis zu 600 kritische Anlagen in Österreich erhalten nun Schutz, https://www.meinbezirk.at/c-lokales/bis-zu-600-kritische-anlagen-in-oesterreich-erhalten-nun-schutz_a8587600
13. CER-Richtlinie » Resilienz kritischer Infrastruktur erklärt, <https://positionen.wienerstadtwerke.at/wissenshub/einfach-erklaert/resilienz-kritischer-einrichtungen>
14. BERATUNG RKE Richtlinie RKE-G - Gesetz zur Resilienz kritischer, <https://www.neukamp.at/rke-richtlinie-rkeg-gesetz-zur-resilienz-kritischer-einrichtungen-beratung/>
15. Large Language Models for Recovery Plan Generation in Internet, <https://www.mdpi.com/1999-5903/18/6/295>
16. A Systematic Review of Smart City Infrastructure Threat Modelling, <https://www.mdpi.com/2071-1050/14/16/10368>
17. Blackout Vorsorge Wien » Das tut die Wiener Stadtwerke Gruppe, <https://positionen.wienerstadtwerke.at/aktuelles/resilienz-kritischer-infrastruktur-die-wiener-stadtwerke-im-blackout-szenario>
18. MA 31 - Wiener Wasser - ÖGL, <https://www.grabenlos.at/de/experten-der-oegl/betriebe/ma-31-wiener-wasser.html>
19. Berufsfeuerwehr Wien - Wikipedia, https://de.wikipedia.org/wiki/Berufsfeuerwehr_Wien
20. Magistratsabteilung 68 - Feuerwehr und Katastrophenschutz, <https://www.wien.gv.at/spezial/leistungsberichte/leistungsberichte-der-magistratsdienststellen/magistratsabteilung-68-feuerwehr-und-katastrophenschutz/>
21. Digitale Souveränität Europas » Relevanz für kritische Infrastruktur, <https://positionen.wienerstadtwerke.at/aktuelles/digitale-souveraenitaet-gastbeitrag>
22. Digitale Souveränität - Wiener Stadtwerke Positionen, <https://positionen.wienerstadtwerke.at/positionen/weitere/digitale-souveraenitaet-resiliente-infrastruktur>
23. Umlaufbeschluss vom 17. Jänner 2026 - Bundeskanzleramt Österreich, <https://www.bundeskanzleramt.gv.at/medien/ministerraete/ministerraete-seit-maerz-2025/37a-mr-17-jan.html>
24. Nationale Risikoanalysen EU CER 2022/2557 - OpenKRITIS, <https://www.openkritis.de/eu/eu-rce-risikoanalyse.html>
25. (PDF) The Resilience of Critical Infrastructure Systems: A Systematic, https://www.researchgate.net/publication/350032338_The_Resilience_of_Critical_Infrastructure_Systems_A_Systematic_Literature_Review
26. The Resilience of Critical Infrastructure Systems: A Systematic, <https://www.mdpi.com/1996-1073/14/6/1571>
27. ONR 49001 - Die österreichische Risikomanagement-Norm, https://www.risikomanagement-wissen.de/risikomanagement/risikomanagement-einfuehrung/onr_49001/
28. ÖNORM D4900 – Risikomanagement für Organisationen und Systeme, <https://fhburgenland.contentdm.oclc.org/digital/api/collection/p15425dc/id/229954/download>
29. RKEG) erlassen und das Tilgungsgesetz 1972 geändert wird - RIS, https://ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2025_I_60/BGBLA_2025_I_60.html
30. Resilienz kritischer Einrichtungen-Gesetz (RKEG) - ÖWAV, <https://www.oewav.at/Page.aspx?target=601706&>
31. Nationalrat stimmt Umsetzung von EU-Richtlinie zum Schutz, https://www.parlament.gv.at/aktuelles/pk/jahr_2025/pk0790
32. Drohnensicherheit für kritische Infrastruktur » Risiken & Lösungen, <https://positionen.wienerstadtwerke.at/positionen/weitere/drohnensicherheit>
33. roelich.pdf - Open Research Online, <https://oro.open.ac.uk/41476/8/roelich.pdf>

- 34. Risk Analysis of Infrastructure Networks in response to extreme, <https://cordis.europa.eu/project/id/608166/reporting>
- 35. Resilienz kritischer Einrichtungen-Gesetz – RKEG; Tilgungsgesetz, <https://www.parlament.gv.at/gegenstand/XXVIII/I/186>
- 36. AI Risk Intelligence Systems | AI Governance, <https://therisk.global/ai-risk-intelligence-systems/>

STAY RESILIENT

