Richtlinie zur Resilienz Kritischer Einrichtungen (RKE)

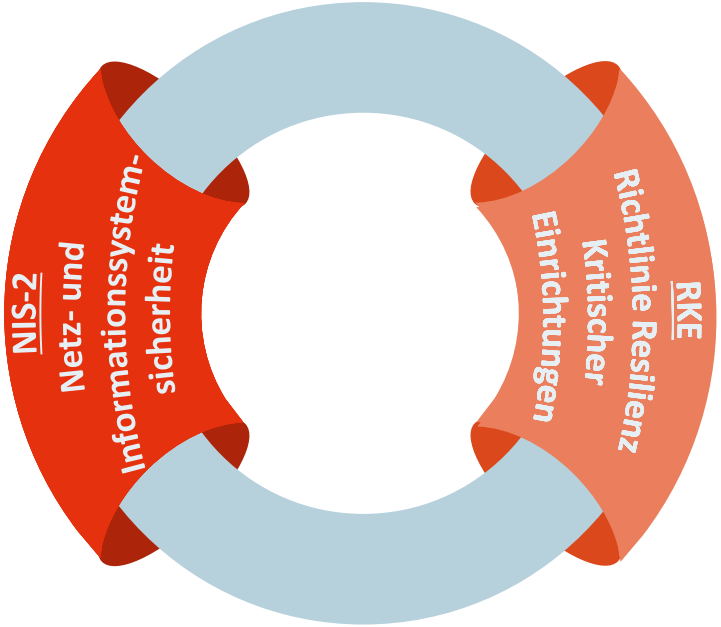
Krisenresilienz und Sicherheit für Unternehmen

St. Pölten, 29. Mai 2024
Direktion Staatsschutz und Nachrichtendienst
Mag. Markus Müller

Hintergrund

NIS-2-Richtlinie

- Im Dezember 2020 von EU-Kommission vorgestellt
- Zusätzliche Aufgaben für das BMI
- Steigende Anforderungen an Strukturen, Prozesse, Kooperation und (Risiko)Management
- Umsetzung wird aktuelles NIS-Gesetz (NISG) ersetzen



RKE-Richtlinie

- Im Dezember 2020 von EU-Kommission vorgestellt
- Ersetzt auf EU-Ebene die Richtlinie zum Schutz kritischer Infrastruktur (EPCIP / (EU) RL 2008/114)
- Umsetzung wird in Österreich APCIP komplementieren
- Umsetzung in nationales Recht bis Oktober 2024

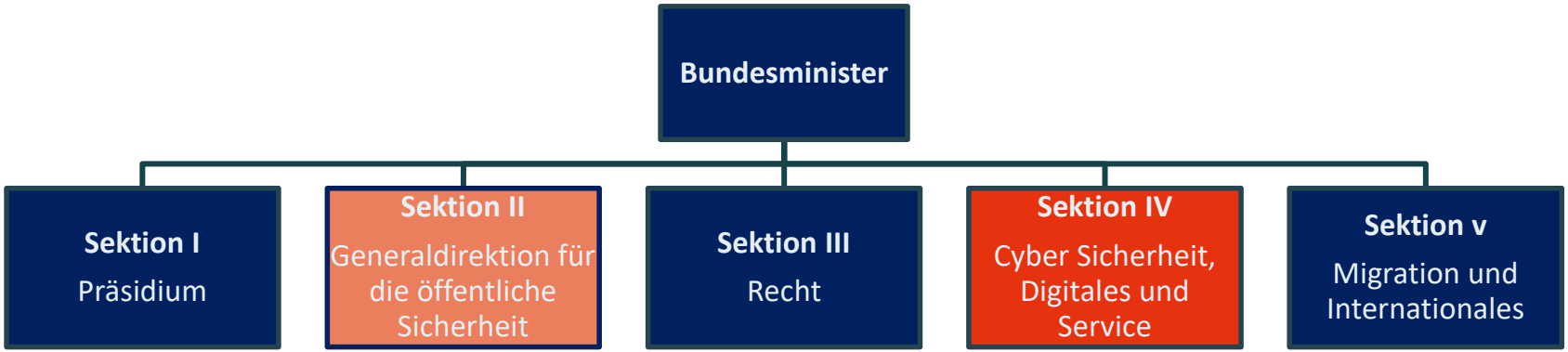
Warum RKE?

- Maßnahmenpaket zur Steigerung der physischen Sicherheit bei „kritischen Einrichtungen“
- Festlegung einer Mindestharmonisierung durch Verpflichtungen und kohärente und gezielte Unterstützungs- und Aufsichtsmaßnahmen
- Ziel: Erhöhung der Widerstandsfähigkeit („Resilienz“) von Einrichtungen, die essenzielle gesellschaftliche Funktionen oder wirtschaftliche Tätigkeiten erbringen
- Verfolgung von „All-Gefahren-Ansatz“ = Berücksichtigung sämtlicher Gefahrenarten egal, ob natürlich oder vom Menschen verursacht

Zuständige Behörde

RKE: BMI II/Direktion Staatsschutz und Nachrichtendienst

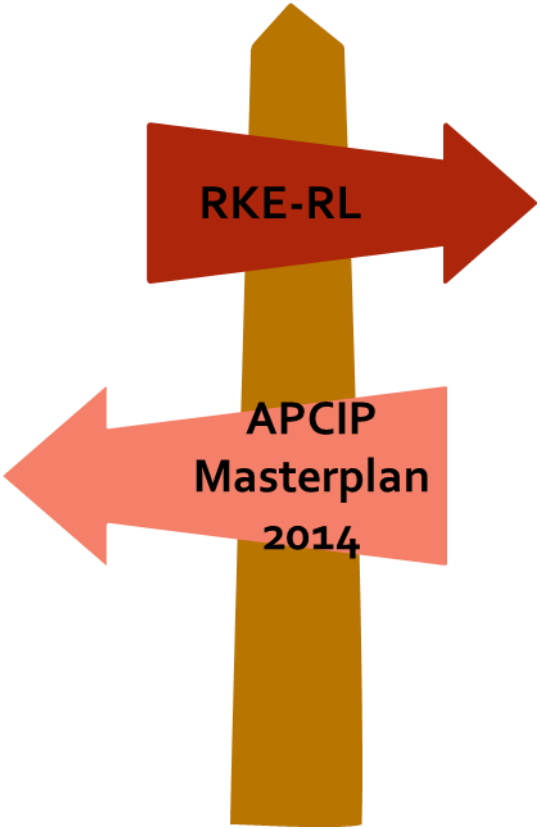
NIS-2: BMI IV/Nationales Cybersicherheitszentrum



Paradigmenwechsel

Bisher: Private Public Partnership

zu einer erhöhten Resilienz und damit zu Schutzstandards durch Eigentümer und Betreiber von strategischen Unternehmen



Künftig: behördlich/ regulatives Umfeld mit Verpflichtungen für Unternehmen

Im Gegensatz zu APCIP werden mit RKE Verpflichtungen für kritische Einrichtungen festgelegt.

Verpflichtungen für kritische Einrichtungen, um Resilienz & Fähigkeit zur Erbringung von wesentlichen Diensten zu verbessern, v.a. bezüglich physischer Sicherheit, Security-Management, Durchführung von Risikoanalysen.

Verpflichtet Mitgliedstaaten, Maßnahmen zu ergreifen, um Erbringung von Diensten, die zur Aufrechterhaltung wichtiger gesellschaftlicher Funktionen & wirtschaftlicher Tätigkeiten nötig sind, zu gewährleisten.

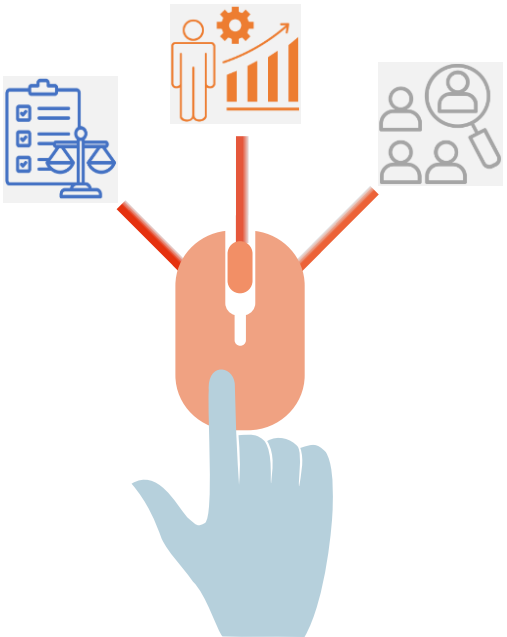
Behördliche Verpflichtungen

- Art 4 – Strategie
  - strategische Ziele und Prioritäten zur Verbesserung der Gesamtresilienz kritischer Einrichtungen
- Art 5 – Risikobewertung
  - gesamter Prozess zur Bestimmung der Art und des Ausmaßes eines Risikos
  - Berücksichtigung entsprechender Risiken (All-Gefahren-Ansatz)
- Art 6 – Ermittlung Kritischer Einrichtungen
  - Feststellung mittels Bescheid
- Art 10 – Unterstützungsmaßnahmen
  - Entwicklung von Leitfäden und Methoden, Organisation von Übungen, Bereitstellung von Beratung und Schulungen für Personal, etc.

Häufigste Fragen

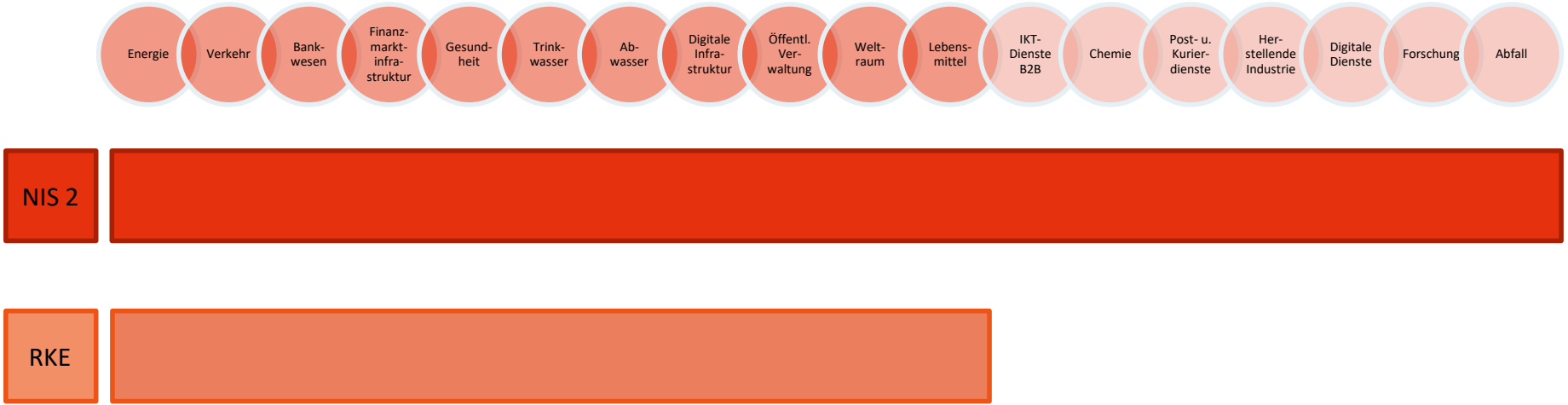
Wer?
Welche Unternehmen fallen unter das RKE-Regime?

Was?
Welche Maßnahmen sind zu ergreifen?



Wann?
Ab wann beginnen die Verpflichtungen zu laufen?

Betroffene Unternehmen - Sektoren



Betroffene Unternehmen – Anwendungsbereich

- Vier **kumulative** Voraussetzungen müssen Vorliegen
  1. Unternehmen ist im Inland tätig
  2. Die kritische Infrastruktur des Unternehmens befindet sich im Inland
  3. Es wird zumindest ein wesentlicher Dienst erbracht
  4. Ein Sicherheitsvorfall könnte eine erhebliche Störung bei dem wesentlichen Dienst oder bei anderen wesentlichen Diensten, die von der Einrichtung abhängig sind, bewirken
- Wann eine Störung erheblich ist, wird vom BMI mittels Verordnung für jeden (Teil-)Sektor näher konkretisiert
- Besonderes Regime für den Sektor öffentliche Verwaltung
- **Bescheidmäßige Feststellung**

Betroffene Unternehmen – Schwellenwerte

- Erwägungsgrund 18:
  - *„Es sollen Kriterien festgelegt werden, um das Ausmaß einer durch einen Sicherheitsvorfall verursachten Störung zu bestimmen. Diese Kriterien sollten sich an den in der* ***Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates (NIS RL)*** *festgelegten Kriterien orientieren, um die Anstrengungen der Mitgliedstaaten zur Ermittlung der Betreiber wesentlicher Dienste im Sinne jener Richtlinie und die diesbezüglich gewonnen Erfahrungen zu nutzen.“*

Betroffene Unternehmen – Schwellenwerte

Sektor	NIS-1	RKE
Energie	✓	✓
Verkehr	✓	✓
Bankwesen	✓	✓
Finanzmarkt Infr.	✓	✓
Gesundheit	✓	✓
Trinkwasser	✓	✓
Abwasser		✓
Digitale Infr.	✓	✓
Öffentliche Verw.		✓
Weltraum		✓
Lebensmittel		✓

Betroffene Unternehmen – Schwellenwerte

- Werden analog NIS-1 Umsetzung in Branchengesprächen erarbeitet
  - Neue Systematik
  - 7 Sektoren aus NIS-G/ NIS-VO müssen adaptiert werden
  - 4 „neue“ Sektoren müssen erarbeitet werden
- Gespräche finden mit Interessenvertretungen und Unternehmen statt
- Schwellenwerte werden mittels Verordnung des Bundesministers kundgemacht
- Start: Q2 2024

Betroffene Unternehmen – Vergleichswerte

- APCIP/ 12 Sektoren
  - Nationale Unternehmen KAT A: ~150
  - Nationale Unternehmen KAT B: ~150
  - Regionale Unternehmen gesamt: ~130
- NIS-1/ 7 Sektoren
  - Betreiber wesentlicher Dienste: ~100

- RKE (Einschätzung)
  - Kritische Einrichtungen: ~ 300 - 600

Zeitlicher Ablauf – „Behördenseite“

Zeitlicher Ablauf – „Unternehmerseite“

Verpflichtungen der kritischen Einrichtungen

- Risikobewertung
- Resilienzmaßnahmen
  - Auf Grundlage der Risikobewertungen (Behörde+KE)
  - geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen
  - Verordnungsermächtigung BMI
- Zuverlässigkeitsüberprüfungen
  - Personen in sensibler Funktion; Zugriff auf sicherheitsrelevante Informationen
- Meldung von Sicherheitsvorfällen
  - Unverzüglich, längstens binnen 24 Stunden

Prüf- und Sanktionsregime

- Risikobewertung und Resilienzplan müssen proaktiv übersendet werden
- BMI kann Nachweis für die Erfüllung der Verpflichtungen verlangen
- Befugnisse
  - Anordnung von Audits durch „Qualifizierte Stellen“
  - Vor-Ort Kontrollen (nach vorheriger Ankündigung)
- Unternehmen haben Kooperationspflicht
- Bei Nichterfüllung der Verpflichtungen Anordnung durch Bescheid
- In letzter Konsequenz: Verwaltungsstrafe
  - Bis zu 7 Mio Euro, oder
  - Bis zu 1,4 % des weltweiten Gesamtnettojahresumsatzes des Vorjahrs
- **Maxime ist Dialog statt Strafen**

Vielen Dank für Ihre Aufmerksamkeit!

St. Pölten, 29. Mai 2024
Direktion Staatsschutz und Nachrichtendienst
Mag. Markus Müller