Cybersicherheit und Verwaltung: Schutz kritischer Verkehrsinfrastrukturen im Rahmen der NIS-2-Richtlinie

Eleonóra Wagenknecht

Panel 3:
Digitalisierung und künstliche Intelligenz im Straßenverkehr
KI und Cybersicherheit

ZVR Verkehrsrechtstag 2024

03.10.2024
WU Wien

SIGMUND FREUD
PRIVATUNIVERSITÄT
WIEN

Überblick

1. Cyberangriff auf kritische Verkehrsinfrastruktur
2. Zuständige Behörden
3. Einordnung und Rechtsschutz
4. Computer-Notfallteams
5. Schlussfolgerungen

1. Cyberangriff auf kritische Verkehrsinfrastruktur

Hackerangriff

ZEIT ONLINE

Hacker greifen Deutsche Flugsicherung an (Zeit, 01.09.2024)

SIGMUND FREUD PRIVATUNIVERSITÄT WIEN

Verkehrsinfrastrukturen als kritische Infrastruktur

- Eisenbahnnetz
- Hochrangiges Straßennetz
- Flughäfen
- Verkehrsleitzentralen
- ….

Spannungsverhältnis

- Notwendigkeit der Einsatzbereitschaft gegenüber Angriffen auf kritische Verkehrsinfrastruktur
- Hohe finanzielle Belastung für Unternehmen
- Wahl eines verhältnismäßigen Regulierungsansatz
- Möglichkeiten und Grenzen der beteiligten Behörden
- Staatliche Überwachung von Unternehmen

Behördliche Perspektive

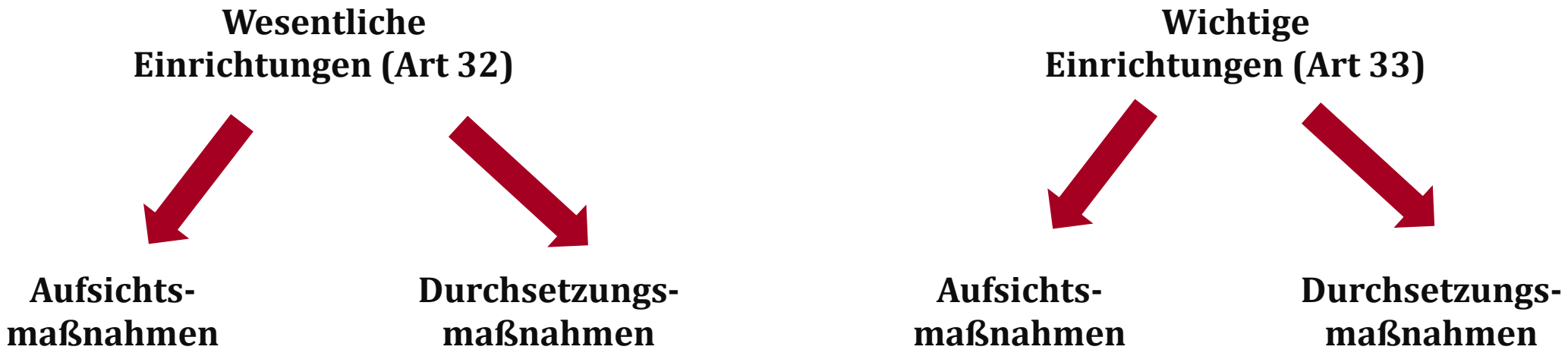
- Entwicklungsperspektiven von NIS 1 zu NIS 2
- Möglichkeiten und Grenzen der Behörden
- Herausforderungen der Behörden
- Behörden und andere Akteure

2. Zuständige Behörden

Zuständige Behörde – NIS-2-RL

NIS-2-RL	Gesetzesentwurf – NISG-Novelle
Art 31: Allgemeine Aspekte der Aufsicht und Durchsetzung • MS können der zuständigen Behörde gestatten, Aufsichtsaufgaben zu priorisieren (risikobasierter Ansatz)	**§ 4: Cybersicherheitsbehörde** • **Bundesminister für Inneres**
Art 32: Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen	**§ 38: Aufsichtsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen**
Art 33: Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen	**§ 39: Durchsetzungsmaßnahmen in Bezug auf wesentliche und wichtige Einrichtungen**

Zuständige Behörde – Aufsichtsmaßnahmen und Durchsetzungsmaßnahmen



Hoheitliche Maßnahmen - Aufsichtsmaßnahmen

Art 32 NIS-2-RL: Wesentliche Einrichtungen

- **Vor-Ort-Kontrollen** und externe Aufsichtsmaßnahmen
- Regelmäßige und gezielte **Sicherheitsprüfungen**
- **Ad-hoc-Prüfungen**
- **Sicherheitsscans**
- Anforderung von **Informationen** zur Bewertung von Risikomanagementmaßnahmen
- Anforderung des **Zugangs zu Daten**
- Anforderung von **Nachweisen** für die Umsetzung der Cybersicherheitskonzepte

Hoheitliche Maßnahmen - Aufsichtsmaßnahmen

Art 33 NIS-2-RL: Wichtige Einrichtungen

- **Vor-Ort-Kontrollen** und externe **nachträgliche** Aufsichtsmaßnahmen
- ~~regelmäßige und~~ gezielte **Sicherheitsprüfungen**
- ~~**Ad-hoc-Prüfungen**~~
- **Sicherheitsscans**
- Anforderung von **Informationen** zur **nachträglichen** Bewertung von Risikomanagementmaßnahmen
- Anforderung des **Zugangs zu Daten**
- Anforderung von **Nachweisen** für die Umsetzung der Cybersicherheitskonzepte

Hoheitliche Maßnahmen - Durchsetzungsmaßnahmen

Art 32 / 33 / 34 NIS-2-RL

- **Warnungen** über Verstöße gegen diese RL
- **Anweisungen**…
  - ein bestimmtes Verhalten einzustellen,
  - Risikomanagementmaßnahmen zu erfüllen,
  - die im Rahmen der Sicherheitsüberprüfung formulierten Empfehlungen umzusetzen
  - Verstöße öffentlich bekannt zu machen,…
- **Geldbußen**

Hoheitliche Maßnahmen – Ultima Ratio

Art 32 Abs 5 NIS-2-RL: Ultima Ratio bei Wesentlichen Einrichtungen

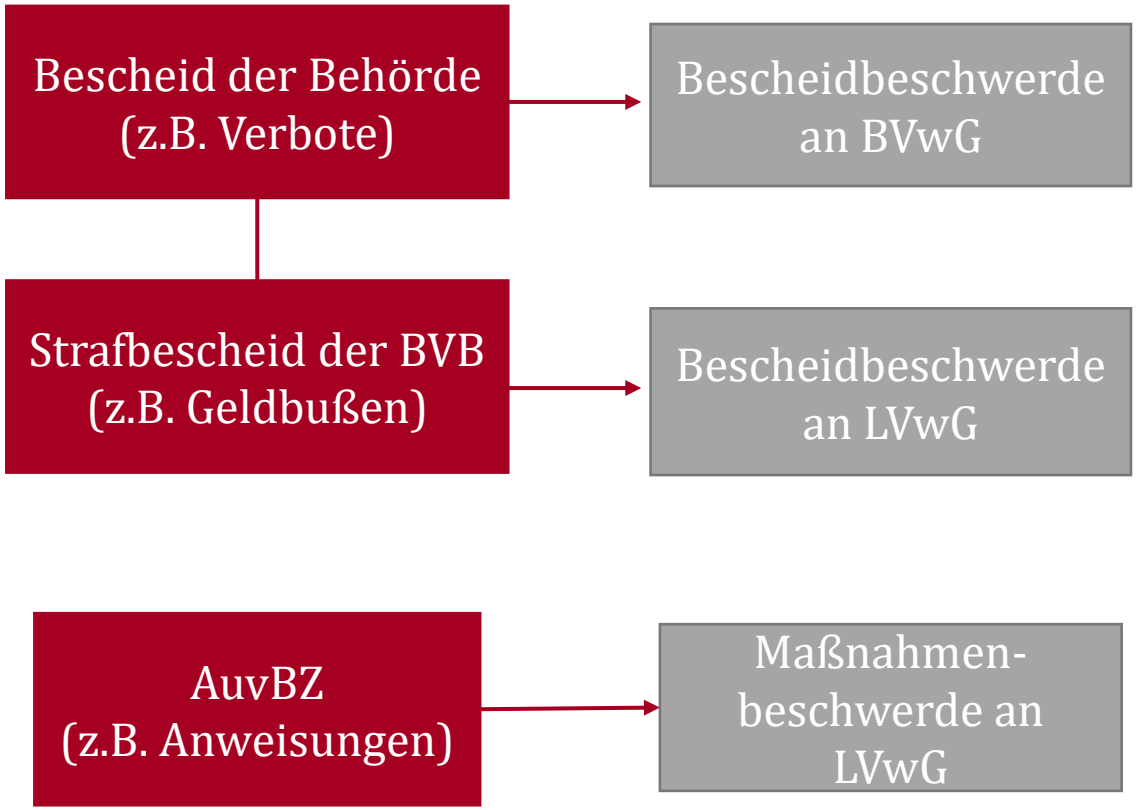
unwirksam

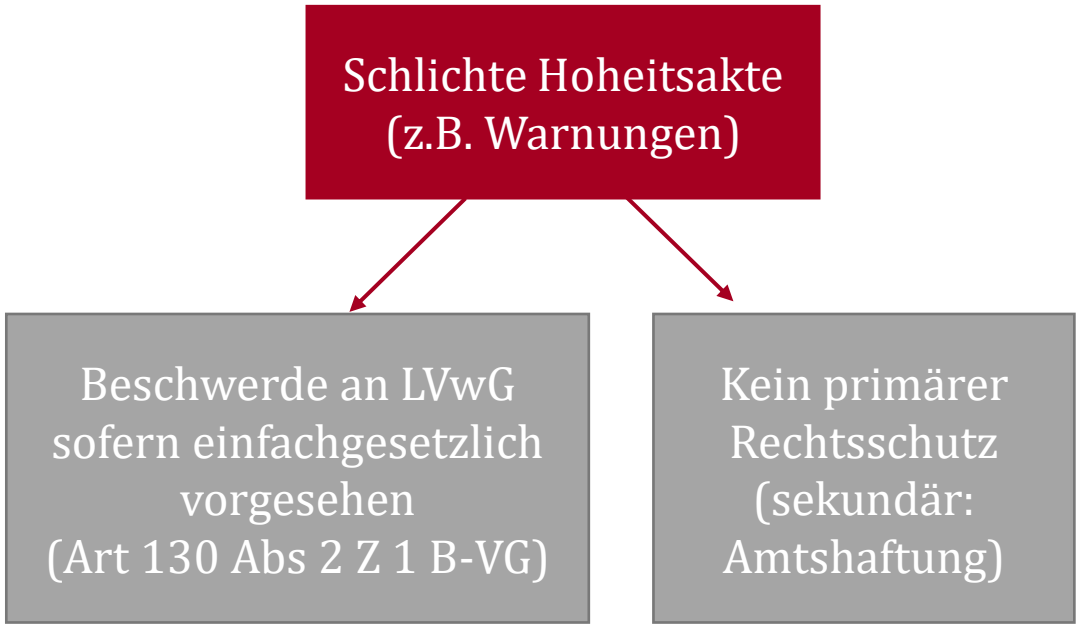
Vorübergehend:

- Zertifizierung oder Genehmigung für (Teile der) Dienste oder Tätigkeiten aussetzen
- Natürlichen Personen, die Leitungsaufgaben wahrnehmen, diese untersagen

3. Einordnung und Rechtsschutz

Rechtsschutz – Hoheitliche Maßnahmen

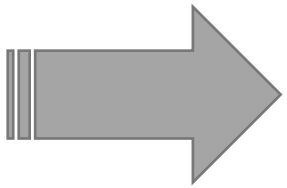




Einordnung – Verwaltungspolizei

Verwaltungspolizei ist die Abwehr von materienspezifischen Gefahren.

→ (zB Baupolizei, Verkehrspolizei, …)



„Cybersicherheitspolizei“

Cybersicherheitspolizei ist die **Abwehr von Gefahren** für die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten oder Diensten im Rahmen von **Netz- und Informationssystemen.**

Rechtsschutz – Schlichthoheitliches Handeln

„Cybersicherheitspolizei“

Kein Rechtsschutz gegen **schlichthoheitliches Handeln** gegenüber der Verwaltungspolizei/Cybersicherheitspolizei.

- **außer** eigenständige gesetzliche Grundlage
- im NISG aktuell **nicht** vorhanden!

Rechtsschutzdefizit – Schlichthoheitliches Handeln

➢ **Unionsrechtliches Effektivitätsprinzip**

- Art 32 Abs 7, 33 Abs 5 NIS-2-RL **„Verteidigungsrechte“**
- durch die EU-Rechtsordnung verliehen
- Rechtsschutz gegen schlichthoheitliche Durchsetzungsmaßnahmen unionsrechtlich geboten

➢ **Unionsrechtliches Äquivalenzprinzip:**

- § 88 Abs 2 SPG – Beschwerde an LVwG als Rechtsschutz „ähnlich und vergleichbar“

4. Computer-Notfallteams

Computer-Notfallteams – Allgemeines

- CSIRTs – Computer Security Incident Response Teams
  CERTs – Computer Emergency Response Teams
- **Technische Unterstützung** für Einrichtungen für die **Bewältigung von Sicherheitsvorfällen**
- Nationales Computer-Notfallteam:
  CERT.at
- Computer-Notfallteam im Sektor öffentliche Verwaltung:
  GovCERT
- Sektorspezifisches Computer-Notfallteam im Sektor Energie:
  AEC

Computer-Notfallteams – NIS-2-RL

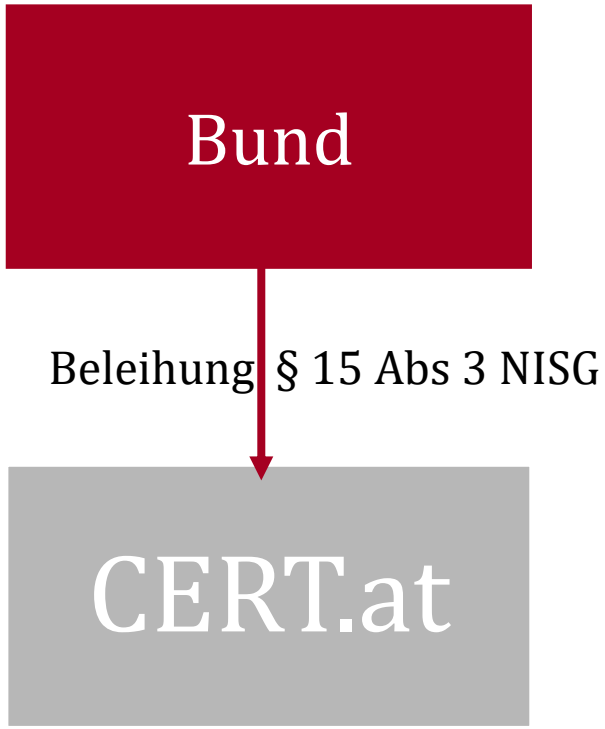
NIS-2-RL	Gesetzesentwurf – NISG-Novelle
Art 10: Computer-Notfallteams (CSIRTs)	
Art 11 Abs 1: Anforderungen • Verfügbarkeit ihrer Kommunikationsdienste • Räumlichkeiten an sicheren Standorten • Betriebskontinuität • Redundanzsysteme und Ausweicharbeitsräume	**§ 9 Anforderungen und Eignung von CSIRTs**
Abs 2: technische Kapazitäten • Notwendige technische Fähigkeiten und Ressourcen zur Aufgabenerfüllung	
Abs 3: Aufgaben	**§ 8 Zweck und Aufgaben der CSIRTs**

Computer Notfallteams – Aufgaben

Art 11 Abs 3 NIS-2-RL

- **Überwachung** und **Analyse** von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen
- Ausgabe von **Frühwarnungen** und **Alarmmeldungen** diesbezüglich
- **Reaktion** auf Sicherheitsvorfälle und Unterstützung
- **Erhebung** und **Analyse** forensischer Daten sowie Risiken und Sicherheitsvorfällen
- **Schwachstellenscan** auf Ersuchen
- **proaktive nicht intrusive Überprüfung** öffentlich zugänglicher NIS

Computer-Notfallteams – Aufgaben hoheitlich?



- **NISG Erläuterungen**:
  Hoheitliche Aufgabe – „Entgegennahme und Weiterleitung von Meldungen“
- Erteilung der Ermächtigung mittels konstitutiven Bescheid
- Andere Aufgaben nicht hoheitlich? Was steht im Bescheid?

5. Schlussfolgerungen

Schlussfolgerungen

- „**Cybersicherheitspolizei**“ als verwaltungspolizeiliche Aufgabe
- **Qualifikation** der Aufsichts- und Durchsetzungsmaßnahmen der zuständigen Behörde im Sinne der österreichischen **Rechtsaktlehre** notwendig → **Rechtsschutz**
- **Rechtsschutzdefizite** im Bereich der schlichten Hoheitsverwaltung
- **Beleihung** der Computer-Notfallteams?

Schlussfolgerungen – Verkehr

- NIS 2 als **zentrales Thema für kritische Verkehrsinfrastruktur**
- Guter Standard und doch permanenter **Handlungsbedarf**
- Verkehrsinfrastruktur und Behörden **zwischen Staat und Privat**
- Kooperative **Verwaltungszusammenarbeit**

Cybersicherheit und Verwaltung: Schutz kritischer Verkehrsinfrastrukturen im Rahmen der NIS-2-Richtlinie

Eleonóra Wagenknecht

Panel 3:
Digitalisierung und künstliche Intelligenz im Straßenverkehr
KI und Cybersicherheit

ZVR Verkehrsrechtstag 2024

03.10.2024
WU Wien

SIGMUND FREUD
PRIVATUNIVERSITÄT
WIEN