Die europäische NIS-Richtlinie – und ihre Auswirkungen auf Österreich

E-Day 2016
franz.vock@bka.gv.a

Status EU-Richtlinie zur Netz- und Informationssicherheit

NIS-RL

Ziel: EU-weit ein hohes Level an Netzwerk- und Informationssicherheit zu erreichen

- (1) Stärkung der Zusammenarbeit zwischen den MS

- (2) Verpflichtung zur Einführung angemessener IT-Sicherheitsmaßnahmen und der (2) Verpflichtung zur Meldung signifikanter Störfälle für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste

Verpflichtungen für MS

- Annahme einer **nationalen NIS-Strategie**
- Bildung nationaler **CERTs/CSIRTs**
- Einrichtung einer/mehrerer **NIS-Behörde(n) und** eines **SPoCs**
- Teilnahme an der **strategischen Kooperationsgruppe** und des **operativen CSIRT-Netzwerks**
- **Identifizierung** von Betreibern wesentlicher Dienste
- Möglichkeit für **freiwillige Meldungen** schaffen

Anwendungsbereich (1)

- **Betreiber wesentlicher Dienste:**
  - **Öffentliche** oder **private** Einrichtung
  - aus den Sektoren **Energie, Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser** und **digitale Infrastrukturen**

- **MS muss konkrete Betreiber identifizieren anhand dieser Kriterien:**
  - Einrichtung betreibt **Dienst** der für die Aufrechterhaltung **kritischer** sozialer und/oder wirtschaftlicher Aktivitäten erforderlich ist
  - Bereitstellung des Dienstes ist abhängig von **Netzwerk- und Informationssystemen**
  - Störfall hätte **signifikante Auswirkungen** auf die weitere Verfügbarkeit dieses Dienstes

Anwendungsbereich (2)

- **Anbieter digitaler Dienste (DSP)**
  - **Öffentliche** oder **private** Einrichtung
  - Bietet einen der drei in der RL genannten **digitalen Dienste** an
    - Online **Marktplatz**
    - Online **Suchmaschine**
    - **Cloud**-Computing-Dienst
  - **Ausgenommen:**
    - natürliche Personen
    - Klein- und Kleinstunternehmen

Verpflichtung für Betreiber und DSPs

- **(1) Pflicht** angemessene technische und organisatorische **Sicherheitsmaßnahmen** zur **Risikobewältigung** zu ergreifen

- **(2) Pflicht zur unverzüglichen Meldung** („*without undue delay*“) **von Störfällen,** die **signifikante/substantielle** Auswirkungen (Dauer, betroffene Nutzer, Verbreitungsgrad) auf die **Aufrechterhaltung** des Dienstes haben

  - Meldung ergeht an NIS-Behörde oder an das **nationale CSIRT**

Unterscheidung Betreiber und DSP

- **Strengere nationale Regelungen** nur für Betreiber wesentlicher Dienste möglich

- **Prüfung der Sicherheitsmaßnahmen** durch NIS-Behörde:
  - Betreiber/jederzeit; DSP/konkreter Anlass (“evidence”)
  - Ergebnis: Betreiber/bindende Anweisungen; DSP/Fehlerbehebung einfordern

- Europäische Kommission erlässt für **DSPs** mittels **Durchführungs-RA** Vorgaben zu den **Sicherheitsanforderungen** und den die **Meldepflicht auslösende Kriterien**

- **Zuständigkeit**:
  - **Betreiber**: MS in dem der Betreiber eine **Niederlassung** hat (können auch mehrere MS sein)
  - **DSP: MS der Hauptniederlassung** (nur dieser); Pflicht zur Namhaftmachung eines **Bevollmächtigten** wenn keine EU-Niederlassung

„NIS-Behörde(n)“- Aufgaben:

- **Überwachen** die Anwendung der RL auf nationaler Ebene
- **Meldestelle** von Störfällen (auch CSIRT)
- Bestimmung möglicher **grenzüberschreitende Auswirkungen** und Kontaktaufnahme zu den betroffenen MS (auch CSIRT)
- **Information der Öffentlichkeit über individuelle Vorfälle** wenn im öffentlichen Interesse gelegen (auch CSIRT)
- **Prüfung der Sicherheitsmaßnahmen**
  - Von Betreibern wesentlicher Dienste (jederzeit)
  - Von Anbietern digitaler Dienste (ex post)

CSIRTs und SPOC - Aufgaben

- ein oder mehrere **CSIRTs/CERTs:**
  - Kontinuierliche **Risikoanalyse** und **Situationsbewusstsein**
  - Ausgabe von **Frühwarnungen**, **Verbreitung von Informationen** über Risiken und Vorfälle
  - Monitoring und Handling von **Störfällen**
  - **Meldestelle** von Störfällen (auch NIS-Behörde)
  - Bestimmung über **grenzüberschreitendes Potential eines Störfalls** (auch NIS-Behörde)
  - Teilnahme am **CSIRT-Netzwerk** auf EU-Ebene

- **Single Point of Contact (SPOC):**
  - **Verbindungsstelle** zwischen **MS, Kooperationsgruppe und CSIRT-Netzwerk**

Kooperationsgruppe - strategische Aufgaben

- **Teilnehmer**: Vertreter aus **MS**, **EK** und **ENISA**
- **Beginn** der Tätigkeit: **6 Monate** nach Inkrafttreten der RL
- **Aufgaben u.a.**:
  - Strategische Beratung des **CSIRT-Netzwerks**
  - Erstellung von **Leitlinien** für sektorspezifische **Kriterien** zur Bestimmung der **„Signifikanz“ eines Vorfalls**
  - **Unterstützung in der Identifikationsphase** der Betreiber – MS sollen einen kohärenten Ansatz finden
  - Austausch von **Informationen** und **bester Praktiken**
    - **Meldung von** Störfällen
    - **Identifikation** von Betreibern
    - **Bewusstseinsbildende** Maßnahmen
    - Forschung und Entwicklung im NIS-Bereich

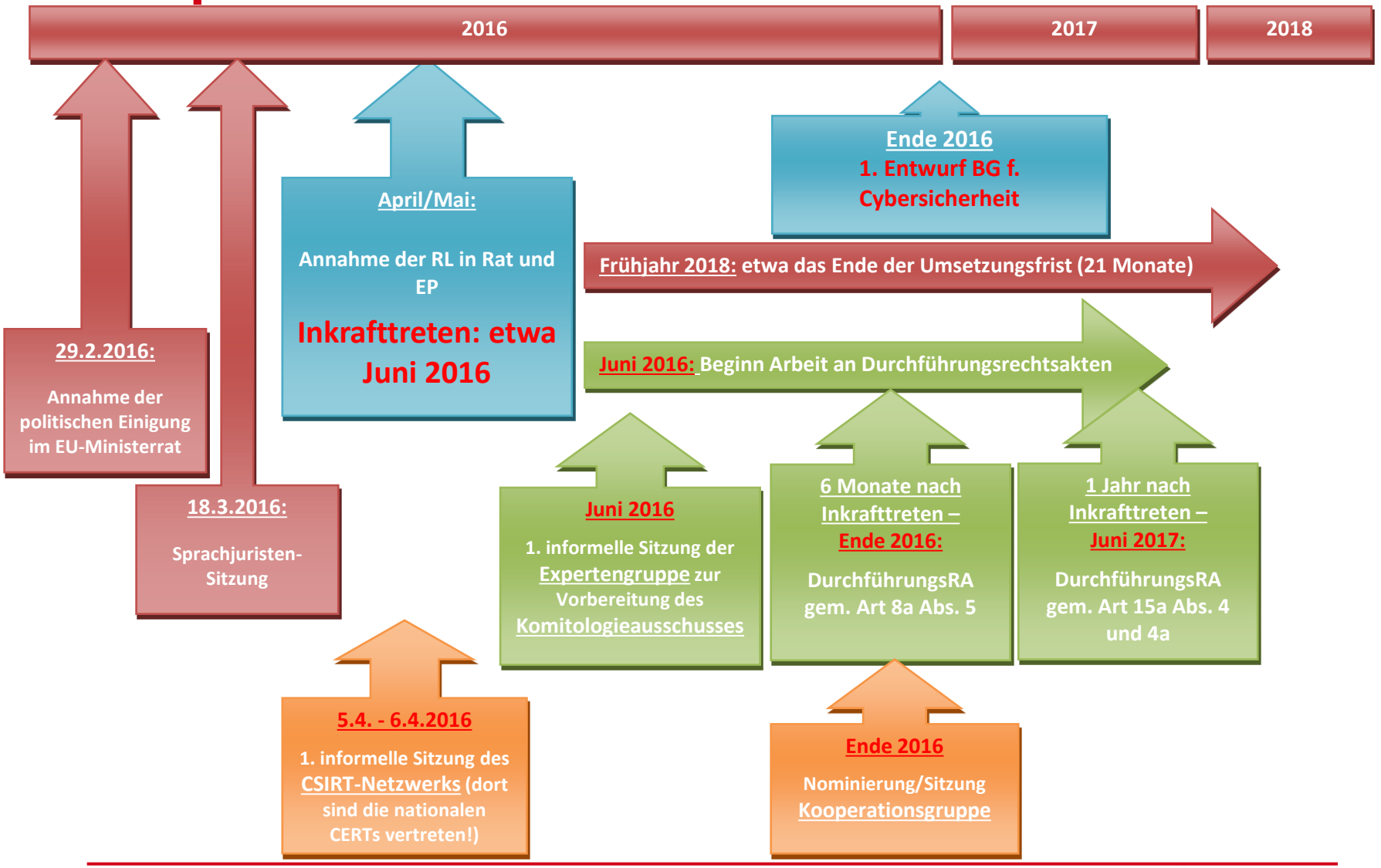
CSIRT-Netzwerk - operative Aufgaben

- **Teilnehmer**: Vertreter der nat. CSIRTs und CERT-EU (EK hat Beobachterrolle)
- **Aufgaben u.a.:**
  - **Vertrauensaufbau** zwischen den MS
  - **Allgemeiner Informationsaustausch** über **Störfälle**
  - **Assistenz** bei **länderübergreifenden Vorfällen**
  - Auf Ersuchen eines MS: **koordinierte Reaktion** auf einen Störfall der sich im Zuständigkeitsbereich des ersuchenden MS ereignet hat
  - **Erfahrungsaustausch** nach **NIS-Übungen**

Nicht mehr im RL-Entwurf enthalten

- Art 9: Secure information sharing system
- Art 10: Early warnings
- Art 11: Coordinated response
- Art 12: Union NIS-cooperation plan

Zeitplan NIS-RL:



Vorbereitungsarbeiten in Österreich

ORDNUNGSPOLITISCHER RAHMEN

ÖSCS - AG Ordnungspolitischer Rahmen

- Parallel zu Verhandlungen der NIS-RL
- Interministerielle Zusammensetzung: BKA, BMI, BMLVS, BMWFW, BMVIT, BMF
- Ziel: den bestehenden ordnungspolitischen Rahmen sowie darauf aufbauend notwendige Änderungen zu untersuchen
- Geht jetzt über in eine interministerielle AG zur Entwicklung des BG für Cybersicherheit (Kick-Off am 23.02.2016)

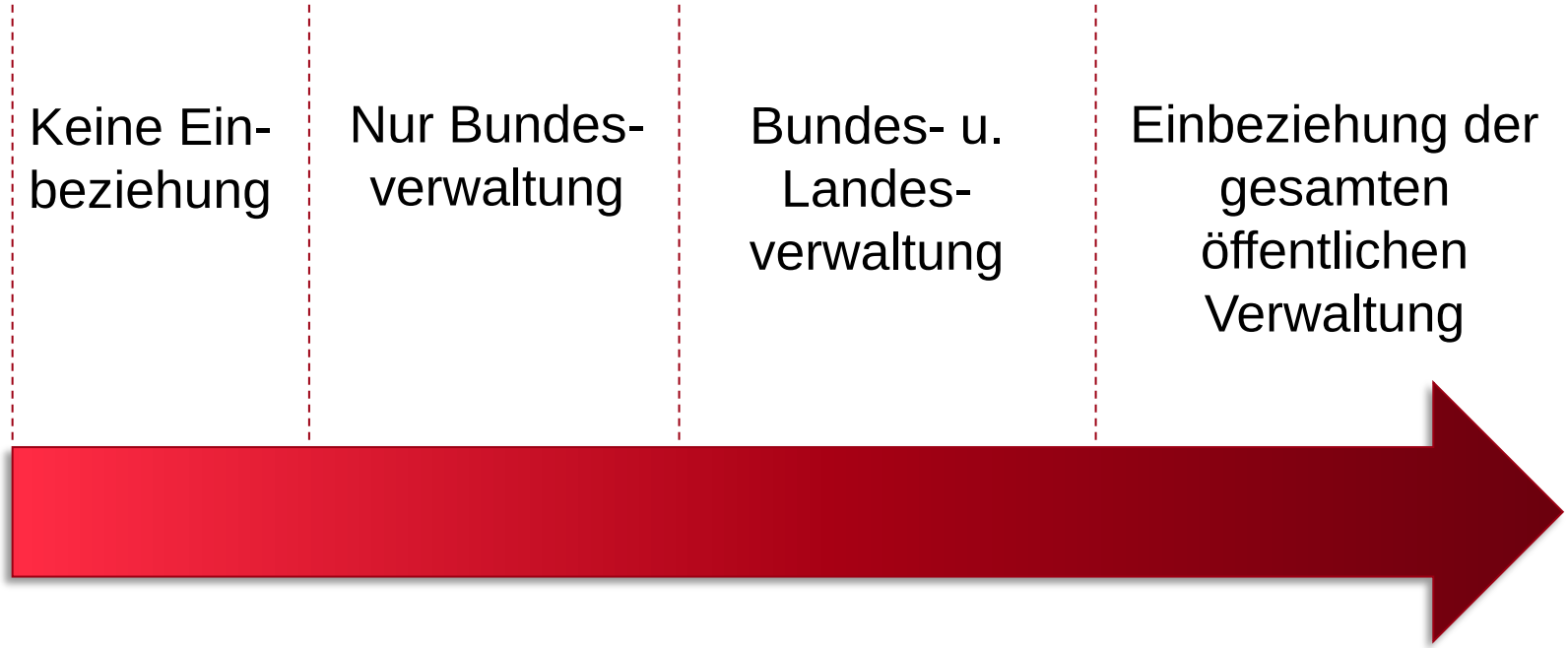
Umsetzungsoptionen zur NIS-RL

- **Hintergrund:** nationale Umsetzung der NIS-RL in Bezug auf
  - einzurichtende Behörden/Strukturen
  - Anwendung auf öffentl. Verwaltung

- **Optionen zu Behörden/Strukturen**
  1. eine NIS-Behörde für strategische Aufgaben + Delegation operativer Aufgaben
  2. eine NIS-Behörde für alle strategischen und operativen Aufgaben
  3. drei NIS-Behörden (Zuständigkeiten nach strategischen/operativen Gesichtspunkten)

Umsetzungsoptionen zur NIS-RL

- **Optionen zur Anwendung auf öffentl. Verwaltung**



Regelungsnotwendigkeiten

- Organisation der **Cybersicherheits-Struktur**
- **Informationsaustausch**
  - Zwischen Privaten
  - Zwischen Behörden
  - zwischen Behörden und Privaten
- **Informationsgewinnung**
- **Meldeverpflichtung/Melderecht**
- Verpflichtendes **IT-Risikomanagement**

Danke!