Netzsicherheit

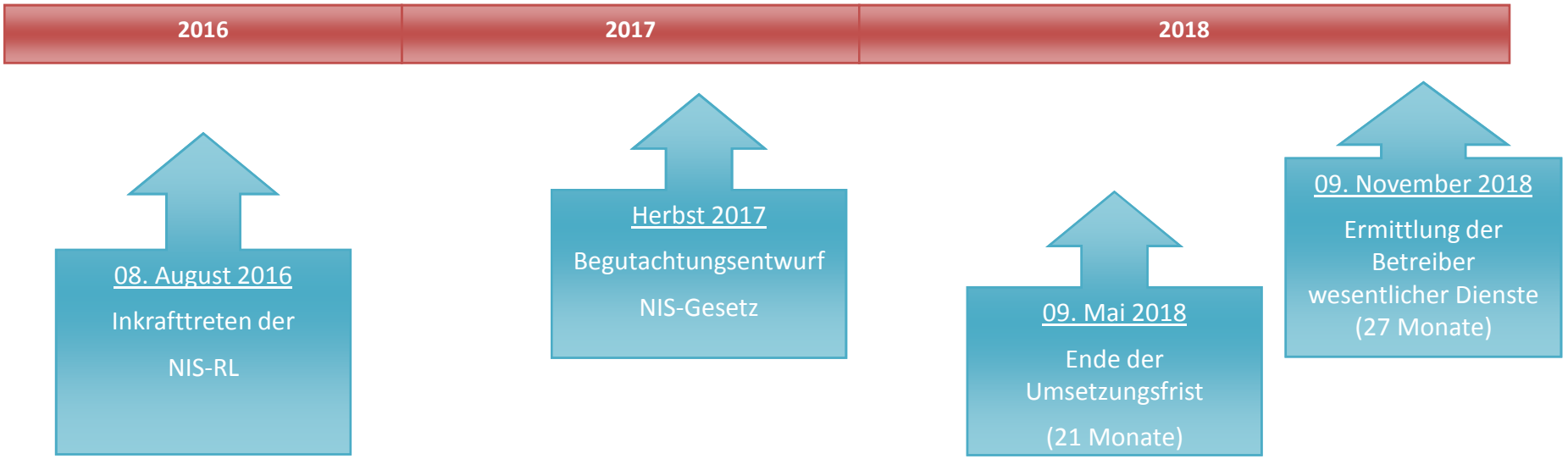
Netzsicherheit im Recht – Was taugt es für die Praxis

Ing. Mag. Sylvia Mayer, MA

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Bundesgesetz zur Gewährleistung der Sicherheit von Netz- und Informationssystemen (NIS-Gesetz)

Zeitplan



EU-Kriterien

Zahl der Nutzer

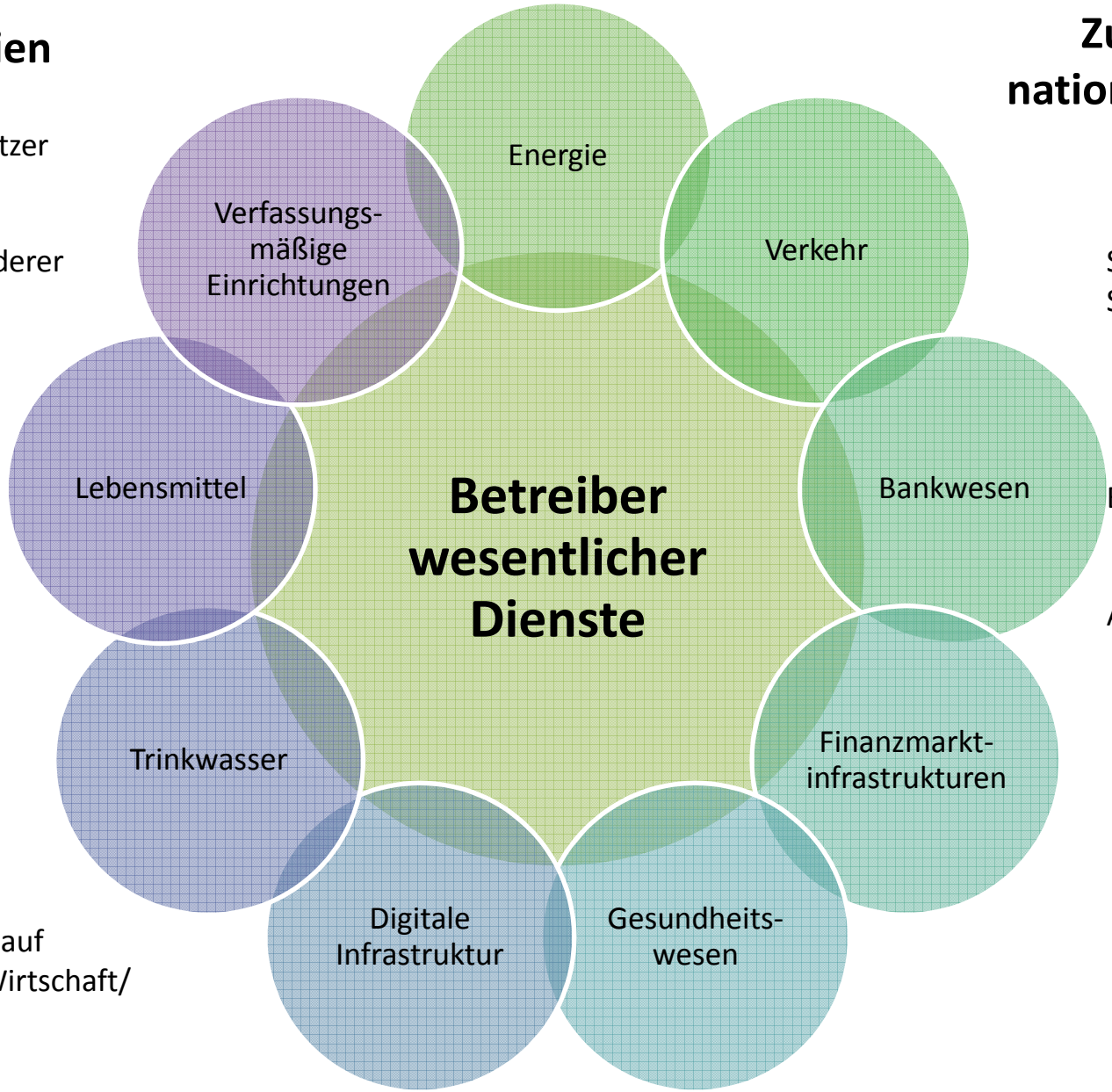
Abhängigkeit anderer Sektoren

Marktanteil

Verfügbarkeit alternativer Mittel

Geografische Ausbreitung

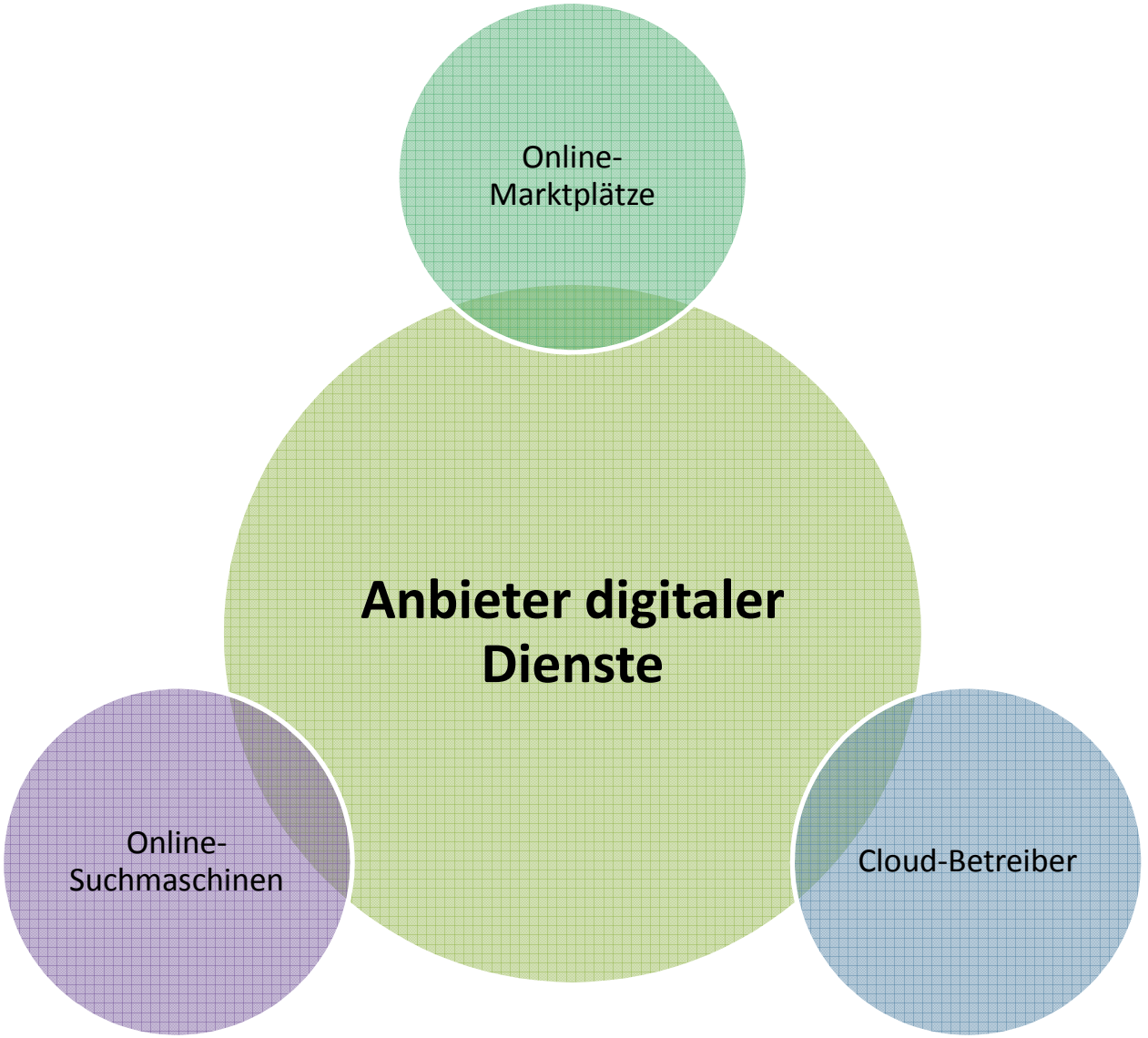
Auswirkungen auf Gesellschaft/Wirtschaft/ Sicherheit



Zusätzliche nationale Kriterien

Sektor-spezifische Schwellwerte

- versorgte Personen
- produzierte Energie
- Zahl stationärer Aufnahmen
- etc.


Online-
Marktplätze
Anbieter digitaler
Dienste
Online-
Suchmaschinen
Cloud-Betreiber

Behörden & Strukturen

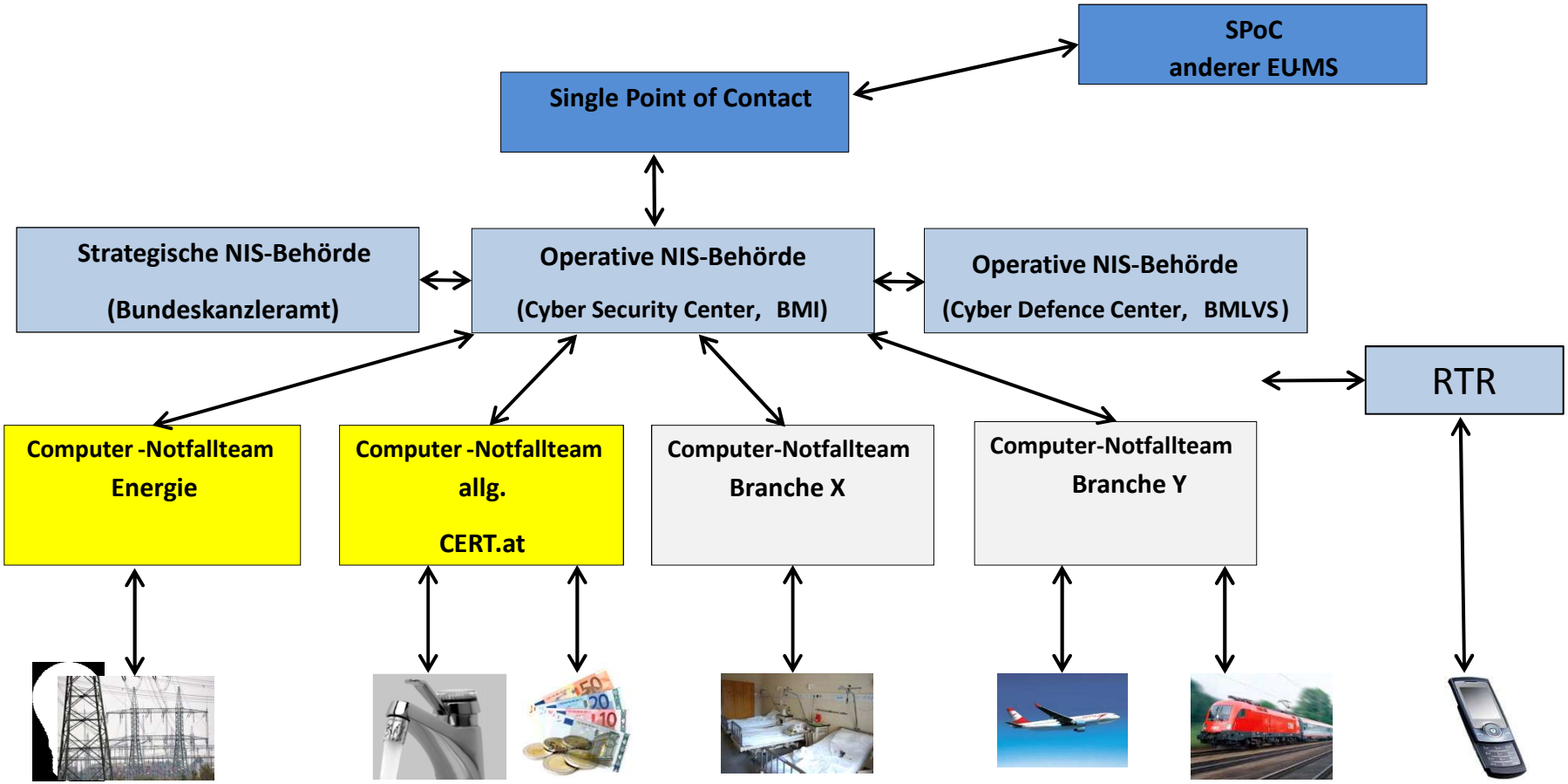
Einrichtung nationaler Organisations-strukturen

- **Drei zuständige Behörden**
  - Strategische NIS-Behörde → Bundeskanzler
  - Operative NIS-Behörde → Bundesminister für Inneres
  - Operative NIS-Behörde → Bundesminister für Landesverteidigung und Sport

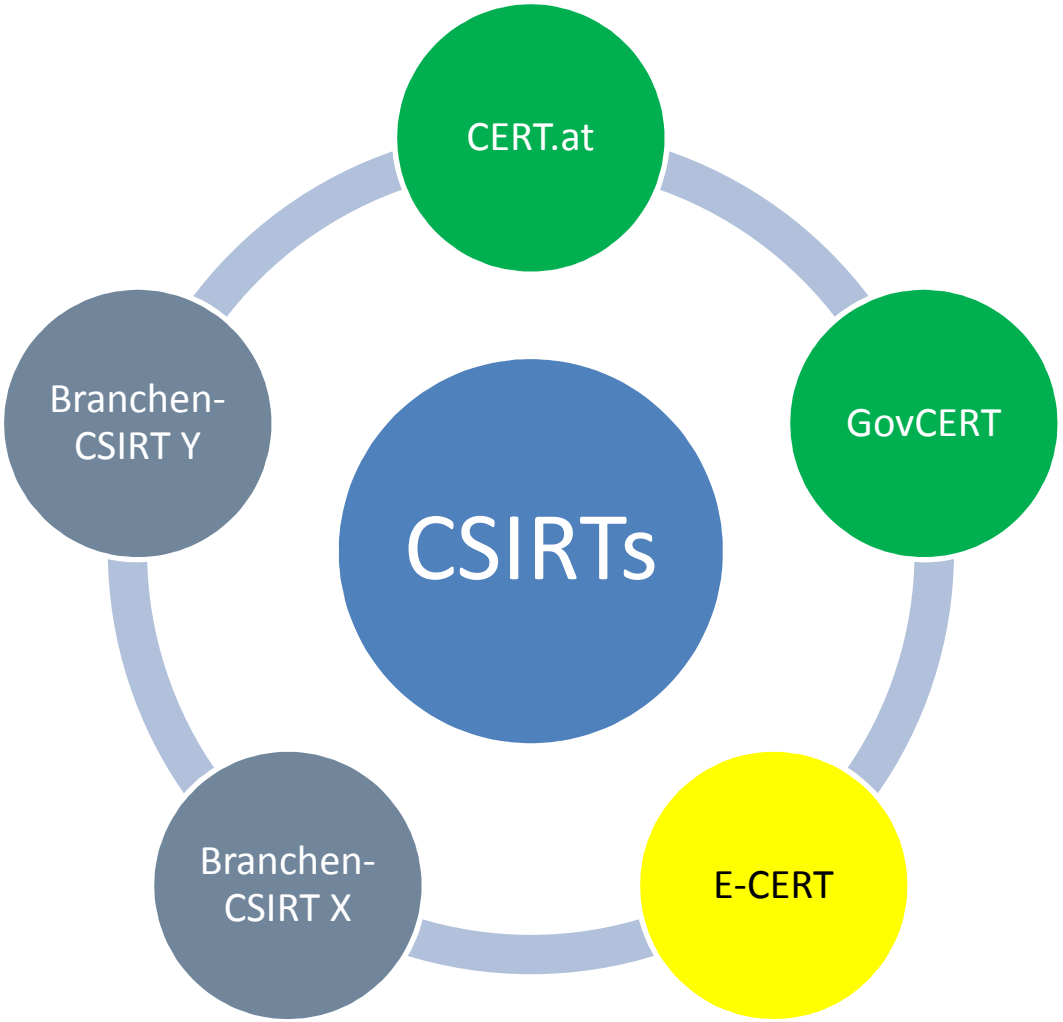
- Eine **zentrale Anlaufstelle** (Single Point of Contact, SPoC)
  - Operative NIS-Behörde → Bundesminister für Inneres

- **Computer-Notfallteams (nach Sektoren) / nationales Computer-Notfallteam** (Computer Security Incident Response Teams, CSIRT)
  - GovCERT/CERT.at
  - Branchen-CERTs (zB E-CERT)

Nationale Strukturen



Computer-Notfallteams in Österreich



Kooperation der NIS-Behörden

- **Innerer Kreis der operativen Koordinierungsstruktur (IKDOK)**
  - **Organisationen**
    - Drei NIS-Behörden
  - **Aufgaben**
    - Erörterung und Aktualisierung des Lagebildes über Sicherheitsvorfälle
    - Beratung im Cyberkrisenmanagement
    - Austausch klassifizierter Informationen

- **Operative Koordinierungsstrukturen (OpKoord)**
  - **Organisationen**
    - Drei NIS-Behörden + BMEIA + Computer-Notfallteams
  - **Aufgaben**
    - Erörterung des gesamtheitlichen Lagebildes (inkl. freiwillige Meldungen)

Verpflichtungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste

Sicherheitsvorkehrungen

- Treffen von **geeigneten organisatorischen und technischen Vorkehrungen** zur Vermeidung von Störungen der **Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** ihrer Netz- und Informationssysteme → Stand der Technik
  - NIS-Behörden können Standards festlegen
  - Vorschlag von sektorenspezifischen Sicherheitsvorkehrungen möglich

- Überprüfung der Betreiber durch **qualifizierte Stellen**

- Regelmäßiger **Nachweis der Überprüfung** gegenüber operativer NIS-Behörde BMI

Meldepflicht

- Betreiber haben **Sicherheitsvorfall unverzüglich** an das für sie zuständige **Computer-Notfallteam** zu melden →
  Weiterleitung dieser Meldung an **NIS-Behörde BMI**

- **Inhalt der Meldung**
  - Angaben zum Sicherheitsvorfall
  - Technische Rahmenbedingungen, insb. vermutete oder tatsächliche Ursache
  - Betroffene Informationstechnik
  - Art der betroffenen Einrichtung oder Anlage

- Geläufiges elektronisches Format unter Verwendung festgelegter Kommunikationskanäle (evtl. **Meldeformular**)

Meldepflicht

- **Sicherheitsvorfall**

*Eine **Störung** der **Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** von Netz- und Informationssystemen, Komponenten oder Prozessen, die zu einem **Ausfall oder einer erheblichen Beeinträchtigung** der Funktionsfähigkeit des betriebenen Dienstes **führen kann oder geführt hat**;*

Parameter für die Erheblichkeit:

- Zahl der vom Sicherheitsvorfall betroffenen Nutzer
- Dauer des Sicherheitsvorfalles
- Geografische Ausbreitung
- Ausmaß der Unterbrechung der Bereitstellung
- Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten

Einbindung der Wirtschaft

- **KSÖ Rechts- und Technologiedialog** im Jahr 2016
- **Cyber Sicherheits Plattform** (CSP)
- Einbindung **Vertreter aller Sektoren** in Q2/Q3 2017
  - 10 durchgeführte Sektorengespräche
    - Umfang der Sektoren bzw. Identifizierung von Teilsektoren
    - Bestehende Meldepflichten
    - Bestehende Sicherheitsvorkehrungen

Nächste Schritte

- Einbindung **betroffener Unternehmen** in Q4/2017

- Arbeiten an den **Verordnungen**
  - Identifizierung Betreiber wesentlicher Dienste
  - Festlegen von Sicherheitsvorkehrungen (→ EU-Kooperationsgruppe)
  - Nähere Umstände bzw. Schwellen für Meldepflicht

Was taugt es für die Praxis?

Vielen Dank für Ihre Aufmerksamkeit!