.BVT

www.bvt.gv.at

# Das NIS-Gesetz

## Umsetzung aus Sicht des BMI

Mag. Gernot Goluch

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für

# NIS-Gesetz: Aktueller Status

- NIS-Gesetz befindet sich in Begutachtung (19.09. – 31.10.2018)
- Einbindung aller betroffenen Sektoren
- Aktuell Finalisierungen der Verordnungen (BKA, BMI).
- Inkrafttreten des NIS-Gesetzes und der dazugehörigen Verordnungen mit Dezember 2018/Jänner 2019

# Adressaten des NIS-Gesetzes

## “Betreiber wesentlicher Dienste”

- **Energie** (Elektrizität, Erdöl, Erdgas)
- **Verkehr** (Luft, Schiene, Schifffahrt, Straße)
- **Bankwesen**
- **Finanzmarktinfrastrukturen**
- **Gesundheitswesen**
- **Trinkwasserlieferung und -versorgung**
- **Digitale Infrastrukturen**

## “Anbieter digitaler Dienste”

- **Online-Marktplatz**
- **Online-Suchmaschine**
- **Cloud-Computing-Dienst**

## Einrichtungen des Bundes

- (Insbesondere) **Ministerien**


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Wesentliche Dienste am Beispiel Energie

- Wesentliche Dienste ergeben sich aus Anhang der NIS-RL pro Sektor

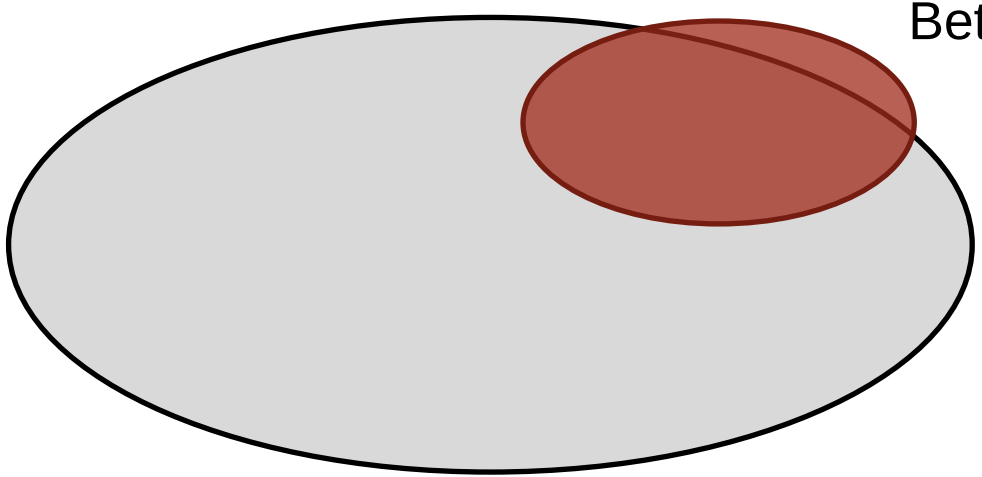
| | | |
|---|---|---|
| **Elektrizität** | **Stromerzeugung** | Betrieb einer Erzeugungsanlage |
| | | Betrieb von Systemen zur Steuerung von Erzeugungsanlagen |
| | **Stromverteilung** | Betrieb eines Verteilernetzes |
| | **Stromübertragung** | Betrieb eines Übertragungsnetzes |
| **Erdöl** | | Betrieb von Erdölfernleitungen |
| | | Betrieb von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl |
| | | Betrieb von Anlagen zur Lagerung von Erdöl |
| | | Betrieb von Anlagen zur Förderung von Erdöl |
| **Erdgas** | **Gasverteilung** | Betrieb einer Gasförderungsanlagen |
| | **Gastransport** | Betrieb eines Fernleitungsnetzes |
| | **Gasförderung** | Betrieb eines Verteilernetzes |
| | **Gasspeicherung** | Betrieb von Speicheranlagen |

# Finanzsektor

- Unternehmen aus dem Finanzsektor (z.B. Kreditinstitute) haben die **Sicherheitsvorkehrungen der PSD 2** umzusetzen
- **PSD 2 als „lex specialis“ zum NIS-Gesetz**
- FMA fungiert als Prüfstelle / Meldestelle

# Kritische Infrastruktur vs. Betreiber wesentlicher Dienste

Kritische Infrastrukturen
nach SPG



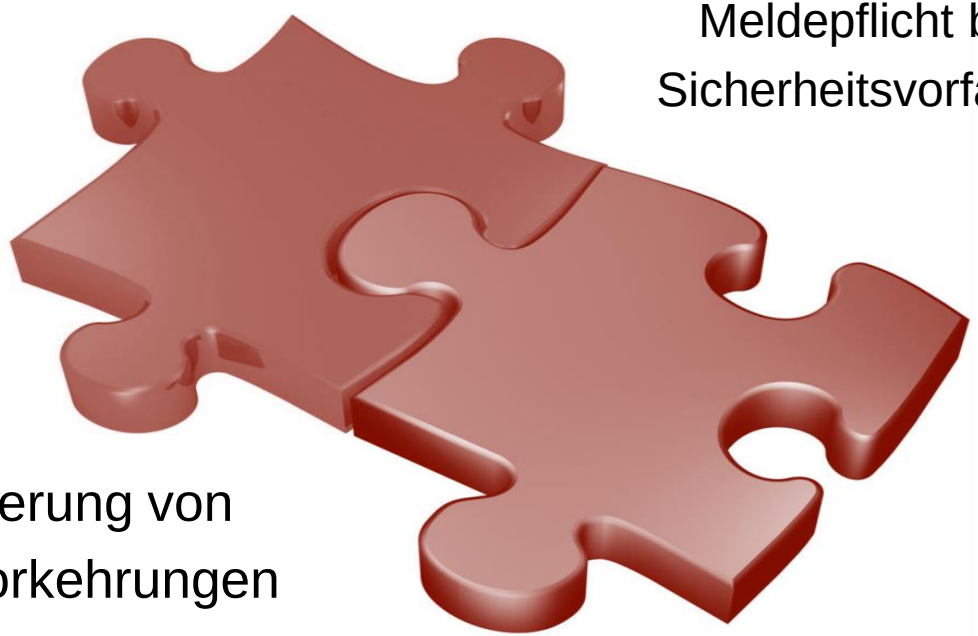
Betreiber wesentlicher
Dienste nach NISG

**Bescheid**


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Pflichten für betroffene Unternehmen

Meldepflicht bei Sicherheitsvorfällen



Implementierung von Sicherheitsvorkehrungen


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Verordnungen

## Bundeskanzler

- Schwellwerte für Identifikation
- Schwellwerte für Meldungen
- Mindestsicherheitsmaßnahmen

## Bundesminister für Inneres

- Qualifizierte Stellen
- Sektorengespräche

# Meldungen

- Meldung von Sicherheitsvorfällen an zuständiges **Computer-Notfallteam (CSIRT)**

- **Pflichtmeldungen**
  - Erstmeldung unverzüglich
  - Nachmeldungen ohne unangemessene weitere Verzögerung
  - CSIRT leitet unverzüglich an BMI weiter (1:1)

- **Freiwillige Meldungen** (können anonymisiert sein)
  - Betreiber eines nicht wesentlichen Dienstes oder Störungen, die kein Sicherheitsvorfall sind
  - werden ebenfalls an BMI weitergeleitet

# Sicherheitsvorkehrungen

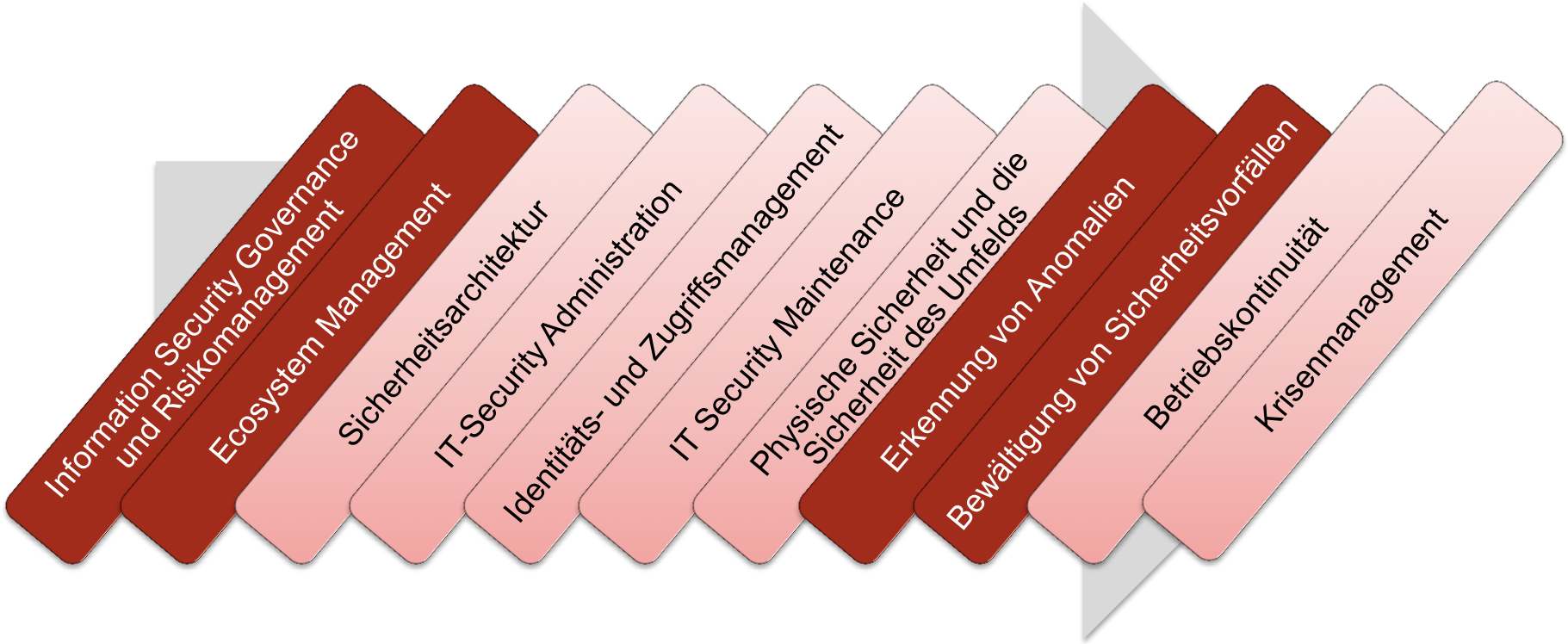
**BKA Verordnung**

**Leitlinien / Leitfaden**

- Mapping
- Beschreibung Sicherheitsvorkehrungen
- Anwendungsbeispiele
- Überprüfungszyklus
- Branchenspezifische Standards


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Mindestsicherheitsvorkehrungen (Entwurf)



# NIS Fact Sheets

- **NIS Fact Sheet 08/2018 an potentielle BwD und QuaSten versandt**
  - **Mapping-Tabelle** von IKT-Sicherheitsstandards und Cyber Security Best Practices (basierend auf Ergebnissen der EU-NIS Cooperation Group)
    - Österreichisches Informationssicherheitshandbuch Version 4.0.1
    - BSI IT-Grundschutz
    - ISO 27001:2013
    - ISA/IEC 62443 3-3
    - CIS – Critical Security Controls (v6 & v7)
    - NIST Cyber Security Framework
  - Wird in Version 2 von BKA / BMI mit zusätzlichen Standards aktualisiert

# Überprüfungszyklus für BwD

Mögliche Prüfung seitens Behörde

**ab 1 Jahr nach Bescheid**

Prüfberichte qualifizierter Stellen

**(„rollierende Teilprüfungen“)**

Generell: Nachweis der Anforderungen

**alle 3 Jahre**


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# „Rollierende“ Teilprüfungen

- **Ermöglichung**
  - des Nachweises im Rahmen bestehender Audits / Prüfungen
  - Beibehaltung etwaiger Audit- / Prüfpläne seitens des BwD
- **Vermeidung**
  - eines großen NIS-Audits / Prüfung über alle Mindestsicherheits-vorkehrungen für alle wesentliche Dienste eines Betreibers
  - konzentrierten Aufwands seitens BwD / qualifizierte Stellen / NIS-Büro im BMI alle 3 Jahre zum gleichen Zeitraum
- **Feedback seitens des NIS-Büros im BMI und damit Rechtssicherheit für BwD pro Teilprüfung!**

# Scope der Audits / der Prüfungen

- **IKT** & dazugehörige **Prozesse** von welchen der **wesentliche Dienst abhängig** ist bzw. welche diesen **unterstützen**
  - **Analyse, Erfassung und Bewertung des Scope!**
- Möglichkeit der **a-priori Abstimmung** mit NIS-Büro im BMI
  - **Kein Rechtsanspruch!** → Abhängig von Ressourcen und Zeitkapazitäten des NIS-Büros
- Realistischer **Audit/Prüfaufwand** seitens qualifizierter Stelle in Bezug auf Scope
- **Bei einigen Sektoren wird der Scope sehr OT-lastig sein!**


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Qualifizierte Stellen

- „**NIS-Prüfungsstelle**“ bezüglich Sicherheits-vorkehrungen
  - eigenständige Unternehmen mit Hauptniederlassung oder Sitz in Österreich
  - Qualifizierung kann sich auch nur auf eine oder mehrere Domänen / Maßnahmen beziehen („Aufgabenbereich“)

# Zentrale Erfordernisse einer QS

„befähigte **Mitarbeiter**“

„adäquate **Zertifizierungen**“

„dem Stand der Technik entsprechende **Werkzeuge**“

„geeigneter **Prüfungsprozess**“


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

# Mehrwert

**Erhöhung des Sicherheitsniveaus**
im IKT-Bereich in Österreich

Je mehr Meldungen,
desto mehr qualitative Information

Weitestmögliche Beibehaltung des **partnerschaftlichen Ansatzes**
in der Zusammenarbeit

**Möglichst wenig Mehraufwand**
für den Nachweis der Einhaltung der Sicherheitsmaßnahmen

# Das CSC als Partner

**Prävention &**
**Schutz Kritischer Infrastrukturen**

Awareness, Beratung

**Koordination &**
**Cyber-Krisenmanagement**

OpKoord, IKDOK

**Behörde für**
**Netz- und Informationssicherheit**

NIS-Gesetz

**Technische Kompetenz &**
**Ansprechpartner**

Phänomene, Analysen, Vernetzung


Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert

.BVT

www.bvt.gv.at

# Q&A!

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundesamt für Verfassungsschutz und Terrorismusbekämpfung Bundes