

# Umsetzungsstand der NIS-2-Richtlinie

Thomas Sievers und Maximilian Rath

„NIS2 – Jetzt gilt’s“, eco AK R&R/AK KRITIS, 17. Oktober 2024, 11:00 – 11:40 Uhr



Bundesministerium  
des Innern  
und für Heimat

# Einleitung und Überblick

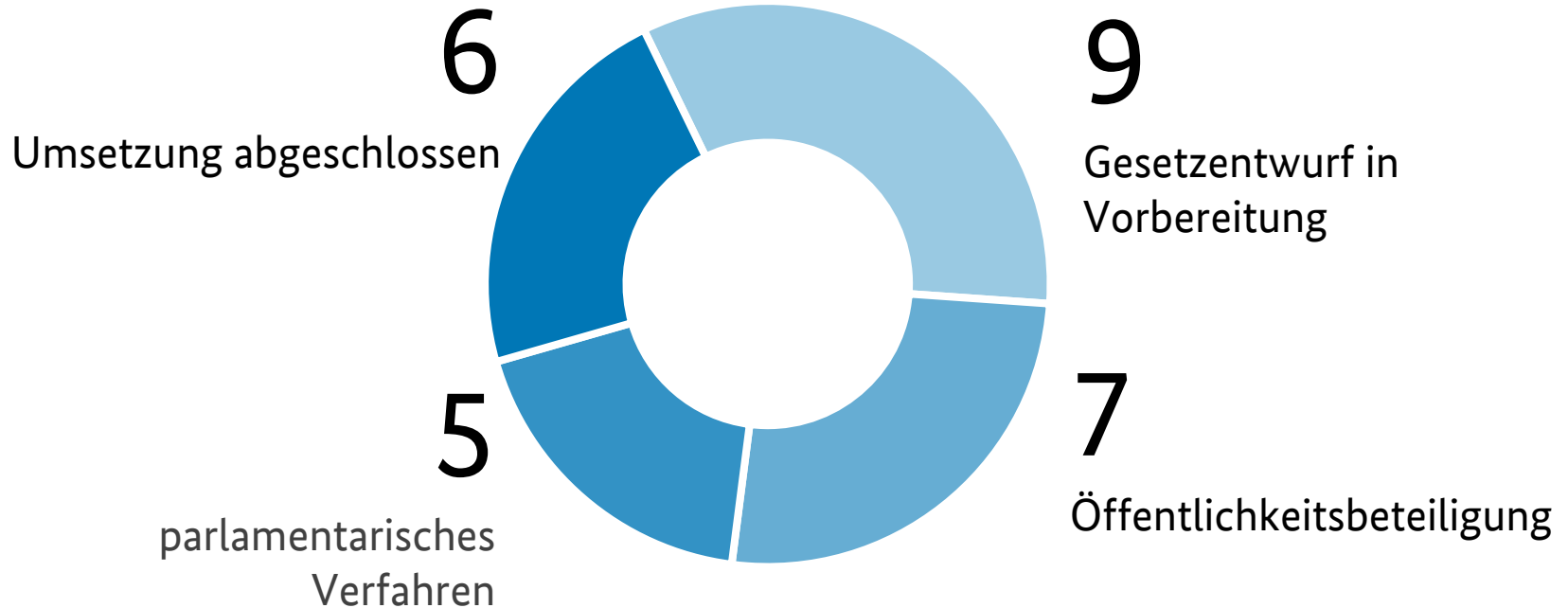
1. NIS-2-Richtlinie im Überblick
2. Aktueller Stand der NIS-2-Umsetzung in der EU und in Deutschland
3. Überblick NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
4. Feststellung der Betroffenheit
5. Risikomanagementmaßnahmen und Registrierungspflichten
6. Meldepflichten
7. Durchführungsverordnung der Kommission betreffend digitaler Anbieter
8. Vorgaben für die Bundesverwaltung
9. Informationsangebote von BSI und BMI
10. Q & A

# Die NIS-2-Richtlinie im Überblick

- Richtlinien bedürfen der Umsetzung ins nationale Recht durch die Mitgliedstaaten
  - keine horizontale Wirkung von Richtlinien
- Hintergrund und Zielsetzung der NIS-2-Richtlinie – Binnenmarktsharmonisierung
- Kerninhalte und Neuerungen:
  - Ausweitung des Anwendungsbereichs (*size cap-rule*)
  - Detailliertere Pflichten: Registrierung, Risikomanagementmaßnahmen und Meldungen
    - ❖ Ermächtigungen für die Kommission zum Erlass delegierter Rechtsakte für Einzelheiten zu Risikomanagementmaßnahmen und Meldungen
  - Neue Maßnahmen der Aufsicht- und Durchsetzung

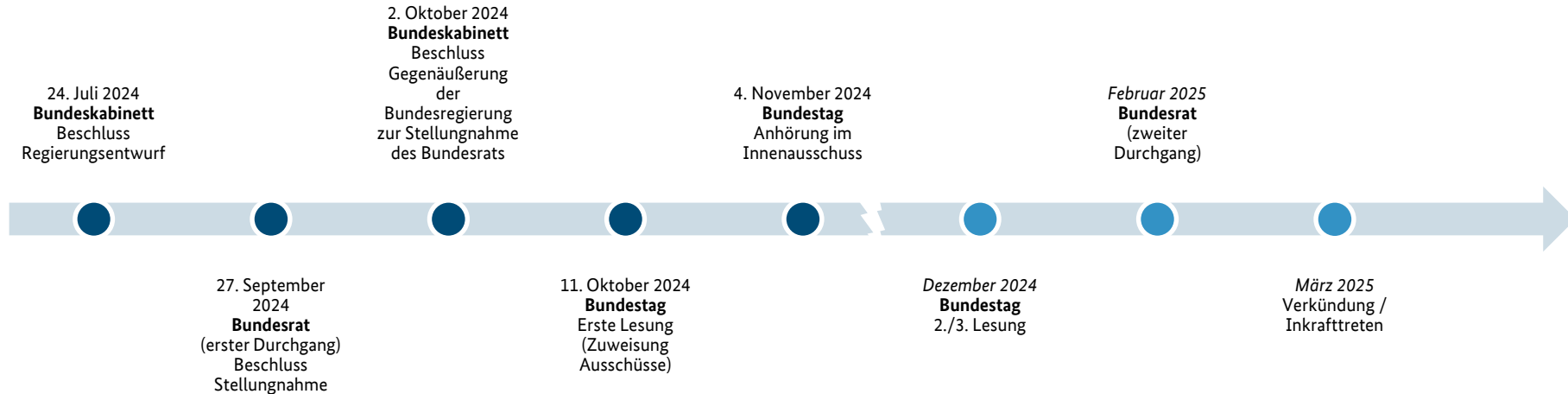
# *Umsetzungsverfahren*

# Aktueller Stand der Umsetzung der NIS-2-Richtlinie in den EU-Mitgliedstaaten



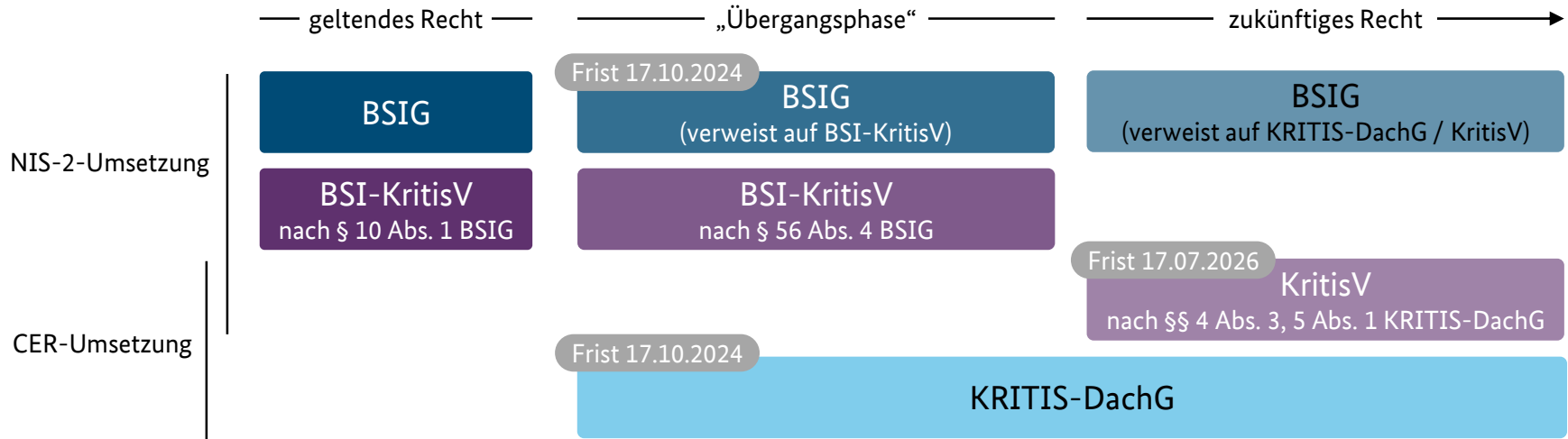
# Aktueller Stand der Umsetzung der NIS-2-Richtlinie in Deutschland

- Zeitlicher Rahmen



- Verfahren: Finanzvorlage, Einspruchsgesetz

# Zeitliches Zusammenspiel von BSIG / KRITIS-DachG



*Mit dem Inkrafttreten der KritisV nach §§ 4 Abs. 3, 5 Abs. 1 KRITIS-DachG findet die Identifizierung von KRITIS (Betreiber kritischer Anlagen) zentral in dieser Rechtsverordnung statt. Grund: Gewährleistung der ununterbrochenen Identifizierung von KRITIS für die Zwecke des BSIG und längere Umsetzungsfrist für die Identifizierung von KRITIS für die Zwecke der Umsetzung der CER-Richtlinie.*



# *Inhalt des deutschen Umsetzungsgesetzes*



# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

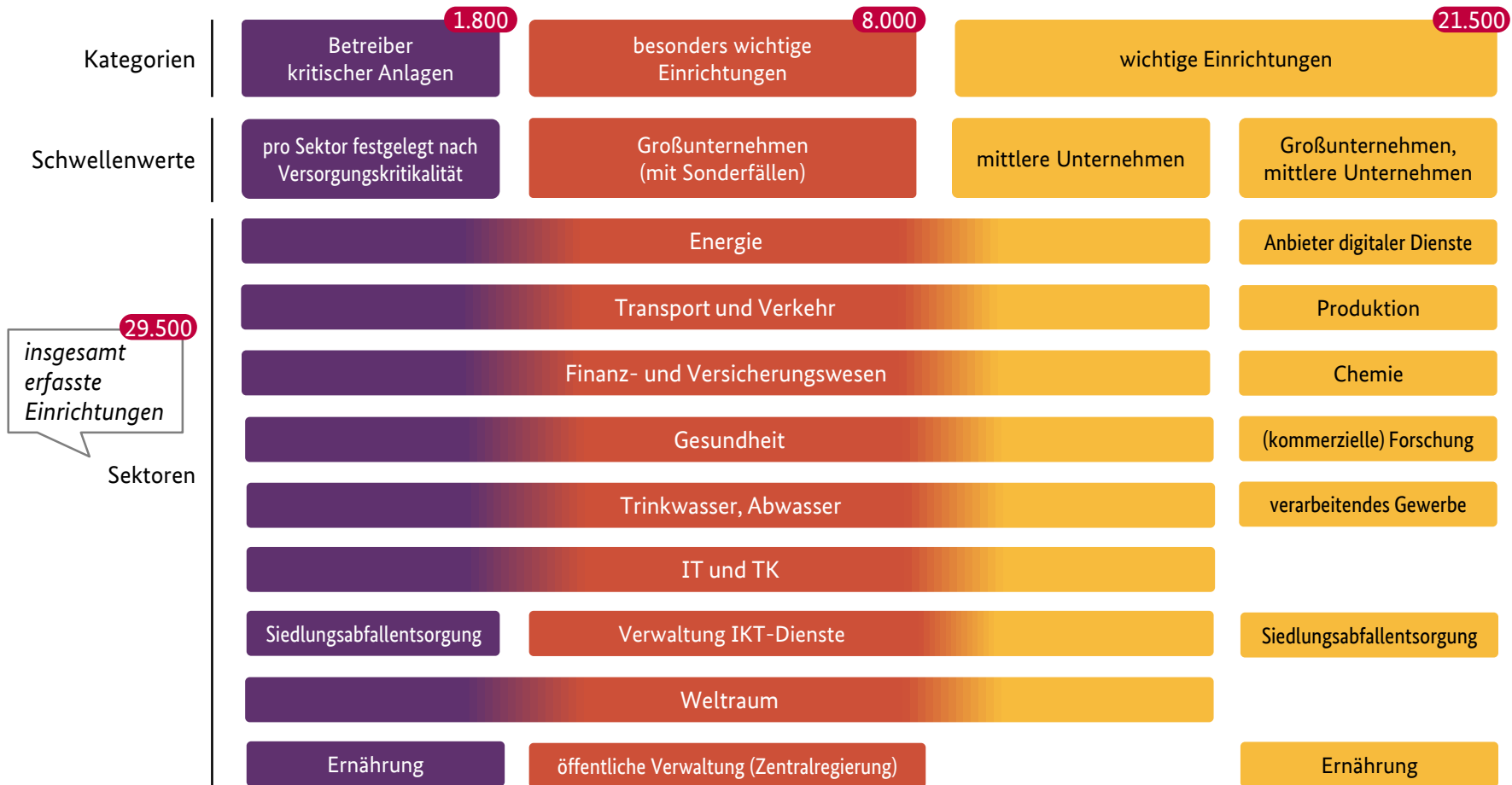
## Überblick

- Führt den mit dem IT-Sicherheitsgesetz (2015) und dem IT-Sicherheitsgesetz 2.0 (2021) geschaffenen Ordnungsrahmen fort
- Artikelgesetz
- BSI-Gesetz-Novelle (Artikel 1) anstatt Änderungsgesetz (wie IT-SiG, IT-SiG 2.0)
  - zukünftig:  
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)
  - Von 41 Paragraphen zu 65, vgl. Synopse geltende Fassung / Regierungsentwurf
- In den übrigen Artikeln im Wesentlichen Folgeänderungen in Fachgesetzen

# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

## Feststellung der Betroffenheit (1)

1. **Niederlassung in Deutschland** – Begriff des Unionsrechts: *Niederlassung ist die effektive und tatsächliche Ausübung einer wirtschaftlichen Tätigkeit durch eine feste Einrichtung.*
2. **Verpflichtungsträger („Einrichtung“)**
  - a) **Person** – natürliche Person ODER juristische Person des Privatrechts (z.B. GmbH, AG) ODER juristische Person des öffentlichen Rechts (z.B. AöR, KdÖR)
  - b) **rechtlich unselbständige**
    - Organisationseinheit einer Gebietskörperschaft** – Landesbetrieb ODER kommunaler Eigenbetrieb
3. **Wirtschaftliche Tätigkeit** („Einrichtungsart“) – Angebot von Dienstleistungen oder Produkten gegen Entgelt
4. **Überschreiten des jeweils maßgeblichen Schwellenwerts („Size Cap Rule“)** – Mitarbeiteranzahl ODER Jahresumsatz/-bilanzsumme



# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

## Feststellung der Betroffenheit (3)

Sektor

Verwaltung IKT-Dienste

Einrichtungs-  
artendefinition

*Wann ist man  
im Sektor  
tätig?*

- (1) „**Managed Service Provider**“ oder „MSP“ ist eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne erbringt
- (2) „**Managed Security Service Provider**“ oder „MSSP“ ist ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt

# NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

## Risikomanagementmaßnahmen, Registrierungspflicht

- 1:1-Umsetzung der Mindestsicherheitsanforderungen der NIS-2-Richtlinie in das BSI-Gesetz
- Intensität der jeweiligen Maßnahme wird aus Gründen der Verhältnismäßigkeit u.a. zwischen den Kategorien differenziert
- Zu den Maßnahmen zählen u.a. Risikoanalysekonzepte, Maßnahmen zur Aufrechterhaltung des Betriebs (z.B. Backup-Management) und Konzepte zum Einsatz von Verschlüsselung
- Registrierungspflicht

# Meldepflichten

- **Sicherheitsvorfall** ist ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt
- **erheblicher Sicherheitsvorfall**
  - hat schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder kann diese verursachen, oder
  - hat Dritte durch erhebliche materielle oder immaterielle Schäden beeinträchtigt oder kann diese beeinträchtigen
- **Dreistufiges Meldesystem:** Erstmeldung binnen 24 Stunden, Update binnen 72 Stunden und ein Abschlussbericht der binnen eines Monats zu übermitteln ist

# Durchführungsverordnung der Kommission betreffend digitale Anbieter (1) – Überblick

- Regelung aufgrund Ermächtigung in Art. 21 Abs. 5 Uabs. 1 und Art. 23 Abs. 11 NIS-2-Richtlinie
- Betrifft Anbieter digitaler Dienste:
  - DNS-Dienstleister
  - TLD-Namensregister
  - Cloud-Computing-Dienstleister
  - Rechenzentrumsdienstleister
  - Anbieter von Content Delivery Networks
  - Managed Service Provider
  - Managed Security Service Provider
  - Anbieter von Online-Marktplätzen
  - Online-Suchmaschinen
  - Plattformen für soziale Netzwerke
  - Vertrauensdiensteanbieter

# Durchführungsverordnung der Kommission betreffend digitale Anbieter (2) – Inhalte

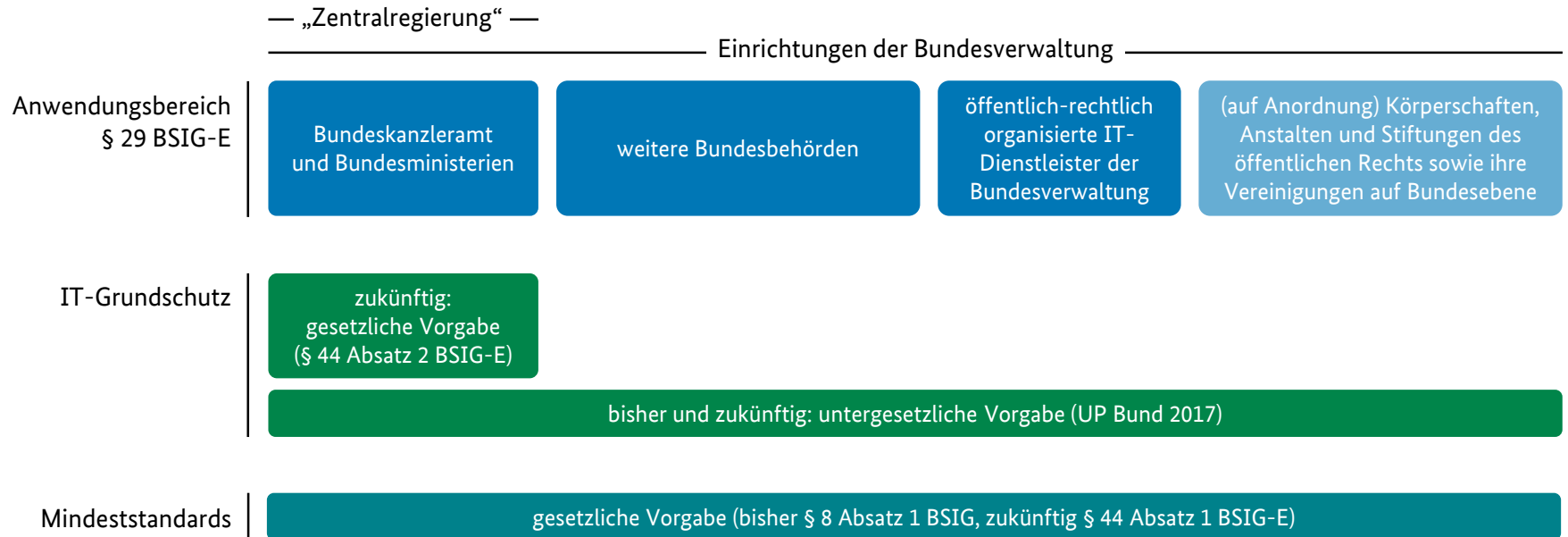
Regelungsgegenstand	Regelungsort
Anwendungsbereich	Art. 1
Konkretisierung der Cybersicherheitsanforderungen nach Art. 21 Abs. 2 NIS2	Art. 2, Annex
Sektorübergreifende Schwellenwerte für signifikante Sicherheitsvorfälle	Art. 3, 4
Sektorspezifische Schwellenwerte für signifikante Sicherheitsvorfälle	Art. 5-14
Inkrafttreten	Art. 16



# Durchführungsverordnung der Kommission betreffend digitale Anbieter (3) – Rechtsetzungsverfahren



# Vorgaben für die Einrichtungen der Bundesverwaltung (1)



# Vorgaben für die Einrichtungen der Bundesverwaltung (2)

## IT-Grundschutz

- Vorgehensweise zur Umsetzung eines ganzheitlichen Informations-sicherheitsmanagementsystems (ISMS) in Institutionen
- Besteht aus BSI-Standards 200-1, 200-2 und 200-3 und IT-Grundschutz-Kompendium
- Basiert auf ISO 27001
- Bis 2026 durch BSI zu modernisieren

## Mindeststandards

- Sollen Anforderungen des IT-Grundschutzes
  - konkretisieren (z.B. Mindestniveau definieren)
  - anpassen (für Besonderheiten der Bundesverwaltung)
  - ergänzen (z.B. Zusatzanforderungen)



# *Informationsangebote von BSI und BMI*

# Informationsangebot von BSI und BMI



<https://www.bmi.bund.de/nis2>

<https://www.bsi.bund.de/dok/nis-2>

Q & A

# Vielen Dank für Ihre Aufmerksamkeit!



Bundesministerium  
des Innern  
und für Heimat

## **Kontakt**

Referat CI 1 – Grundsatz;  
Cyber- und Informationssicherheit  
Thomas Sievers, Referent

Referat CI 3 – Cybersicherheit für Wirtschaft  
und Gesellschaft  
Maximilian Rath, Referent

E-Mail: [NIS2@bmi.bund.de](mailto:NIS2@bmi.bund.de)