# Kritische Infrastrukturen 2024

**OpenKRITIS Konferenz – Sicherheit in kritischen Infrastrukturen**

—

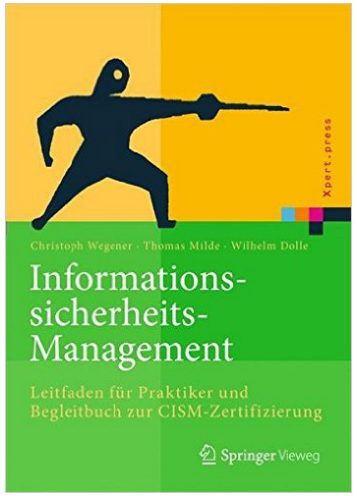
12. März 2024

# Zur Person Wilhelm Dolle

## Wilhelm Dolle (wdolle@kpmg.com)

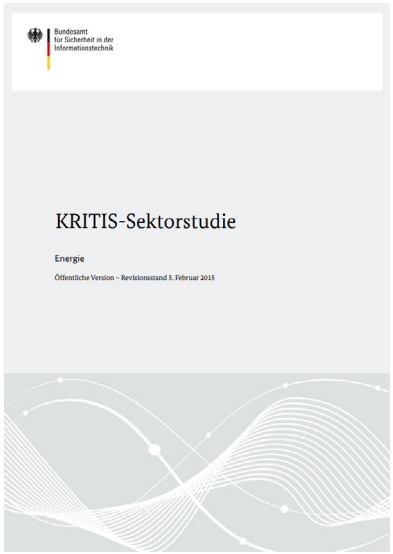
Partner, Head of Cyber Security KPMG und
Geschäftsführer KPMG Cert GmbH

- 10 Jahre Grundschutzauditor, Mitautor vom BSI IT-Grundschutz
- Leiter der §8a BSIG Prüfstelle, seit 2017 Ausbilder für KRITIS-Prüfer
- ISO 27001 Lead Auditor, ISO 22301 Lead Auditor, COBIT-/PRINCE2-/ITIL-zertifiziert
- Schwerpunkte: kritische Infrastrukturen, Cyber Sicherheit im Public Sector
- Mitglied in diversen Gremien:
  - Lenkungskreis Erfa KRITIS Audits
  - Sicherheitslagebild beim BSI
  - Expertenkreis Cyber Sicherheit beim BSI
- Vorlesungen an verschiedenen Hochschulen
- Zahlreiche Veröffentlichungen im Bereich Informationssicherheit



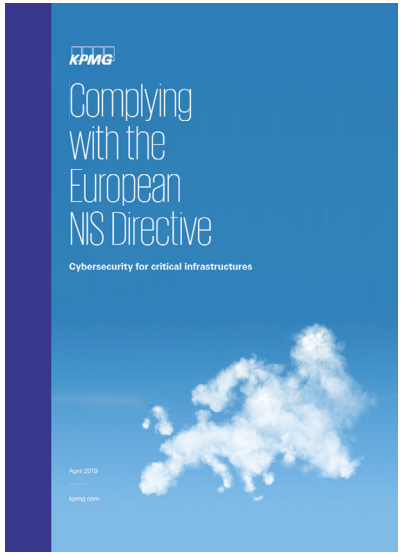
# Kritische Infrastrukturen und KPMG


2014 Studie mit dem BDI und Bitkom zum IT-SiG



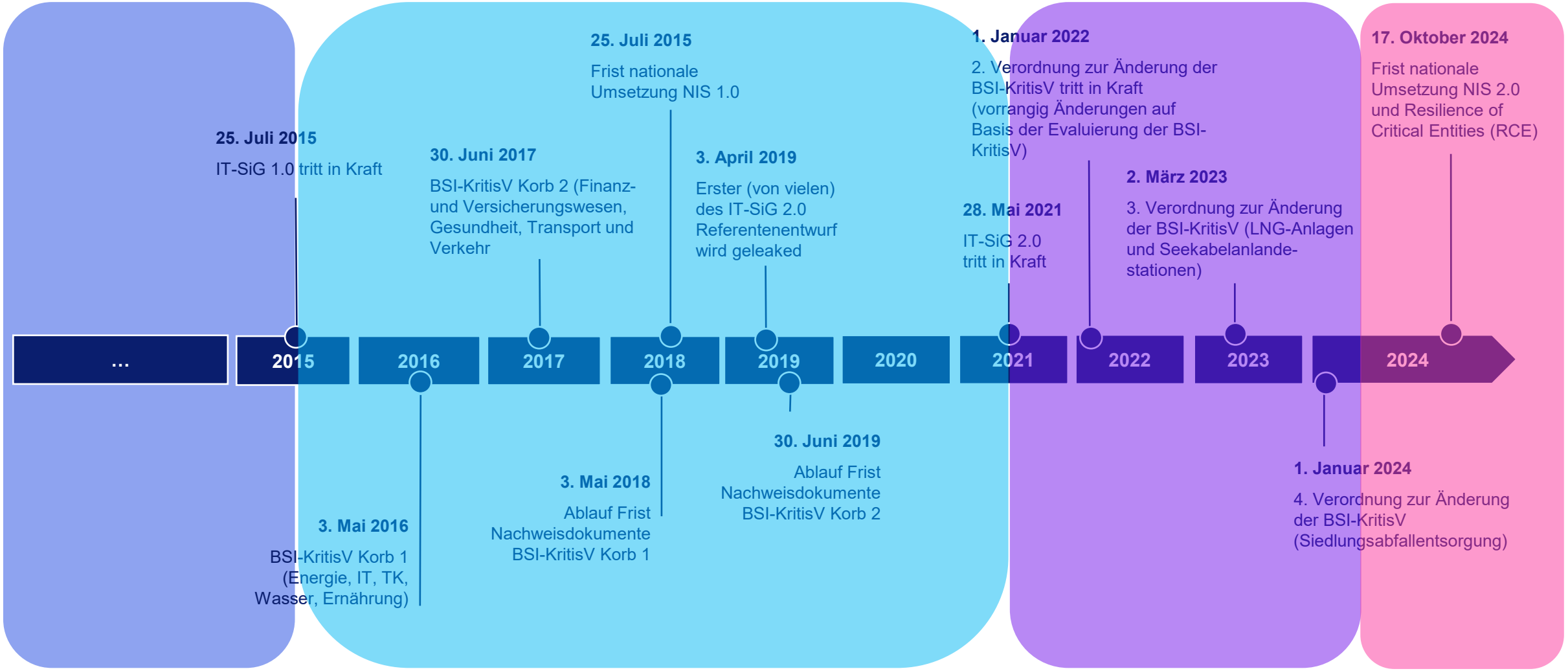

2014-2016 Fünf von 8 KRITIS-Sektorstudien des BSI


Seit 2016: diverse Erfahrungsaustausch-formate mit anderen Beratern, Prüfern, prüfenden Stellen, dem BSI und dem BMI




Seit 2016: diverse internationale Studien und Veröffentlichungen zum Thema NIS Directive

# Kurze Agenda (fast 9 Jahre IT-Sicherheitsgesetz)



# Die Zeit vor dem IT-Sicherheitsgesetz


https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/archiv-lagebericht_node.html

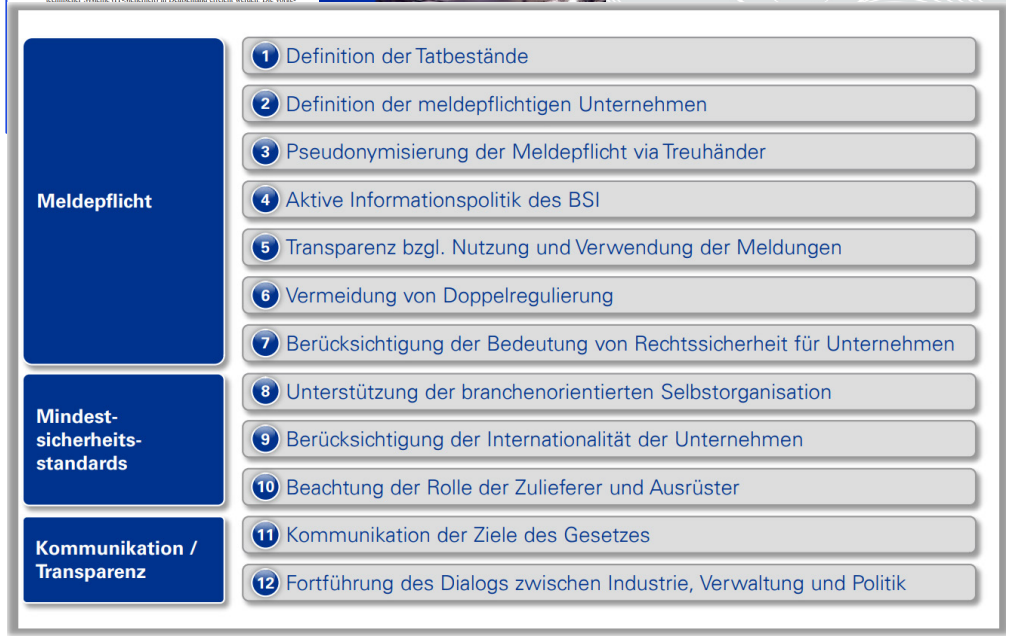
- Staat, Wirtschaft und Gesellschaft immer stärker vom Internet abhängig
- Cyber-Sicherheitslage in Deutschland (weiterhin) angespannt

- Freiwilligkeit in der Cyber-Sicherheit funktioniert nur sehr eingeschränkt

- Sehr unterschiedliches Cyber-Sicherheitsniveau in Unternehmen und Behörden (oft stark abhängig von Regulierung)
- Insbesondere die kritischen Infrastrukturen unterscheiden sich stark
  - 2011 verständigen sich Bund und die Länder auf eine einheitliche Einteilung der Kritischen Infrastrukturen (KRITIS) in 9 Sektoren
  - 2021 kommt Siedlungsabfallentsorgung dazu

- Idee: Analog zur Vorreiterrolle im Datenschutz möchte Deutschland zum sichersten Land der Welt / in Europa werden

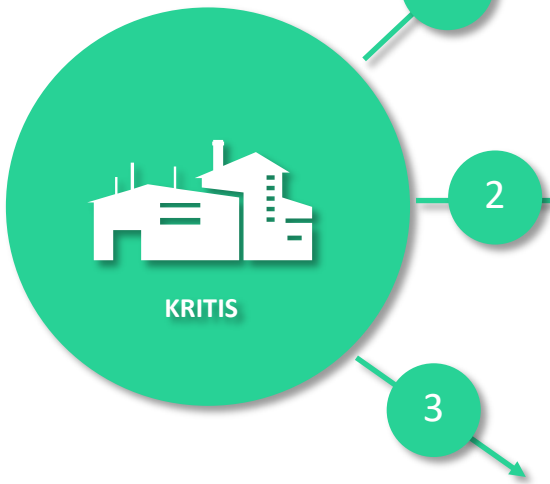
# Wie könnte ein IT-SiG aussehen (NIS Umsetzung)?


- Deutschland ging einen eher unkonventionellen, relativ komplexen Weg (später BSI KritisV Qualitäts- und Quantitätskriterien)
- Behörden/Ressorts wirkten nicht abgestimmt
- Europäische Sicht der regulierten Unternehmen wurde weitgehend ausgeblendet
- Deutsche Wirtschaft agiert sehr arbeitsteilig – Rolle der Zulieferer und Ausrüster fehlte
- Aufwände der Wirtschaft wurden nicht realitätsnah geschätzt
- Dialog zwischen Politik, Verwaltung und der Wirtschaft / Branchenverbänden war ausbaufähig

# Das IT-Sicherheitsgesetz 1.0

## Drei Hauptanforderungen an KRITIS-Betreiber




### Meldung von Sicherheitsvorfällen

Erhebliche **Sicherheitsvorfälle** müssen zeitnah erkannt, analysiert und bewertet werden. Ferner ist eine Meldung an das BSI als zuständige Behörde notwendig, wobei alle Anforderungen des BSI an zu meldende Informationen berücksichtigt werden müssen. Meldungen umfassen u.a. technische Rahmenbedingungen, vermutete oder tatsächliche Ursachen, betroffene Informationstechnik und die Art der betroffenen Einrichtung/Anlage.

### Etablierung von Sicherheitsstandards

Es müssen **allgemeine** (z.B. ISO/IEC 27001 oder BSI IT-Grundschutz) und **branchenspezifische Sicherheitsstandards** implementiert und gelebt werden. Dies betrifft sowohl organisatorische als auch technische Vorkehrungen und erfordert eine strukturierte, weitsichtige Lenkung aller Einzelmaßnahmen. Gefordert ist der „Stand der Technik“.

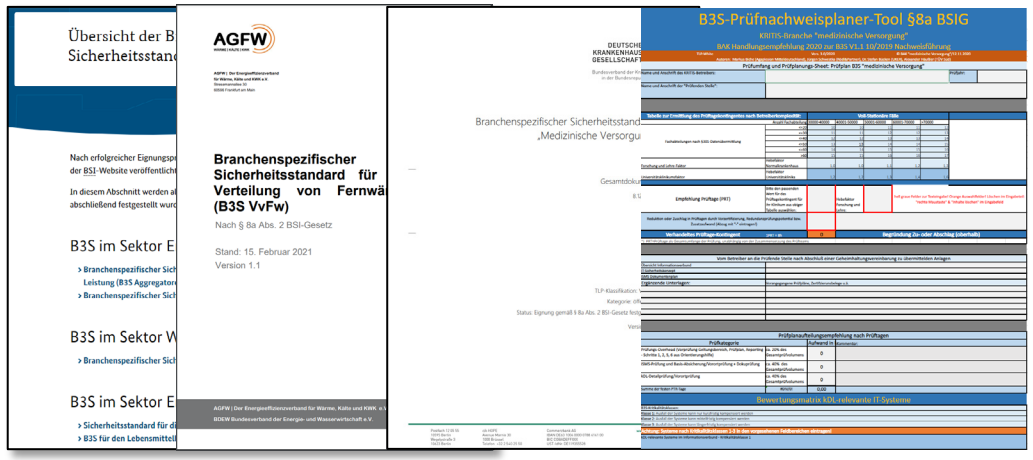
### Nachweis der Umsetzung

In regelmäßigen Zeitabständen muss die **Erfüllung der Vorgaben** zu Sicherheitsstandards und **Meldepflicht** gegenüber dem BSI **nachgewiesen** werden (z.B. durch Ergebnisberichte der Überprüfung). Hierfür müssen fortlaufend geeignete Nachweise gesammelt und durch Managementebenen ausgewertet werden.

# Herausforderungen in der Praxis

## Was ist Stand der Technik?








## Wer darf prüfen?

Akkreditierung bei der DAkkS zur ISO/IEC 27001-Zertifizierung (muss die Umsetzung und Einhaltung der ISO/IEC 17021-1 und ISO/IEC 27006 gegenüber der DAkkS nachweisen)

externes Quality Assessment gemäß „Internationalen Standards für die berufliche Praxis der internen Revision“ (IIA) bzw. DIIR-Revisionsstandard Nr. 3 „Prüfung von Internen Revisionssystemen (Quality Assessments)“ (DIIR)

**Geeignete prüfende Stelle**

Zertifizierung als IT-Sicherheitsdienstleister oder eine Anerkennung als Prüfstelle beim BSI

Zulassung als Wirtschaftsprüfungsinstitution beim IDW

individueller Nachweis der Eignung durch Selbsterklärung gegenüber dem BSI

**Prinzipiell kann z.B. auch eine interne Revisionsstelle geeignet sein!**

**Zusätzliche Prüfverfahrenskompetenz für § 8a BSIG**

**z.B. bestandene 2- bis 3-tägige Zusatzqualifikation**

| Kompetenz-bereiche | Audit-Kompetenz | IT-Sicherheits-Kompetenz | Branchen-Kompetenz |
|---|---|---|---|
| Kompetenz-anforderungen | z.B. Projektmanagement, Prüfmethoden, Tests, Fragetechniken, Berichtswesen, Teamkompetenz | z.B. IT und ISMS KnowHow, Sicherheitskonzeption, BCM, Asset-Management, Risikomanagement, ISO 2700x, IT-Grundschutz | Branchenkenntnisse und technisches Wissen im Bereich der Erbringung der kritischen Dienstleistungen des geprüften KRITIS-Betreibers; z.B. ICS, Branchenspezifische Gefährdungslage, Netzwerk-, Steuerungs- und Anlagentechnik |

# Das IT-Sicherheitsgesetz 2.0

## Wesentliche Änderungen

### Aufgaben und Befugnisse des BSI

- Marktbeobachtung, Testung & Entwicklung sicherer IT-Produkte, Vergabe IT-Sicherheitskennzeichen
- Anordnungsbefugnisse ggü. IT-Dienstleistern und Dienstanbietern für Verwaltungs-TK & ggü. KRITIS-Betreibern zur Auskunft
- Fungieren als nationale Behörde für EU-Cybersicherheitszertifizierung darunter Ernennung Überwachung von Konformitätsbewertungsstellen
- Befugnis in ungeschützten IT-Systeme der „Weißen Liste“ Sicherheitslücken zu detektieren

### Erweiterung schutzwürdiger Akteure

- Neuer KRITIS-Sektor Siedlungsabfallentsorgung
- Unternehmen im besonderen öffentlichen Interesse (UBI)
- KRITIS-Komponenten-Hersteller: Vertrauenswürdigkeitserklärung
- Erweiterung der KRITIS-Betreiber durch Herabsenkung von Schwellenwerten und der Erweiterung der KRITIS-Anlagen

### Pflichten für Akteure

- Registrierungspflicht beim BSI
- Auskunftspflicht ggü. dem BSI (drohende Sanktionierung)
- Anzeigepflicht beim erstmaligen Einsatz Kritischer Komponenten, die einer Zertifizierungspflicht unterliegen
- Explizite Nennung von Angriffserkennung im Kontext „Stand der Technik“
- Bußgeldhöhe für Betreiber zu Abschreckungszwecken deutlich erhöht

# Spezifizierung der Prüfungsinhalte



PE.1 Reifegrad des ISMS

1. Bewertung des Reifegrads
   - 1 ☐ ISMS ist geplant, aber nicht etabliert.
   - 2 ☐ ISMS ist zum Teil etabliert.
   - 3 ☐ ISMS ist etabliert und dokumentiert.
   - 4 ☐ Zusätzlich zum Reifegrad 3 wurde das ISMS regelmäßig auf Effektivitä
   - 5 ☐ Zusätzlich zum Reifegrad 4 wurde das ISMS regelmäßig verbessert.
2. Begründung der vorgenommenen Bewertung des Reifegrads des ISMS

PE.2 Reifegrad des BCMS

1. Bewertung des Reifegrads
   - 1 ☐ BCMS ist geplant, aber nicht etabliert.
   - 2 ☐ BCMS ist zum Teil etabliert.
   - 3 ☐ BCMS ist etabliert und dokumentiert.
   - 4 ☐ Zusätzlich zum Reifegrad 3 wurde das BCMS regelmäßig auf Effektivität überprüft.
   - 5 ☐ Zusätzlich zum Reifegrad 4 wurde das BCMS regelmäßig verbessert.
2. Begründung der vorgenommenen Bewertung des Reifegrads des BCMS

1. Bewertung des Umsetzungsgrads
   - 0 ☐ Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.
   - 1 ☐ Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
   - 2 ☐ In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen[7] erfüllt worden.
   - 3 ☐ Alle MUSS-Anforderungen[7] wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.
   - 4 ☐ Alle MUSS-Anforderungen[7] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
   - 5 ☐ Alle MUSS-Anforderungen[7] wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse/Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

# Anpassung der BSI-KritisV - (historisches) Beispiel Energie

## Fernwärmeversorgung

Kritische DL: Erzeugung, *Steuerung, Überwachung* und Verteilung

**Schwellenwerte**

- Erzeugung: Durchschnittlich 2300 GWh/Jahr ausgeleitete Wärmeleistung
- Verteilung: 250.000 angeschlossene Haushalte
- *Steuerungsanlage: 250.000 Haushalte oder 2.300 GWh/Jahr*

## Stromversorgung

Kritische DL: Erzeugung, Übertragung und Verteilung

**Schwellenwerte**

- ~~Stromerzeugung (zentral / dezentral): 420 MW Leistung~~
- *Erzeugungsanlage: 104 MW, 0 MW (Schwarzstartanlage), 36 MW (Erbringung Primärregelleistung)*
- ~~Speicheranlage: 420 MW Leistung~~
- *Anlage oder System zur Steuerung/Bündelung elektrischer Leistung : 104 MW, 0 MW (Schwarzstartanlage), 36 MW (Erbringung Primärregelleistung)*
- Übertragungsnetz: 3.700 GWh/Jahr
- Zentrale Anlagen/Systeme Stromhandel: ~~200~~ *3,7* TWh/Jahr
- Verteilernetz: 3.700 GWh/Jahr
- ~~Messstelle für Leistung angeschlossener Verbraucherstellen/Einspeisung: 420 MW~~

## Gasversorgung

Kritische DL: Förderung, Transport, *Handel* und Verteilung

**Schwellenwerte**

- Gasförderanlage: 5.190 GWh/Jahr
- *Gassteuerungsanlage: 5.190 GWh/Jahr*
- Gasspeicher: 5.190 GWh/Jahr
- Fernleitungsnetz: 5.190 GWh/Jahr
- *Gasgrenzübergabestelle: 5.190 GWh/Jahr*
- Verteilernetz: 5.190 GWh/Jahr
- *Gashandelssystem: 5.190 GWh/Jahr*

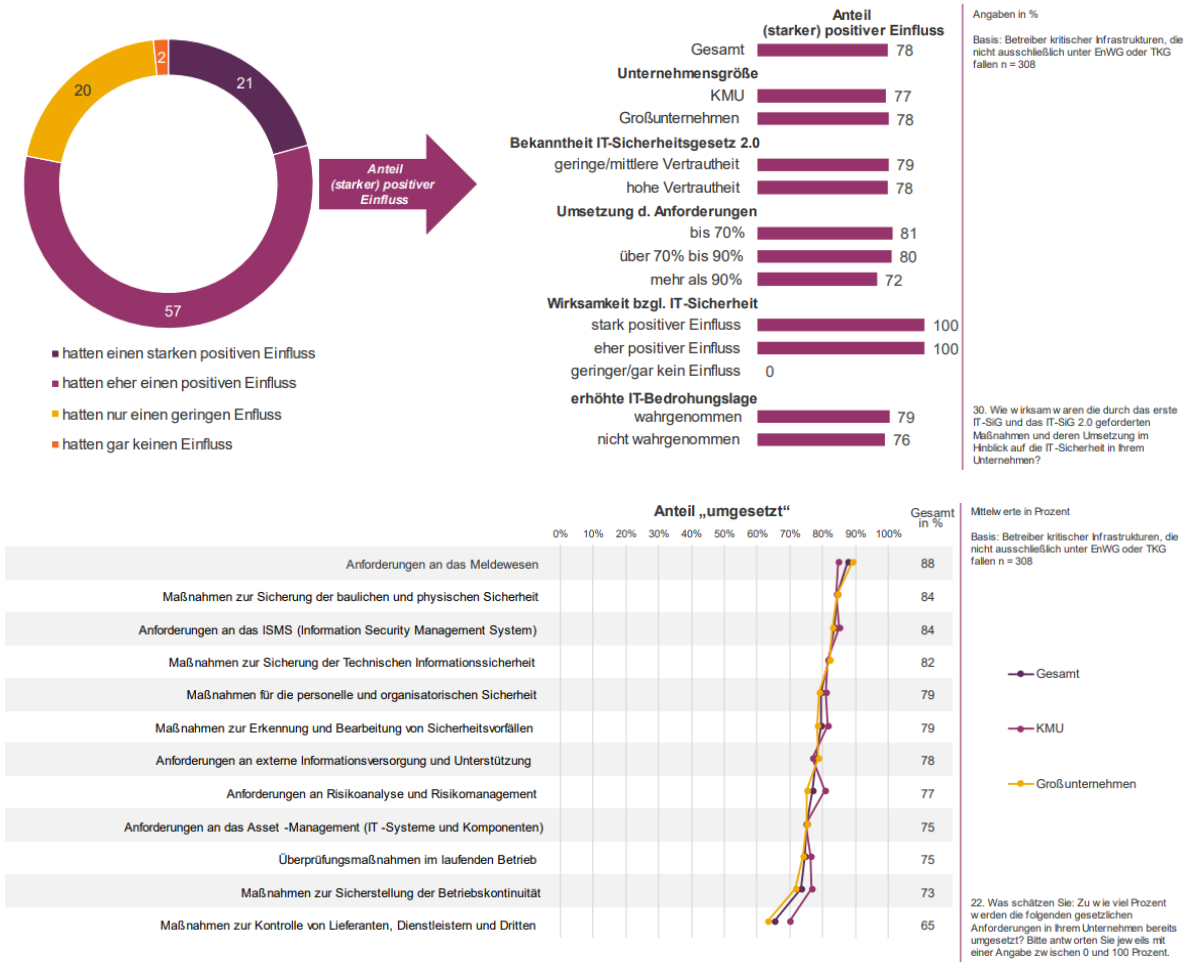
## Kraftstoff- und Heizölversorgung

Kritische DL: Rohölförderung, Produktherstellung, *Mineralölhandel*, Öltransport und Kraftstoff- und Heizölverteilung

**Schwellenwerte**

- Ölförderanlage: 4,4 Mio. Tonnen Rohöl/Jahr
- Raffinerie: 420.000 Tonnen Kraftstoff/Jahr oder 620.000 Tonnen Heizöl/Jahr *oder 63.750 Tonnen Flugkraftstoff / Jahr*
- *Steuerungsanlage & Mineralölfernleitung: Gefördertes / transportiertes Rohöl 4,4 Mio. Tonnen/Jahr oder 420.000 Tonnen Kraftstoff/Jahr oder 63.750 Tonnen Flugkraftstoff / Jahr oder 620.000 Tonnen Heizöl/Jahr*
- Öl- und Produktenlager sowie Kraftstoff- & Heizölverteilung : 4,4 Mio. Tonnen Rohöl/Jahr oder 420.000 Tonnen Kraftstoff/Jahr oder 620.000 Tonnen Heizöl/Jahr *oder 63.750 Tonnen Flugkraftstoff / Jahr*
- *Mineralölhandel: 4,4 Mio. Tonnen Rohöl/Jahr oder 420.000 Tonnen Kraftstoff/Jahr oder 620.000 Tonnen Heizöl/Jahr oder 63.750 Tonnen Flugkraftstoff / Jahr*

# Evaluierung des IT-Sicherheitsgesetzes




- Online Befragung im Februar/März 2023 mit insgesamt 379 KRITIS-Unternehmen (von ca. 1.800 registrierten Betreibern)
- Zusätzlich Input von weiteren Fachkreisen wie UP KRITIS, verschiedene Fachverbände Kritischer Infrastrukturen, einschlägige Universitäten und Forschungseinrichtungen im Bereich der IT-Sicherheit, das Institut der Wirtschaftsprüfer sowie Vertreter der Zivilgesellschaft, darunter die AG KRITIS und die Stiftung Neue Verantwortung.
- Die Wirksamkeit des ersten IT-SiG sowie des IT-SiG 2.0 kann daher insgesamt als gut bewertet werden.
- An einigen Stellen Wirksamkeitslücken sowie konkrete Änderungs- und Konkretisierungsbedarfe festgestellt.
- Sie sollten, wenn möglich, im Zuge der NIS-2 Umsetzung oder weiterer erforderlicher Gesetzesanpassungen sowie im Rahmen zur Verfügung stehender Haushaltsmittel umgesetzt werden.

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/evaluierung-itsig2-ergebnisbericht.pdf

# Die aktuelle Lage 2024

PSI-SOFTWARE-HACK

## KRITIS-Spezialist bestätigt Ransomware-Angriff

Wie die PSI Software AG mitteilt, ist eine Ransomware-Attacke für seine vor kurzem bekanntgewordenen Security-Turbulenzen verantwortlich.

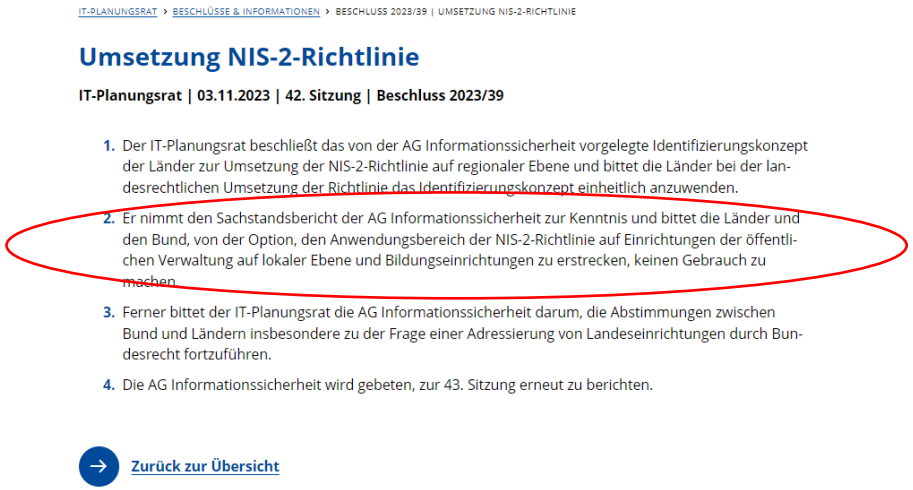
**Von Redaktion CSO**

CSO | 21. FEBRUAR 2024 07:58 UHR


Eine Ransomware-Attacke hat die internen Systeme des KRITIS-Spezialisten PSI lahmgelegt. Kundendaten sollen dabei nicht kompromittiert worden sein.

https://www.csoonline.com/de/a/hacker-legen-kritis-dienstleister-lahm,3681265

- Cyber-Sicherheitslage in Deutschland (weiterhin) angespannt
- Deutlich besseres Cyber-Security Niveau als vor 10 Jahren (lange noch nicht ausreichend)
- Cyber-Sicherheit ist in der „Chef-Etage“ angekommen (Vorstände, Aufsichtsräte, Geschäftsführer)
- Der öffentliche Sektor hinkt (weit) hinterher (Bund > Land > Kommune)



IT-PLANUNGSRAT › BESCHLÜSSE & INFORMATIONEN › BESCHLUSS 2023/39 | UMSETZUNG NIS-2-RICHTLINIE

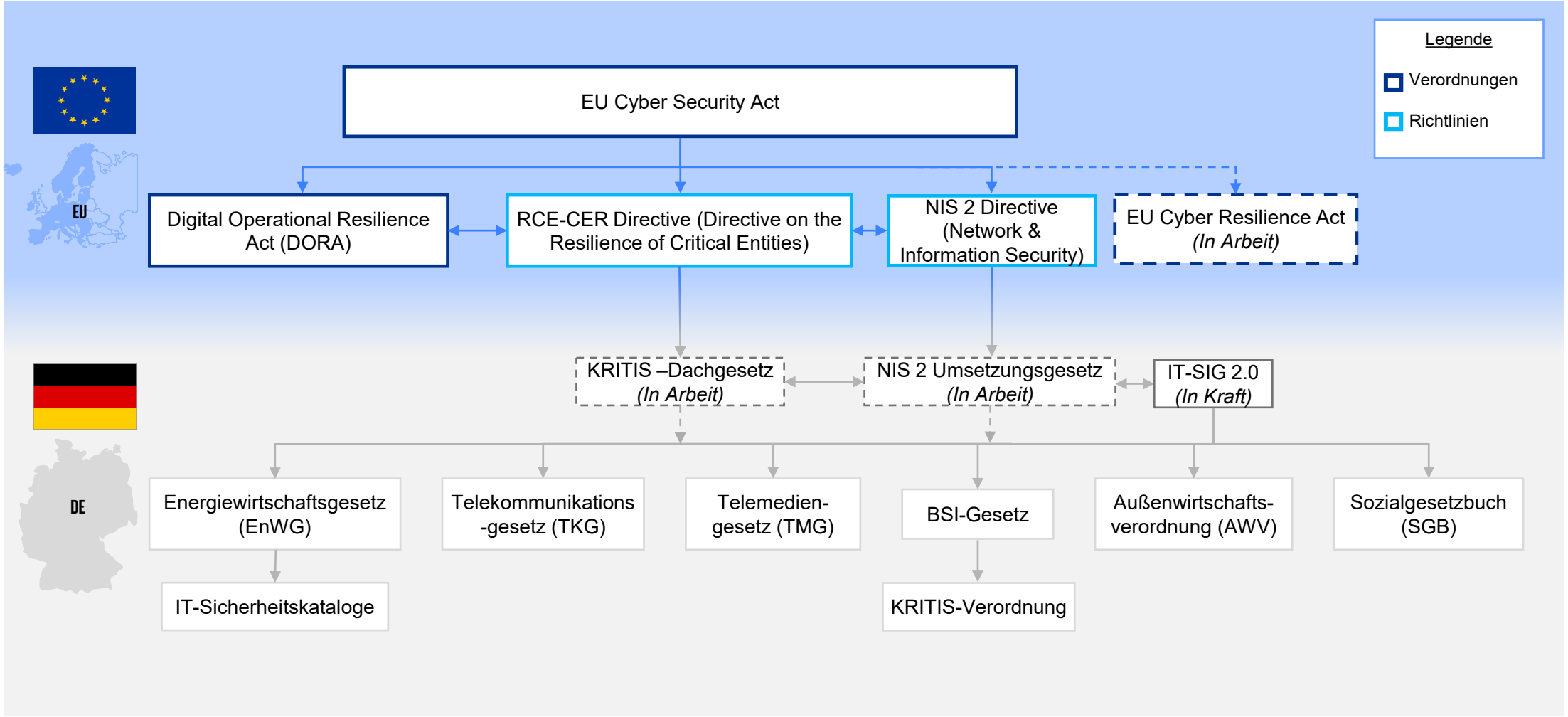
**Umsetzung NIS-2-Richtlinie**

**IT-Planungsrat | 03.11.2023 | 42. Sitzung | Beschluss 2023/39**

1. Der IT-Planungsrat beschließt das von der AG Informationssicherheit vorgelegte Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie auf regionaler Ebene und bittet die Länder bei der landesrechtlichen Umsetzung der Richtlinie das Identifizierungskonzept einheitlich anzuwenden.
2. Er nimmt den Sachstandsbericht der AG Informationssicherheit zur Kenntnis und bittet die Länder und den Bund, von der Option, den Anwendungsbereich der NIS-2-Richtlinie auf Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene und Bildungseinrichtungen zu erstrecken, keinen Gebrauch zu machen.
3. Ferner bittet der IT-Planungsrat die AG Informationssicherheit darum, die Abstimmungen zwischen Bund und Ländern insbesondere zu der Frage einer Adressierung von Landeseinrichtungen durch Bundesrecht fortzuführen.
4. Die AG Informationssicherheit wird gebeten, zur 43. Sitzung erneut zu berichten.

Zurück zur Übersicht

# Die aktuelle Lage 2024 - Ausblick



# Kontakt

KPMG AG
Wirtschaftsprüfungsgesellschaft

**Wilhelm Dolle**
Partner, Consulting Cyber Security
T +49(0)30 20682323
wdolle@kpmg.com

**kpmg.de/socialmedia**

**kpmg.de**