



# DAS NEUE IT-SICHERHEITSGESETZ - SEGEN ODER FLUCH?

Jens Marschall

Deutsche Telekom AG, Group Security Governance



ERLEBEN, WAS VERBINDET.

# ÜBERBLICK DIE THEMEN

1. Eckdaten
2. Zielsetzungen
3. Kritische Sektoren
4. Pflichten für den TK-Sektor
5. Pflichten für den IT-Sektor
6. Fazit



# 1. ECKDATEN

**VERABSCHIEDET:**

12. JUNI 2015

**INKRAFTGETRETEN:**

25. JULI 2015

**WIRKUNGSGRAD:**

UMSTRITTEN

**GESETZESART:**

ARTIKELGESETZ

**EVALUIERUNG:**

NACH 4 JAHREN

**ZAHL GEÄNDERTER GESETZE:**

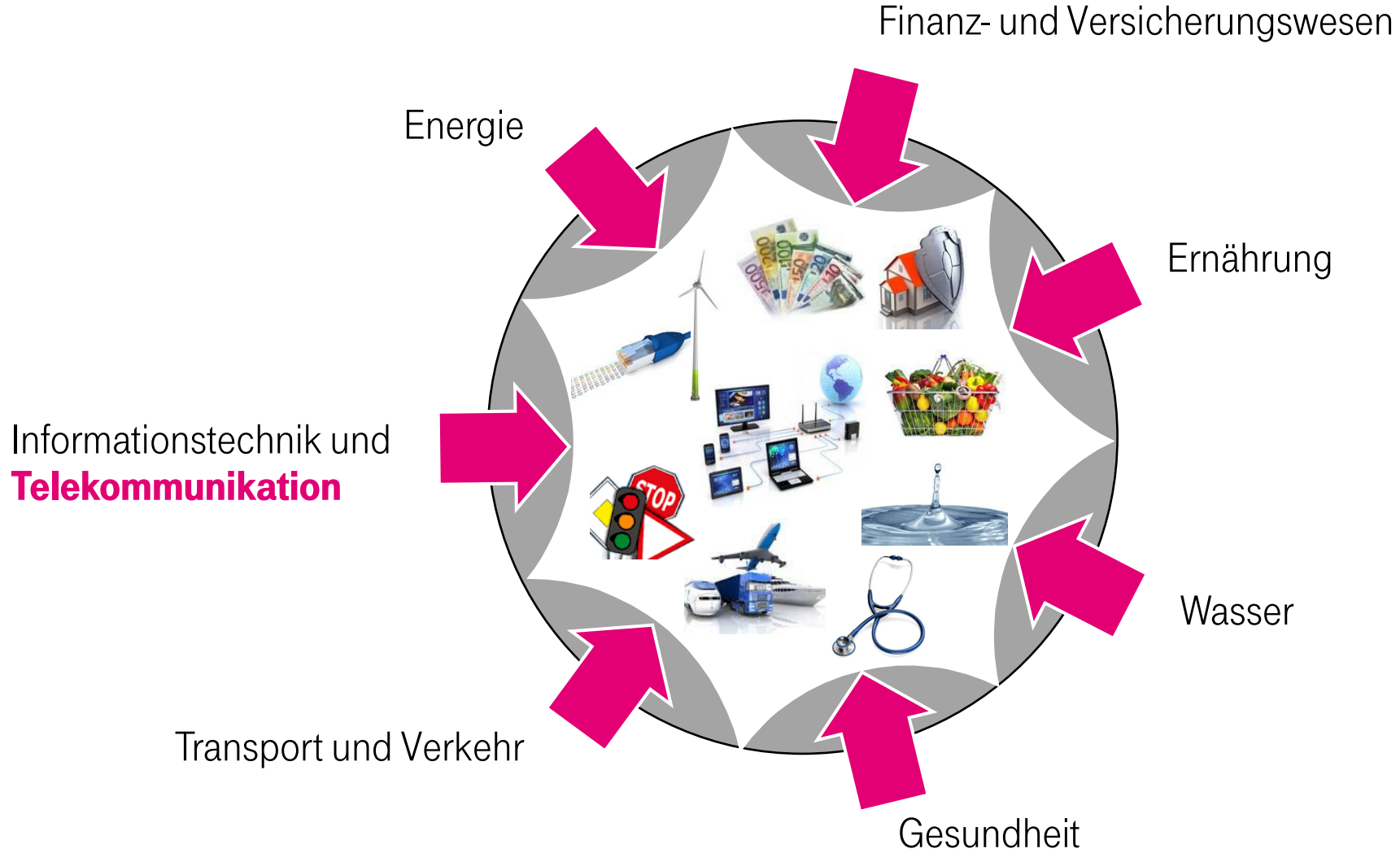
8

# 2. ZIELSETZUNGEN

- Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen einführen
- Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit datenverarbeitender Systeme verbessern – an die gestiegene Bedrohungslage anpassen
- Bürgerinnen und Bürger in einem sicheren Netz schützen
- IT-Sicherheit bei Unternehmen verbessern
- IT-Sicherheit der Bundesverwaltung ausbauen
- BSI und Bundeskriminalamt (BKA) stärken



# 3. KRITISCHE SEKTOREN



# 3. DIE KRITISCHEN SEKTOREN

## KRITISCHE INFRASTRUKTUR

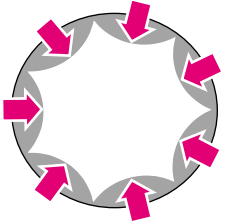


Einrichtungen, Anlagen oder Teile hiervon, [die bestimmten Sektoren angehören] und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden

*§ 2 Abs. 10 BSI-Gesetz*



# 4. ANWENDUNGSBEREICH



**Kritische Sektoren** werden insb. durch die §§ 8a und 8b BSI-Gesetz verpflichtet.

Ausnahmen:

- **Telekommunikationsanbieter**, Betreiber von Energieanlagen oder –netzen und Genehmigungsinhaber nach dem Atomgesetz sind von den neuen BSIG-Pflichten befreit, § 8 c Abs. 2 BSIG. Für diese gelten die spezielleren Gesetze (TKG, TMG).
- Kleinunternehmen sind ebenfalls vom Anwendungsbereich des BSIG ausgenommen, § 8 c Abs. 1 BSIG.



# 5. PFLICHTEN FÜR DEN TK-SEKTOR

## TECHNISCHE SCHUTZMAßNAHMEN - § 109 TKG

**ANHEBUNG!**

Maßnahmen		Alt	Neu
	<p><u>§ 109 Abs. 2 TKG:</u> Schutz von Telekommunikations- und Datenverarbeitungssystemen</p>	Angemessen	<b>Stand der Technik</b>
	<p><u>§ 109 Abs. 4 TKG:</u> Umsetzung des Siko durch die BNetzA</p>	Kann prüfen	<b>Soll mindestens alle 2 Jahre erfolgen</b>
	<p><u>§ 109 Abs. 5 TKG:</u> Meldepflicht bzgl. Störungen und Sicherheitsverletzungen</p>	Nur bei Eintritt	<b>Wenn Eintritt möglich ist</b>





# 5. PFLICHTEN FÜR DEN TK-SEKTOR

## INFORMATION DER NUTZERINNEN - § 109a TKG

NEU!

### Maßnahme




- Information der Nutzer über Verletzungen der IT-Sicherheit, die von deren datenverarbeitenden System ausgehen



# 5. PFLICHTEN FÜR DEN TK-SEKTOR

## ERHEBUNG / VERWENDUNG VON DATEN- § 100 ABS. 1 TKG

Maßnahme	Alt	Neu
	<ul style="list-style-type: none"><li>Bestands- und Verkehrsdaten erheben und verwenden für Erkennung, Eingrenzung und Beseitigung von Störungen</li></ul>	<p><b>Auch bei Störungen an Informations- und Kommunikationsdiensten</b></p>

**ANHEBUNG!**

# 5. PFLICHTEN FÜR DEN TK-SEKTOR

## SCHUTZ VON TELEMEDIENDIENSTEN - § 13 TMG

NEU!

### Maßnahmen



### Vorkehrungen gegen

- unerlaubten Zugriff auf techn. Einrichtungen
- Verletzung personenbezogener Daten
- Störungen
- ✓ nach dem Stand der Technik
- ✓ soweit wirtschaftlich zumutbar



# 6. PFLICHTEN FÜR IT-SEKTOR

## SICHERHEITSMABNAHMEN NACH § 8a BSI-GESETZ

### Maßnahmen



- Angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der Systeme, Komponenten und Prozesse.
- die für die Funktionsfähigkeit Kritischer Infrastrukturen maßgeblich sind
- Stand der Technik

**2jährige Umsetzungsfrist  
läuft frühestens Ende 2017 ab**

**NEU!**

Nachweispflicht  
mindestens alle 2 Jahre

# 6. PFLICHTEN FÜR IT-SEKTOR

## SICHERHEITSMABNAHMEN NACH § 8b BSI-GESETZ

### Maßnahmen



- Einrichtung Kontaktstelle für BSI.
- Meldung von Störungen an Systemen, Komponenten oder Prozessen an das BSI die zu einer Beeinträchtigung / einem Ausfall geführt haben oder führen können.
- Mitwirkung an Beseitigung oder Vermeidung von Störungen.

**NEU!**

**6monatige  
Umsetzungsfrist  
läuft frühestens  
Mitte 2016 ab**

# FAZIT

## SEGEN ODER FLUCH?

- **Detaillierte Meldepflichten** sind Basis der Schaffung höherer Transparenz hinsichtlich der IT-Sicherheitslage.
- **Höhere Transparenz** ist Grundlage für wirkungsvolle Maßnahmen zur Vermeidung und Beseitigung von Störungen Kritischer Infrastrukturen.
- **Abmilderung der Auswirkungen** von Störungen dieser Systeme tragen der immer stärkeren Abhängigkeit Rechnung.
- **Konkretisierung der Pflichten** ist erforderlich.
- Anwendungsbereich muss möglichst **alle relevanten Strukturen erfassen**, bspw. Bundes- und Landesverwaltungen.



HACKER-ATTACKE KÜRZ VOR DER AUFKLÄRUNG

# Jens Marschall

## Rechtsanwalt

Deutsche Telekom AG  
Group Security Governance  
Public Safety

53111 Bonn  
Friedrich-Ebert-Allee 140

E-Mail: [jens.marschall@telekom.de](mailto:jens.marschall@telekom.de)  
Internet: [www.telekom.com](http://www.telekom.com)