# Rechtliche Anforderungen an die IT-Sicherheit in der Energiewirtschaft

Dipl.-Ing. Kay Tidten
Abteilung Betriebswirtschaft, Steuern und Digitalisierung
BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
E-Mail: kay.tidten@bdew.de
Tel: +49 30 300 199 1526

# Die BDEW-Hauptgeschäftsstelle Berlin

**Außenansicht**

**Konferenzbereich außen**

# Interessenvertretung vor Ort – Die Landesgruppen und Landesverbände

bdew
Energie. Wasser. Leben.

bdew
Energie. Wasser. Leben.
Landesgruppe
Norddeutschland

**Landesgruppe Norddeutschland: Hamburg**

bdew
Energie. Wasser. Leben.
Landesgruppe
Nordrhein-Westfalen

**Landesgruppe Nordrhein- Westfalen: Bonn**

LDEW
Hessen/Rheinland-Pfalz

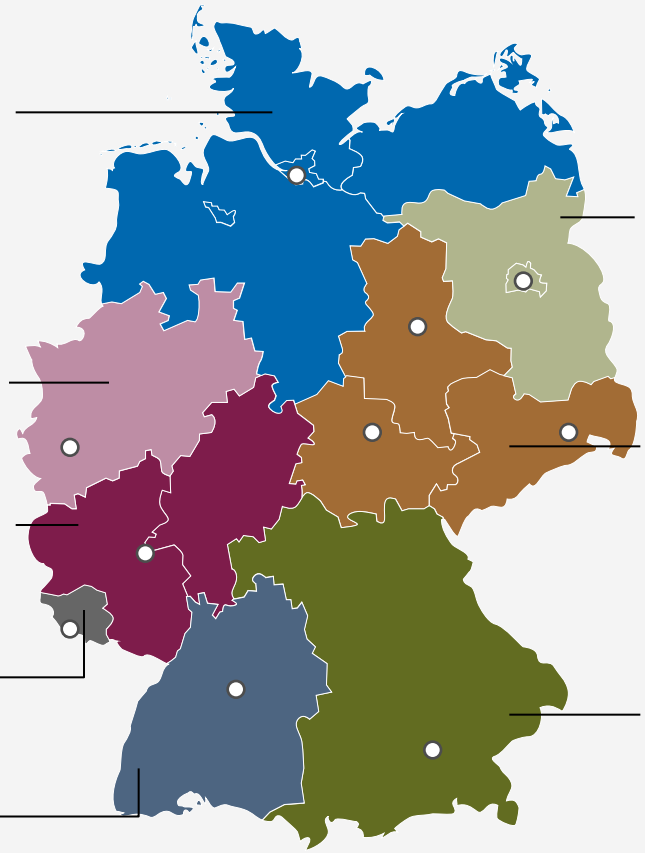
**LDEW Hessen /Rheinland-Pfalz: Mainz**

vewsaar
Energie. Wasser. Leben.

**VEWSaar Saarland: Saarbrücken**

vfew

**VfEW Baden-Württemberg: Stuttgart**



bdew
Energie. Wasser. Leben.
Landesgruppe
Berlin | Brandenburg

**Landesgruppe Berlin/Brandenburg: Berlin**

bdew
Energie. Wasser. Leben.
Landesgruppe
Mitteldeutschland

**Landesgruppe Mitteldeutschland: Dresden, Erfurt, Magdeburg**

VBEW
Energie. Wasser. Leben.

**VBEW Bayern: München**

# Ausgangslage

BDEW extra 7/2016

bdew
Energie. Wasser. Leben.

WIRED /LATEST 1049/4119 NÄCH

ZEIT ONLINE

Politik Gesellschaft Wirtschaft Kultur Wissen Digita

Energie

IT-Sicherheit: Verfassungsschutz warnt v

Suche

bizz energy. Das Wirtschaftsmagazin für die Energiezukunft

Log In
onomy Companies Tech Autos Video stock tickers

Wirtschaftsclub ePaper Archiv Abo Veranstaltungen Freitag, 04.11.2016 Login | Registrieren

Bundesregierung

## De Maizière w
## Stromversorg

Der Innenminister hält Attacke
Stromnetz für möglich. Mit der
Bevölkerung darauf vorbereite

24. August 2016, 16:26 Uhr / Quelle: ZEI

ZUR US-WAHL: 6 WOCHEN GRATIS.

Handelsblatt

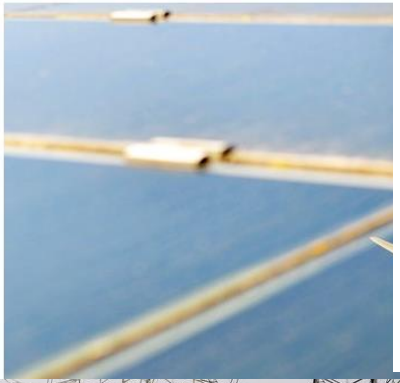
Suchbegriff, WKN, ISIN

Digitalpass Finanzen Unternehmen Politik Technik Auto Sport Panorama Social Media Video Service

IT + Internet Gadgets Forschung + Innovation Medizin Energie + Umwelt

Handelsblatt > Technik > Mit Sicherheit im Netz > Hackerangriffe: Offene Flanke Cybersicherheit

MIT SICHERHEIT IM NETZ



HACKERANGRIFFE

## Offene Flanke Cybersicherheit

von: Dana Heide
Datum: 03.11.2016 06:00 Uhr

Cyberangriffe auf Unternehmen und staatliche Institutionen werden immer heftiger. Die Bundesregierung hat das Problem erkannt und legt nun ihren Strategie-Entwurf dagegen vor. Auch die Wirtschaft soll sich einbringen.

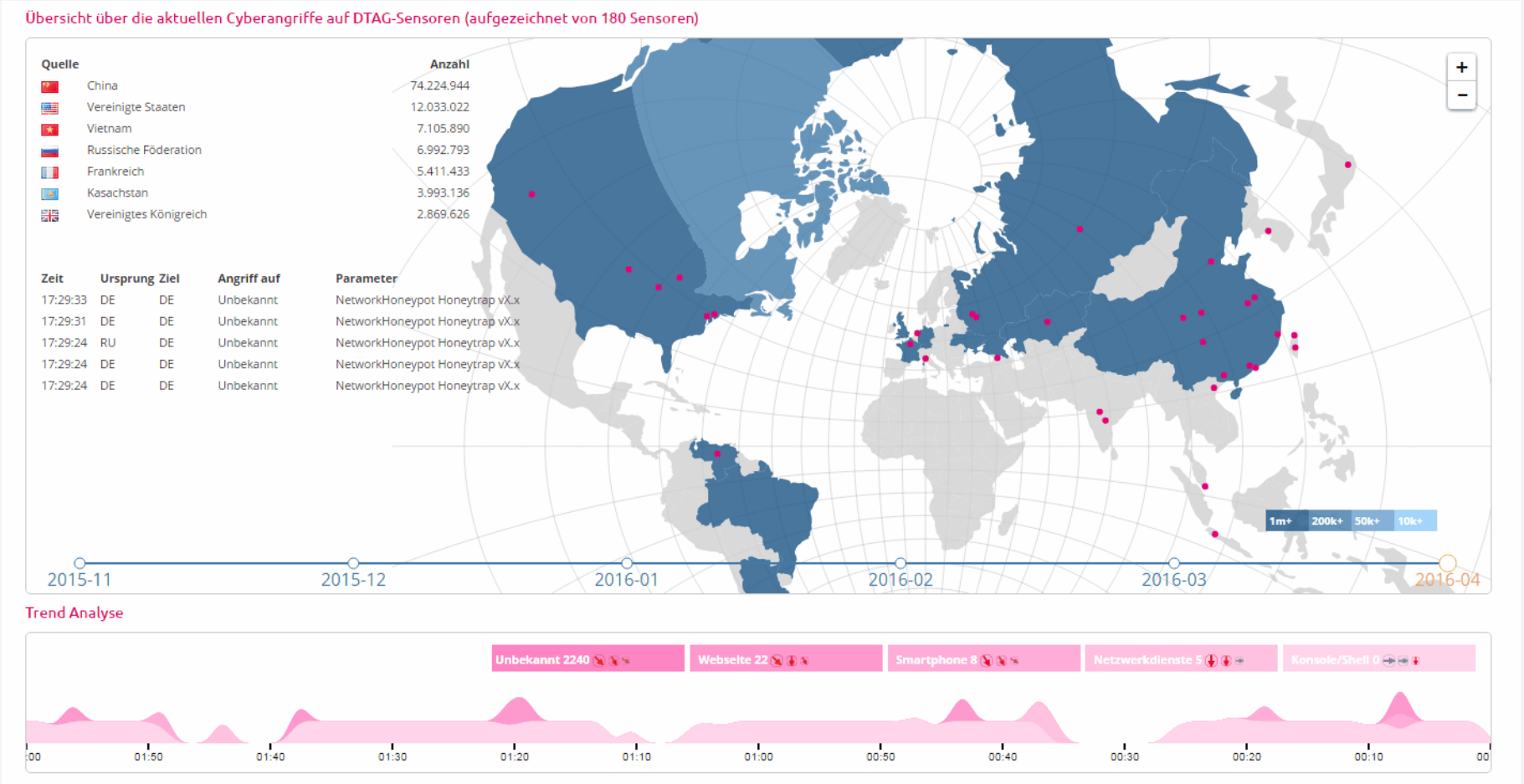


They even managed to infect at least three energy companies with Cryptolocker ransomware, a

Finance Management Media

# Live-Attacks on Deutsche Telekom Honeypots (www.sicherheitstacho.eu)

bdew
Energie. Wasser. Leben.



# IT-Sicherheit im Kontext zunehmender Digitalisierung

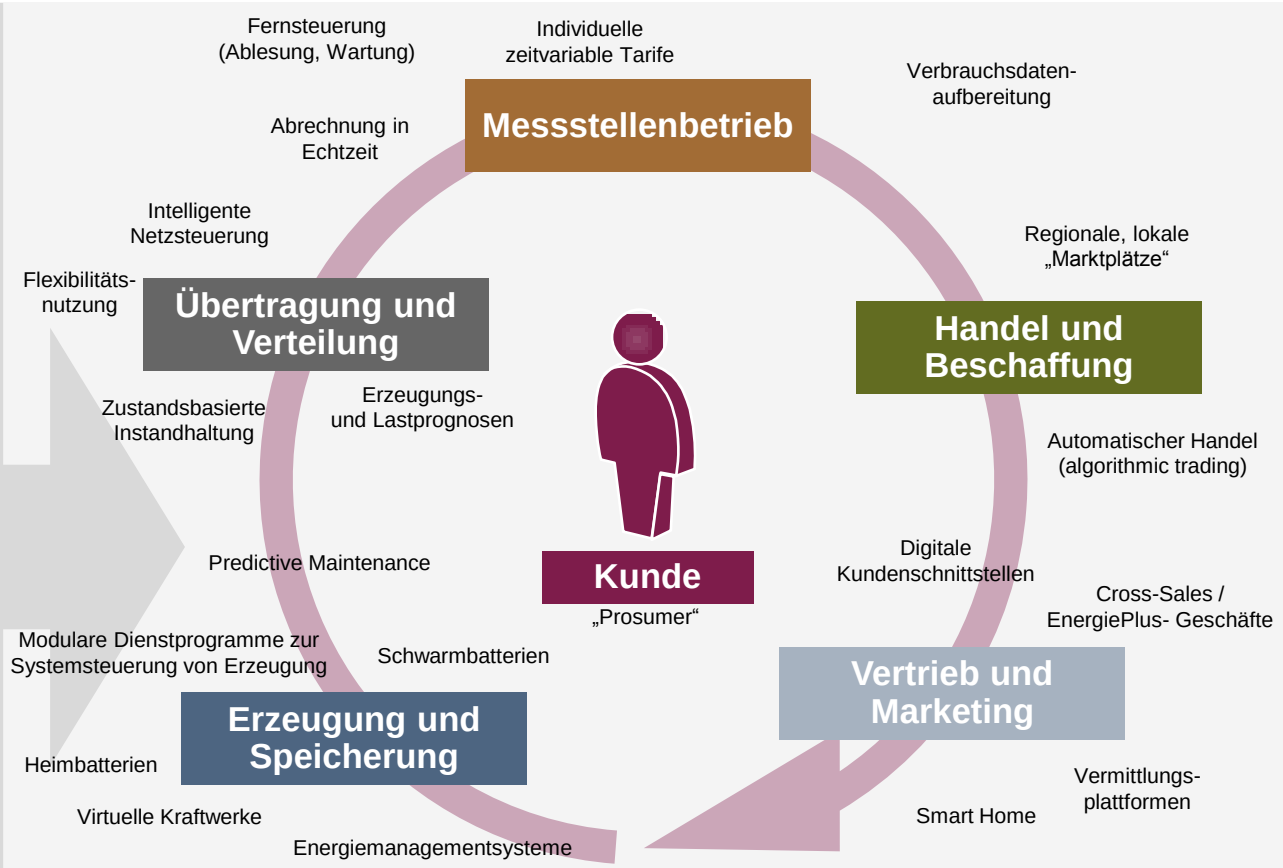
bdew
Energie. Wasser. Leben.

**Technologien**:
Internettechnologien
Big Data
Cloud Computing
Mobile

**Neue Geschäftsprozesse und -modelle**
**Neue Wettbewerber**

**Energiewirtschaftliche Treiber:**
Ausbau Erneuerbare
Roadmap Smart Grid
Flexibilisierung & Vernetzung

**Kundennachfrage und Anbieterdruck**




**Von Wertschöpfungsstufen zum Wertschöpfungsnetzwerk**

**Die Anforderungen des (digitalen) Kunden stehen im Mittelpunkt**

# IT-Sicherheitsanforderungen in der Energiewirtschaft

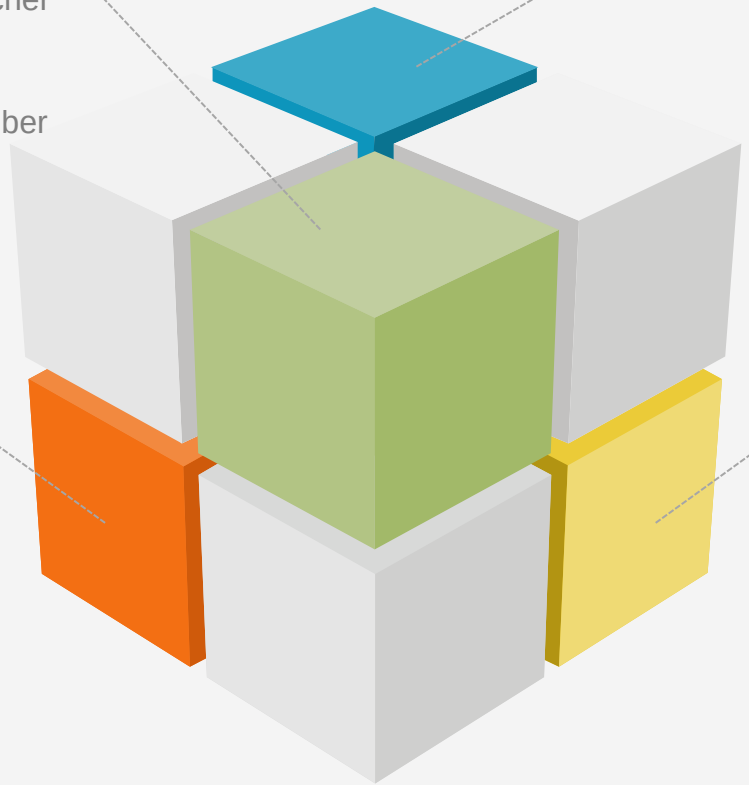
bdew
Energie. Wasser. Leben.

## 01 IT-Sicherheitsgesetz

- In Kraft getreten am 24. Juli 2015
- IT-Sicherheitsmindeststandards für Netzbetreiber sowie Betreiber Kritischer Infrastrukturen (KRITIS)
- Meldepflichten für erhebliche IT-Sicherheitsvorfälle für KRITIS-Betreiber

## 02 EU-NIS Richtlinie

- In Kraft getreten im Juli 2016
- Umsetzung in nationales Recht innerhalb von 21 Monaten



## 03 Marktkommunikation

- EDI@Energy - Kommunikationsrichtlinie
- EDI@Energy - Regelungen zum Übertragungsweg
- Erhöhte Anforderungen im Zielmodell

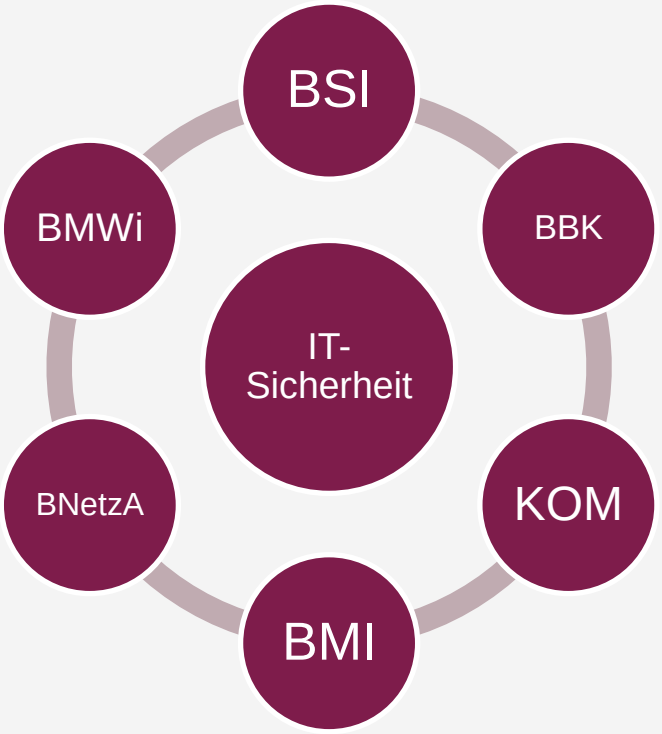
## 04 Gesetz zur Digitalisierung der Energiewende

- Maßnahmen nach dem Stand der Technik für „berechtigte Stellen“ (§49 Abs. 1 MsbG)
- BSI TR und Schutzprofile für Smart Meter
- ISMS für Smart-Meter Gateway Administrator

# Aktueller Stand der Regelungen zur IT-Sicherheit in der Energiewirtschaft

bdew
Energie. Wasser. Leben.

- IT-Sicherheitsgesetz ✓
- IT-Sicherheitskatalog für die Prozess-, Leit- und Steuertechnik von Energienetzbetreibern ✓
- IT-Sicherheitskatalog für Betreiber von Energieanlagen ⚠
- Verordnung zur Bestimmung Kritischer Infrastrukturen ✓
- Meldepflicht für IT-Sicherheitsvorfälle ✓
- Branchenstandard für Fernwärmenetze ⚠
- IT-Sicherheitsanforderungen für den „intelligenten Messstellenbetreiber“ ✓
- IT-Sicherheitsanforderungen für die Marktkommunikation (Interimsmodell) ✓
- IT-Sicherheitsanforderungen für die Marktkommunikation (Zielmodell) ⚠
- EU-Richtlinie zur Netz- und Informationssicherheit ✓

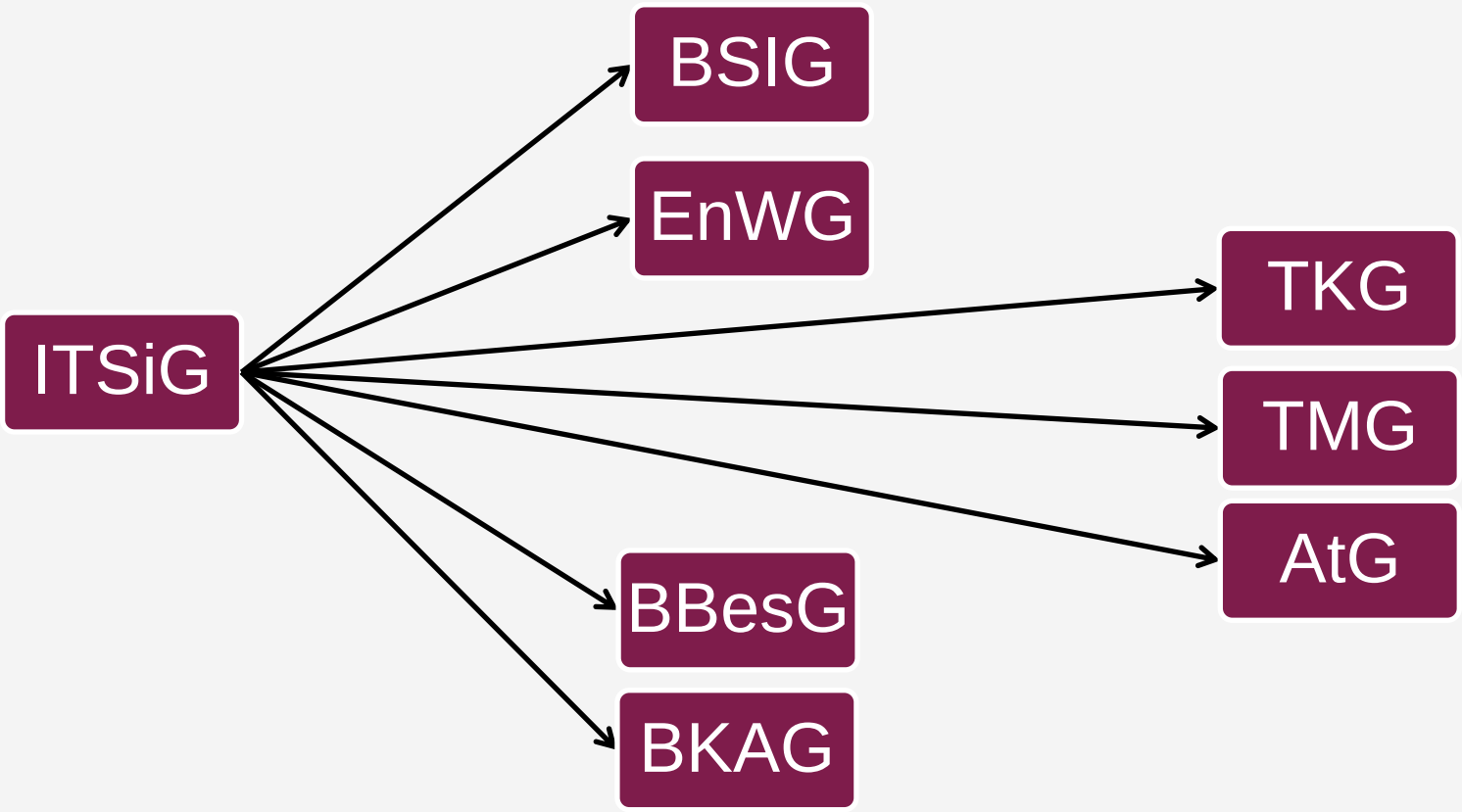


# Einige Grundziele der Informationssicherheit

bdew
Energie. Wasser. Leben.

| | |
|---|---|
| Verfügbarkeit | • Informationstechnische Systeme sind innerhalb vordefinierter Zeiträume verfügbar<br>• Vier Stufen der Verfügbarkeit sind definiert in der DIN/EN 50600 |
| Integrität | • Informationen sind vollständig und unverändert<br>• Und können nur von autorisierten Entitäten geändert werden |
| Authentizität | • Informationsquelle kann verifiziert werden |
| Vertraulichkeit | • Informationen sind nur für autorisierte Entitäten zugänglich oder dekodierbar |

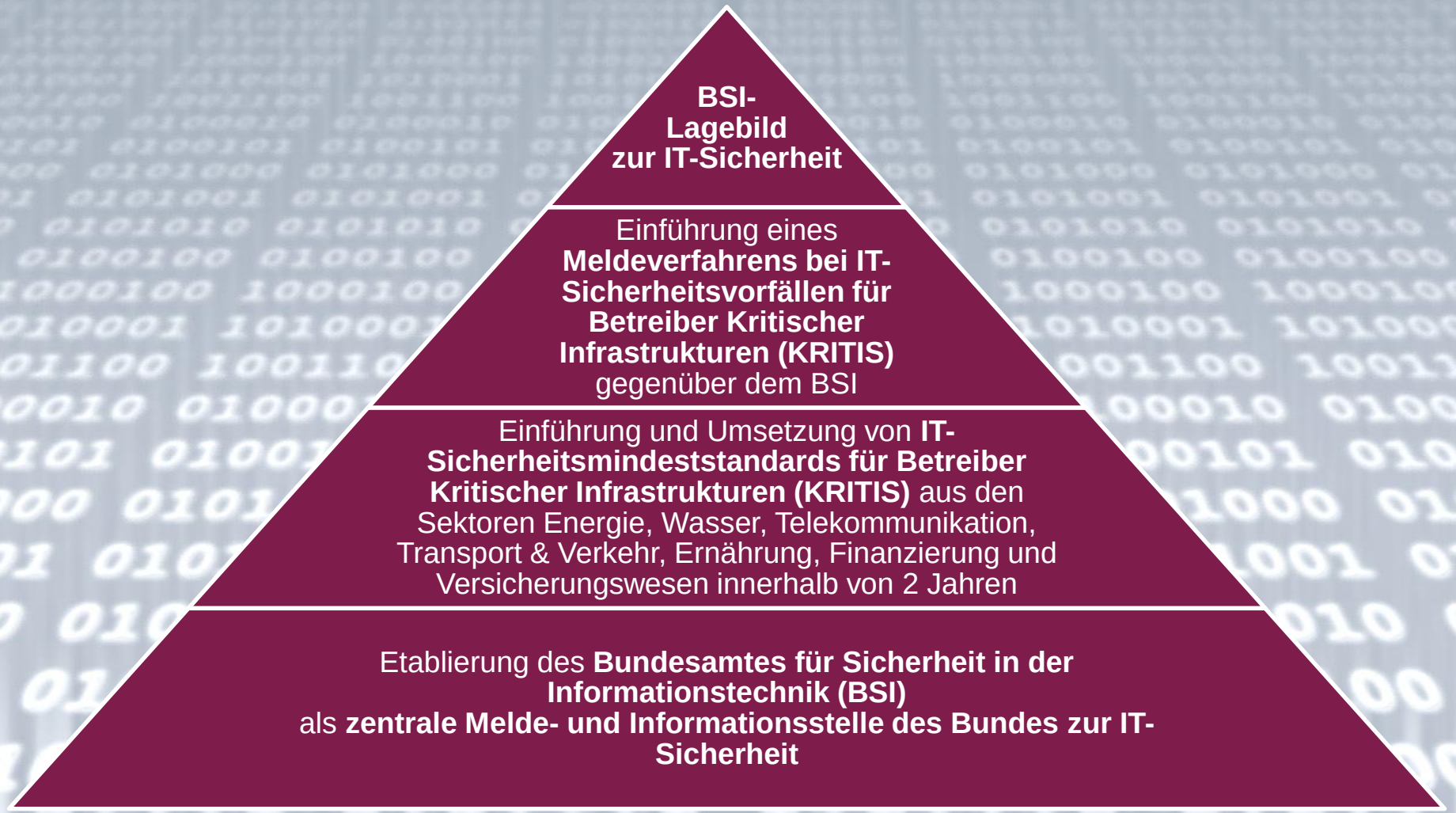
# Struktur des IT-Sicherheitsgesetzes (In Kraft getreten am 24. Juli 2015)




**IT-Sicherheitsgesetz:**
Es änderte nur bestehende Gesetze. Es ist kein neues „IT-Sicherheitsgesetz“.

# Allgemeine Eckpunkte des IT-Sicherheitsgesetzes

bdew
Energie. Wasser. Leben.



bdew

Energie. Wasser. Leben.

# Regelungen im EnWG für Strom- und Gasnetze, Stromerzeugungsanlagen und Gasspeicher

# Übersicht der Verpflichtungen nach EnWG für die Bereiche Elektrizität und Gas

bdew
Energie. Wasser. Leben.

| Wer? | Was? | Wann? | Norm |
|---|---|---|---|
| **Sämtliche Betreiber von Energieversorgungsnetzen (Strom und Gas)** | Umsetzung des IT-Sicherheitskatalogs für Netze:<br>• Benennung eines Ansprechpartners für IT-Sicherheit bei der Bundesnetzagentur<br>• Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 sowie dessen Zertifizierung | Ansprechpartner: 30.11.2015<br><br>Zertifizierung ISMS: 31.01.2018 | § 11 Abs. 1a EnWG |
| **Betreiber von Energie-versorgungsnetzen, die auch Betreiber Kritischer Infrastrukturen sind** | • Meldepflicht für erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik | Seit 3. Mai 2016 | § 11 Abs. 1c EnWG |
| **Betreiber von Energieanlagen, die auch Betreiber Kritischer Infrastrukturen sind** | • Meldepflicht für erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik<br>• Umsetzung des IT-Sicherheitskatalogs für Energieanlagen (liegt noch nicht vor) | Meldepflicht: Seit 3. Mai 2016<br><br>IT-Sicherheitskatalog: Frist wird im Katalog festgeschrieben | § 11 Abs. 1c EnWG;<br><br>§ 11 Abs. 1b EnWG |

# IT-Sicherheitskatalog für Energieanlagen

- Gilt für: Anlagen zur Stromerzeugung und Gasspeicher, die durch die BSI-KritisV als Kritische Infrastrukturen bestimmt wurden
- „Energieanlagen“ nach § 3 Nr. 15 EnWG:
  *„Anlagen zur Erzeugung, Speicherung und Fortleitung von [Strom und Gas]“*
- Beinhaltet voraussichtlich auch die Pflicht zur Einführung und Zertifizierung eines Informationssicherheits-Managementsystems
- Erste Gespräche mit der BNetzA wurden geführt über den Branchenarbeitskreis Strom im UP KRITIS.

# Änderungen im § 11 EnWG durch das Strommarktgesetz vom 23. Juni 2016

bdew
Energie. Wasser. Leben.

**Umgesetzt:**

- IT-Sicherheitskatalog für Energieanlagen nach § 11 Abs. 1b EnWG
  - Streichung der vormals starren Umsetzungsfrist bis Mai 2018
  - Umsetzungsfrist kann von der Bundesnetzagentur im Katalog festgeschrieben werden

**Ursprünglich geplant, aber vorläufig zurückgezogen:**

- Ausweitung der Meldepflicht für Betreiber von Energieversorgungsnetzen nach § 11 Abs. 1c EnWG

bdew

Energie. Wasser. Leben.

# Regelungen für alle anderen Betreiber Kritischer Infrastrukturen im BSI-Gesetz

# Das BSI-Gesetz gilt für alle KRITIS-Betreiber, die nicht unter § 11 EnWG fallen!

- Betreiber Kritischer Infrastrukturen, die keine Erzeugungsanlagen, Gasspeicher, oder Strom- bzw. Gasnetze sind, fallen unter das BSI-Gesetz!
- Im Sektor Energie betrifft dies unter anderem:
  - Direktvermarkter
  - Messstellen
  - Fernwärmenetze
  - Heizwerke
- Sowie andere Sektoren, z.B. Wasser / Abwasser

# Übersicht der Verpflichtungen nach BSI-G u.a. für Fernwärme, Wasser und Abwasser

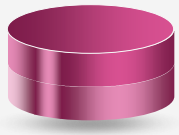
bdew
Energie. Wasser. Leben.

| Wer? | Was? | Wann? | Norm |
|---|---|---|---|
| **Alle KRITIS-Betreiber (außer Energieanlagen, Energieversorgungsnetze und kerntechnische Anlagen)** | • Benennung einer Kontaktstelle beim Bundesamt für Sicherheit in der Informationstechnik<br>• Sicherstellung einer jederzeitigen Erreichbarkeit über diese Kontaktstelle | Bis 03. November 2016 | § 8b Abs. 3 BSI-G |
| **Alle KRITIS-Betreiber (außer Energieanlagen, Energieversorgungsnetze und kerntechnische Anlagen)** | • Meldepflicht für erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik über die o. g. Kontaktstelle | Ab 03. November 2016 | § 8b Abs. 4 BSI-G |
| **Alle KRITIS-Betreiber (außer Energieanlagen, Energieversorgungsnetze und kerntechnische Anlagen)** | • Umsetzung angemessener organisatorischer und technischer Vorkehrungen zur Vermeidung von Störungen ihrer informationstechnischen Systeme (Branchenstandard)<br>• Nachweis der o. g. Vorkehrungen über z. B. Sicherheitsaudits, Prüfungen oder Zertifizierungen | Bis 03. Mai 2018<br><br>Alle 2 Jahre ab Umsetzung | § 8a Abs. 1 BSI-G<br><br>§ 8a Abs. 3 BSI-G |

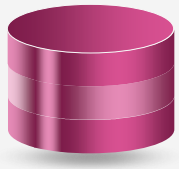
# Inhalte des branchenspezifischen Sicherheitsstandards nach BSI-Gesetz für Fernwärmenetze

- Der Geltungsbereich umfasst die IT-gestützte zentrale und dezentrale Prozesssteuerungs-, Leit-, Automatisierungs- und Überwachungstechnik.

DIN ISO/IEC TR 27019: Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung



DIN ISO/IEC 27002: Leitfaden für das Informationssicherheits-Management



DIN ISO/IEC 27001:Informationssicherheits-Managementsysteme

bdew
Energie. Wasser. Leben.

# Kontaktstelle beim BSI vs. Ansprechpartner IT-Sicherheit bei der BNetzA

# Kontaktstelle beim Bundesamt für Sicherheit in der Informationstechnik (1/2)

- **Gesetzliche Grundlage:** § 8b Abs. 3 BSI-Gesetz
- **Frist:** Donnerstag, 3. November 2016
- **Verpflichtete:** Betreiber Kritischer Infrastrukturen, die unter das BSI-Gesetz fallen (im Sektor Energie u.a.: Direktvermarkter/virtuelle Kraftwerke, Messstellen, Fernwärme)
- Ausgenommen von dieser Pflicht, jedoch freiwillige Benennung möglich: Stromnetzbetreiber, Gasnetzbetreiber, Erzeugungsanlagen, Gasspeicher
- **Ausgestaltung:** Jederzeitige Erreichbarkeit (24/7), Meldung von IT-Sicherheitsvorfällen hat über die Kontaktstelle zu erfolgen, zusätzlich sog. gemeinsame übergeordnete Ansprechstelle möglich, z.B. über Single Point of Contact (SPOC)

# Kontaktstelle beim Bundesamt für Sicherheit in der Informationstechnik (2/2)

bdew
Energie. Wasser. Leben.

- Benennung unter: Melde- und Informationsportal des BSI https://mip.bsi.bund.de
- Vorteile bei freiwilliger Benennung: Einbeziehung in Informationskanäle des BSI (IT-Sicherheitsmeldungen, Lagebilder)

# Ansprechpartner IT-Sicherheit bei der Bundesnetzagentur (1/2)

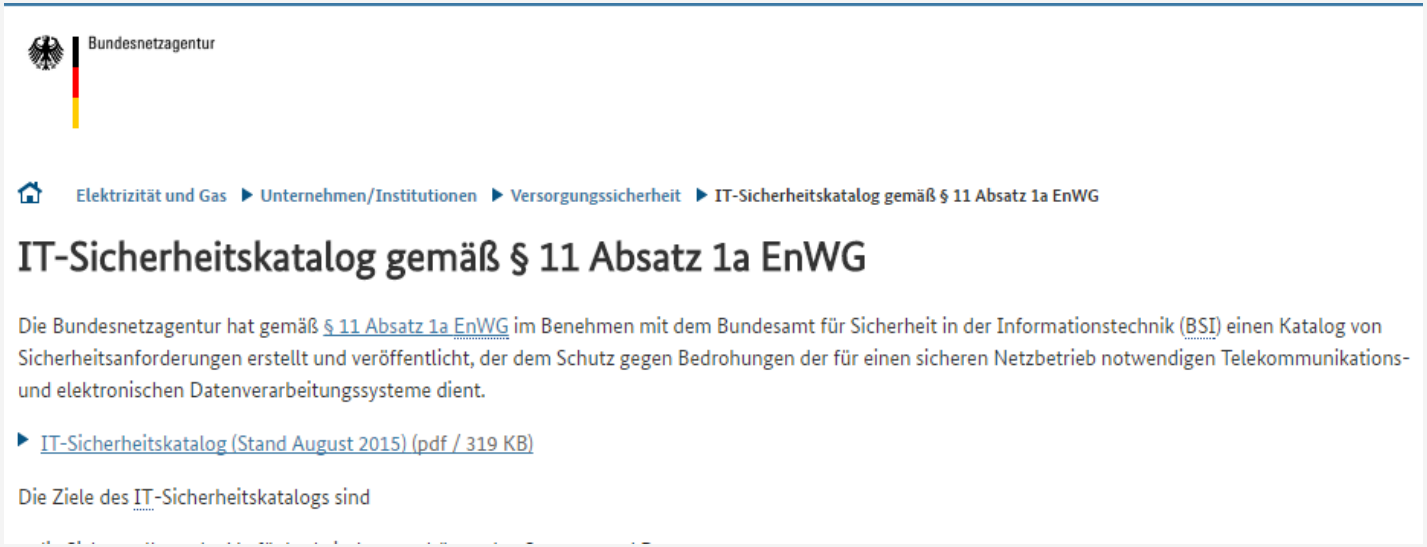
- **Grundlage:** IT-Sicherheitskatalog für Betreiber von Energieversorgungsnetzen nach § 11 Abs. 1a EnWG
- **Frist:** Donnerstag, 30. November 2015
- **Verpflichtete:** Sämtliche Betreiber von Energieversorgungsnetzen (Strom und Gas)

- **Ausgestaltung:** Sicherstellung der Erreichbarkeit zu üblichen Bürozeiten (auch bei Krankheit und Urlaub), Auskunftsfähig zum Stand der Umsetzung des IT-Sicherheitskatalogs und zu aufgetretenen IT-Sicherheitsvorfällen

# Ansprechpartner IT-Sicherheit bei der Bundesnetzagentur (2/2)

- Benennung per Formular unter: it-sicherheitskatalog@bnetza.de

http://www.bundesnetzagentur.de/DE/Sachgebiete/ElektrizitaetundGas/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheit.html


Bundesnetzagentur

Elektrizität und Gas ▶ Unternehmen/Institutionen ▶ Versorgungssicherheit ▶ IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG

IT-Sicherheitskatalog gemäß § 11 Absatz 1a EnWG

Die Bundesnetzagentur hat gemäß § 11 Absatz 1a EnWG im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Katalog von Sicherheitsanforderungen erstellt und veröffentlicht, der dem Schutz gegen Bedrohungen der für einen sicheren Netzbetrieb notwendigen Telekommunikations- und elektronischen Datenverarbeitungssysteme dient.

▶ IT-Sicherheitskatalog (Stand August 2015) (pdf / 319 KB)

Die Ziele des IT-Sicherheitskatalogs sind

bdew

Energie. Wasser. Leben.

# Meldepflicht für erhebliche IT-Sicherheitsvorfälle

# Meldepflicht für erhebliche IT-Störungen an das BSI

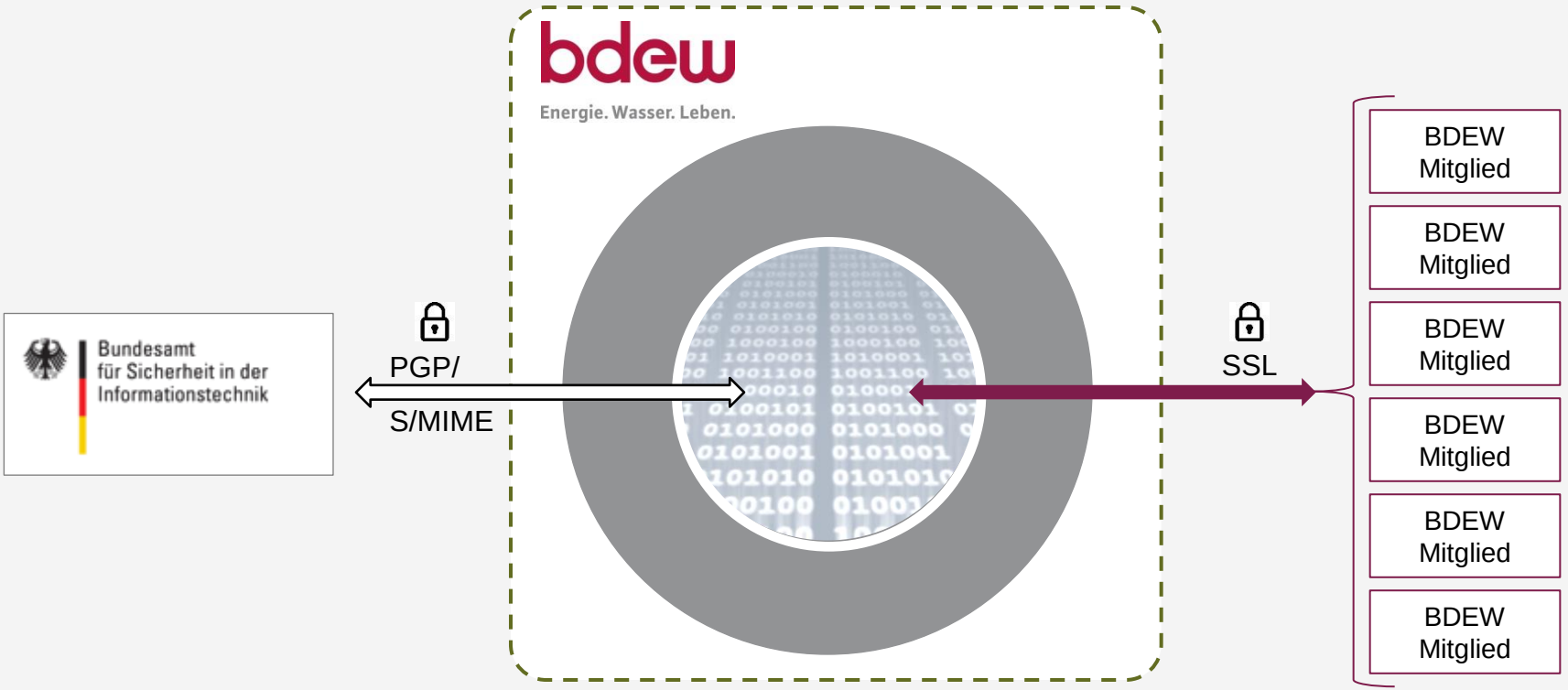
bdew
Energie. Wasser. Leben.

| Beispiele für erhebliche IT-Störungen | Beispiele für nicht-erhebliche IT-Störungen |
|---|---|
| • neuartige oder außergewöhnliche IT-Störungen<br>• gezielte Angriffe<br>• neue Modi Operandi<br>• Vorfälle, die nur mit deutlich erhöhtem Ressourcenaufwand bewältigt werden können (z. B. erhöhter Koordinierungsaufwand, Hinzuziehen zusätzlicher Experten, Nutzung einer besonderen Aufbauorganisation, Einberufung eines Krisenstabs) | • Spam E-Mails<br>• übliche Schadsoftware, die standardmäßig im Virenscanner abgefangen wird<br>• Hardwareausfälle im üblichen Rahmen |

Meldepflichtig sind „*erhebliche Störungen der Verfügbarkeit, der Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse*“, die zu einem Ausfall oder einer Beeinträchtigung der betreffenden Kritischen Infrastruktur geführt haben oder hätten führen können.

# Automatisierter BDEW Dienst zur pseudonymen Meldung

**Eine pseudonyme Meldung ist möglich für Vorfälle, die lediglich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur führen könnten, es aber nicht haben**



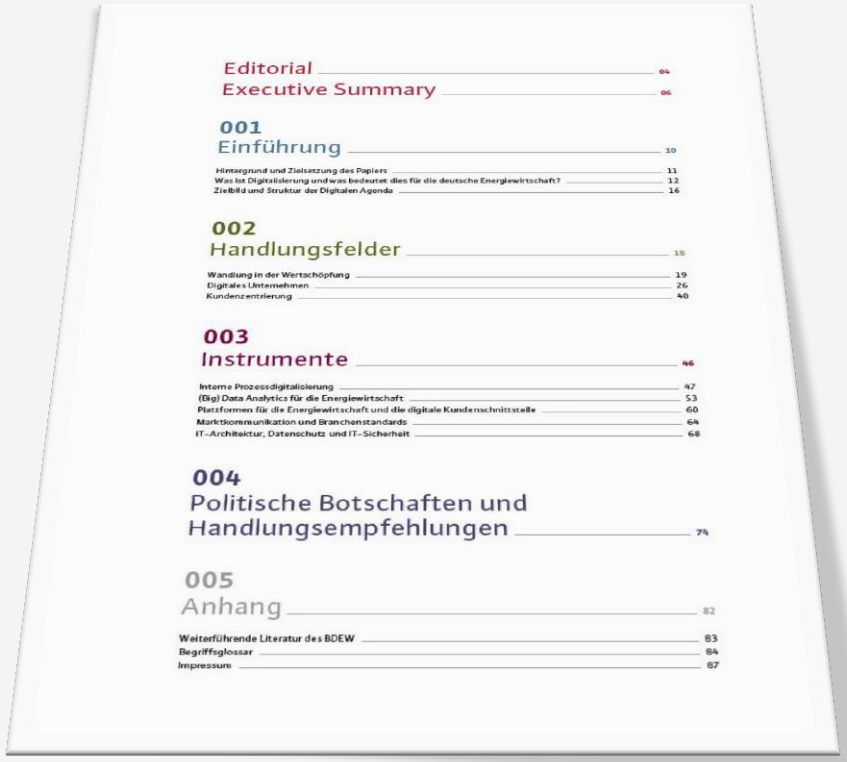
# Anwendungshilfe zur BSI-KritisV: www.bdew.de (Home > Energie > Betriebswirtschaft > IT-Sicherheit)

bdew
Energie. Wasser. Leben.

| Wer? | Was? | Wann? | Norm |
|---|---|---|---|
| **Betreiber von Energieversorgungsnetzen (Strom und Gas)** | Umsetzung des IT-Sicherheitskatalogs für Netze:<br>• Benennung eines Ansprechpartners für IT-Sicherheit bei der Bundesnetzagentur<br>• Einführung eines Informationssicherheits-Managementsystems (ISMS) gemäß DIN ISO/IEC 27001 sowie dessen Zertifizierung | Ansprechpartner: 30.11.2015<br><br>Zertifizierung ISMS: 31.01.2018 | § 11 Abs.1, 1a EnWG |
| **Betreiber von Energieversorgungsnetzen, die auch Betreiber Kritischer Infrastrukturen sind** | • Meldepflicht für erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik | voraussichtlich ab Anfang Mai 2016 | § 11 Abs. 1c EnWG |
| **Betreiber von Energieanlagen, die auch Betreiber Kritischer Infrastrukturen sind** | • Meldepflicht für erhebliche IT-Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik<br>• Umsetzung des IT-Sicherheitskatalogs für Energieanlagen (liegt noch nicht vor) | Meldepflicht: voraussichtlich ab Anfang Mai 2016<br><br>IT-Sicherheitskatalog: frühestens ab Mai 2018 | § 11 Abs. 1c EnWG;<br><br>§ 11 Abs. 1b EnWG |

# „Die digitale Energiewirtschaft - Agenda für Unternehmen und Politik“

bdew
Energie. Wasser. Leben.


Kostenloser Download unter http://pf.bdew.de/digitalisierung

# Vielen Dank für Ihre Aufmerksamkeit!

Dipl.-Ing. Kay Tidten
Abteilung Betriebswirtschaft, Steuern und Digitalisierung

BDEW Bundesverband der Energie- und Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin

Telefon +49 (0)30 - 300199-1526
kay.tidten@bdew.de
www.bdew.de