IT- und Informationssicherheit im EVU

Michael Burgwinkel
19.01.2017

Neue Herausforderungen der digitalisierten Welt

WELT N24 DIGITAL ZEITUNG TV

HOME LIVE TV MEDIATHEK POLITIK WIRTSCHAFT SPORT MEHR ABO

NEU: Lesen Sie die WELT Edition jetzt auch im Web JETZT TESTEN

HOME » WIRTSCHAFT » WEBWELT & TECHNIK » Telekom: Internet-Ausfall in 900.000 Haushalten - Hacker-Angriff wird geprüft

WEBWELT & TECHNIK INTERNET, TELEFONIE, FERNSEHEN

900.000 Router ausgefallen - Telekom prüft Hacker-Angriff

Veröffentlicht am 28.11.2016 | Lesedauer: 4 Minuten

Die bundesweite Störung bei der Telekom dauert offenbar an. Auf Facebook macht das Unternehmen seinen Kunden wenig Hoffnung. Betroffen ist das Mobilfunknetz, sowie die Internet- und Fernsehdienste.

AUTOPLAY

Quelle: Die Welt

Seit Sonntagnachmittag gibt es bei der Telekom eine massive Störung be Festnetz, Internet und Fernsehen.

IT-Sicherheit

Blackout

Ein Hacker brauchte nur zwei Tage, um die Kontrolle über die Stadtwerke in Ettlingen zu übernehmen. Er zeigte: Die Stromnetze in Deutschland sind nicht sicher.

Von **Christiane Grefe**

10. April 2014, 8:00 Uhr / Editiert am 17. April 2014, 8:47 Uhr / DIE ZEIT Nr. 16/2014 / 30 Kommentare

Blackout

- Wie konnte FX die Schutzmauern in durchdringen?

- Angriff auf Ettlingen Ermutigendes zutage

Es ist Zeit für einen Anruf. "Noch ein paar Klicks, dann ist es dunkel", sagt Felix Lindner. Wenn er jetzt seine Finger bewegt, geht in der süddeutschen Stadt Ettlingen das Licht aus. 40.000 Einwohner haben dann keinen Strom mehr. 200.000 Wasserpumpen könnten jetzt still stehen, weil der Hacker Felix Lindner sein Ziel erreicht hat.

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Anmelden

NETZWELT Schlagzeilen | Wetter | DAX 11.620,80 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > Hacker > Ferngesteuertes Wasserwerk: Hacker führen US-Behörden vor

Ferngesteuertes Wasserwerk

Hacker führen US-Behörden vor

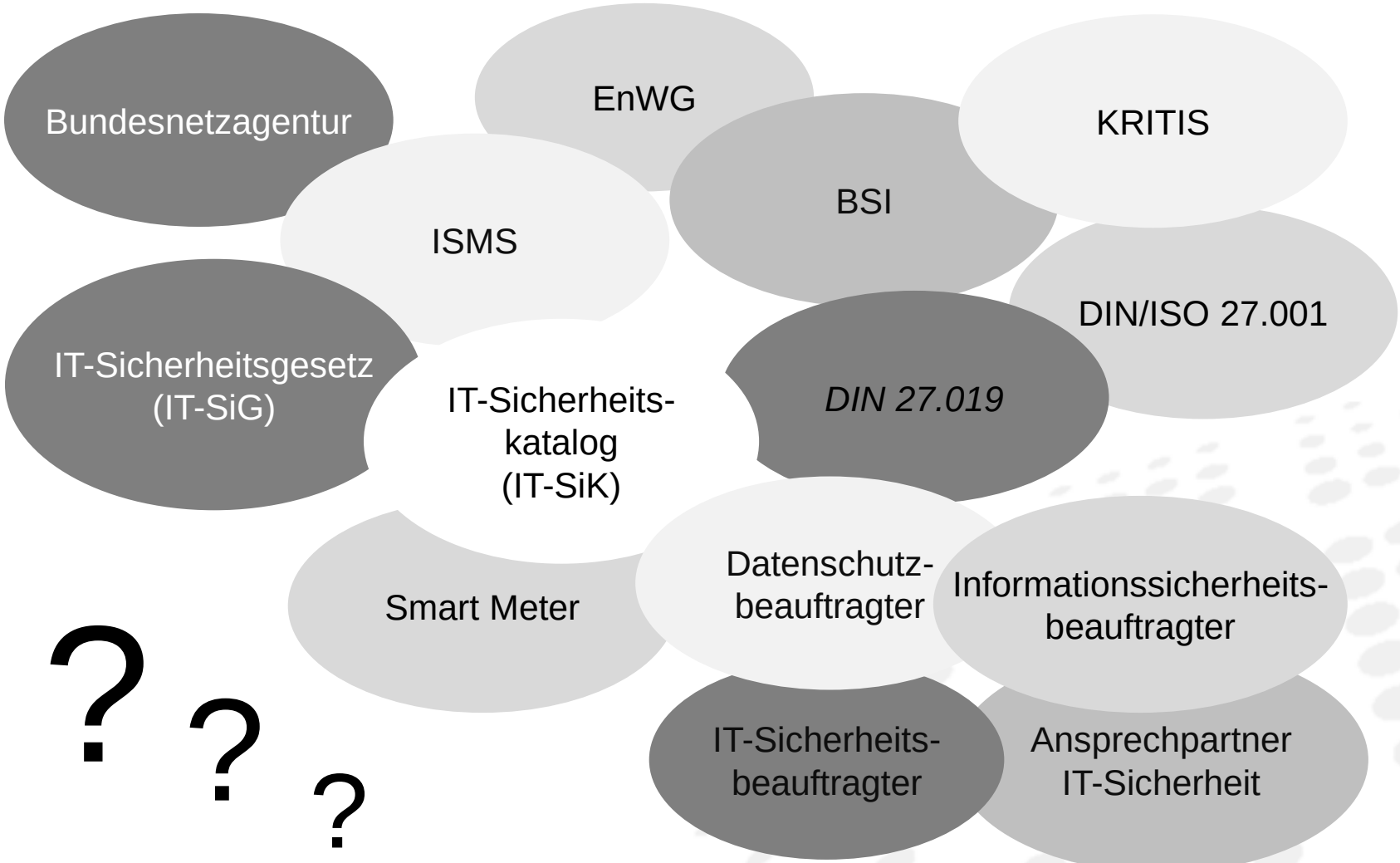
Im US-Bundesstaat Illinois wurde ein Wasserwerk offenbar Ziel eines Hackerangriffs. Behörden spielen den Fall herunter, Experten hingegen schlagen Alarm: Kriminelle könnten per Fernsteuerung in das System eingedrungen sein. Zum Beweis knackte ein Unbekannter eine weitere Anlage.

Von Ole Reißmann

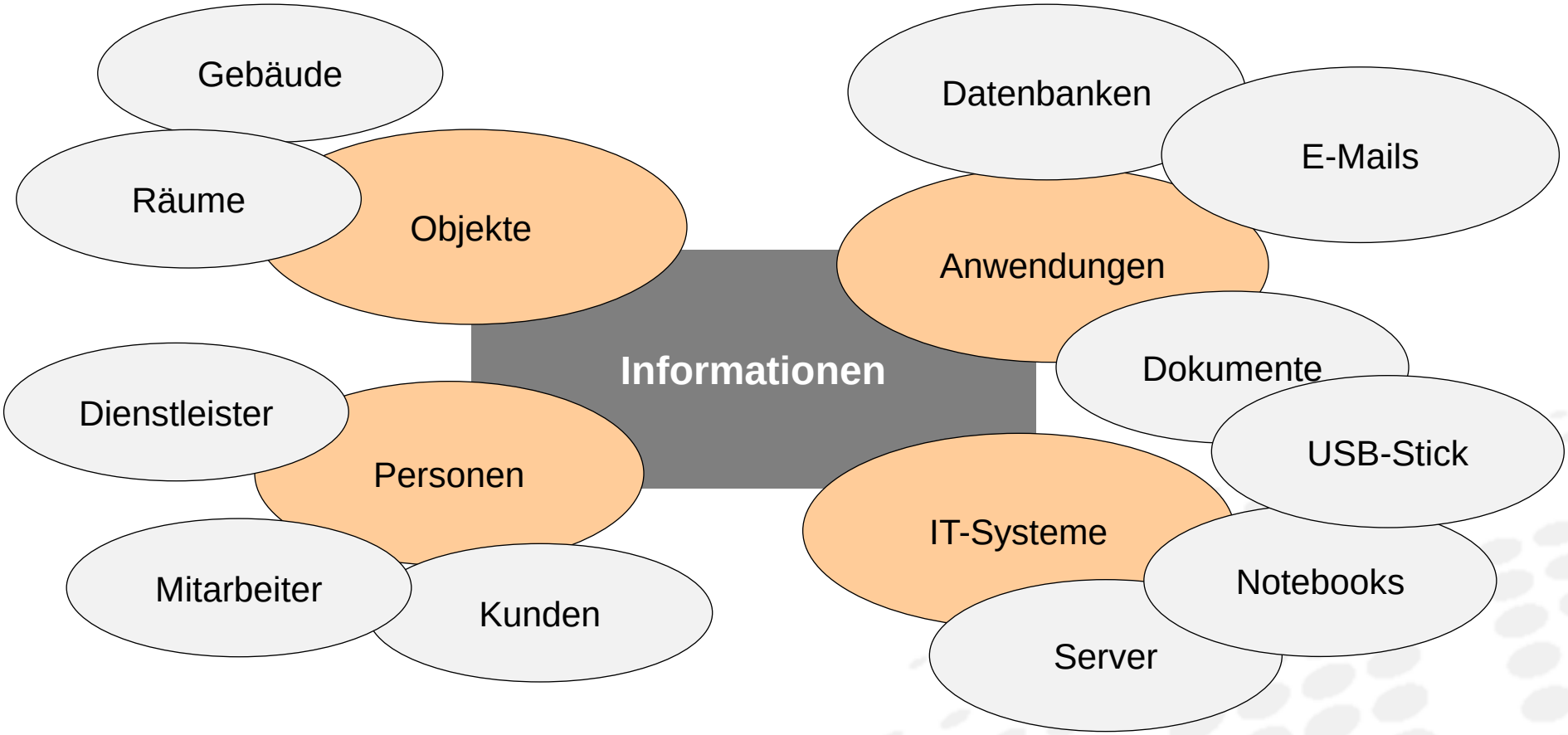
Agenda

1. Was ist Informationssicherheit
2. Das IT-Sicherheitsgesetz – ein Artikelgesetz
3. Das BSIG und die BSI-KRITISV

Das Themenfeld IT- und Informationssicherheit ist sehr umfänglich und ggf. missverständlich

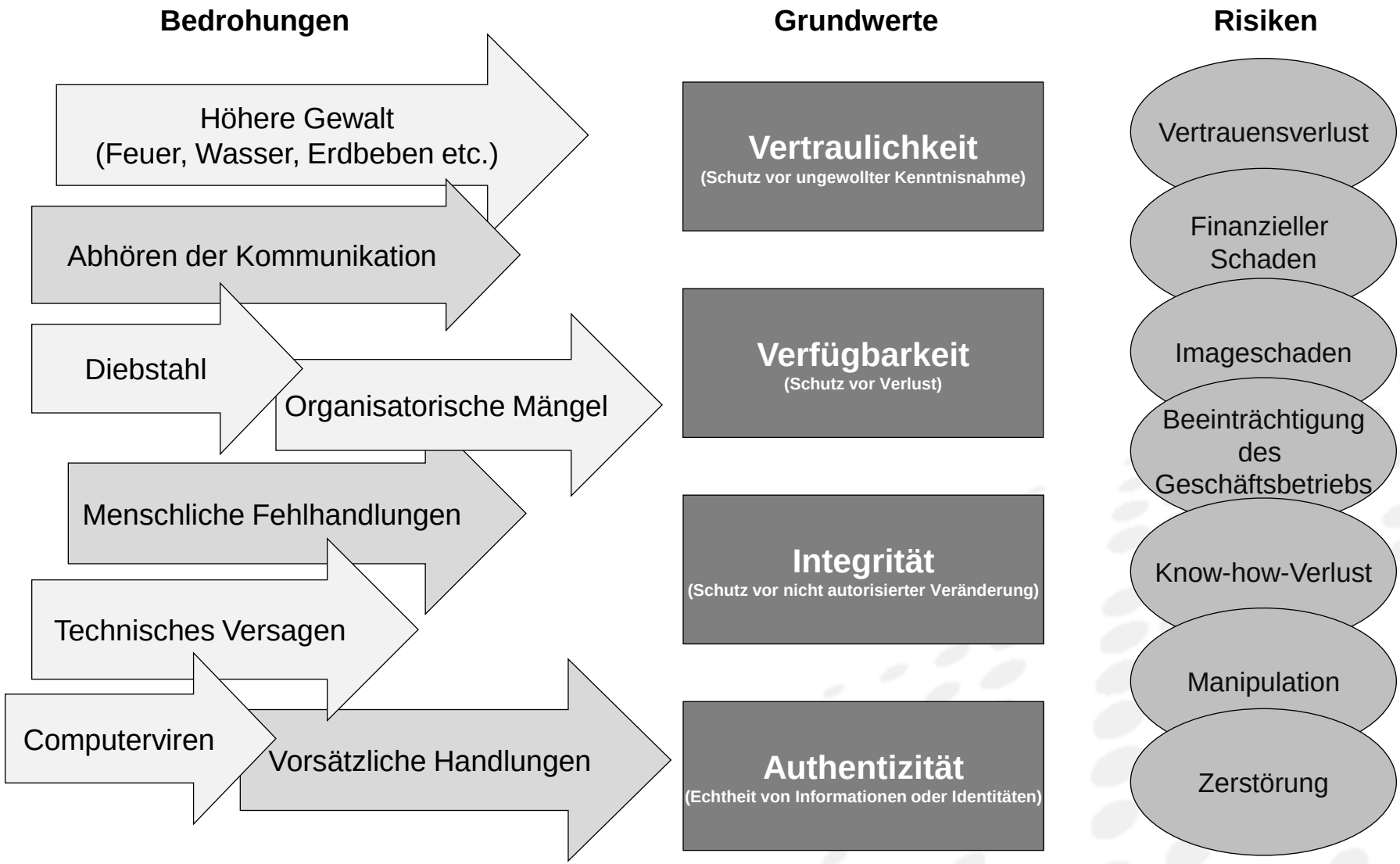


Informationen sind ein essentielles Gut jedes Unternehmens



Um sichere Geschäftsprozesse zu ermöglichen, muss die Informationssicherheit für schutzwürdige und sensible Informationen stets gewährleistet und der Kommunikations-prozess gesichert sein.

Einfluss und Auswirkungen auf die Informationensicherheit von Außen



Informationssicherheit ist nicht nur IT-Sicherheit sondern ein ganzheitlicher Ansatz

IT-Sicherheit

- IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung.

Informationssicherheit

- Informationssicherheit hat als Ziel den Schutz von Informationen jeglicher Art und Herkunft.
- Dabei können Informationen sowohl auf Papier, in Rechnersystemen oder auch in den Köpfen der Nutzer gespeichert sein.

Datenschutz

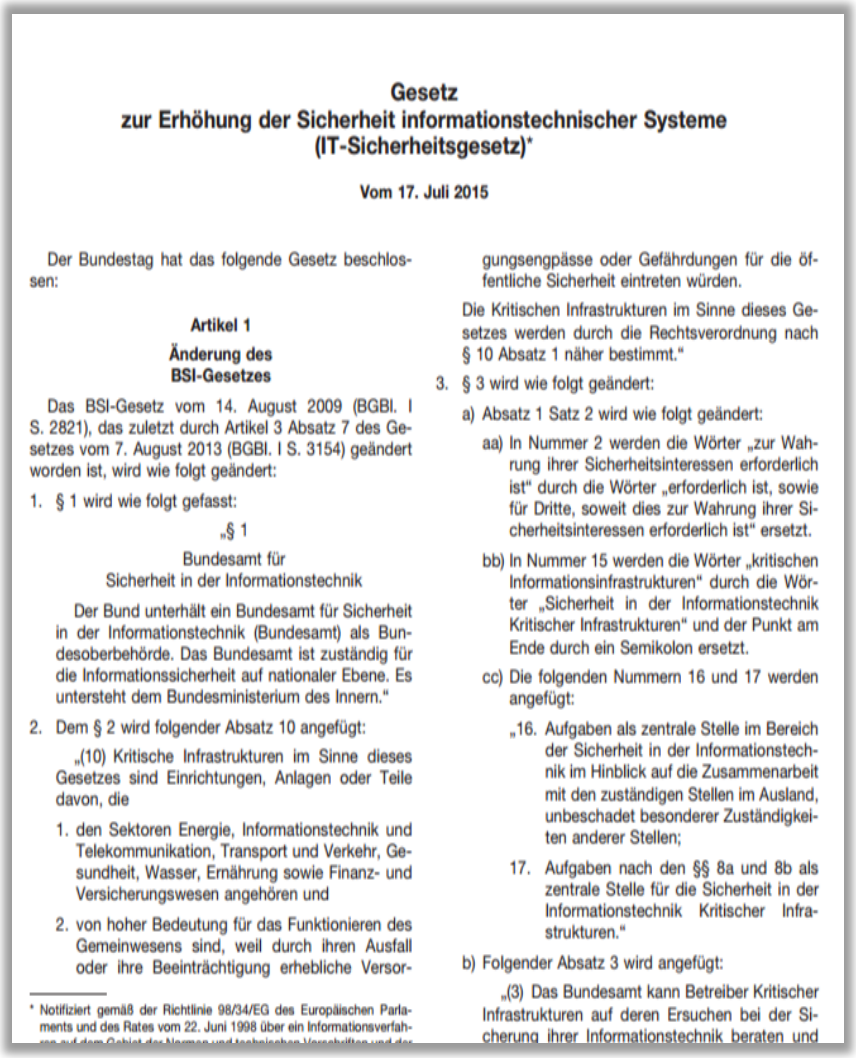
- Schutz des Grundrechts auf informationelle Selbstbestimmung
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung und Schutz der Privatsphäre

Aber: Die IT-Infrastruktur ist von zentraler Bedeutung für den Schutz von Informationen!

Agenda

1. Was ist Informationssicherheit
2. Das IT-Sicherheitsgesetz – ein Artikelgesetz
3. Das BSIG und die BSI-KRITISV

Das IT-Sicherheitsgesetz



Gesetz
zur Erhöhung der Sicherheit informationstechnischer Systeme
(IT-Sicherheitsgesetz)*

Vom 17. Juli 2015

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für
Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

2. Dem § 2 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. 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.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" ersetzt.

bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt am Ende durch ein Semikolon ersetzt.

cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen."

b) Folgender Absatz 3 wird angefügt:

„(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und

* Notifiziert gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der

Gesetzgebungsverfahren:

- **Gesetzesinitiative:** *BMI*
- **Beschluss der Bundesregierung:** *17.12.2014*
- **Stellungnahme des Bundesrates:** *06.02.2015*
- **Beschluss des Bundestages:** *12.06.2015*
- **Beschluss des Bundesrates:** *10.07.2015*
- **Verkündung im BGBl.:** *BGBl. 2015 I Nr. 31, Seite 1324 - verkündet am **24.07.2015***

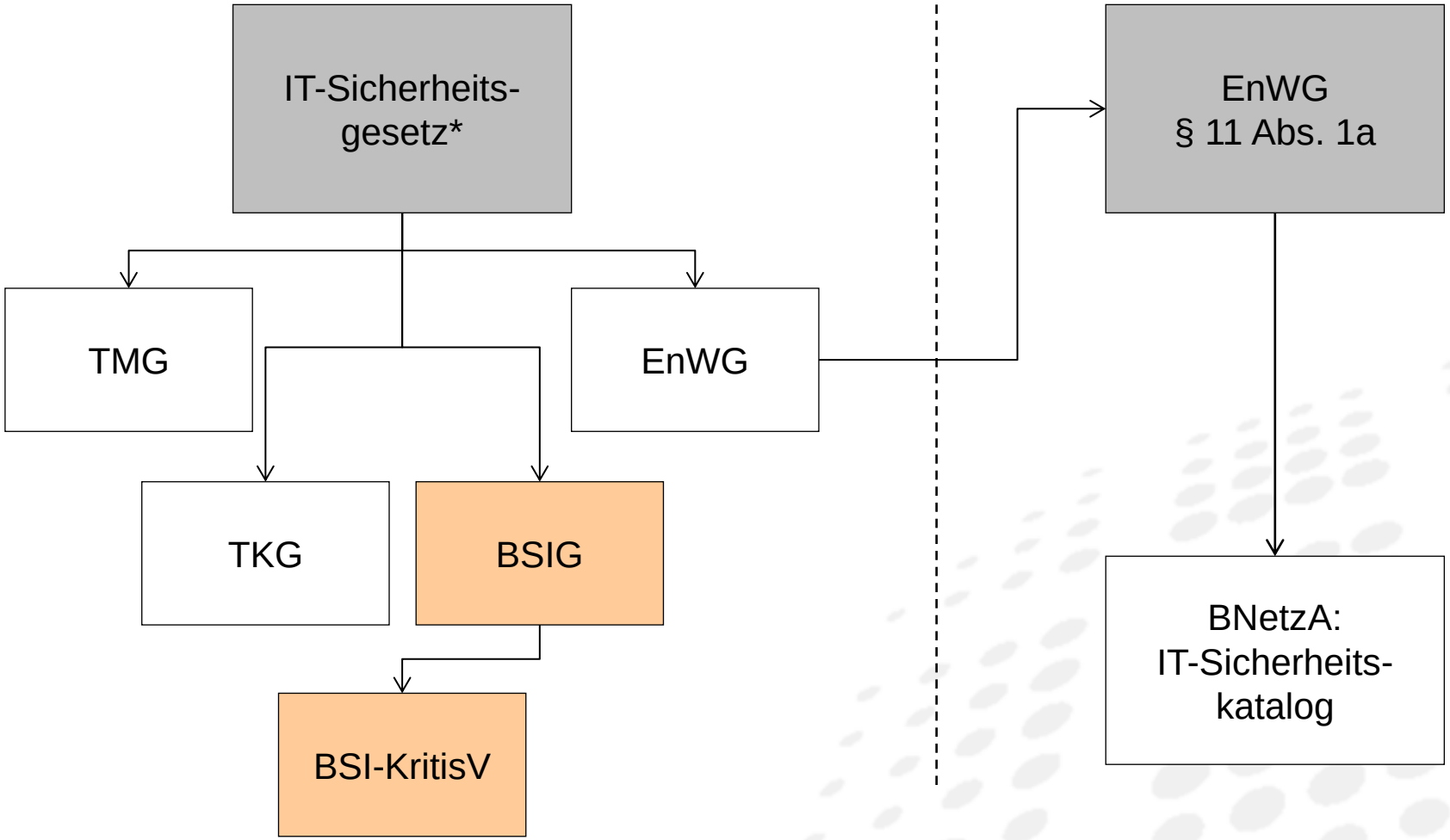
Das IT-Sicherheitsgesetz

Auf einen Blick	• Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme • Sog. „Artikelgesetz“ (Ändert das EnWG, BSI, TKG, etc.)
Adressatenkreise	• Unternehmen mit besonderem Fokus auf Kritische Infrastrukturen (KRITS) = Infrastrukturen, die für das Funktionieren des Gemeinwesens zentral sind • Bürger im Internet besser schützen • BSI und Bundeskriminalamt
Ziele	• Signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland • Verbesserung der Zusammenarbeit und des Informationsaustauschs zwischen Staat und Betreibern kritischer Infrastrukturen.
Kernforderungen	• **Meldung von IT-Sicherheitsvorfällen** • Festschreibung eines **Mindestniveaus** an IT-Sicherheit für kritische Infrastrukturen auf dem aktuellen **Stand der Technik** • **Branchen können selber Standards entwickeln**, die dann vom Bundesamt für Sicherheit in der Informationstechnik (BSI) genehmigt werden. • **Alle Betreiber von KRITIS müssen Mindeststandards einhalten** • **Keine Zertifizierung erforderlich**, aber Nachweis, dass Anforderungen erfüllt werden

Der gesetzliche Rahmen – kurze Orientierung

Sparten: Strom, Gas, Wasser, Wärme

Strom, Gas



*Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

Agenda

1. Was ist Informationssicherheit
2. Das IT-Sicherheitsgesetz – ein Artikelgesetz
3. Das BSIG und die BSI-KRITISV

Die neuen Vorschriften des BSI-Gesetzes

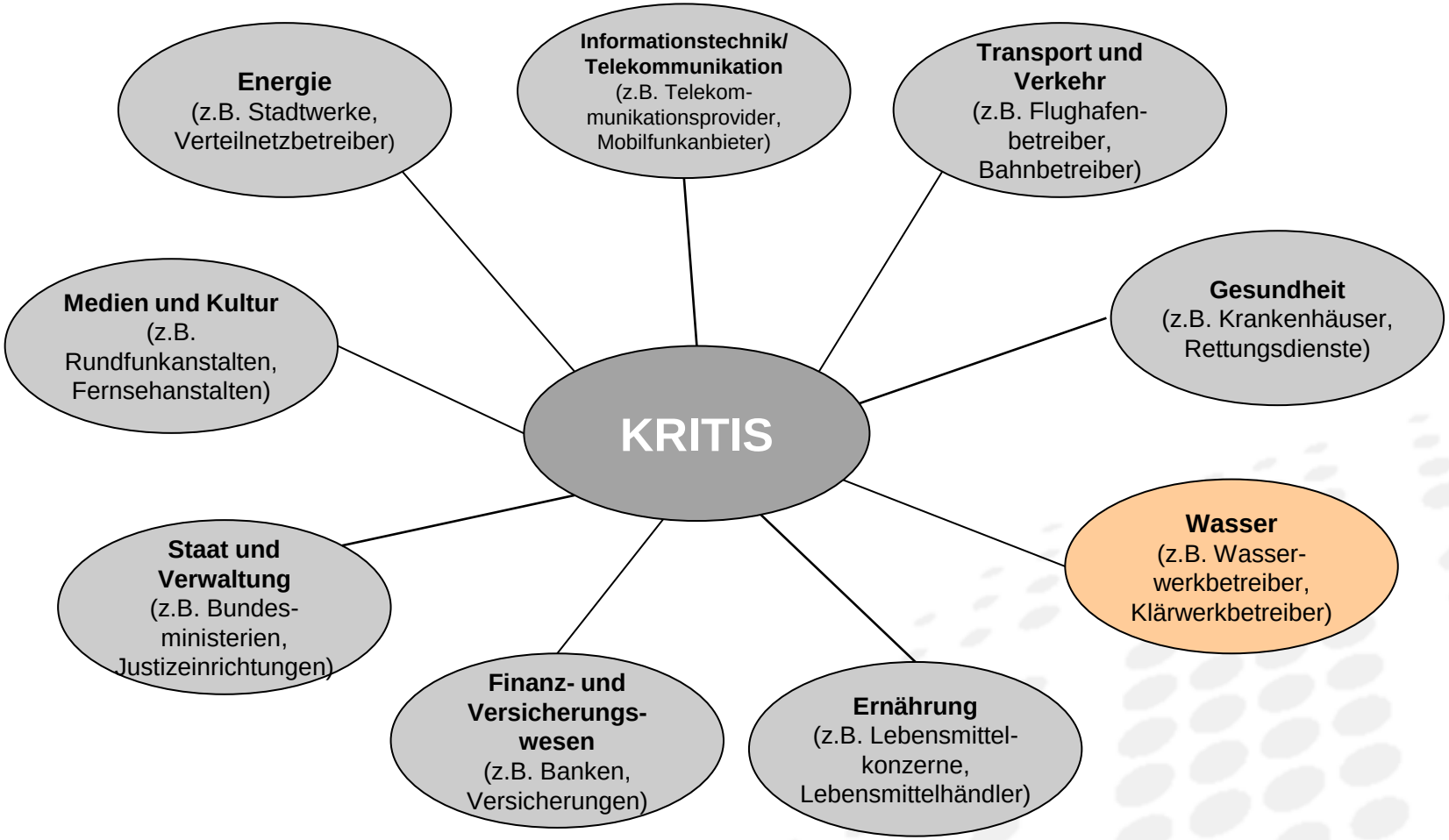
§ 2 Abs. 10 Kritische Infrastrukturen	Grunddefinition KRITIS
	Verweis auf Ermächtigungsgrundlage für RVO gemäß § 10 Abs.
§ 4 Zentrale Meldestelle	Informationen von KRITIS auswerten, Lagebild, Unterrichtung
§ 7a Untersuchung der Sicherheit der IT	Befugnis des BSI Produkte und IT-Systeme zu untersuchen
§ 8a Sicherheit in der Informationstechnik	(1) **Spätestens 2 Jahre nach Inkrafttreten der RVO**: KRITIS-Betreiber müssen techn. und org. Vorkehrungen zur Vermeidung von Störungen der IT-Sicherheit treffen, Nachweis alle 2 Jahre (2) KRITIS-Betreiber können zusammen mit ihre Branchenverbände **branchenspezifische Sicherheitsstandards** vorschlagen.
§ 8b Zentrale Stelle für IT-Sicherheit KRITIS	Das BSI wird zentrale Melde- und Informationsstelle, KRITIS-Betreiber müssen **6 Monate nach Inkrafttreten der RVO** Kontaktstelle einrichten.
§ 8c Anwendungsbereich	Ausnahme für KMU bzgl. § 8a und b BSI-G
	Ausnahme für Betreiber von Telekommunikations- und Energieversorgungsnetzen sowie AKWs bzgl. § 8 a und b Abs. 3 bis 5 BSI-G wegen spezialgesetzlichen Regelungen
§ 8d Auskunftsverlangen	Auskunftsanspruch ggü. BSI über Informationen gemäß § 8 a und Meldungen nach § 8b, keine Übermittlung personenbezogener Daten
§ 14 Bußgeldvorschriften	Verstoß gegen § 8 a Abs. 3 S. 4 (Beseitigung von Sicherheitsmängeln) bis 100.000,00 €

Was sind „KRITIS“?

- **KRITIS wird seit 2003 auf Bundesebene diskutiert**
- 2005: Verabschiedung des Nationalen Plans zum Schutz der Informationsinfrastrukturen (NPSI)
  - Der Umsetzungsplan KRITIS (**UP KRITIS**) und der Umsetzungsplan Bund (UP Bund) sind aus dem NPSI abgeleitete Arbeitsprogramme
  - **Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen.**
- Ziel des UP KRITIS:
  - Der UP KRITIS hat das zentrale Ziel, die Resilienz („Widerstandsfähigkeit“) der Kritischen Infrastrukturen, und dabei insbesondere der kritischen Informationsinfrastrukturen, zu erhöhen bzw. auf hohem Niveau zu stabilisieren.

„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“ (Quelle: BBK, BSI)

Welche Sektoren sind KRITIS?



Wer ist Betreiber einer kritischen Infrastruktur?

§ 2 Abs. 10 BSI-G:

Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und

2. 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.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

BSI-Kritisverordnung – BSI-KritisV

vom 03.05.2016

Wer die Kriterien der RVO erfüllt, betreibt eine Kritische Infrastruktur im Sinne des Gesetzes

Berechnungsformel basiert auf der Annahme von **500 000 „versorgten Personen“**

- **Stromverteilung**
  - **3 700 GWh/Jahr** entnommene Jahresarbeit
- **Gasverteilung**
  - **5 190 GWh/Jahr** entnommene Arbeit
- **Trinkwasserversorgung**
  - **22 Millionen m³/Jahr** verteilte Wassermenge*

* Genaue Schwellenwerte auf Seite 17

Anlagenkategorien und Schwellenwerte

Berechnungsformeln unter der Annahme eines Durchschnittsverbrauchs von 44 m^3 pro versorgter Person pro Jahr bei 500 000 versorgten Personen

→ **22 Millionen m^3/Jahr** = 44 m^3/Jahr x 500 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	**Anlagenkategorie**	**Bemessungskriterium**	**Schwellenwert**
2.	Trinkwasserversorgung		
2.1	Gewinnung		
2.1.1	Gewinnungsanlage	Gewonnene Wassermenge in Millionen m^3/Jahr	22
2.1.2	Wasserwerk	Wasseraufkommen in Millionen m^3/Jahr	22
2.2	Aufbereitung		
2.2.1	Aufbereitungsanlage	Aufbereitete Trinkwassermenge in Millionen m^3/Jahr	22
2.2.2	Wasserwerk	Wasseraufkommen in Millionen m^3/Jahr	22
2.3	Verteilung		
2.3.1	Wasserverteilungssystem	Verteilte Wassermenge in Millionen m^3/Jahr	22
2.3.2	**Leitzentrale**	**Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete Menge Wasser in Millionen m^3/Jahr**	**22**

Haben Sie noch Fragen?
Gerne helfen wir weiter!

Dipl.-Ing. **Michael Burgwinkel**

Management Berater
Informationssicherheitsbeauftragter (ISB)

Dienstleistungsgeschäft
Beratung und Projektmanagement
Telefon 0221.93731 – 441
Telefax 0221.93731 – 51441
michael.burgwinkel@rhenag.de

rhenag Rheinische Energie AG
Bayenthalgürtel 9, 50968 Köln
Telefon 0221.93731-0, Fax 0221.93731-170
dienstleistung@rhenag.de, www.rhenag.de

Informationen

- Übersicht von **Cyberattacken** über weltweite Datennetze.
  - map.norsecorp.com
  - http://www.sicherheitstacho.eu

- **Telekom Ausfall**: http://www.deutschlandfunk.de/telekom-stoerung-war-letztendlich-auch-ein-gewisser.697.de.html?dram:article_id=372625

- Ein Hacker brauchte nur zwei Tage, um die **Kontrolle über die Stadtwerke** in Ettlingen zu übernehmen http://www.zeit.de/2014/16/blackout-energiehacker-stadtwerk-ettlingen

- Buchtip: **Blackout** von Marc Elsberg

Denkanstoß!

http://kompass.im/2013/12/zombie-buegeleisen-aus-der-hoelle-das-dunkle-internet-der-haushalts-dinge