Consulting. Solutions. Services.
Erfahrung macht den Unterschied.

prego. services

Das neue

IT-Sicherheitsgesetz:

Wen betrifft es,

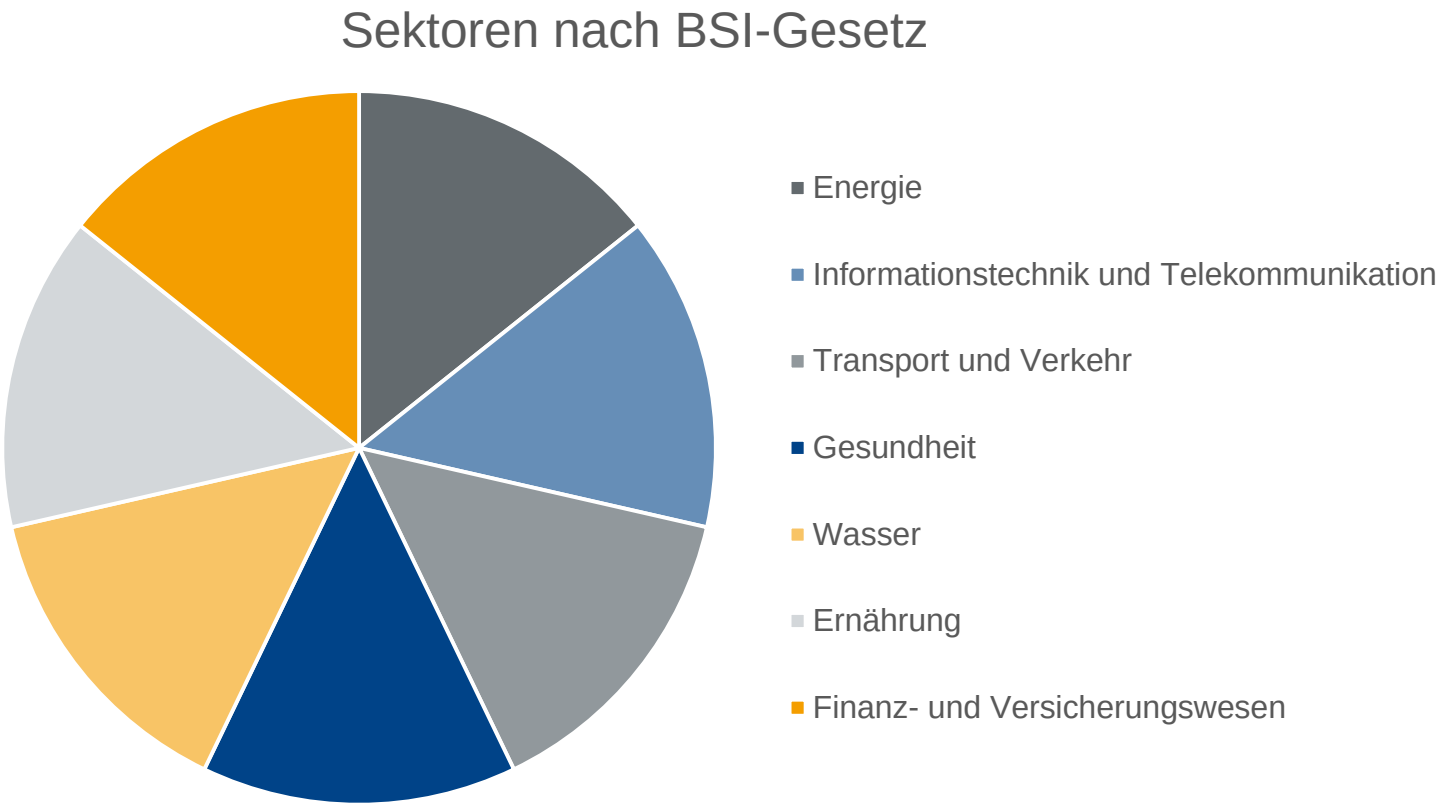
was ist zu tun ?

2. Tag der IT-Sicherheit
Saarbrücken, 2. Februar 2016

Der Rechtsrahmen

- Das **‚Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme‘** (IT-Sicherheitsgesetz) ist am **25. Juli 2015** in Kraft getreten, ist ein wesentlicher Baustein und eines der ersten konkreten Ergebnisse der **Digitalen Agenda der Bundesregierung.**
- Ziel des Gesetzes ist eine signifikante Verbesserung der **Sicherheit informationstechnischer Systeme in Deutschland**; dies soll erreicht werden durch
  - die Verbesserung der **IT-Sicherheit** (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) von Unternehmen,
  - einen verstärkten **Schutz von Bürgern** im Internet,
  - die **Stärkung des BSI und des BKA.**
- Das IT-Sicherheitsgesetz ist ein **Artikelgesetz** mit dem einzelne Vorschriften des BSI-Gesetzes, des Atomgesetzes, des Energiewirtschaftsgesetzes, des Telemediengesetzes, des Telekommunikationsgesetzes und weiterer Gesetze geändert werden.

Wen betrifft es ? Der Ausgangspunkt



Sektoren **'Staat und Verwaltung'** und **'Medien und Kultur'** nicht vom IT-Sicherheitsgesetz betroffen

Wen betrifft es ? Eine noch offene Aufgabe …

Kritische Infrastrukturen

Gesetzentwurf: maximal 2.000 Unternehmen

Umsetzung in zwei Körben

Korb 1: Energie – Informationstechnik und Telekommunikation – Wasser – Ernährung

Korb 2: Transport und Verkehr – Gesundheit – Finanz- und Versicherungswesen

Rechtsverordnung nach § 10 BSI-Gesetz

Qualitative Kriterien

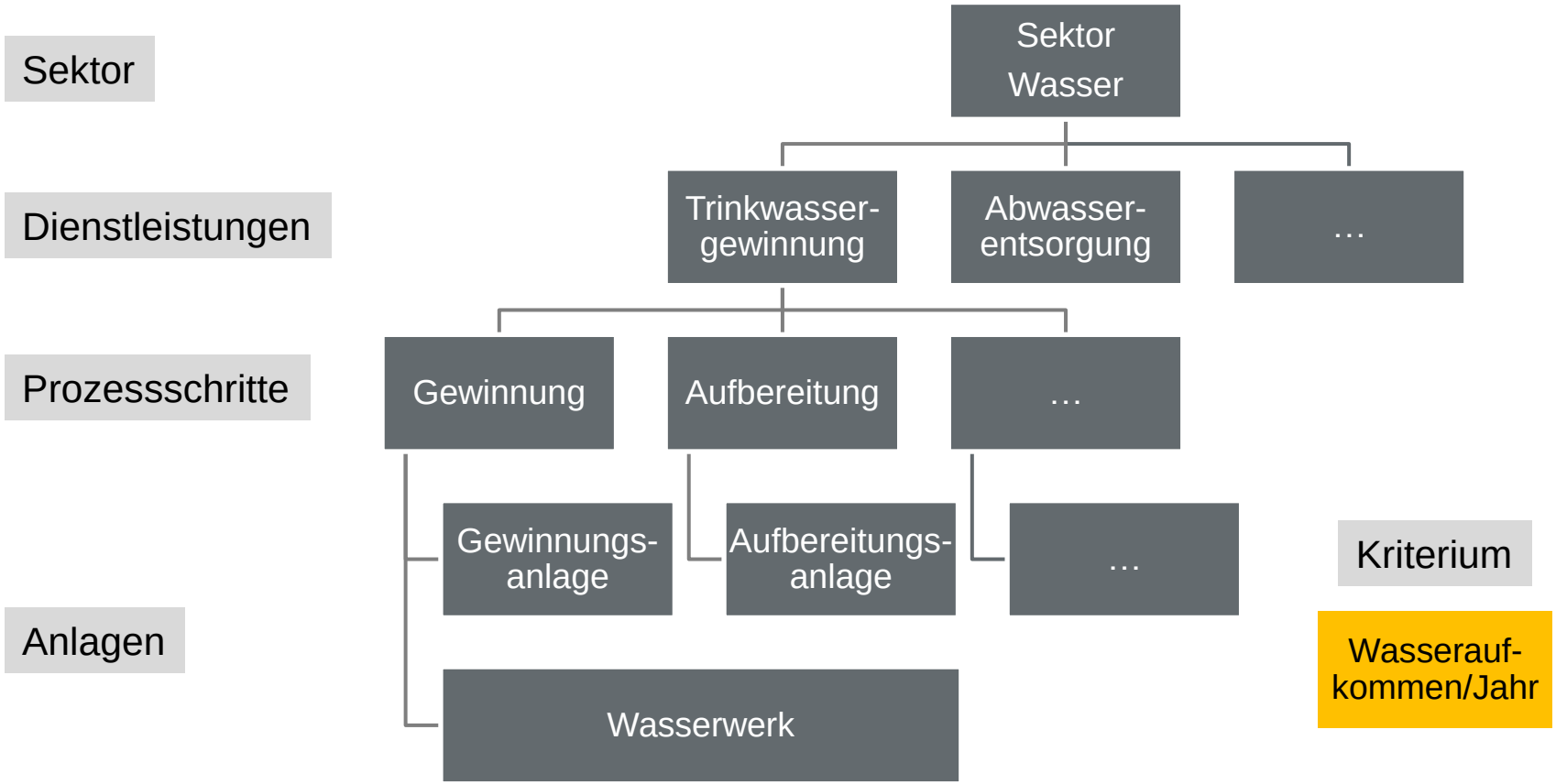
- **Wird eine für die Gesellschaft kritische Dienstleistung erbracht?**
- Sicherheit für Leib, Leben, Gesundheit und Eigentum
- Identifizierung **kritischer Dienstleistungen** in den Sektoren
- Identifizierung von **Anlagen- und Einrichtungstypen** nach Prozessschritten einer kritischen Dienstleistung

Betreiber kritischer Infrastrukturen

Quantitative Kriterien

- **Gibt es wesentliche Folgen für wichtige Schutzgüter und die Funktionsfähigkeit des Gemeinwesens?**
- Versorgungsgrad – Bildung spezifischer Schwellenwerte
- Zuordnung **quantitativer Kriterien** zu den Anlagen- und Einrichtungstypen
- Bildung von **Schwellenwerten** je Dienstleistung und Anlagen- und Einrichtungstyp

Exemplarisch*: Sektor Wasser



* nach einem Arbeitspapier des BSI

Was ist zu tun ? Allgemeine Regelung: BSI-Gesetz

Umsetzung	▪ Pflicht zur **Einhaltung eines Mindestniveaus an IT-Sicherheit** (organisatorische und technische Vorkehrungen nach Stand der Technik) ▪ ggf. **branchenspezifische Sicherheitsstandards**	spätestens **zwei Jahre** nach Inkrafttreten der Rechtsverordnung
Überprüfung	▪ **Geeigneter Nachweis** der Umsetzung durch Sicherheitsaudits, Prüfungen oder Zertifizierungen	mindestens alle **zwei Jahre**
Kommunikation	▪ Benennung einer **Kontaktstelle** zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung und Koordinierung der Zusammenarbeit zum Schutz der Sicherheit	**sechs Monate** nach Inkrafttreten der Rechtsverordnung
Meldung	▪ **Unverzügliche Meldung** erheblicher Sicherheitsvorfälle an das BSI (grundsätzlich anonym; Nennung Betreiber nur bei tatsächlichen Ausfällen oder Beeinträchtigungen)	**sechs Monate** nach Inkrafttreten der Rechtsverordnung

Vorsätzliche oder fahrlässige Verletzung der Pflichten ist eine **Ordnungswidrigkeit nach § 14 BSIG**

Was ist zu tun ? Sonderfälle

- **Nicht** in den Anwendungsbereich fallen **Kleinstunternehmen** im Sinne der Empfehlung der Europäischen Kommission (weniger als 10 Mitarbeiter und Jahresumsatz/ Jahresbilanzsumme höchstens 2 Mio. EUR)
- **Nicht** in den Anwendungsbereich fallen Betreiber Kritischer Infrastrukturen, die aufgrund von Rechtsvorschriften **vergleichbare oder weitergehende Anforderungen** erfüllen müssen (möglicher erster Anwendungsfall: Telematikinfrastruktur im Gesundheitswesen)
- **Vorrangige Sonderregelungen** ergeben sich aus den nebenstehenden Gesetzen

Sonderregelung Atomgesetz

Umsetzung Überprüfung Kommuni-kation	▪ Regelungen im Atomgesetz einschließlich darauf beruhender Rechtsverordnungen mit dem unter-gesetzlichen Regelwerk sind **gleichwertig** zu den Anforderungen des BSI-Gesetzes ▪ Erfüllung der IT-Sicherheitsanforderungen im Rahmen der **Gewährleistung der nuklearen Sicherheit** und **Sicherung kerntechnischer Anlagen**	bestehende Pflichten
Meldung	▪ **Unverzügliche Meldung** erheblicher Sicherheitsvorfälle an das BSI ▪ **Weiterleitung** an die zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder	mit **Inkrafttreten** des IT-Sicherheits-gesetzes

Pflichten bestehen **unabhängig** von der Einstufung als Kritische Infrastruktur (auch die neue Meldepflicht!)

Sonderregelung Energiewirtschaftsgesetz – Netzbetreiber

Umsetzung	▪ Erfüllen der Sicherheitsanforderungen nach einem von der BNetzA erstellten **Sicherheitskatalog 'Netz'**	Umsetzung bis zum **31.01.2018**
Überprüfung	▪ Geeigneter Nachweis der Umsetzung durch **gesondert entwickelte Zertifizierung** des verbindlich vorgegebenen Informationssicherheits-Managementsystems	im Rahmen der **Rezertifizierung**
Kommunikation	▪ Benennung eines Ansprechpartners für IT-Sicherheit	bis zum **30.11.2015**

Pflichten bestehen **unabhängig von Rechtsform und Größe** und unabhängig von der **Einstufung als Kritische Infrastruktur**

Sonderregelung Energiewirtschaftsgesetz – Betreiber von Energieanlagen nach KRITIS-Rechtsverordnung

Umsetzung	▪ Erfüllen der Sicherheitsanforderungen nach einem von der BNetzA erstellten **Sicherheitskatalog 'Erzeugung'**	offen
Überprüfung	▪ **Offen – wahrscheinlich:** Geeigneter Nachweis der Umsetzung durch gesondert entwickelte Zertifizierung des verbindlich vorgegebenen Informationssicherheits-Managementsystems	offen
Kommuni-kation	▪ **Offen – wahrscheinlich:** Benennung eines Ansprech-partners für IT-Sicherheit	offen

Pflichten bestehen **nur** bei **Einstufung als Kritische Infrastruktur**

Sonderregelung Energiewirtschaftsgesetz – Netzbetreiber/Betreiber von Energieanlagen nach KRITIS-Rechtsverordnung

Meldung	▪ **Unverzügliche Meldung** erheblicher Sicherheitsvorfälle an das BSI ▪ **Weiterleitung** an die Bundesnetzagentur	**sechs Monate** nach Inkrafttreten der Rechtsverordnung

Pflichten bestehen **nur** bei **Einstufung als Kritische Infrastruktur** – auch im Hinblick auf Netzbetreiber

Sonderregelung Telemediengesetz

'Sonderfall'

- **Schutz vor unerlaubten Zugriffen** auf die genutzten technischen Einrichtungen durch technische und organisatorische Vorkehrungen, die den Stand der Technik berücksichtigen
- insbesondere geeignet sind **Verschlüsselungsverfahren** und – bei personalisierten Telemedien – **Authentifizierungsverfahren**
- **nur** Diensteanbieter, die Telemedien **geschäftsmäßig** anbieten – Einordnung als kritische Infrastruktur ist **nicht erforderlich**

mit **Inkrafttreten** des IT-Sicherheits-gesetzes

Vorsätzliche oder fahrlässige Verletzung der Pflicht ist eine **Ordnungswidrigkeit nach § 16 TMG**

Sonderregelung Telekommunikationsgesetz

Umsetzung*	▪ **bestehende Pflichten** werden um die Berücksichtigung des '**Stands der Technik**' bei der IT-Sicherheit ergänzt ▪ Sicherheitsanforderungen der BNetzA künftig im **Einvernehmen** mit dem BSI	mit **Inkrafttreten** des IT-Sicherheits-gesetzes
Überprüfung	▪ Kannvorschrift wird durch **Pflicht zur regelmäßigen Überprüfung** der Umsetzung ersetzt, die mindestens alle zwei Jahre stattfinden **soll**	mindestens alle **zwei Jahre**
Kommuni-kation	▪ Zusätzlich: **Information der Nutzer**, wenn Störungen von Datenverarbeitungssystemen von diesen ausgehen ▪ Hinweis auf **technische Mittel zur Abhilfe** sofern technisch möglich und zumutbar	mit **Inkrafttreten** des IT-Sicherheits-gesetzes
Meldung	▪ Erweiterung der bestehenden **Meldepflichten gegenüber der BNetzA** um IT-Sicherheitsvorfälle ▪ Weiterleitung IT-Sicherheitsmeldungen an das **BSI**	mit **Inkrafttreten** des IT-Sicherheits-gesetzes

***** Pflichten bestehen für Betreiber **öffentlicher** Telekommunikationsnetze/Erbringer **öffentlich zugänglicher** Telekommunikationsdienste – Einordnung als kritische Infrastruktur ist **nicht erforderlich**

Vorsätzliche oder fahrlässige Verletzung der Pflichten ist eine **Ordnungswidrigkeit nach § 149 TKG**

Fazit

- Wegen der rechtlichen Architektur des IT-Sicherheitsgesetzes mit dem **Nebeneinander von Alt- und Neuregelungen**, dem **Nebeneinander von KRITIS-Pflichten und Pflichten, die unabhängig bestehen** und den **'noch offenen Baustellen'** ist der Umgang mit den Anforderungen für die Beteiligten eine Herausforderung.
- Weder die Frage **'Wen betrifft es?'** noch die Frage **'Was ist zu tun?'** kann heute schon abschließend rechtssicher beantwortet werden.
- Die für die Beantwortung der Frage der Betroffenheit entscheidende **KRITIS-Rechtsverordnung nach § 10 BSIG** soll in zwei Körben **im ersten und dritten Quartal 2016** kommen; aktuell werden die erarbeiteten qualitativen und quantitativen Kriterien für eine Abgrenzung mit Behörden, Verbänden und Betroffenen diskutiert.
- Wir gehen davon aus, dass **das zu beachtende Mindestniveau an IT-Sicherheit** zeitnah durch die jeweils betroffenen **Branchenverbände** definiert und mit unterschiedlicher Verbindlichkeit vorgegeben wird.
- **Aktuell schon umzusetzende Rechtspflichten** gibt es nur in den Sonderbereichen Atom – Energie – Telemedien und Telekommunikation.

Consulting. Solutions. Services.
Erfahrung macht den Unterschied.

prego. services

Herzlichen Dank

für Ihre

Aufmerksamkeit

prego services GmbH

Neugrabenweg 4
66123 Saarbrücken

Franz-Zang-Straße 2
67059 Ludwigshafen

Kontakt

Fon: +49 (0)681 95943–0
Fax: +49 (0)681 95943–1000

Internet: www.prego-services.de
E-Mail: info@prego-services.de