

Dipl.-Wirtsch.-Ing. Frank Hallfell  
enbiz gmbh, Kaiserslautern

# Das neue IT-Sicherheitsgesetz: Welche Unternehmen sind betroffen? Was ist zu tun?

perspektive.IT, Boppard, 12. Mai 2016

## Kurze Erklärung (Disclaimer)

- ▶ Inhalte juristischer Art stellen eine erste Orientierung und keine Rechtsberatung dar!
- ▶ Die Präsentation ist nach bestem Wissen und Gewissen zusammengestellt – Wir übernehmen keine Haftung für die Vollständigkeit und Richtigkeit!
- ▶ Bei konkreten rechtlichen Fragen wenden Sie sich bitte an die zitierten Stellen oder an einen professionellen Rechtsberater

## Agenda

- ▶ IT-Sicherheitsgesetz
- ▶ Kritische Infrastrukturen
- ▶ Umsetzung
- ▶ Empfehlungen

## Das IT-Sicherheitsgesetz

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (Seit 25. Juli 2015 in Kraft)

- ▶ Kein alleinstehendes Gesetz wie z.B. TMG, BDSG
- ▶ Es enthält Modifikationen und Ergänzungen für bestehende Gesetze:
  - ▶ BSI-Gesetz (BSIG) von 2009
  - ▶ Telemediengesetz (TMG) von 2007
  - ▶ Telekommunikationsgesetz (TKG) von 2004
  - ▶ Atomgesetz (AtG) von 1985
  - ▶ Energiewirtschaftsgesetz (EnWG) von 2005
  - ▶ BKA-Gesetz (BKAG) von 1997

## Sinn und Zweck

- ▶ Signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland
- ▶ Verbesserung der Systeme hinsichtlich der Schutzziele:
  - ▶ Vertraulichkeit
  - ▶ Integrität
  - ▶ Authentizität
  - ▶ Verfügbarkeit
- ▶ Verbesserung der IT-Sicherheit von kritischen Unternehmen zum verstärkten Schutz der Bürger

## Wer ist betroffen?

- ▶ Betreiber sogenannter „Kritischen Infrastrukturen“
- ▶ Genehmigungsinhaber nach dem Atomgesetz
- ▶ Betreiber von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur eingestuft sind
- ▶ Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste
- ▶ Telemediendiensteanbieter

## Was bedeutet „kritische Infrastrukturen“?

§2 Abs. 10 BSIg: „Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

- ▶ Den Sektor **Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung** sowie **Finanz- und Versicherungswesen** angehören und
- ▶ 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.“

## Beispiele Kritischer Infrastrukturen Korb 1:

Sektor	Bereich	Beispielhafte Schwellenwerte
Energie	Stromversorgung	Stromerzeugungsanlage 420 MW
	Gasversorgung	Gasverteilernetz 5.190 Gwh / Jahr
	Versorgung mit Kraftstoff und Heizöl	Handel 420.000 Tonnen Heizöl / Jahr
	Versorgung mit Fernwärme	250.000 Haushalte
Wasser	Versorgung mit Wasser	Wasserwerk 22 Mio m <sup>3</sup> / Jahr
	Beseitigung von Abwasser	Kanalisation 500.000 Einwohner



## Beispiele Kritischer Infrastrukturen Korb 1:

Sektor	Bereich	Beispielhafte Schwellenwerte
Ernährung	Lebensmittelproduktion	Produktion 434.500 t Speisen / Jahr
	Lebensmittelverarbeitung	Verarbeitung 350 Mio L Getränke / Jahr
	Lebensmittelhandel	Verkauf 424.500 t Lebensmittel / Jahr
Informationstechnik und Telekommunikation	Sprach- und Datenübertragung	Zugangsnetz 100.000 Teilnehmeranschlüsse
	Datenspeicherung und -verarbeitung	DNS Resolver 2.500.000 anfragende IP-Adressen / Tag

## Betreiber kritischer Infrastrukturen

- ▶ Geschätzte Zahl meldepflichtige Betreiber: 2.000 (Schätzung der Regierung)
- ▶ Ergänzende und konkretisierende Rechtsverordnung ist bisher für Energieversorgungsnetze (08/2015) und die Sektoren Energie, Wasser, Ernährung, Telekommunikation veröffentlicht (05/2016)
- ▶ Sektoren Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen geplant Anfang 2017

## Betreiber kritischer Infrastrukturen

- ▶ Einrichtung einer Kontaktstelle für das BSI 6 Monate nach Veröffentlichung
- ▶ Verpflichtende Umsetzung der technischen und organisatorischen Maßnahmen innerhalb von 2 Jahren nach Veröffentlichung (Stand der Technik)
- ▶ Bußgeld bei Zuwiderhandlung

## Wer ist nicht betroffen von KRITIS?

- ▶ Kleinunternehmen im Sinne der Empfehlung 2003/361/EC:
  - ▶ Weniger als 10 Mitarbeiter und
  - ▶ Jahresumsatz oder Jahresbilanzsumme geringer als 2 Mio €

### **ABER**

Änderung des Telemediengesetz §13 (Pflichten des Telemedienanbieters) gilt für jeden Betreiber einer kommerziellen Webseite!

## Umsetzung

- ▶ 6 Monate nach Veröffentlichung der Rechtsverordnungen
- ▶ 24 Monate nach Veröffentlichung der Rechtsverordnungen
- ▶ Sofort und für Jeden

## Umsetzung innerhalb von 6 Monaten

- ▶ Einrichtung einer Kontaktstelle (Name, Email, Adresse, Telefon, Mobil, Fax), die **jederzeit** erreichbar ist
- ▶ Meldung der Kontaktstelle an das BSI
- ▶ Benennung und Beschreibung der Kritischen Infrastruktur

Für Betreiber von Energieversorgungsnetzen:

- ▶ 30.11.2015

Sektoren Energie, Wasser, Lebensmittel, IKT:

- ▶ 03.11.2016

## Umsetzung innerhalb von 24 Monaten

- ▶ Durchführung und Nachweis von IT-Sicherheitsaudits alle 2 Jahre
- ▶ Umsetzung der Vorgaben des BSI (ggf. Branchenstandards) beim Audit
- ▶ Rückmeldung der durchgeführten Audits und der Ergebnisse an das BSI
- ▶ BSI kann Beseitigung der Sicherheitsmängel verlangen
- ▶ Meldung von IT-Sicherheitsvorfällen an das BSI

Für Betreiber von Energieversorgungsnetzen:

- ▶ Auditierung bis 31.01.2018

Sektoren Energie, Wasser, Ernährung, IKT:

- ▶ Auditierung bis 03.05.2018

## Sofort (Telemediengesetz §13)

- ▶ Regelmäßige Aktualisierung der Betriebssysteme
- ▶ Regelmäßige Aktualisierung der Software (Webserver und Content-Management-Software)
- ▶ Verhinderung von Drive-by-Downloads
- ▶ Einsetzen von anerkannten Verschlüsselungsverfahren, z.B. https
- ▶ Verantwortung nach Telemediengesetz nicht nicht übertragbar auf Dritte, z.B. Dienstleister
- ▶ Abmahngefahr bei Verstoß bis zu 50.000 Euro



## IT-Sicherheitskatalog (Rechtsverordnung)

- ▶ Forderung eines Informations-Sicherheits-Management-Systems (ISMS) nach DIN/ISO 27001
- ▶ Kontinuierliche Weiterentwicklung in der Organisation verankern

 konkrete Umsetzung

## Prozessmanagement

### Prozessdokumentation:

- ▶ Dokumentation der internen Abläufe
- ▶ Gelenkte Dokumente auch im Bereich IT
- ▶ Verfahrensanweisungen
- ▶ Integration in Qualitätsmanagement (wenn vorhanden)

### Mitarbeiterschulung:

- ▶ Regelmäßige Schulung der Mitarbeiter über das richtige Verhalten und die richtige Nutzung der IT

## Prozessmanagement mit ITIL

### IT Infrastructure Library

- ▶ Sammlung von Beispielen (Best Practice) zur Umsetzung eines IT Service Managements
- ▶ Umsetzung kann in kleinen Teilschritten erfolgen
- ▶ Teile auch Sinnvoll für kleine Unternehmen
- ▶ Bekannte Teile: Service Desk mit Incident-Management (und Problem-Management)

# Systemdokumentation kritischer Systeme

## Hard- und Software-Inventarisierung:

- ▶ Automatisierte Erfassung der Hard- und Software im Unternehmen
- ▶ Erfassung Standort und Einsatzzweck
- ▶ Regelmäßige Aktualisierung der Daten

## Notfalldokumentation:

- ▶ Aufbereitete Sammlung von Telefon-Nummern und Ansprechpartner
- ▶ Dokumentation Wiederanlauf und Disaster-Recovery

## Mindeststandards nach Empfehlung BSI

- ▶ Firewall mit Zertifizierung, z.B. Common Criteria EAL 4+
- ▶ Aktuelle Virens Scanner (Scan-Engine und Viren-Pattern)
- ▶ Aktuelle Software mit aktuellen Patches und aktueller Hersteller-Unterstützung
- ▶ Netzwerksegmentierung mit Zugriffskontrolle
- ▶ Passwortrichtlinien und Überwachung der Einhaltung

## Technische Hilfsmittel (Beispiele)

### Hard- und Softwareinventarisierung

- ▶ OCS NG: kostenloses Tool zur automatischen Hard- und Software-Inventarisierung
- ▶ JDisc: Inventarisierungs-Tool
- ▶ Docusnap: automatisierte IT-Dokumentation

### Configuration Management Database (CMDB)

- ▶ i-doit: Web-Tool für CMDB
- ▶ itop: Komplettes Tool zur Abbildung von ITIL auf Grundlage der CMDB

# Vielen Dank für Ihre Aufmerksamkeit!

---

Weitere Informationen zu

**KRITIS / IT-Sicherheitsgesetz**

**direkt bei enbiz gmbh**