# IT-Sicherheitsgesetz – und nun?

Umsetzung bei Betreibern Kritischer Infrastrukturen

Frankfurt, den 25.02.2016

# AGENDA

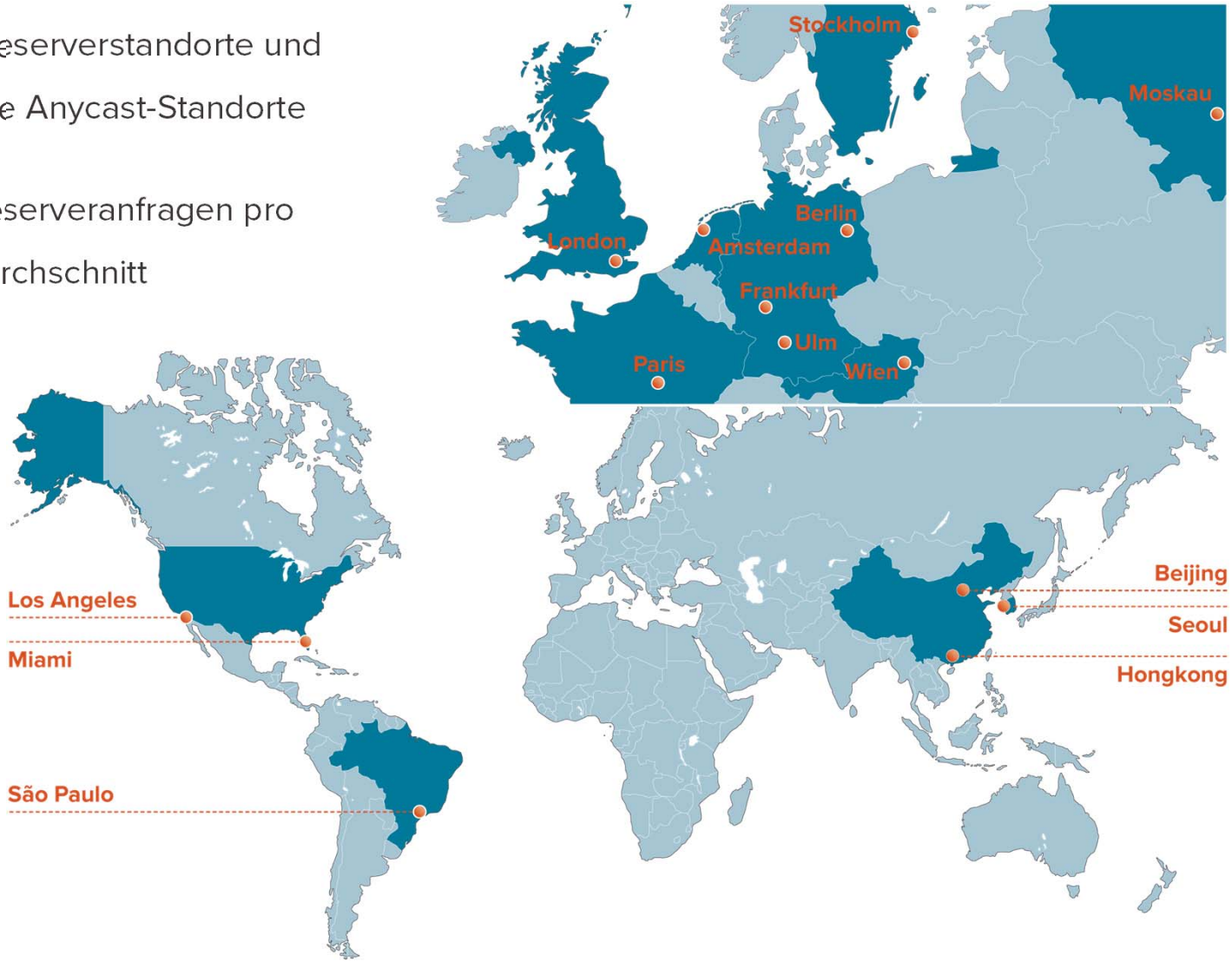
- Kurzvorstellung DENIC eG
- UP KRITIS
- IT-Sicherheitsgesetz
- Überlegungen zur Umsetzung
- Weiteres Vorgehen

# Kurzvorstellung - DENIC eG

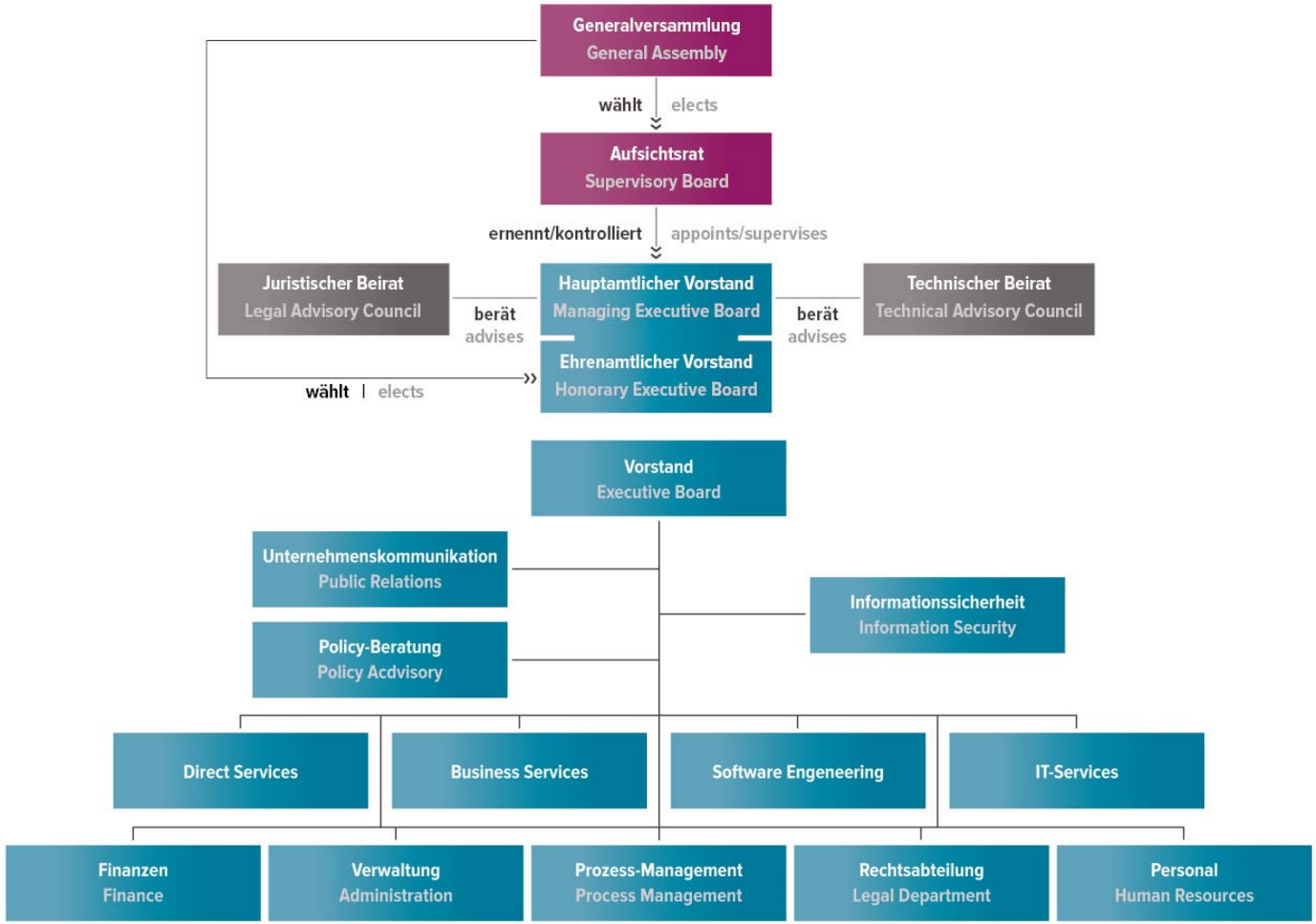
- Eingetragene Genossenschaft mit Sitz in Frankfurt am Main, gegründet 1996.
- Zentrale Registrierungsstelle für alle Domains unterhalb der länderbezogenen Top Level Domain .de sowie für ENUM-Domains (**E**.164 **NU**mber **M**apping) unter .9.4.e164.arpa, dem deutschen Rufnummernraum.
- Selbstverständnis als neutraler, diskriminierungsfreier, Not-for-Profit-Dienstleister für die Internet Community, der seiner Verantwortung gemeinsam mit den mehr als 320 Mitgliedern (Registrare) der Genossenschaft nachkommt.
- Aufgaben und Tätigkeitsbereiche:
  - Betrieb des Nameservices für .de und für .9.4.e164.arpa
  - Betrieb eines automatischen Registrierungssystems und der Domaindatenbank
  - Bereitstellung von Auskunftsdiensten (whois) und einer Service Hotline

# Kurzvorstellung – DENIC eG – Nameservice für .de

- 19 eigene Nameserverstandorte und 35+ ergänzende Anycast-Standorte
- > 40.000 Nameserveranfragen pro Sekunde im Durchschnitt



# Kurzvorstellung – DENIC eG – Organisation



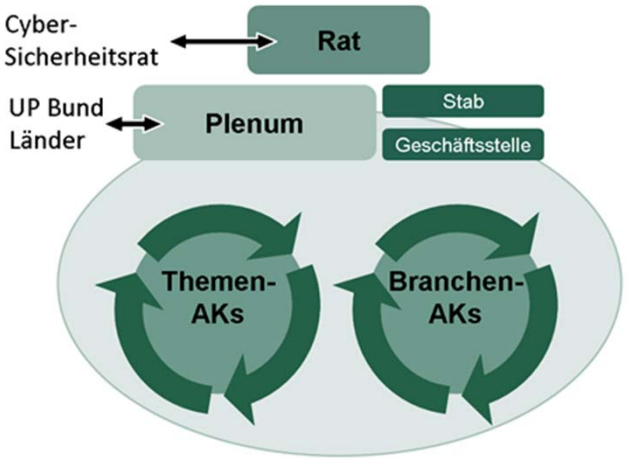
# Kurzvorstellung - DENIC eG – Zusammenarbeit

- Aktive Mitgestaltung an der Weiterentwicklung des Internets in diversen Gremien:
  - Council of European TLD-Registries (CENTR)
  - Deutscher CERT-Verbund
  - DNS-Operations, Analysis and Research Center (DNS-OARC)
  - Internet Corporation for Assigned Names and Numbers (ICANN)
  - Internet Governance Forum (IGF)
  - Internet Engineering Task Force (IETF)
  - Internet Society (ISOC)
  - RIPE Network Coordination Centre (RIPE NCC)
- Weiterentwicklung von Internetstandards
- Unterstützung bei der Zusammenarbeit der ccTLDs

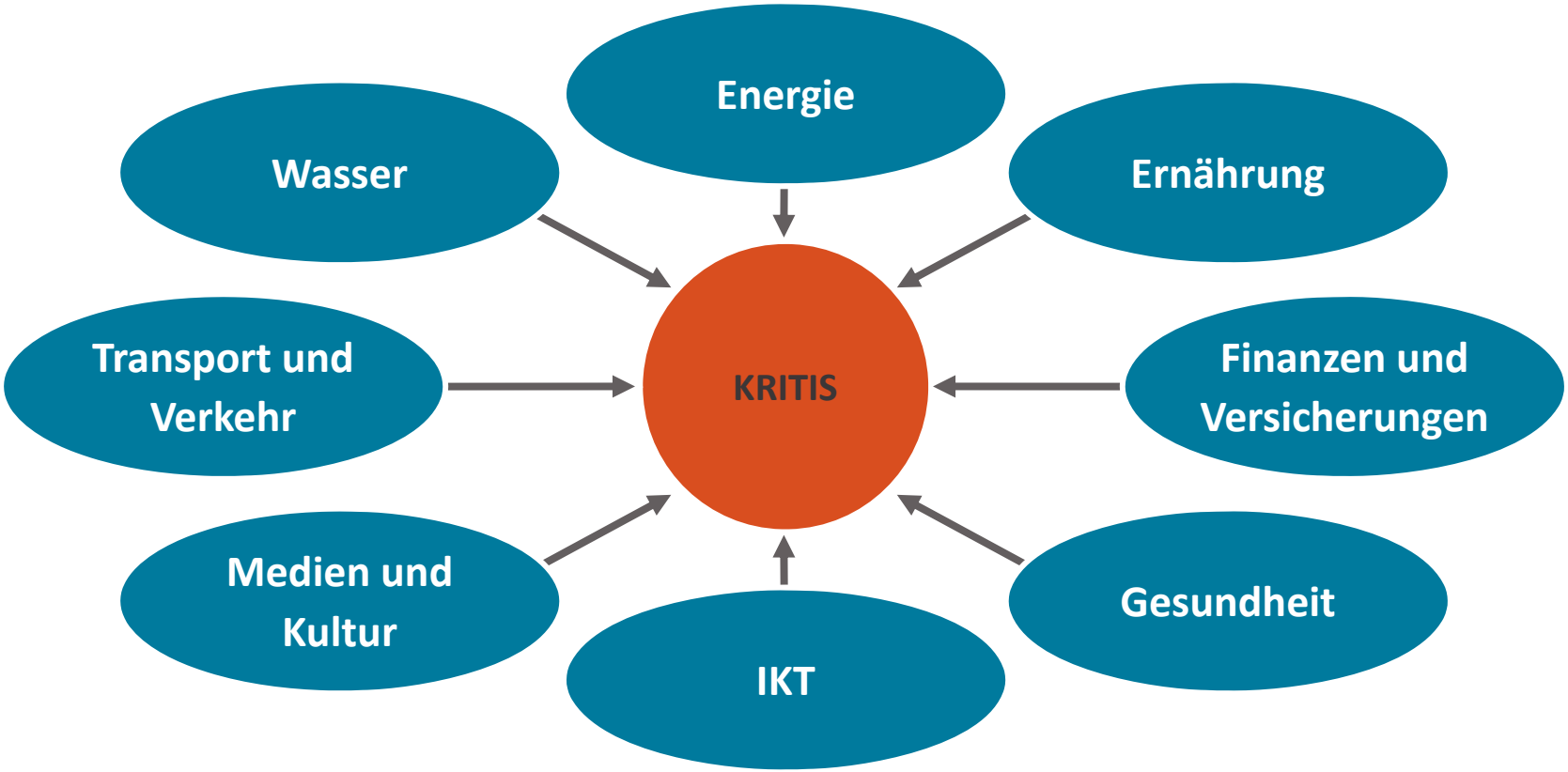
# UP KRITIS – Überblick

- Public Private Partnership (*2005)
  - BMI, BSI, BBK + Wirtschaftsvertreter
- Ziel: Versorgung mit Dienstleistungen Kritischer Infrastrukturen (KI) in DEU aufrechterhalten
- ca. 250 Betreiber aus den 8 relevanten KI-Sektoren
- Strategisch-konzeptionelle Zusammenarbeit in Arbeitskreisen seit 2013
  - Branchen – und Themenarbeitskreise
- Operativer Informationsaustausch mit Anbindung an BSI-Lagezentrum
  - SPOC - Konzept

UP KRITIS



# UP KRITIS – Sektorenübersicht



# UP KRITIS – Mitarbeit der DENIC eG

- Aktive Mitarbeit am UP KRITIS seit 2011 (Mitglied im Plenum)
- Leiter / Sprecher des Branchenarbeitskreises Internet-Infrastruktur
  - Mitglieder: BCIX, DE-CIX, DENIC, Deutsche Telekom, ECIX, STRATO
  - Gäste: 1&1, Amazon, Bitkom, BMI, BSI, eco
  - Primäres Ziel: Vernetzung, vertrauensvoller Informationsaustausch sowie Entwicklung gemeinsamer Positionen und Dokumente für die Branche
- Mitarbeit im Kernteam (BAK-Leiter, BMI und BSI) zur Beschreibung der sektorspezifischen Dienstleistungen, qualitativen (Anlagen) und quantitativen (Schwellenwerte) Kriterien als Grundlage für BSI-KritisV.

# IT-Sicherheitsgesetz – Überblick

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- In Kraft getreten am 25.07.2015
- Identifikation von Betreibern Kritischer Infrastrukturen über BSI-KritisV

## Artikelgesetz

Das Gesetz umfasst mehrere Änderungen in bestehenden Gesetzen

- Gesetz über das Bundesamt für Sicherheit der IT (BSIG)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Energiewirtschaftsgesetz (EnWG)
- Atomgesetz (AtG)

## Wesentlichen Ziele

- Mindestniveau an IT-Sicherheit einzuhalten zum Schutz von Unternehmen und Bürger/Innen, bspw. durch die Umsetzung von branchenspezifischen Sicherheitsstandards (B3S).
- Betreiber Kritischer Infrastrukturen müssen dem BSI IT-Sicherheitsvorfälle mit einer hohen Kritikalität melden.
- Stärkung des BSI hinsichtlich Rechten, Pflichten und Zuständigkeiten.

## Mandat

- Das BSI kann KRITIS-Betreiber beraten und wird zentrale Meldestelle.
- Verpflichtung dem Bundesministerium des Inneren (BMI) jährlich Auskunft zu geben (Lagebild).
- Produkte und Systeme auf Sicherheitsaspekte untersuchen.
- Erkenntnisse können weitergegeben und veröffentlicht werden.

# IT-Sicherheitsgesetz – Anforderungen

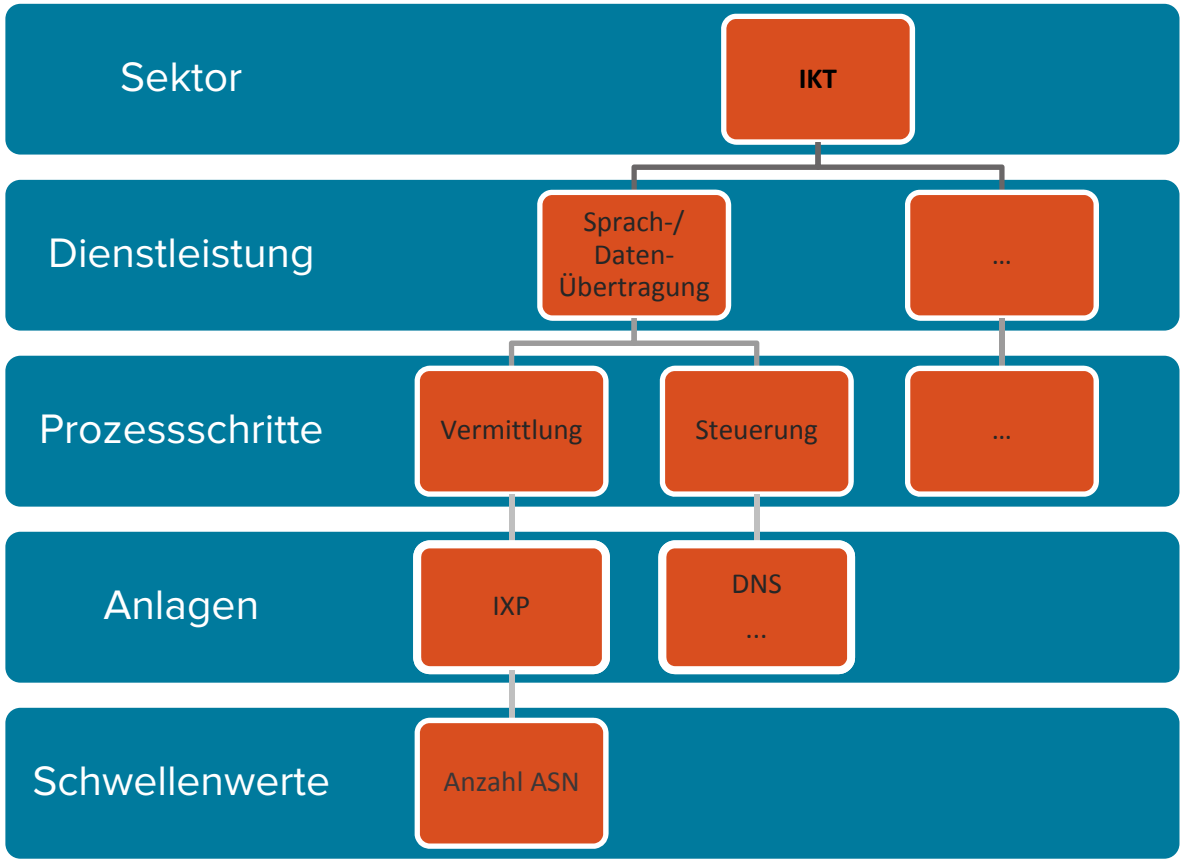
- § 8a
  - Treffen von angemessenen organisatorischen und technischen Vorkehrungen
  - Stand der Technik ist zu berücksichtigen
  - Betreiber können einen Branchenspezifischen Sicherheitsstandard vorschlagen
  - Nachweispflicht durch Audits alle 2 Jahre gegenüber dem BSI
- § 8b
  - BSI als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen
  - Kontinuierliches Lagebild mit Pflicht zur unverzüglichen Weitergabe an Betreiber
  - Alarmierungskontakt ist innerhalb von 6 Monaten zu benennen
  - Verpflichtung zur Meldung von (absehbaren) Sicherheitsvorfällen

# BSI-KritisV – Vorgehensweise

Versorgung der Gesellschaft mit wichtigen Dienstleistungen

**Qualität**: Dienstleistungen in den KRITIS-Sektoren, die für die Versorgungskette relevant sind und abstrakte Anlagen

**Quantität**: Schwellenwerte innerhalb dieser Dienstleistungen



# BSI-KritisV – Vorläufige Schwellenwerte

- 500.000 Menschen als Schwellenkorridor zur Festlegung Kritischer Infrastrukturen
- Umrechnung auf anlagenspezifische Kriterien oder Expertenbefragung

| Anlagentyp | Kriterium | Schwelle |
|---|---|---|
| Internet Exchange Point (IXP) | Anzahl der angeschlossenen AS | 300 |
| DNS-Resolver außerhalb von öffentlichen TK-Netzen | Anzahl der abfragenden IP-Adressen pro Tag | 2.500.000 |
| Autoritativer DNS-Server | Anzahl der Domains, für die der Server autoritativ ist oder die aus der Zone delegiert werden | 250.000 |

# Überlegungen zur Umsetzung von § 8a und § 8b

- Was sind die kritischen Dienstleitungen und damit verbundene Schutzziele?
- Welche Gefährdungslage ist innerhalb der Branche zu beobachten?
- Was ist der Reifegrad zur Umsetzung von sicherheitsrelevanten Anforderungen innerhalb der Branche?
- Wie ist der Umsetzungsstatus von getroffenen Maßnahmen?
- Sind eventuell Zertifizierungen, die das Schutzziel umfassen, vorhanden?
- Wollen wir einen eigenen (internationalen) Standard entwickeln?
- Sollen wir den Weg der Normierung einschlagen?

Umsetzung von § 8a in Anlehnung an internationale Normen und Best Practices

# Überlegungen zur Umsetzung von § 8a und § 8b

- Definition und Beschreibung der Kritischen Dienstleistung und der IT-Systeme
- Konsequente Etablierung:
  - eines Information Security Management Systems nach ISO/IEC 27001:2013,
  - eines Business Continuity Management Systems nach ISO 22301,
  - eines Risikomanagement-Prozesses nach ISO/IEC 27005

  in einem integrierten Ansatz und unter Berücksichtigung der strategischen Ausrichtung
- Betrachtung von branchenspezifischen Bedrohungen und Umsetzung von Best Practices
- Umsetzung des Meldewesens und Benennung der Kontaktstellen
- Definition von Kriterien zur Meldung von Sicherheitsvorfällen nach ISO/IEC 27035:2011
- Auditierung des ISMS und Nachweis gegenüber dem BSI

# Weitere Vorgehensweise

- Referentenentwurf BMI Ende Januar 2016
- Verbändebeteiligung (02.02.2016 – 23.02.2016)
- Anhörung im BMI am 02.03.2016
- Fertigstellung des B3S innerhalb des BAK
- Inkrafttreten der BSI-KritisV Ende März / Anfang April 2016
- Einreichung des B3S beim BSI (Anerkennung)
- Benennung Kontaktstelle und Etablierung Meldewesen in Richtung BSI
- GAP Analyse zur Ermittlung des aktuellen Umsetzungsstatus in den kDL

DANKE !

FRAGEN ?

KONTAKT:

Boban Krsic
<krsic@denic.de>

PGP Key-ID:
0x43C89BA9