Bundesamt
für Sicherheit in der
Informationstechnik

Schutz Kritischer Infrastrukturen als gemeinsame Herausforderung für Staat und Wirtschaft

11. Security Forum – TH Brandenburg
19. Januar 2017

Dr. Uwe Jendricke
Bundesamt für Sicherheit in der Informationstechnik

Router-Ausfall

```
POST /UD/act?1 HTTP/1.1
Host: 127.0.0.1:7547
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
SOAPAction: urn:dslforum-org:service:Time:1#Se
Content-Type: text/xml
Content-Length: 534

<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://sche
 SOAP-ENV:encodingStyle="http://schemas.xmlsoa
  <SOAP-ENV:Body>
    <u:SetNTPServers xmlns:u="urn:dslforum-org
      <NewNTPServer1>192.0.2.1</NewNTPServer1>
```

TLP-GREEN

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Angriffe des Mirai Botnetzes auf Port 7547

Versuchte Infektion von Routern über das Protokoll TR-064

CSW-Nr. 2016-454513-11k3, Version 1.1, 01.12.2016

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten

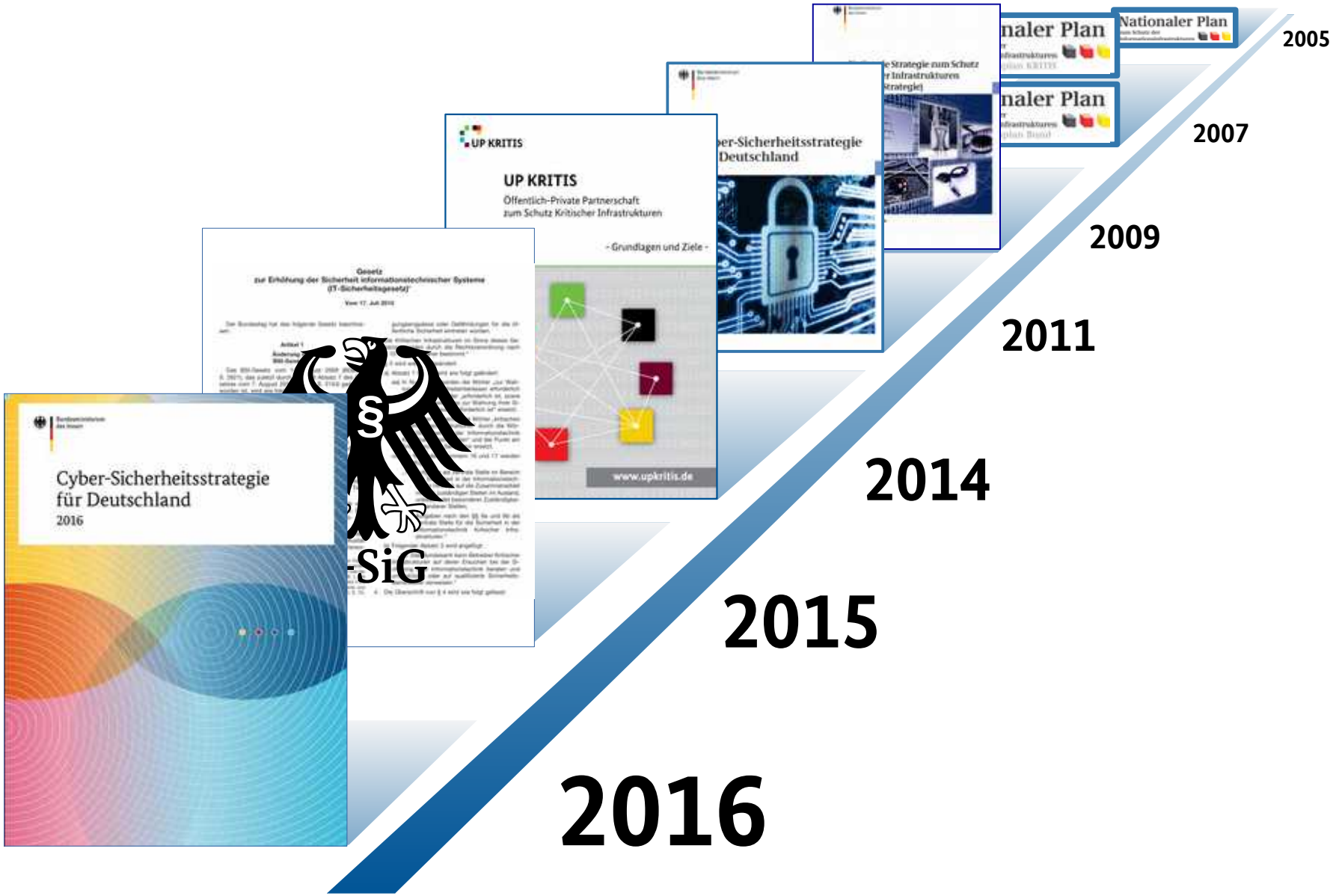
November/Dezember 2016

Vorfälle der letzten Zeit

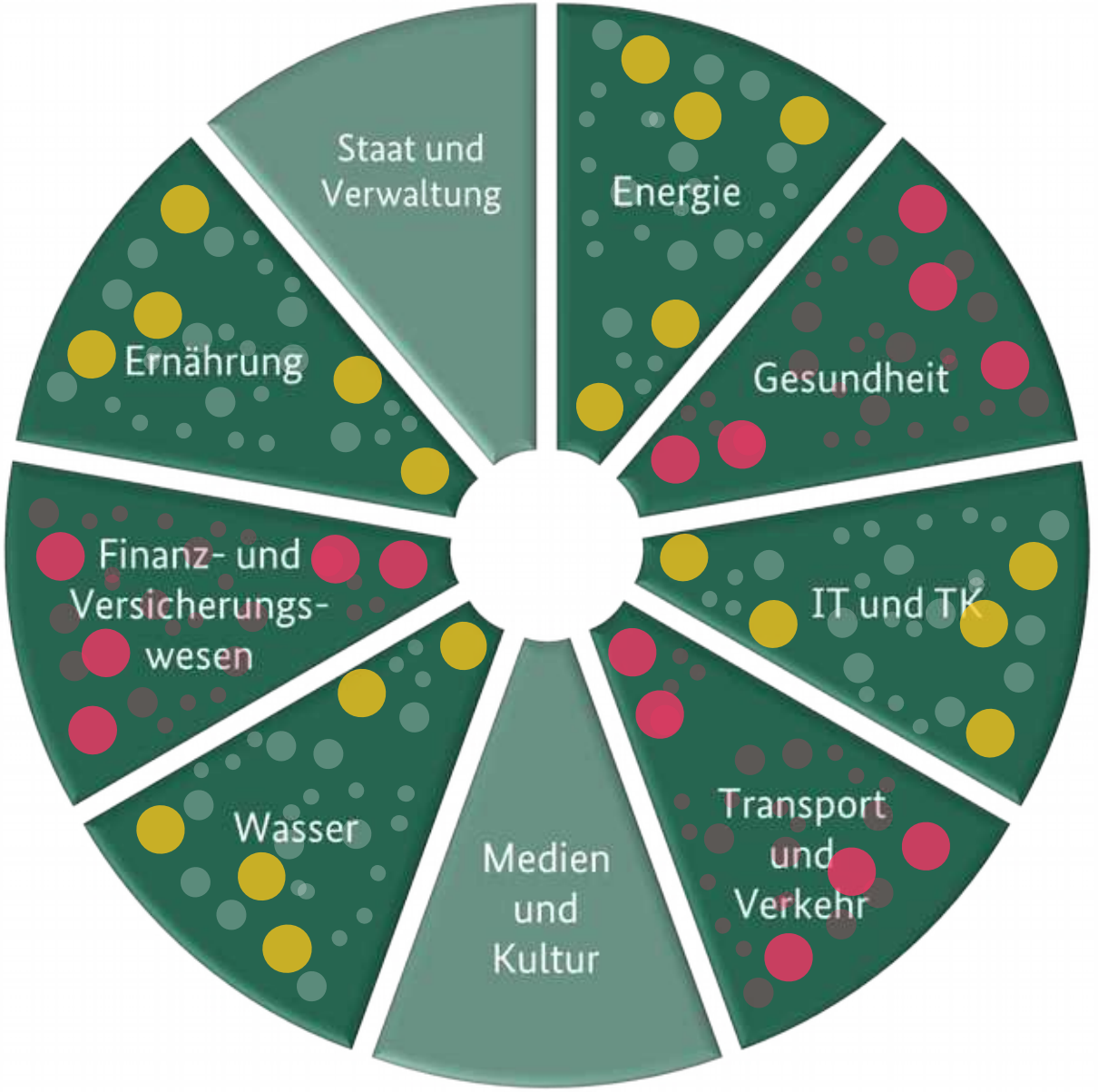
- *Informationstechnik und Telekommunikation:*
  - 11/16: Router Telekom AG
- *Gesundheit:*
  - 02/16: Ransomware–Virus in Krankenhäusern
- *Finanzen:*
  - 05/16: Cyber-Angriff auf Zentralbank Bangladesch - 81 Millionen Dollar erbeutet (SWIFT)
- *Energie:*
  - 12/15: Angriff auf Stromversorgung Ukraine
  - 04/16: AKW Gundremmingen
- *Transport:*
  - 09/16: DDoS Angriff Flughafen Schwechat

Schutz Kritischer Infrastrukturen

- Historie -



Wer ist KRITIS im Sinne des IT-SiG?



1. Korb: Sektoren IT & TK, Energie, Ernährung, Wasser

2. Korb: Sektoren Finanzen, Transport+Verkehr, Gesundheit

IT-Sicherheitsgesetz (IT-SiG) und BSI-Kritisverordnung (BSI-KritisV)

BSI-Kritisverordnung

- Identifikation von KRITIS

IT-SiG § 8a

Maßnahmen, Standards

- Stand der Technik
- Branchenspezifische Sicherheitsstandards

Prüfung der Maßnahmen

- Audits, Zertifizierungen
- Erfüllung der Anforderungen: Nachweise

IT-SiG § 8b

Meldewesen, Lagebild, Bewältigung

- BSI: zentrale Meldestelle, Lagebild
- Betreiber: Meldepflicht, Meldewesen
- Hersteller: Mitwirkung

Identifikation von KRITIS: Auszüge aus der Verordnung

1.	**Stromversorgung**		
1.1	Stromerzeugung		
1.1.1	Erzeugungsanlage	installierte Netto-Nennleistung (elektrisch) in MW	420
1.1.2.	Erzeugungsanlage mit Wärmeauskopplung (KWK-Anlage)	installierte Netto-Nennleistung (direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wär-menennleistung ohne Ko MW	420

2.	**Trinkwasserversorgung**		
2.1	Gewinnung		
2.1.1	Gewinnungsanlage	Gewonnene Wasser-menge in Mio. m³/Jahr	22
2.1.2	Wasserwerk	Wasseraufkommen in Mio. m³/Jahr	22

2.	**Datenspeicherung und-verarbeitung**		
2.1	Housing		
2.1.1	Rechenzentrum	vertraglich vereinbarte Leistung in MW (am 30. Juni eines Kalen-derjahres)	5
2.2.	IT-Hosting		
2.2.1	Serverfarm	Anzahl der laufenden Instanzen (Jahres-durchschnitt)	25 000

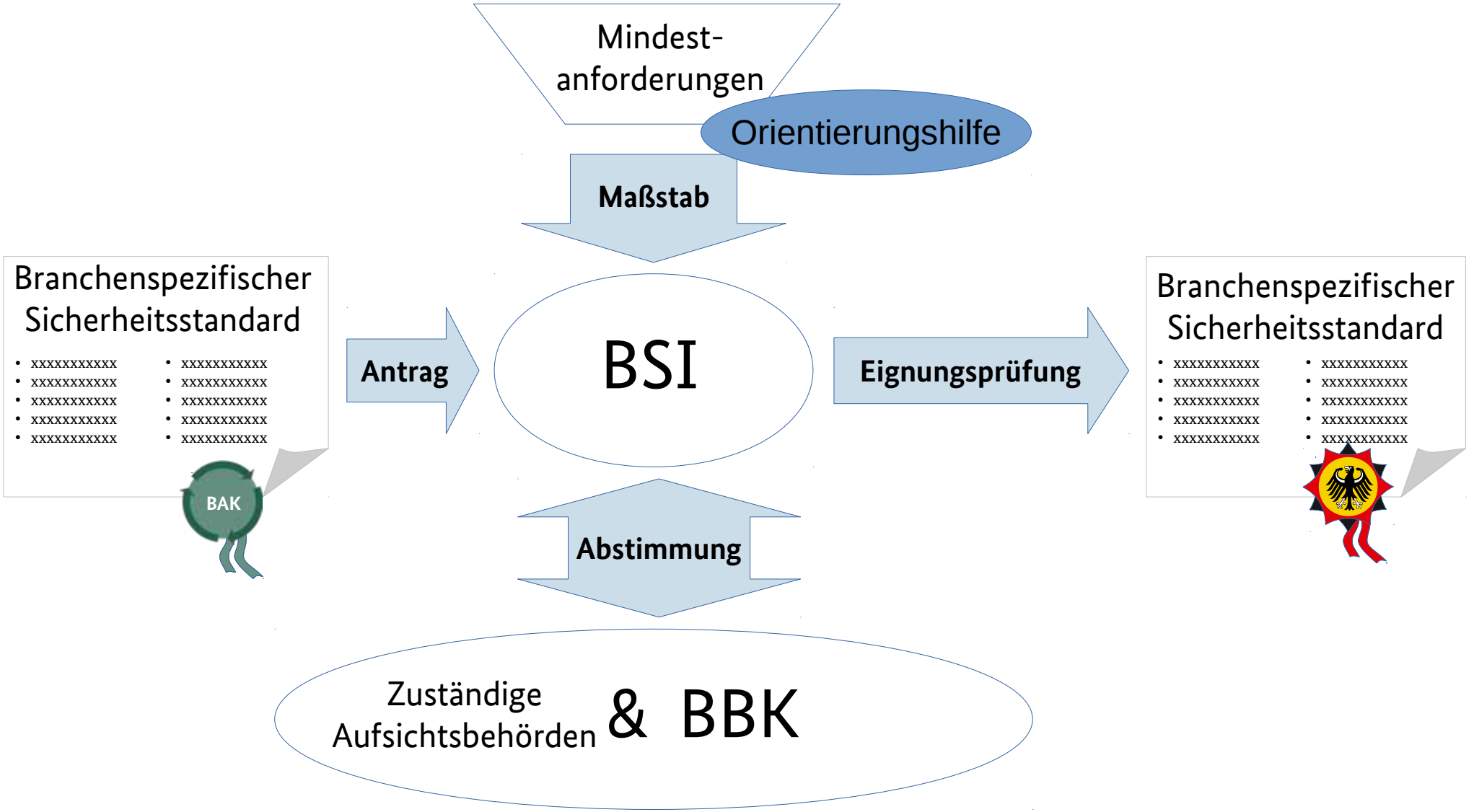
Zeitplan IT-Sicherheitsgesetz

	Sachstand	2017				2018		2019	
IT-Sicherheits-gesetz	In Kraft seit Juli 2015								
1. Korb*	In Kraft seit Mai 2016 - Registrierung - Meldepflicht	Branchenspezifische Sicherheitsstandards werden erstellt				5/18 Nach-weis Stand der Technik			
2. Korb**	Entwurf der Verordnung	BSI-KritisV wird abgestimmt	Verordnung tritt in Kraft	Melde-pflicht beginnt	Registrierungs-frist endet			Nach-weis Stand der Technik	

*1. Korb: Sektoren Energie, IT+TK, Ernährung, Wasser

**2. Korb: Sektoren Finanzen, Transport+Verkehr, Gesundheit

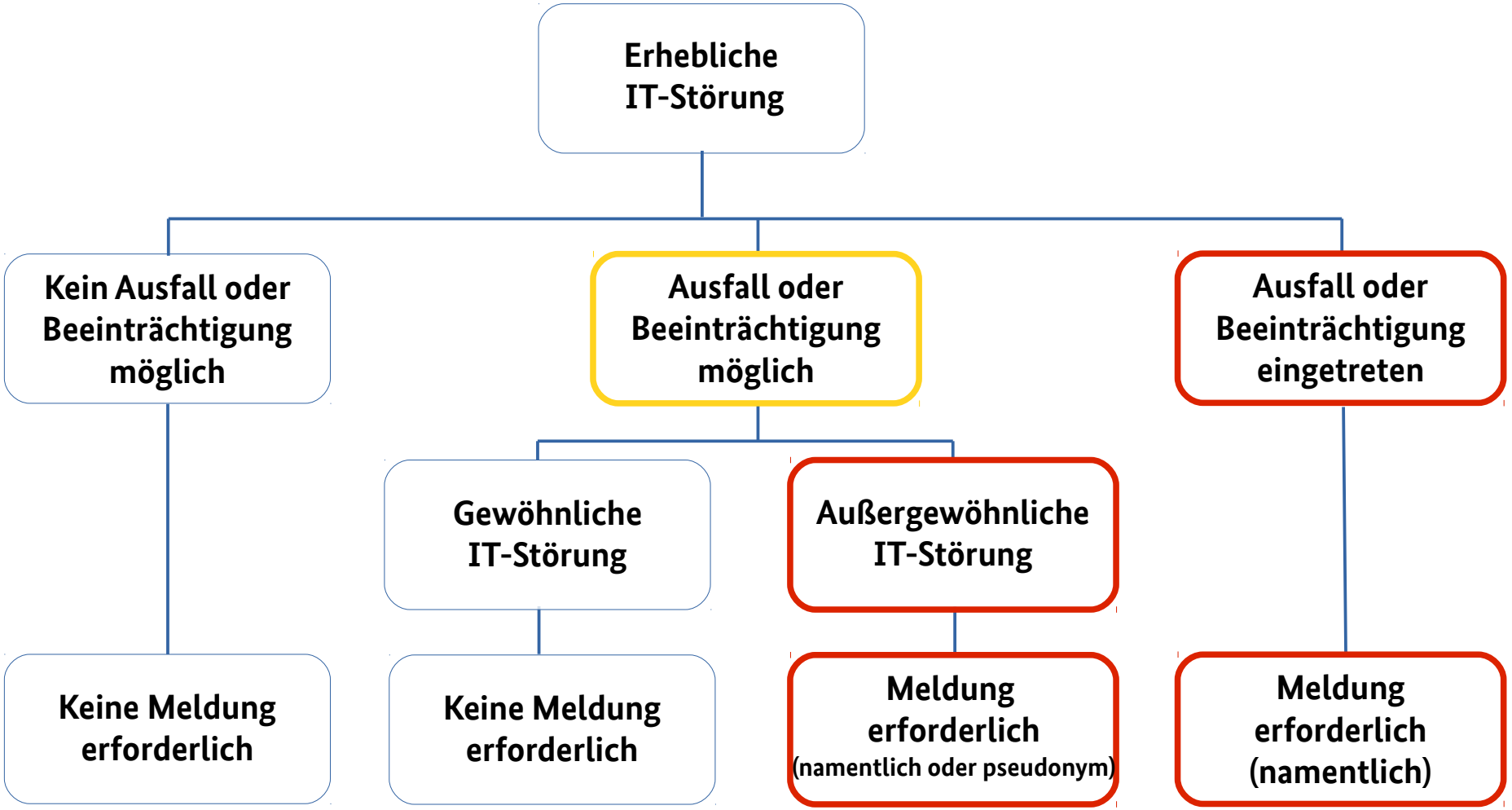
§ 8a: Anerkennungsprozess branchenspezifische Sicherheitsstandards



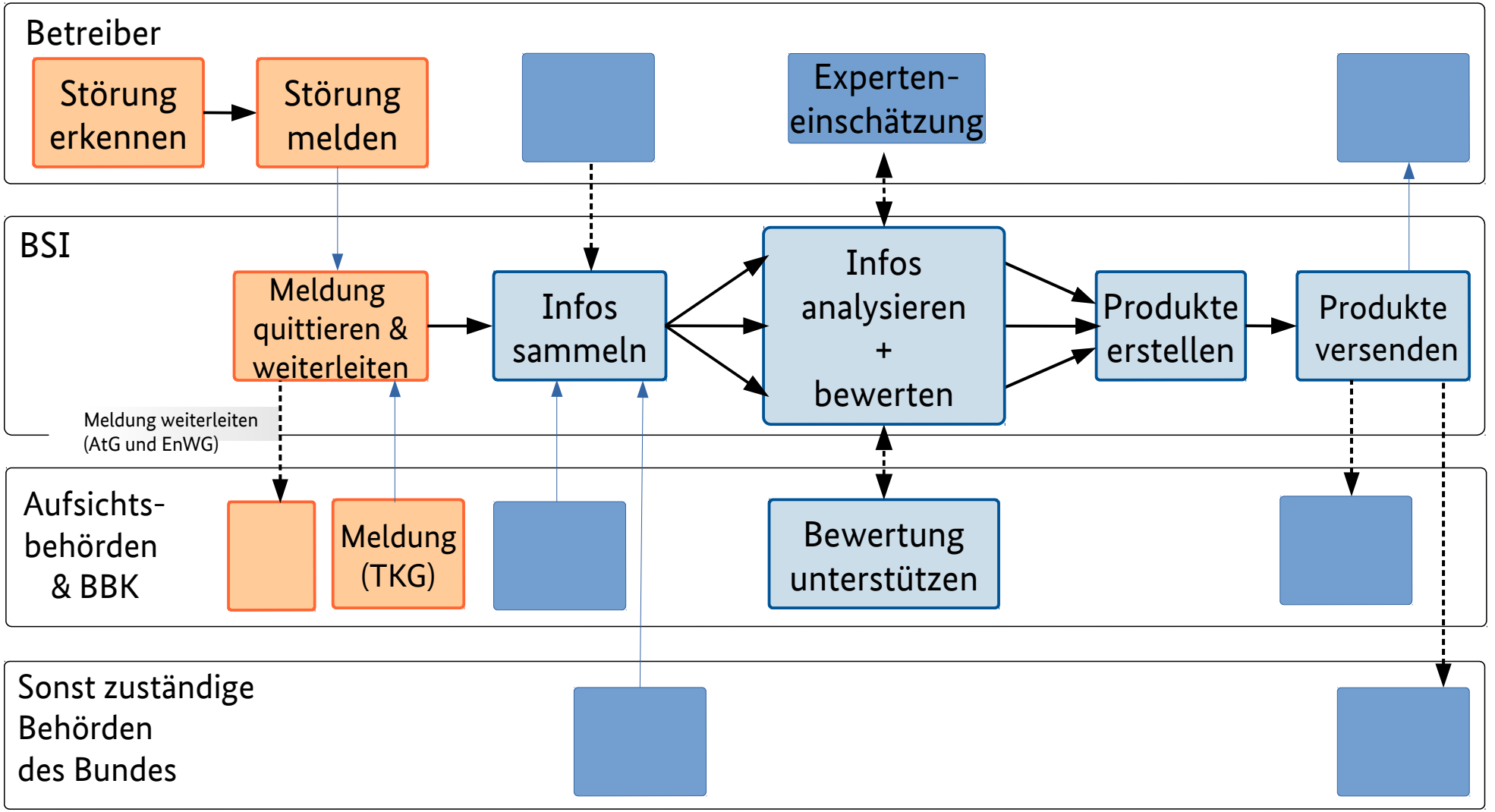
BBK: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe

§ 8b: Wann muss gemeldet werden?

Meldekriterien und -schwellen



§ 8b: Informations- und Meldeflüsse



UP KRITIS

UP KRITIS

- Ziele -

Operative Zusammenarbeit

Basis der Zusammenarbeit

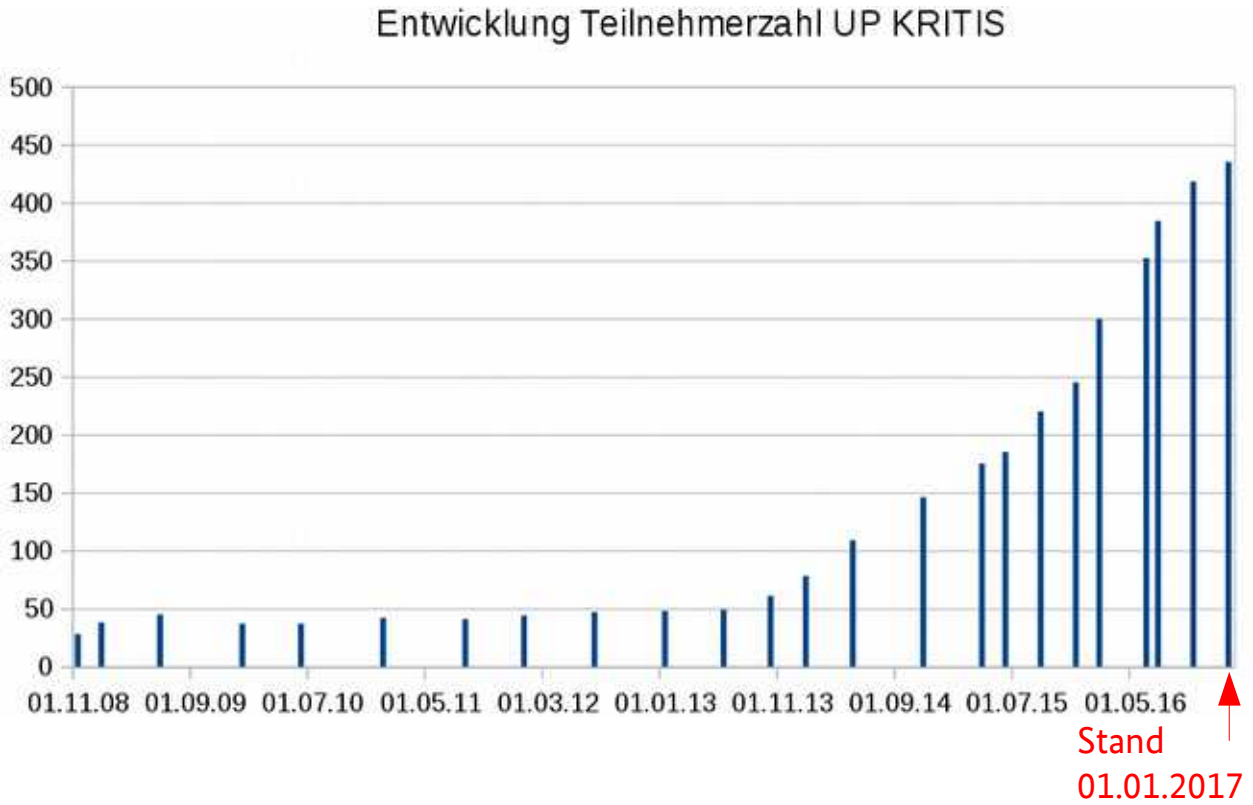
Strategisch-konzeptionelle Zusammenarbeit

UP KRITIS

- Teilnehmer -

Wer kann teilnehmen?

- Alle **Organisationen** mit Sitz in Deutschland, die Kritische Infrastrukturen in Deutschland betreiben
- Nationale **Fach- und Branchenverbände** aus den KRITIS- Sektoren
- Die zuständigen **Behörden**



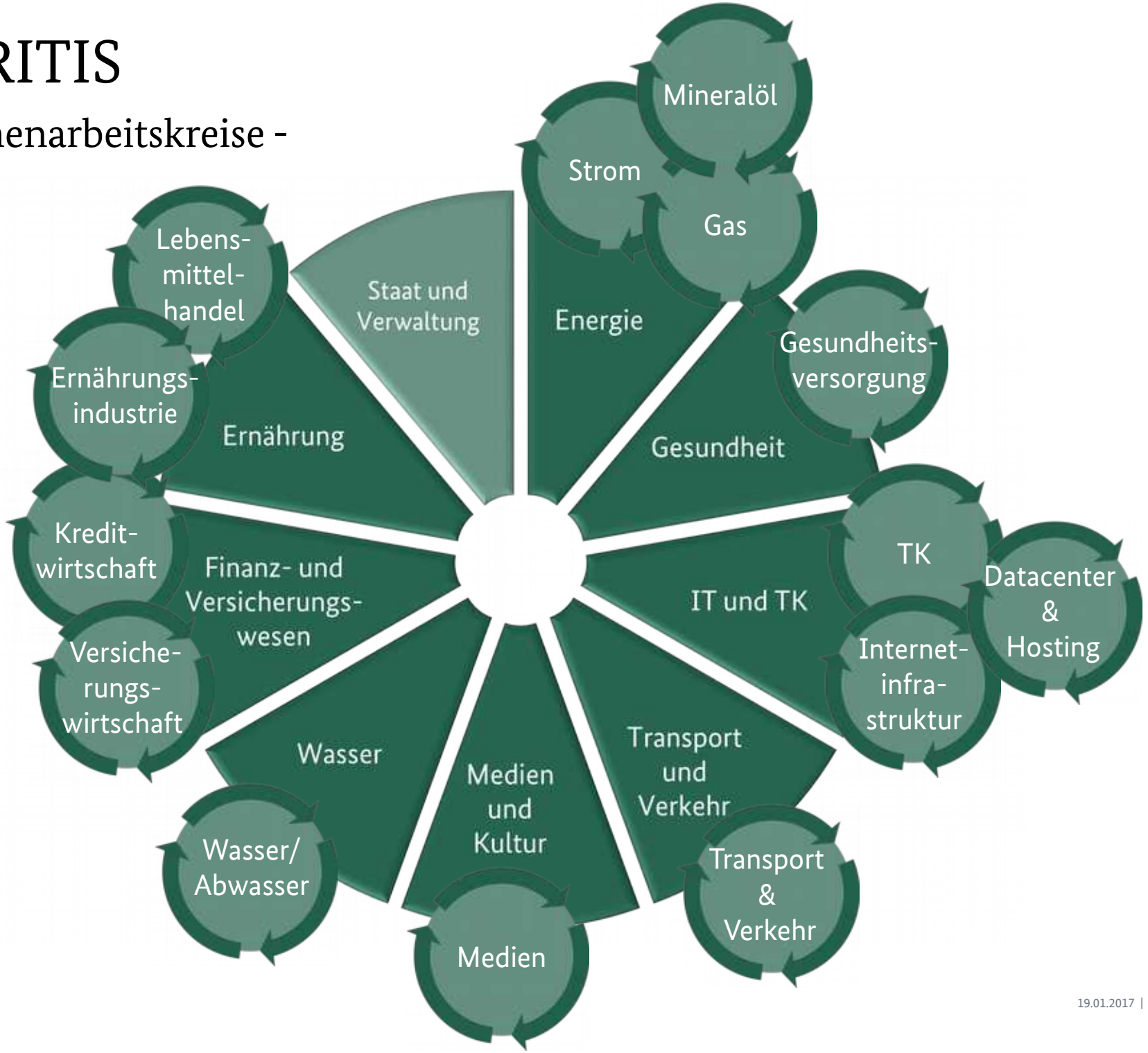
UP KRITIS

- Themenarbeitskreise -

- Anforderungen an Lieferanten
- Audits & Standards
- Krisenkommunikationssystem
- KRITIS-Tagung
- Operativer Informationsaustausch
- SPOC-Austausch
- Szenariobasierte Krisenvorsorge
- Übung

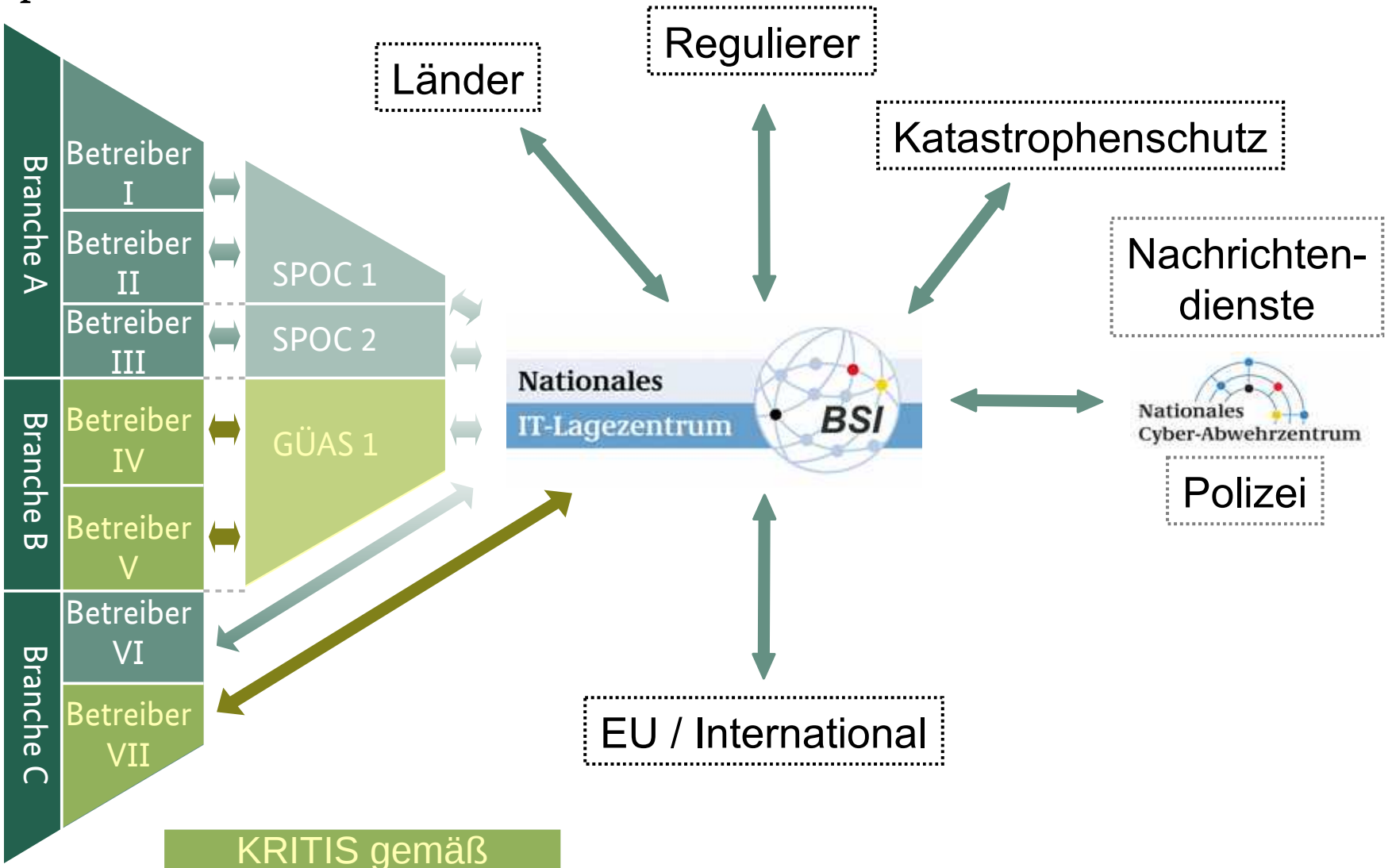
UP KRITIS

- Branchenarbeitskreise -



UP KRITIS

- Operativ-technische Zusammenarbeit -



GÜAS: Gemeinsame übergeordnete Ansprechstelle (BSIG)
SPOC: Single Point of Contact (UP KRITIS)

Router-Ausfall

November/Dezember 2016

TLP-GREEN

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

Angriffe des Mirai Botnetzes auf Port 7547

Versuchte Infektion von Routern über das Protokoll TR-064

CSW-Nr. 2016-454513-11k3, Version 1.1, 01.12.2016

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten

UP KRITIS

Best-Practice-Empfehlungen

für Anforderungen an Lieferanten

zur Gewährleistung der Informationssicherheit

in Kritischen Infrastrukturen

Version 1.2 vom 05.07.2016

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
Referat CK32 Kritische Infrastrukturen - Grundsatz
Dr. Uwe Jendricke
Godesberger Allee 185-189
53175 Bonn

Tel. +49 (0) 228 99-9582 5507
Fax +49 (0) 228 99-10-9582-5507

uwe.jendricke@bsi.bund.de
www.bsi.bund.de
www.upkritis.de