ENERGY

Sicherheit kritischer Infrastruktur - weit mehr als nur IT

IT-Sicherheitstag Sachsen – 14.Juni 2018

Dr. Thomas Werner

Decarbonisierung

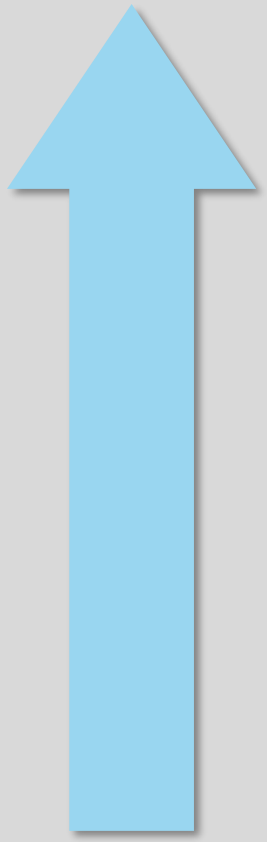
Dezentralisierung

Digitalisierung

CO_2

01001001
10010100
01010010
01010100
01110101

Die Bedrohung steigt und die Gefahr ist real



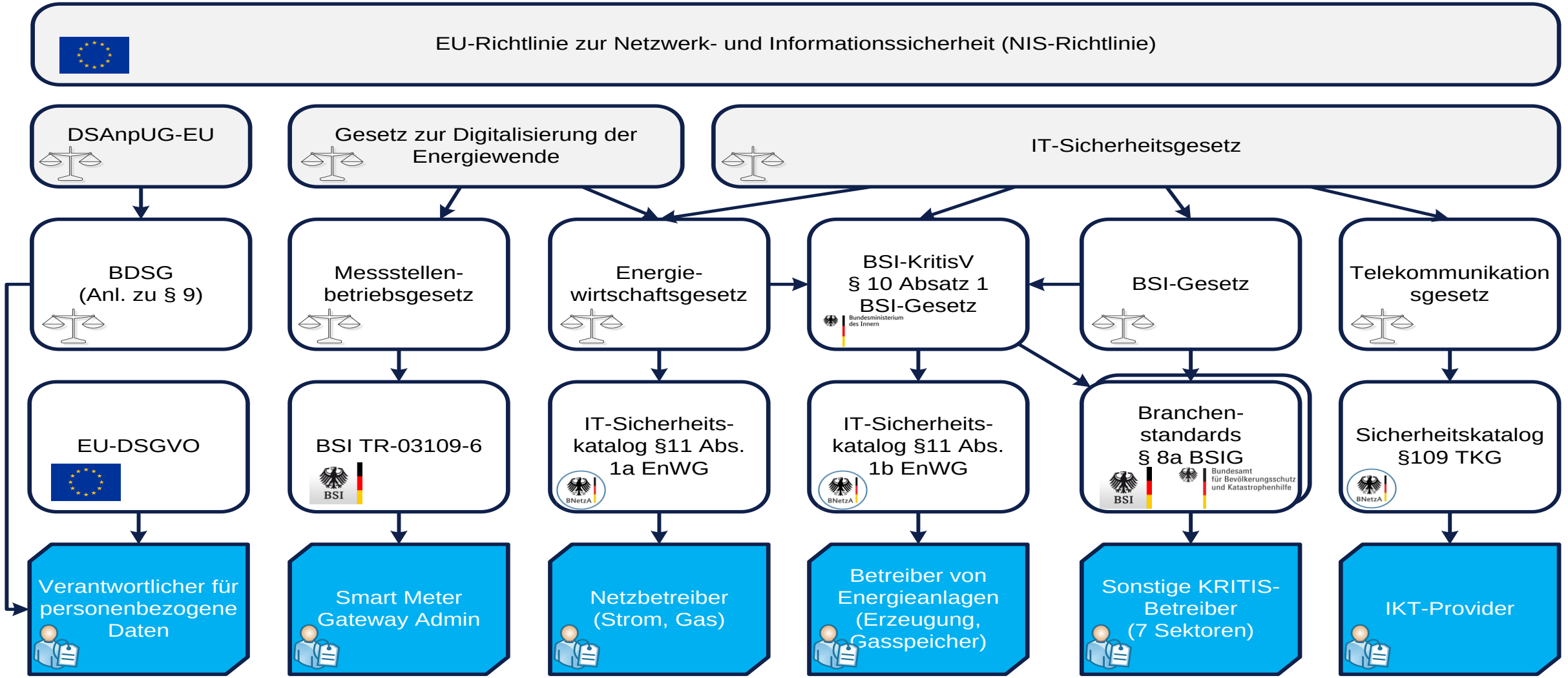
2017	> 200,000 computers in 150 countries	WannaCry ransomware cyber attack
2016	German nuclear power plant	Computer viruses infection
2015	Ukraine power grid and cyber attack	Outages resulted which lasted several hours and affected approximately 225,000 people in the regions
2014	Nuclear power plant in South Korea	The attackers released sensitive and confidential information online, including the designs and manuals for the plant's equipment
2014	US public utility network infiltrated	Chinese hacker 'Ugly Gorilla' infiltrated the network
2013	US power company turbine control system	A technician inserted an infected USB drive into a computer on the network. The incident kept a plant off-line for three weeks
2012	Qatar's RasGas hit by virus	A virus which infiltrated 30,000 computer workstations forcing oil traders to revert to communicating by fax and telex
2011	Stuxnet worm targets Iran's Natanz nuclear factory	Reportedly ruined a fifth of the country's nuclear centrifuges

Top 10 Bedrohungen 2016

Nr. (Nr. alt)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering und Phishing†	Infektion mit Schadsoftware über Internet und Intranet
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

Legende: †NEU Quelle: BSI-CS 005

Rechtliche Randbedingungen (vereinfachte Darstellung)



Integrale und umfassende Betrachtung aller Bereiche

Recht und Regulierung

Betrieb und Organisation

Systeme, IT und OT