OPENKRITIS

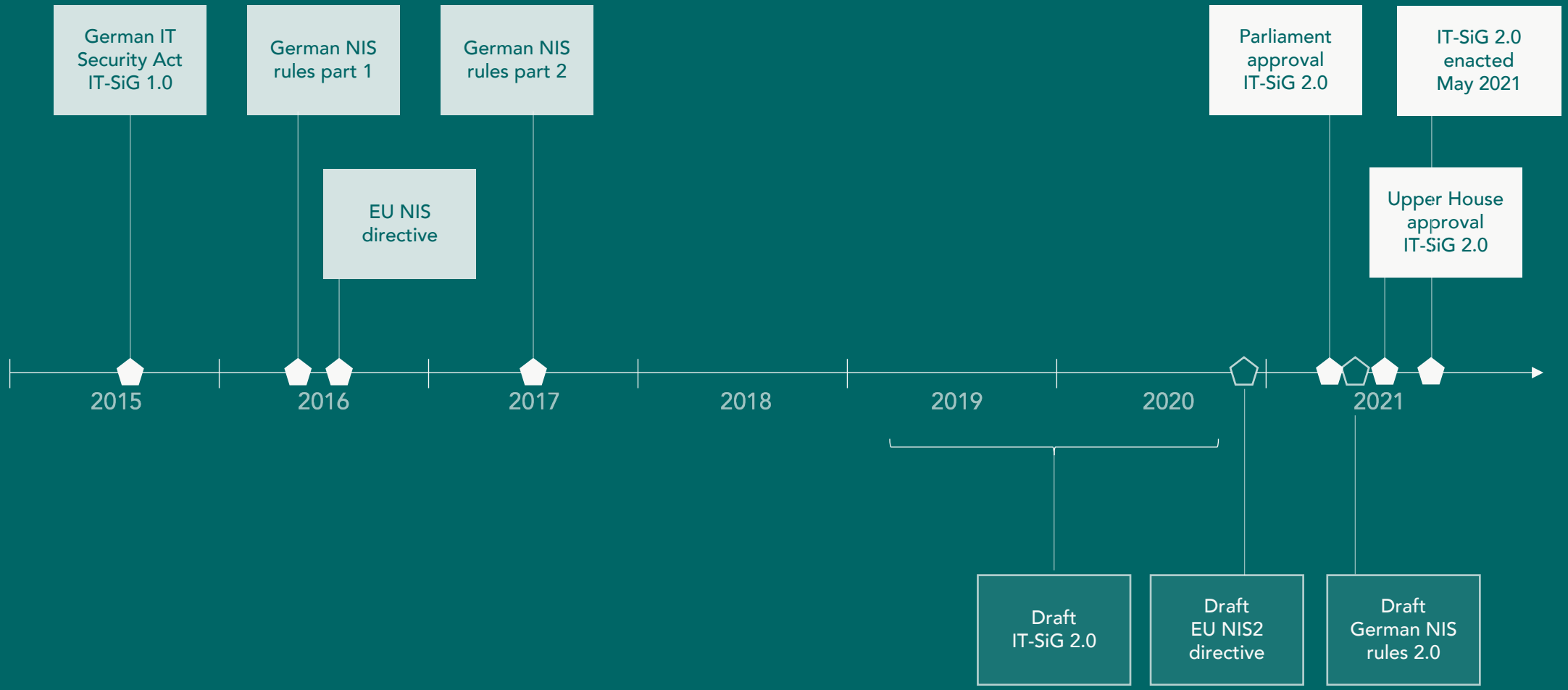
German IT Security Act 2.0

IT-Sicherheitsgesetz 2.0

Briefing kit

June 17, 2021 · OpenKRITIS

German critical infrastructure law



Changes in IT Security Act 2.0

New rules for operators

Detection of cyber attacks
More incident reporting
Critical components
Immediate registration

More operators in scope

Critical sector waste management
Special public interest entities (SPIE)
Lower thresholds (↓ 6)
More asset types (+17)

More federal rights

Central reporting office
Deep inspections
Protection of federal networks
More staff

Fines and consumer protection

Higher fines for operators
More possible violations
More certifications

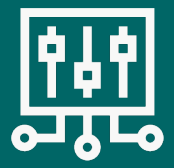
Stronger Cyber security

Detection of attacks

- Cyber attack detection
- Mandatory systems and processes for attack detection
- = SOC, SIEM, correlation

Incident reporting

- More reporting to BSI needed
- Notification during emergencies on reaction and response
- To include PII/PID



Components

- Critical components in critical (infrastructure) assets
- Approval required from the German interior ministry
- Defined for the telco sector

Registration

- Immediate registration required at BSI as operator
- Includes central SPOC
- BSI might register operators

New in scope: Waste and SPIE

More businesses affected

Waste management

- ❑ New critical sector *Municipal waste*
- ❑ Essential service *Disposal of municipal waste:*
  - a. Collection
  - b. Disposal
  - c. Recycling
- ❑ Asset classes and thresholds still to be defined

SPIE (UNBÖFI)

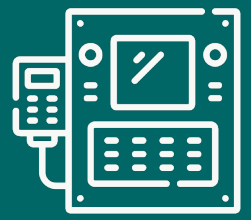
- ❑ Special public interest entities (German UNBÖFI)
- ❑ Important but ≠ critical infrastructure, 3 groups:
  1. SPIE defense, arms, federal IT (export control)
  2. SPIE economic relevant entities
  3. SPIE hazardous materials (chemicals)
- ❑ Separate SPIE cyber security requirements

More critical assets and operators

Lower thresholds

- ❑ Lower thresholds = more affected critical infrastructures
- ❑ 6 thresholds lowered ↓
- ↓ Electricity supply lower
- ↓ IT hosting/housing/exchanges lower
- ❑ 5 other changes to thresholds

More critical infrastructures



- ❑ New critical infrastructure types in existing sectors = more operators
- → Energy: 6 new, 2 removed
- → Health: 1 new, 2 removed
- → Transport: 6 new, 1 removed
- → IT/telco: 1 new
- → Finance: 3 new

More operators

- ❑ More critical operators expected with the new IT-SiG 2.0 act
- ❑ +270 more operators to 1600 current
- ❑ Strong impact: energy and finance
- ❑ New SPIE, waste not yet defined

Stronger sanctions

More violations listed

- 17+ violations defined in IT-SiG 2.0
- Infringements against KRITIS regulation are administrative violations
- e.g. incomplete or missing evidence, lack of registration, incomplete measures

Higher fines

- Higher fines for the listed violations
- Between 100k and 2M EUR per violation
- Up to 20M EUR for legal entities/bodies

And what now?

Existing operators	New operators	Telecom operators	SPIE
Detection of cyber attacks - SIEM/SOC	Identify critical infrastructures	Identify critical components	Register as SPIE with government
Identify new critical infrastructure	Register as operator at BSI	Report and clear critical components	Implement cyber security measures
Check for lower critical thresholds	Implement cyber security measures		Implement reporting reqs
Implement new reporting reqs	Implement reporting reqs		

Want to learn more on German CI regulation?

openkritis.de – free information resource (in German)

Still missing the right approach?

I help with that: insignals.net

OpenKRITIS

Open information resource on critical infrastructures.

Briefing Kit IT Security Act 2.0
Date: June 17, 2021
Version: 1.4

Imprint

Paul Weissmann c/o Insignals GmbH
Rheinwerkallee 6
53227 Bonn, Germany

https://www.openkritis.de · ISSN 2748-565X
info@openkritis.de · +49 176 58952135

Annex – IT-SiG 2.0 articles

§8a (1a)	**Attack detection**	§8b (3) §8b (3a)	**Immediate registration requirements** **BSI is allowed to designate operators**
§8b (4a)	Incident notification requirements	§14 (1-4)	Higher fines up to 20M EUR More listed violations (+11)
§9b	Critical components	§4b §5c	BSI as central reporting office for IT security Information collection on telco data
§2 (10)	Critical sector waste management	§7a-§7d	BSI inspections of IT products, operator networks, instructions to telcos/DSPs
§8f	Special public interest entities SPIE (German UNBÖFI)	§9a §9c	BSI certification and conformity methods IT security labels
KritisV	Lower thresholds (↓ 7) More critical infrastructure classes (+14)	§4a §5a	Federal network protection by BSI Access to protocols and logs from federal IT

Sources

- IT-Sicherheitsgesetz 2.0: Bundesgesetzblatt, .pdf, 27.5.2021
- Beschlussempfehlung IT-SiG 2.0: 19/28844, .pdf
- Entwurf IT-SiG 2.0 Regierung: 19/26106, .pdf
- Entwurf KritisV 2.0: 26.4.2021, .pdf
- Alle verfügbaren Versionen: AG KRITIS
- Das neue IT-Sicherheitsgesetz 2.0: OpenKRITIS