German and EU Critical Infrastructures
IT-Sicherheitsgesetz 2.0 and EU NIS2/RCE
German and EU KRITIS law

- German IT Security Act (IT-SiG 1.0)
- German KRITIS group 1
- KritisV group 2
- EU NIS directive
- IT-SiG 2.0 Drafts
- KritisV 2.0 approved 18.8.2021
- New sectors, UBI, rules etc. 2020/2023

Timeline:
- 2015: German IT Security Act (IT-SiG 1.0)
- 2016: German KRITIS group 1
- 2017: KritisV group 2
- 2018: EU NIS directive
- 2019: Drafts IT-SiG 2.0
- 2020: IT-SiG 2.0 enacted May 2021
- 2021: KritisV 2.0 approved 18.8.2021
- 2022: New sectors, UBI, rules etc. 2020/2023

Enactment EU NIS2/RCE
Transposition in national law EU members
## Extended KRITIS scope in IT-SiG 2.0

<table>
<thead>
<tr>
<th>New rules for operators</th>
<th>More operators in scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection of cyber attacks</td>
<td>CI sector waste management</td>
</tr>
<tr>
<td>More incident reporting</td>
<td>Special public interest entities (UBI)</td>
</tr>
<tr>
<td>Critical components</td>
<td>Lower thresholds (↓ 6)</td>
</tr>
<tr>
<td>Immediate registration</td>
<td>More CI asset types (+17)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>More government rights</td>
<td>Fines and consumer protection</td>
</tr>
<tr>
<td>Central reporting agency</td>
<td>Higher fines for operators</td>
</tr>
<tr>
<td>Deep inspections</td>
<td>More possible violations</td>
</tr>
<tr>
<td>Protection of federal networks</td>
<td>More certifications</td>
</tr>
<tr>
<td>More staff</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Further enhancements:
- Lower thresholds (↓ 6)
- More CI asset types (+17)
- More government rights
- Higher fines for operators
- More possible violations
- More certifications
- More staff
More IT-SiG 2.0 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
- Notifications in emergencies on reaction and response
- To include personal data (PID)

Components
- Critical components in critical infrastructures
- 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 IT-SiG 2.0: Waste and UBI

Waste management

- New critical sector Municipal waste
- Essential service Disposal of municipal waste:
  - Collection
  - Disposal
  - Recycling
- Asset classes and thresholds still to be defined

UBI (UNBÖFI)

- Special public interest entities (German "UBI")
- Important but ≠ critical infrastructure, 3 groups:
  1. UBI defense, arms, VS-IT (export controlled)
  2. UBI economic relevant entities + suppliers
  3. UBI hazardous materials (chemicals)
- Special cyber security requirements for UBIs
More operators in IT-SiG 2.0 scope

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

- More critical infrastructures
  - More critical infrastructures defined in existing sectors = more operators
  - Energy: 6 new, 4 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 new IT-Sicherheitsgesetz 2.0
  - +270 more operators to 1600 current
  - Most impact in energy and finance
  - New UBI & waste not yet covered, to be handled in more regulation
EU with additional KRITIS regulation

**EU RCE**
Directive on the resilience of critical entities

RCE is the resilience baseline for EU operators. Companies that provide critical services in the EU will be regulated for resilience and risk and supervised.

**RCE regulation**
- 10 Critical EU sectors and entities
- Resilience requirements for operators
- National governance, EU oversight

**EU NIS2**
Directive for a high common level of cybersecurity across the Union

NIS2 is the cyber security rulebook for EU operators. Companies that provide essential services and infrastructure in the EU will be regulated for cyber security and supervised.

**NIS2 regulation**
- 10 Essential and 6 important EU sectors
- Cyber security requirements for operators
- National governance, EU oversight
## EU and German KRITIS regulation

<table>
<thead>
<tr>
<th>Sectors</th>
<th>EU RCE</th>
<th>EU NIS2</th>
<th>IT-SiG 2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operators</td>
<td>10 Critical</td>
<td>10 Essential 6 Important</td>
<td>8 Critical KRITIS 3 Important UBI</td>
</tr>
<tr>
<td>Identified by national gov's Entities reported to EU</td>
<td>Medium and large enterprises DSP register with ENISA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>For critical services:</td>
<td>For networks and IT systems:</td>
<td>National thresholds with operators self-identification</td>
<td></td>
</tr>
<tr>
<td>a. Prevention</td>
<td>a. Policies</td>
<td>For IT of critical services:</td>
<td></td>
</tr>
<tr>
<td>b. Physical security</td>
<td>b. Incident Management</td>
<td>a. Security organization</td>
<td></td>
</tr>
<tr>
<td>c. Crisis management</td>
<td>c. BCM and crisis management</td>
<td>b. Secure technologies</td>
<td></td>
</tr>
<tr>
<td>d. BCM and suppliers</td>
<td>d. Supply chain security</td>
<td>c. Cyber attack detection</td>
<td></td>
</tr>
<tr>
<td>e. Personnel security</td>
<td>e. Test and audit</td>
<td>d. Critical components</td>
<td></td>
</tr>
<tr>
<td>f. Awareness</td>
<td>f. Cryptography</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Measures

### For critical services:
- Prevention
- Physical security
- Crisis management
- BCM and suppliers
- Personnel security
- Awareness

### For networks and IT systems:
- Policies
- Incident Management
- BCM and crisis management
- Supply chain security
- Test and audit
- Cryptography

### For IT of critical services:
- Security organization
- Secure technologies
- Cyber attack detection
- Critical components

## Reporting

### Incident reporting

### Risk analysis and planning

### Resilience authority
- Inspections and audits

### Incident reporting

### Audit and evidence

### Cyber authorities, CSIRT
- Enforcement, audits, sanctions

## National

- Resilience authority
- Inspections and audits

- Incident reporting

- Audit and evidence

- Cyber authorities, CSIRT
- Enforcement, audits, sanctions

- BSI
- Evidences, audits, sanctions
KRITIS in Germany: What now?

**Existing KRITIS**
- Detection of cyber attacks - SIEM/SOC
  
**New KRITIS**
- Identify critical infrastructures

**Telecom operators**
- Identify "critical components"

**UBI/UNBÖFI**
- Register as SPIE with government

- Detection of cyber attacks - SIEM/SOC
- Identify new critical infrastructure
- Check for lower critical thresholds
- Implement new reporting reqs

- Identify critical infrastructures
- Register as operator at BSI
- Implement cyber security measures
- Implement reporting reqs

- Identify "critical components"
- Report and clear critical components
- Implement cyber security measures
- Implement reporting reqs

- Register as SPIE with government
- Implement cyber security measures
- Implement reporting reqs

- All: Prepare for EU regulation

*from 2023*
*from 2021/23/24*
*from 2023/24*
*from ~2022*
Don't miss out on Critical Infrastructures:

OpenKRITIS.de

(40+ articles, podcast, webinars)
OpenKРИTIS

Open information resource on critical infrastructures.

German and EU KRITIS

Date: November 17, 2021
Version: 1.0

© Copyright Paul Weissmann 2021

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