

A large, complex hedge maze in a park. The hedges are made of dense, brownish-green bushes, some with yellow-green leaves. The maze is set in a park with many trees in the background, some with green leaves and some with autumn-colored leaves. The sky is overcast.

The regulation maze

EU and German cyber security laws for critical service providers

criticality /ˌkrɪt.ɪˈkæɪl.ə.ti/

noun

a relative measure of the importance of a given infrastructure in terms of the impact of its disruption or functional failure on the security of supply, i.e. providing society with important goods and services.

Federal Ministry of the Interior and Community: National Strategy for Critical Infrastructure Protection

38 %

**adoption rate of a fully integrated resilience management
programme in the telecommunications sector**

Criticality in telecommunications

The vulnerability paradox



The Mirai incident

Wakeup call for Dt. Telekom

- ~ 1 mio CPEs affected in botched botnet takeover attempt
- Was supposed to be used for DDoS attacks in Liberian (!) telco wars, ended up as a denial of service to Arcadyan Speedport routers...



Photo: Thamizhparithi Maari, Wikimedia Commons, CC BY-SA 3.0 DEED
<https://creativecommons.org/licenses/by-sa/3.0/>

Epiphany after the Mirai incident

Immediate legal repercussions

- Network provider, in the event of a disruption:
 - may restrict, redirect or prevent use of services (to customers)
 - may cut traffic to „sources of interference“
- Federal Office for Information Security (BSI) may „take the measures necessary to restore the security or functionality of the information technology system concerned“
- Same applies to the Federal Network Agency (BNetzA), the supervisory authority for the telecommunication sector

Further changes to telco regulations

IT Security Act 2.0 - amendments to TKG and BSI-G in 2021

- BSI gets authorisation to perform portscans
- Introduction of restrictions on the use of „critical components“
 - Need to apply for authorisation of use by the Federal Ministry of the Interior and Community (BMI)
 - Can be refused or asked to provide proof of trustworthiness of the equipment's manufacturer
-

90 %

of all companies under KRITIS regulation endorse its usefulness

65 %

adoption rate for cybersecurity measures required by regulation

77 %

adoption rate for cybersecurity measures required by regulation

79 %

adoption rate for cybersecurity measures required by regulation

84 %

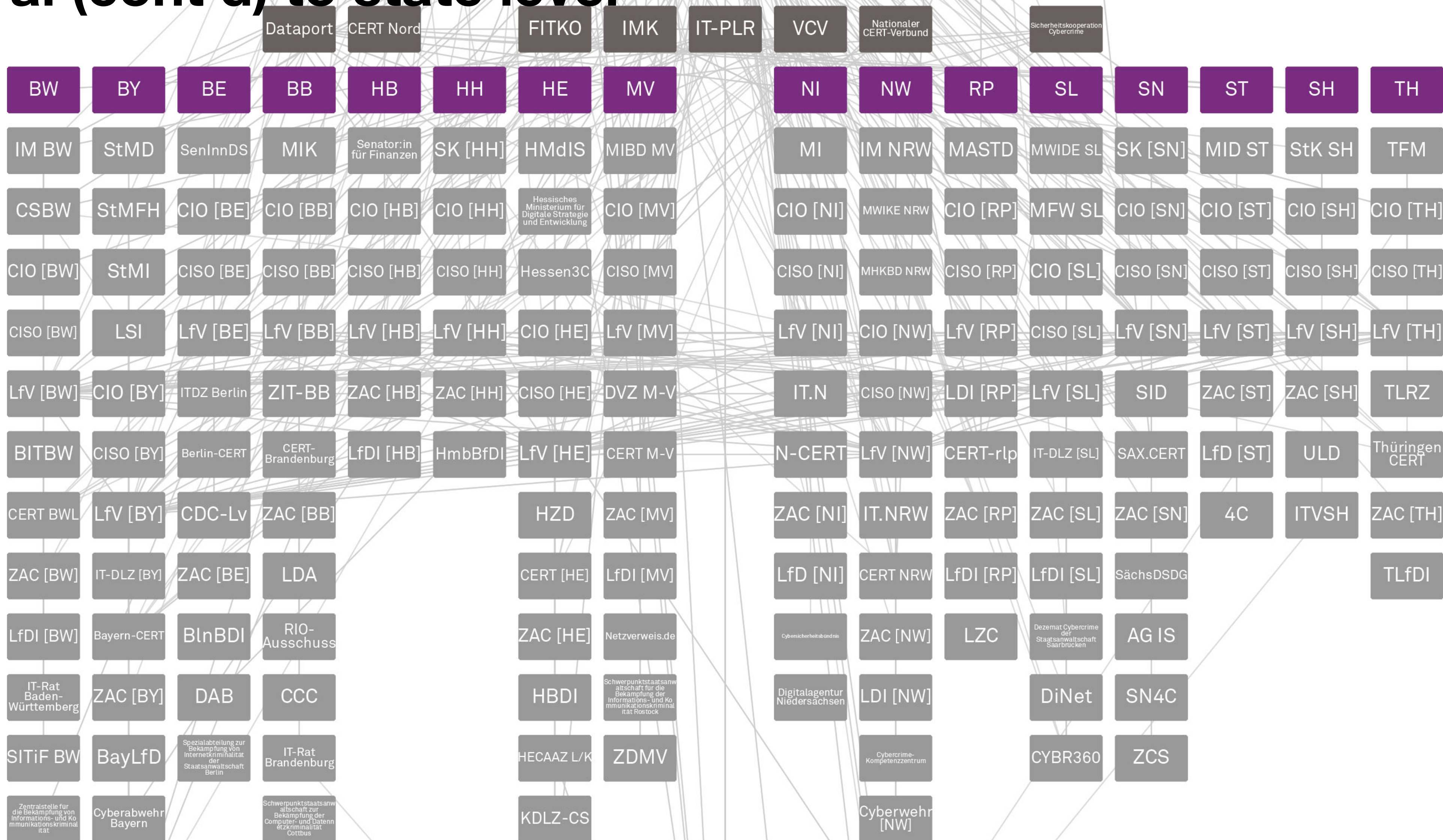
adoption rate for cybersecurity measures required by regulation

89 %

adoption rate for cybersecurity measures required by regulation

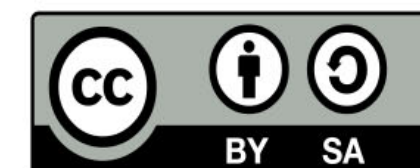
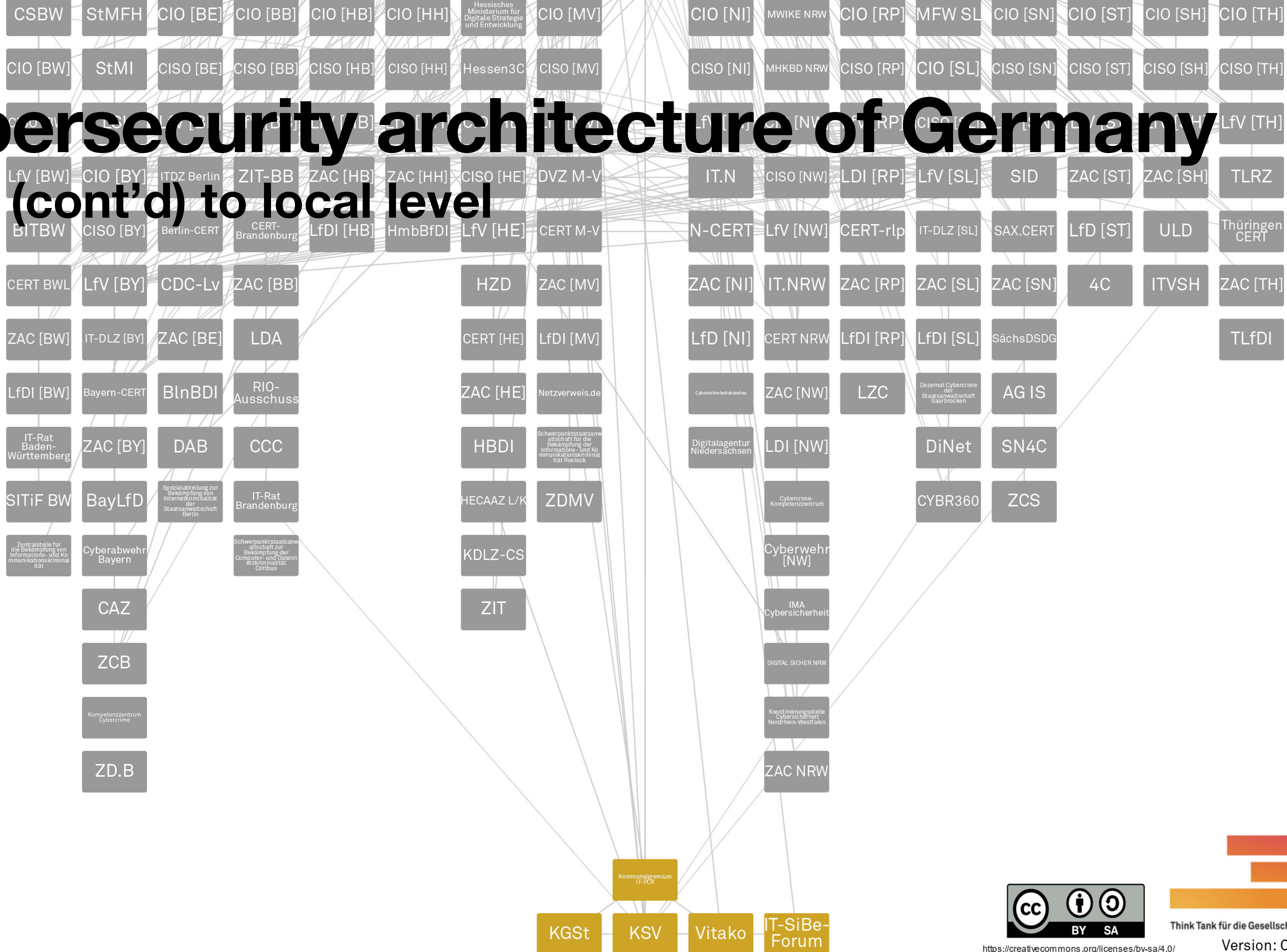
Cybersecurity architecture of Germany

Federal (cont'd) to state level



Cybersecurity architecture of Germany

State (cont'd) to local level



<https://creativecommons.org/licenses/by-sa/4.0/>



Think Tank für die Gesellschaft im technologischen Wandel

Version: October 2023








NIS 2 +

CER +

CRA



**NIS 2 +
CER +
CRA +
DORA**



**NIS 2 +
CER +
CRA +
DORA +
EUUCS**



**NIS 2 +
CER +
CRA +
DORA +
EUCS
etc.**

Cybersecurity risk-management measures

NIS 2 Art. 21 par. 2 (a)-(i)

- policies on risk analysis and information system security;
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;
- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- basic cyber hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography and, where appropriate, encryption;
- human resources security, access control policies and asset management;
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Kthxbye

Do not leave your device unattended

