



IT-Security Law 2016

Current developments in Germany and Europe

Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen
20.09.2016

Gefördert vom
FKZ: 16KIS0213
bis 16KIS0216



National legal standards regarding IT Security

The IT Security Act / “IT-Sicherheitsgesetz” (IT-SiG)

- Legal status of IT-SiG:
 - **Amending act** („Artikelgesetz“)
 - Therefore **no codification**
 - Only amends various existing laws, including:
 - Act on the Federal Office for Information Security (BSiG)
 - Atomic Energy Act (AtG)
 - Energy Industry Act (EnWG)
 - Telemedia Act (TMG)
 - Telecommunications Act (TKG)
 - Act on the Federal Criminal Police Office (BKAG)
- IT-SiG entered into force on 25 July, 2015
- mainly, but not exclusively referring to Critical Infrastructures
 - E.g. includes a general extension of power of the BSI according to Sec. 7 BSiG (warnings), Sec. 7a BSiG (examination of IT security)

IT Security Act and Critical Infrastructures

Scope of application:

Who is an operator of a Critical Infrastructure
within the meaning of the law?

- IT security and Critical Infrastructures:
 - Critical Infrastructures (Sec. 2 para. 10 BSIg) ≠ KRITIS (Federal Ministry of the Interior (BMI), National Strategy for the Protection of Critical Infrastructures, so-called KRITIS Strategy)
 - KRITIS: broader definition, including government + administration, media + culture
 - Meeting cumulative criteria to be categorized as a Critical Infrastructure according to Sec. 2 para. 10 BSIg:
 - 1. **Sectoral belonging** to Energy, Information Technology, Telecommunication, Transport, Traffic, Health, Water, Food, Finance and Insurance +
 - 2. **Relevance of failure consequences**: Great importance for a functioning community; incidents and breakdowns lead to a significant shortage of supply or a threat to public safety

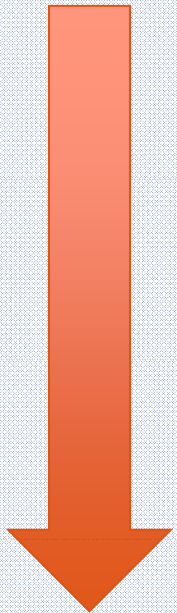
- Requirements for a determination of Critical Infrastructures:
 - Sectoral belonging only defines the parties concerned in general
 - Specified by a legislative decree in pursuance of Sec. 2 para. 10 sent. 2 in conjunction with Sec. 10 para. 1 BSIG (**BSI-KritisV**)
 - defines which entities, installations or subsectors cause an obligation within the meaning of BSIG
 - **Criteria: quality + quantity**
 - Quality: relevance as a service considered critical
 - Quantity: supply coverage
 - decree was implemented in accordance with science, operators, industry associations, Federal Ministries

- Requirements for a determination of Critical Infrastructures:
 - **Public authorities** included, too?
 - Not seen as a Critical Infrastructure within the meaning of the law!
 - Contrary to the definition by BMI KRITIS: **no sector „Government and Administration“** in Sec. 2 para. 10 BSI-G
 - Not explicitly included in BSI-KritisV as well
 - **But take note of Secs. 4, 5 BSI-G**
 - BSI as the central reporting point for the IT security of the Federal Government
 - Defence against malware and threats to the communication technology of the Federal Government

- **Timetable BSI-KritisV:**
 - **Basket 1:**
 - Energy, Water, Food, ICT
 - executed on 22 April, 2016
 - **Basket 2:**
 - Transport, Traffic, Health, Finance and Insurance services
 - Completion planned for the end of 2016
 - Entry into force expected in first quarter of 2017

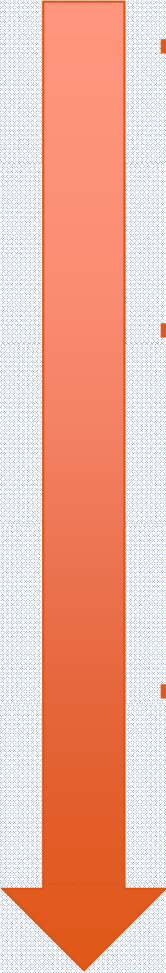
- Contents of BSI-KritisV:

- Based on sector studies by the BSI
- Determination of affected operators **divided into three steps:**



- 1. Which **services** are to be seen critical due to their **importance**?
- 2. Which categories of **installations** are necessary for the **provision** of the critical services identified in Step 1?
- 3. Which **concrete systems or parts** of it show a **significant supply coverage** from the perspective of society as a whole?

■ Example: Sector Energy, Sec. 2 BSI-KritisV + Annex 1

- 
- **1st Step**, Sec. 2 para. 1 BSI-KritisV: Critical infrastructures in the sector Energy are:
 - Electricity supply
 - Gas and fuel supply
 - Fuel oil supply
 - District heating supply
 - **2nd Step**, Sec. 2 paras. 2-4, para. 5 no. 1 BSI-KritisV + Annex 1, Part 3, Column B:
 - Electricity supply includes:
 - 1. Production, 2. Transmission and 3. Distribution
 - Categories of installations:
 - 1. Generation plant, decentralized power generation plant, storage facility, plants of pool providers
 - 2. Transmission network, central system and systems for electricity trading
 - 3. Distribution network, measuring point
 - **3rd Step**, Sec. 1 nos. 4 + 5, Sec. 2 para. 5 no. 2 BSI-KritisV + Annex 1, Part 2, Part 3, Columns C + D:
 - Supply coverage/dimensioning criterion and sector-specific thresholds
 - E. g. an electricity generation plant with a net rated output of ≥ 420 MW installed = KRITIS within the meaning of the BSIG (+)

- **Structure of the BSI-KritisV:**
 - **Sec. 1 Definitions:** Definitions of installation, operator, critical service, supply coverage, sector-specific threshold
 - **Sec. 2 Sector Energy:** Designation of **critical services in this sector** due to their importance for a functioning community + **reference to the annex** of the decree with a figure of the **sector-specific thresholds**
 - **Sec. 3 Sector Water:** as in Sec. 2, for Water
 - **Sec. 4 Sector Food:** as in Sec. 2, for Food
 - **Sec. 5 Sector Information Technology and Telecommunication:** as in Sec. 2, for ICT
 - **Sec. 6 Evaluation:** Instruction to evaluate i.a. sector-specific categories and thresholds four years after the entry into force of the BSI-KritisV
 - **Sec. 7 Entry into force**

- **Structure of the BSI-KritisV – Annexes:**
 - **Annex 1** – Installation categories and thresholds for sector Energy:
 - **Part 1** Principles and Deadlines (i.a. to determine the supply coverage)
 - **Part 2** Calculation formula to determine sector-specific thresholds
 - **Part 3** Installation categories and thresholds
 - **Annex 2** – Installation categories and thresholds for sector Water: **as Annex 1**, for Water
 - **Annex 3** – Installation categories and thresholds for sector Food: **as Annex 1**, for Food
 - **Annex 4** – Installation categories and thresholds for sector Information Technology and Telecommunication: **as Annex 1**, for ICT
 - **Annex ... for other KRITIS domains** according to Sec. 2 para. 10 BSIG: Transport and Traffic, Health, Finance and Insurance
 - Further information, particularly about the **basis for calculation**, can be found in the **legislative reasons of the decree**, p. 13 et seq.

IT Security Act and Critical Infrastructures

Responsibilities:

Secs. 8a to 8d BSIg as central novelties
for the operators of Critical Infrastructures

- Sec. 8a BSIG – Information security of KRITIS:
 - **Aim:** Avoiding disruptions in IT systems that are essential for the Critical Infrastructure's functioning
 - **Method:** Operators must take appropriate technical and organisational measures (TOM) which comply with the state of the art
 - „State of the art“ as indeterminate legal term/general clause:
 - International, European + national norms and standards (**ISMS** according to ISO/IEC 27001)
 - Specific standards by operators/sector associations in coordination with BSI/Consultation UP KRITIS (**B3S**)
 - **Suitability:** Relation of effort and threat, especially cost relevance
 - Providing evidence of TOM every two years by means of **audits, controls, certifications**

- Sec. 8b BSIg – Central reporting point for IT security of Critical Infrastructures:
 - BSI as the **central reporting point** for IT security:
 - Collecting and evaluating information: Security gaps, malware, completed or attempted attacks, attackers' strategies
 - Analysing the consequences of attacks for the availability of KRITIS
 - Updating situation report about information security of KRITIS
 - Informing operators about risks and threats
 - Informing other responsible (supervisory) authorities
 - Obligation on operators to set up a **contact point** to prevent and manage crises
 - Deadline: within 6 months after entry into force of the BSI-KritisV
 - **For first basket (Energy, Water, Food, ICT): Deadline 23 October, 2016**
 - Optional: Designation of a corporate, **superordinate stakeholder** possible, as far as belonging to the same domain

- Sec. 8b BSIG – Notification requirement:
 - **When to report?** Significant disruptions of availability, integrity, authenticity, confidentiality of IT systems, components or processes that *led* or *might lead* to failure or disruption of the critical infrastructure's functioning
 - **Significant disruption:** Threatens functionality; Indication: Can not be fixed automated or with little effort
 - **Categories required to notify** may be orientated by Annex 1 of the general administrative regulation about the notifying procedure according to Sec. 4 para. 6 BSIG

- Annex 1 of the general administrative regulation about the notifying procedure according to Sec. 4 para. 6 BSIg, **categories required to notify:**
 - External attack (DoS, hacking, misuse of passwords)
 - Data loss (hardware failures, unauthorized data flow)
 - Security gap (exploit)
 - Disruption of software or hardware components (serious system failure, overload situations)
 - Violation of IT security guidelines (internal offender)
 - Internal causes (safeguard, cooling, UPS)
 - External factors (forces of nature/force majeure)
 - Specific findings (according to the reporter's assessment)

■ Sec. 8b BSIG – Notification requirement (continued):

- **What to report?** Information about the disruption, technical conditions, the assumed or actual cause, the type of the institution or installation concerned and about the operator's sector
- **Designation of the concrete operator?** Only required if the disruption actual led to a failure or disruption of functioning, otherwise **pseudonymized** notification
- **What happens to the reported data?** BSI as central reporting point, this means...
 - Collection and evaluation (partially along with BBK)
 - Warning and alarm messages
 - Updating the situation report for information security
 - Information for operators and (supervisory) authorities
 - Long-termed annual reports for the public
- **Who does not need to report?** Sec. 8c BSIG – Scope/EU law: Does not apply to micro-enterprises (employees < 10; annual balance not more than 2 million €)
→ **Exception applies to TOM as well**

- Sec. 8c BSIg – Special regulations/notification requirements and TOM based on other laws:
 - Operators of telecommunications networks or services
 - Sec. 109 TKG
 - Operators of energy supply networks or installations
 - Sec. 11 EnWG
 - Licensees according to the Atomic Energy Act
 - Sec. 44b AtG
 - Only in case that no special laws exist for the respective infrastructure sector = BSIg is applicable
 - Universal legal principle (lex specialis rule)

European law standards regarding IT security

IT Security Law 2016 – European standards

- Again: IT security is **not codified**
- Numerous **individual regulations, different legally binding nature**
- Depending on the respective **business or infrastructure sector**
- Various examples:
 - Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (RED)
 - Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)
 - Directive 2013/40/EU on attacks against information systems
 - Directive 2009/72/EC concerning common rules for the internal market in electricity
 - Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
 - Directive 2006/32/EC on energy end-use efficiency and energy services
 - Directive 2002/58/EC on privacy and electronic communications (E-Privacy Directive) and Directive 2009/136/EC (Cookie Directive)
 - Partially overlapping with EU data protection law concerning personal data, cf. Articles 29 et seq. **General Data Protection Regulation (GDPR)**, data security
 - **NIS Directive???**

■ NIS Directive – Milestones:

- **07.02.2013:** Proposal for NIS Directive by the European Commission
- ...
- **06.07.2016:** Adoption of NIS Directive by the European Parliament
- **19.07.2016:** Publication in the Official Journal of the EU
- **08.08.2016:** Entry into force of the NIS Directive
- **09.02.2017:** Deadline for the representation in the Cooperation Group and in the CSIRTs network
- **09.05.2018:** Deadline for the implementation of the new legal and administrative regulations in EU Member States
- **10.05.2018:** Application of the new Member State regulations for NIS
- **09.11.2018:** Deadline for identification of operators of essential services
- **09.05.2019:** Consistency report about identification of operators of essential services
- **09.05.2021:** First progress report of the European Commission about the implementation of NIS

- **NIS Directive – Legal nature:**
 - Key element of the **Cybersecurity Strategy of the EU**
 - EU Directive ≠ EU Regulation
 - Article 288 TFEU (Treaty on the Functioning of the EU):
 - „A regulation shall have **general application**. It shall be **binding** in its entirety and **directly applicable** in all Member States.” → No national implementation act required to become effective (e. g. GDPR)
 - „A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, **but shall leave to the national authorities the choice of form and methods.**” → National implementation act required to become effective
 - Germany: **National implementation act “IT-SiG 2”**, amendment of individual laws required due to the adoption of the directive
 - **Minimum harmonisation:** Germany can provide a higher level of IT security than NIS prescribes (Article 3)

- NIS Directive – Considerations in terms of legal policy:
 - NIS as key factor for a **functioning community and economy** of the EU
 - Scope, frequency and consequences of security issues increase
 - **EU-wide coordinated Cybersecurity Strategy** requires a minimum level for all Member States
 - Existing abilities are not sufficient to ensure a high level of NIS in the EU
 - **Inconsistent level of protection in Member States**
 - Common requirements for operators of „essential services“ are missing
 - **NIS Directive designed as „global approach [...]** covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers”

- NIS Directive – Subject matter and scope (Articles 1, 2):
 - **Not** directly addressed to individuals/operators, but to EU Member States that enact national implementation acts
 - **Obligations of Member States** as an overview:
 - Determining a national strategy for NIS
 - Establishing a Cooperation Group for strategic cooperation and for exchange of information among Member States
 - Establishing a CSIRTs network (Computer Security Incident Response Teams Network) to support the operational cooperation in IT security between Member States
 - Determining security and notification requirements for the operators of essential services and for digital service providers
 - Designating national competent authorities, single points of contact and CSIRTs

- **Exception to the scope** for:
 - Operators of public communications networks (Directive 2002/21/EC)
 - Operators of publicly available electronic communications services (Directive 2002/21/EC)
 - Trust service providers (Regulation No 910/2014)
 - Processing of personal data according to EU data protection law
 - General definition: sector-specific requirements of EU law take precedence (*lex specialis*)
 - Scope regarding micro-enterprises is not restricted by the directive itself, but by thresholds to determine operators of essential services (Article 5 (2), Article 6)

- NIS Directive – Extract of Definitions (Article 4):
 - Broad definition of so-called „**Network and information systems**“:
 - Electronic communications network (cable; radio; optical, electromagnetic equipment; satellite networks; „Internet“; power lines as far as used for signal transmission; sound broadcasting; television)
 - Devices that, pursuant to a program, perform automatic processing of digital data
 - Digital data processed in abovementioned entities
 - **Operators of essential services**: includes public and private entities
 - No wider scope than in IT-SiG under this aspect; Annex II of NIS does not mention the category „government and administration“ as well
 - **Digital service**: any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services
 - **Incident**: any event having an actual adverse effect on the security of network and information systems
 - **Further technical definitions** for IXP, DNS, TLD, online marketplace and online search engine, cloud computing service
 - **Further specifications by Annexes I to III**

IT Security Law 2016 – European standards

- NIS Directive – Protection of essential services (Articles 5, 6, 14, 15):
 - **Member States' obligation** to identify the operators of essential services with an establishment on their territory by 9 November, 2018
 - **In their meaning, „essential services“ correspond to „Critical Infrastructures“** according to the IT-SiG
 - Relevant sectors and subsectors (Annex II, „Quality“):
 - **Energy** (electricity, oil, gas)
 - **Transport** (air transport, rail transport, water transport, road transport)
 - **Banking** (credit institutions)
 - **Financial market infrastructures** (stock exchange)
 - **Health sector** (health care settings, hospitals, private clinics)
 - **Drinking water supply and distribution**
 - **Digital Infrastructure** (IXPs, DNS service providers, TLD name registries)
 - **IT-SiG: Food**
 - **IT-SiG: Insurance**
 - Criteria for the identification of a service as „essential“ („Quantity“):
 - Essential for the maintenance of critical societal/economic activities
 - Provision of the service depends on network and information systems
 - Incident causes significant disruptions (as measured by i.a. number of users, domino effects, market share, alternative means)
 - **Member States compile a list of essential services: BSI-KritisV**
 - List of designated operators has to be checked at least every two years
 - Aim: **EU-wide standardised evaluation benchmark** to determine Critical Infrastructures

IT Security Law 2016 – European standards

- NIS Directive – Protection of essential services (Articles 5, 6, 14, 15):
 - Security requirements: appropriate and proportionate TOM, having regard to the **state of the art, integration of standards and technical guidelines by ENISA (Article 19)**
 - „Regard“ **weaker than Sec. 8a BSIg**, though minimum harmonisation
 - Supporting a maximum of service availability
 - Establishing a **content-related notification requirement** for operators in case of incidents with a significant effect on service availability
 - **IT-SiG is more far-reaching**: Potential impairment of service is enough, minimum harmonisation
 - Criteria for activating the notification requirement:
 - Number of users affected
 - Duration
 - Geographic spread
 - NIS Directive provides opportunity to determine EU-wide criteria for the activation of the notification requirement
 - Notification gets included in **transnational, EU-wide exchange of information**
 - National authority (BSI) provides **instructions for the reporting persons** to manage the incident where appropriate
 - Possibility of official **information to the public** in individual cases

- NIS Directive – Protection of essential services (Articles 5, 6, 14, 15):
 - Art. 15 (1) NIS Directive: Member States shall ensure that the competent authorities have the powers to assess **if operators fulfil their obligations regarding TOM and notification**
 - Practice: How could/should this be implemented? → German government: approx. 2,000 affected operators
 - In addition, Member States shall ensure appropriate **official capabilities to control security requirements**
 - Member States shall ensure that authorities have the powers to issue instructions for operators in case security deficiencies are identified

■ NIS Directive – Protection of digital service providers (Articles 16, 17, 18):

- **Digital service:** Information Society service; any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services
- **Specified by Annex III:** Online marketplace, online search engine, cloud computing service
- **IT-SiG: Sec. 13 para. 7 TMG**, service providers offering telemedia on a commercial basis must ensure that, having regard to the state of the art,
 - unauthorised access to technical facilities is not possible
 - protection against data breaches and external attacks is provided
- **NIS-RL:** service providers must provide appropriate and proportionate TOM to manage risks for NIS, taking into account the state of the art
 - Risk according to Article 4 no. 9: „any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems “
 - Integration of standards and technical guidelines by ENISA (Article 19)
- **NIS Directive slightly broader as regards content, but categorically restricted by Annex III, whereas TMG refers to any telemedia**

- NIS Directive – Protection of digital service providers (Articles 16, 17, 18):
 - In addition to TOM, **notification requirements** for service providers in case of incidents with significant effects on the provision of the service
 - Similar criteria for the assessment of the significance as for „essential services“
 - Notification requirement as well if essential services and digital services are combined and an incident at the digital service implicates a restriction of continuity at the essential service
 - Official **information to the public possible** if in the interest of the public
 - **Exceptions from the notification requirement:**
 - Provider does not have access to the information relevant for the assessment of the incident
 - Micro-enterprises: Employees < 10; annual balance not more than 2 million €
 - Possibility of subsequent **official review** if indications of failure to comply with TOM and notification requirement
 - **Digital service providers not established in the EU shall designate a representative in the EU.** The legal jurisdiction is determined by the establishment of the representative.

- NIS Directive – Notification by uncritical entities (Article 20):
 - **Voluntary notification** by:
 - Operators of non-essential services
 - No digital service providers
 - Restricted to incidents with significant effects to the availability of service
 - Processing in accordance with the processing for operators of essential services, but:
 - Only processed if it does not constitute a disproportionate burden
 - Possibly subordinate to mandatory notifications
 - **No obligations resulting** for the notifying entity

■ NIS Directive – National regulatory framework (Articles 7, 8, 9, 10):

- Each Member State adopts a **national strategy on NIS**, for Germany:
 - The National Plan for Information Infrastructure Protection, 2005, replaced by
 - Comprehensive Cybersecurity Strategy of the Federal Government in 2011
- Designation of the competent authority for NIS: **BSI**
- Designation of the single point of contact for NIS: **BSI**
 - Liaison function for cross-border cooperation
 - Cooperation with national law enforcement authorities and national data protection authorities
- Notification about strategy on NIS and national competent authorities to the European Commission, publication of an EU-wide list
- **Designation of Member State CSIRTs** (Computer Security Incident Response Team) or CERTs (Computer Emergency Response Team)
 - „CERT-Bund“, located at BSI
 - already meets the requirements from Annex I NIS Directive
- Informing the European Commission about the work of CSIRTs
- **Annual interim reports** by BSI about national IT security incidents at EU level

- NIS Directive – European and international regulatory framework (Articles 11, 12, 13):
 - Establishment of an **EU-wide Cooperation Group** for strategic cooperation and to develop trust and confidence among Member States concerning NIS
 - Composition:
 - Representatives of the Member States
 - European Commission
 - ENISA
 - Possible participation of stakeholders
 - Key tasks:
 - Developing work programmes/strategic guidances
 - Exchange of information to improve the EU-wide coordination and cooperation
 - Exchange of information concerning awareness, research + development , best practice regarding to the identification of essential services, notification requirements
 - Evaluating and improving national strategies on NIS
 - Supporting European standardization
 - Collecting information about the coordination of IT security incidents
 - Preparing periodic reports to assess the transnational cooperation
 - **Incorporating the Cooperation Group into international agreements** concerning IT security/data protection

- NIS Directive – European and international regulatory framework (Articles 11, 12, 13):
 - Establishing a CSIRTs network to promote a supranational, **operational cooperation**, comprising national CSIRTs
 - Composed of representatives of the Member States' CSIRTs and CERT-EU, supported by ENISA
 - Tasks of the CSIRTs network:
 - Planning operational cooperation of the national CSIRTs
 - Exchange of information among the CSIRTs
 - Identifying a coordinated response to incidents
 - Supporting Member States in addressing cross-border incidents
 - Informing the Cooperation Group
 - Analysing exercises relating to network and information security
 - **Periodic reports** by the CSIRTs network about the results of the cooperation among Member States

- NIS Directive – Penalties (Article 21):
 - Member States' obligation to lay down rules on penalties applicable to infringements against the requirements of the directive
 - Stipulation: „**effective, proportionate and dissuasive**“
 - **IT-SiG: probably an appropriate regulation** in Sec. 14 BSiG and Sec. 16 TMG

- NIS Directive – Suggestions for operators?
 - Implementing the requirements by the IT-SiG **as before**
 - **Wide modification/extension** of the sectors of Critical Infrastructures according to the BSI-KritisV by the NIS Directive **is rather not to be expected**
 - No big modifications in terms of TOM/notification requirements for operators expectable as well
 - **No „double implementation effort“**, only fine adjustment
 - The **focus** of the implementation of NIS is to establish a cross-national **European cooperation framework**, mediated by the BSI



Dr. iur. Dennis-Kenji Kipker

Institut für Informations-, Gesundheits- und Medizinrecht (IGMR)

Universität Bremen

Universitätsallee GW1

28359 Bremen

Tel.: +49 421 218 66049

Mail: kipker@uni-bremen.de

Visit our website: www.itskritis.de

Follow us on Twitter: [@itskritis](https://twitter.com/itskritis)

