German IT Security Law 2.0

New challenges for stakeholders and companies

Dr. Dennis-Kenji Kipker

Legal Advisor

CERT@VDE & Cybersecurity

DKE

VDE DIN

German IT Security Law "1.0"

- Amending act, **no codification of IT security**
- Entered into force on 25th July 2015
- Amended various existing laws:
  - Act on the Federal Office for Information Security (**BSIG**)
  - Atomic Energy Act (**EnWG**)
  - Telemedia Act (**TMG**)
  - Telecommunications Act (**TKG**)
  - Act on the Federal Criminal Police Office (**BKAG**)

German IT Security Law "1.0"

- Mostly referring on the **protection of Critical Infrastructures**, but also including a general extension of power of the BSI according to Sec. 7 BSIG (warnings), Sec. 7a BSIG (examination of IT security)
- Concretization of the scope of application through the **BSI-Kritis Regulation**, referring to Critical Infrastructures which are defined by certain thresholds in numbers: Energy, Water, Food, ICT, Transport, Traffic, Health, Finance, Insurance

German IT Security Law "1.0"

- **Important duties for Critical Infrastructures as defined by law:**
  - § 8a BSIG: Duties of information security, operators must take **appropriate technical and organizational measures** which comply with the state of the art, e.g. through the ISMS according to ISO/IEC 27001 or sector specific standards by operators/sector associations (B3S)
  - § 8b BSIG: **Central reporting point for IT security** of Critical Infrastructures, collection and evaluation of information about security gaps, malware, completed or attempted attacks, attackers' strategies
    - Obligation of operators to set up a **contact point for crisis prevention and management**, duties to report significant breaches of cybersecurity

German IT Security Law 2.0 – Timeline

- Based on the German IT Security Law "1.0"
- Part of the **German Cybersecurity Strategy of 2016**, many speculations about the upcoming second part of the German IT security regulation in the recent years
- Ministerial draft of the IT-SiG 2.0 published on **27th March 2019**

- Proposed regulations with only **preliminary character**

- Time of adoption of the law currently unclear, assumed for **fall 2019**
- **Expected economic impact:** 16,71 million € once, yearly 45,09 million € more, compared to the compliance duties by IT-SiG

German IT Security Law 2.0 – Regulatory goals

- **Main intention:** Further development of cybersecurity for the society as a whole
- Not only protection of Critical Infrastructures, but for all relevant companies and the state, as well as for consumers, **including IoT products**
- **Co-regulation** of EU Cybersecurity Act and German IT Security Law 2.0 in certain fields of interest (it can be assumed that the German regulator influenced the European cyber legislation)

German IT Security Law 2.0 – Regulatory goals

- **Core elements of the new regulatory approach include:**
  - **Protection of citizens:** Unified IT security mark, so that a higher visibility for IT security can be reached especially for consumer products/applications
  - **Extensions of the legal power of the German BSI**, as well as for criminal prosecution authorities to fight against cybercrime
  - Extensions in the **German Criminal Code** and the **German Criminal Prosecution Code**
  - **New cybersecurity duties especially for providers**, e.g. concerning the deletion, reporting, and the provision of information regarding cybercrime issues
  - **More and effective cooperation** among authorities to deal with cybercrime
  - Amended regulations for operators of **Critical Infrastructures**

German IT Security Law 2.0 – Affected laws

- Act on the Federal Office for Information Security (**BSIG**)
- Telemedia Act (**TMG**)
- Telecommunications Act (**TKG**)
- Criminal Code (**StGB**)
- Criminal Prosecution Code (**StPO**)
- Federal Crimial Police Law (**BKAG**)

German IT Security Law 2.0 – New tasks for the BSI

- §§ 4a, 4b BSIG-E (E=draft version):
  - Security checks of the **information technology which is used by federal authorities** (including technical infrastructures which are necessary for their functioning)
  - **Central reporting unit** for IT security not only for Critical Infrastructurs and federal authorities, but for IT security in general:
    - Collection of information about IT security breaches, malware, succesful or attempted attacks, procedures of attackers
    - Possibility of anonimyzed notifications by corporations, private entitites, etc.
  - **New reporting tools of the BSI:**
    - Third parties, regarding cyber attacks or lacking cybersecurity measures
    - The public about **lacking IT security in products or services** (corresponding regulation: § 7a BSIG – authorization of the BSI to conduct security testing of products which are publicly available
    - Federal authorities, Critical Infrastructures

German IT Security Law 2.0 – New tasks for the BSI

- **§ 5 BSIG-E – Protection of the IT systems of the Federal Government:** Power of the BSI to collect technical data (e.g. protocol data) of IT service providers, which offer essential IT services in sensitive areas of the Federal Government
- **§ 5d BSIG-E: Authorization of the BSI to collect inventory data** such as names, addresses, birthdates, IP addresses, etc. at telecommunication providers for reasons of IT security, especially if IT systems of third parties are involved in/affected of a cyberattack

German IT Security Law 2.0 – Public warnings regarding IT security

- **§ 7 BSIG-E:** Already existing powers of the BSI (which will be expanded by IT-SiG 2.0) **to issue IT security relevant warnings to the public** with regard to the following cases:
  - IT security breaches
  - Warnings about public malware
  - Warnings in case of data breaches
  - Recommendations to use certain security measures/products
  - Information about IT security relevant features of products
- Authorization of the BSI to warn the public in case of **insecure products**
- **Normally:** Duty to inform the manufacturers of affected products on time

German IT Security Law 2.0 – Examination of the security of IT systems

- **§ 7a BSIG-E:**
  - Already existing legal grounds based on the **first IT-SiG**
  - **Duty of the product manufacturer to cooperate with the BSI** regarding all relevant facts which are necessary for evaluation, including technical details as well
  - **Publication of the evaluation results is possible:** In this case, the manufacturer has the possibility of a prior statement
  - **Sanctions for non-cooperation**, e.g. public announcement of the company, the product, the IT security risk or breach

German IT Security Law 2.0 – Detection of IT security risks in publicly available IT systems

- **§ 7b BSIG-E:**
  - If there is any assumption that a publicly available IT system is insecure, then the BSI will be allowed to **conduct detections** and to create a report
  - **Definition:** An IT system is insecure in the case of publicly known IT security breaches or if it is obvious that the IT system is not protected in a sufficient manner
  - **Information duty of the BSI** if IT-security breaches have been tracked
  - Creation of **Honeypots**
  - **BSI as a "hacker authority"**

German IT Security Law 2.0 – Critical Infrastructure protection

- **§ 8a BSIG-E:**
  - Permission of operators of Critical Infrastructures to implement **measures for detection of cyberattacks** (proactive approach) including the use of personal data
  - Core components of IT in Critical Infrastructures can only be used by manufacturers that have **officially declared their trustworthiness**:
    - This declaration refers to the IT security of the **complete supply chain of the manufacturer**
    - The minimum requirements of the declaration of trustworthiness will be enacted in a **general ruling of the German Federal Ministry of Interior**
    - **Definition of core components** may be found in § 2 par. 13 BSIG-E with a distinction between different sectors, mostly linked to the **control of relevant systems** or to the processing/transfer of relevant data

German IT Security Law 2.0 – Extended definition of Critical Infrastructures

- **§§ 8f, 8g, 2 par. 14 BSIG-E:**
  - Armament; Culture and Media
  - No Critical Infrastructures according to § 2 par. 10 BSIG, but **companies with significant relevance** because of their economic importance in Germany
    - Operators according to § 2 par. 14 BSIG-E will be identified by a **legal decree, issued by the Federal Ministry of Interior**
  - § 8g BSIG-E: **„Cybercriticality“** as a subsidiary catch-all element

German IT Security Law 2.0 – Reporting duties for manufacturers of IT products

- **§ 8h BSIG-E:**
  - Duty of manufacturers of IT products to report **relevant IT security breaches** to the BSI, if the breach can result in a malfunction of the systems of Critical Infrastructures or companies which underly the extended definition of Critical Infrastructures
    - **Broad legal definition of IT products** (§ 2 par. 9 BSIG-E): software, hardware, embedded systems
  - Duty of manufacturers of **core components of IT in Critical Infrastructures** to report IT incidents, including information about the affected software, cross-border impacts, technical reasons and results
  - Duty of incident reporting will start **one year after the IT-SiG 2.0** came into force

German IT Security Law 2.0 – Voluntary IT security mark

- **§ 9a BSIG-E:**
  - On application of the companies, the **BSI will issue an IT security mark**
  - Concretization through **legal decree** ("RVO IT-Sicherheitskennzeichen") based on § 10 par. 2a BSIG-E, **issued by the Federal Ministry of Interior**
  - The **affected product categories** will be listed and explained in the "RVO IT-Sicherheitskennzeichen"

German IT Security Law 2.0 – Voluntary IT security mark

- **Content of the IT security mark:**
  - **Description of the manufacturer**, including the relevant IT security features of the product
  - **BSI security information** about IT security breaches or any other relevant information
- Broad **definition of the manufacturer** according to the German Product Security Law (ProdSichG), § 2 No. 14: Every natural or juristic person which produces or constructs a product, which produces the product by a third party or which just prints its name on to the product
  - **Resellers** are affected as well

German IT Security Law 2.0 – Voluntary IT security mark

- The IT security mark will be printed on the **product** itself or on its **packaging**
- An electronic publication is possible as well, e.g. a **QR code** which can be scanned and linked to the website of the manufacturer
- **Advertising use of the IT security mark** is possible
- The BSI will regularly check if the preconditions of the IT security mark are still met by the manufacturer

German IT Security Law 2.0 – Telecommunication Act

- **Generally:** More extensive measures on IT security than ever before
- Question for quick check-up of applicability: Is the Federal Network Agency (**BNetzA**) involved?
- Technical measures regarding IT security should follow a **proactive approach**, so that telecommunication providers should implement **cyberattack detection systems** into their IT security management
- **Duties of the telecommunication providers to report and to delete:**
  - Duty to report to the German Federal Criminal Police (BKA), if an operator of a telecommunication service recognizes any **unlawful use of data** in his network
  - In the case of sufficient indication, the unlawful used data has to be **banned** from access, if necessary to be **deleted**

Expected impact on businesses & consumers

- **Holistic legal approach** of cybersecurity
- **New resources** will have to be developed to be compliant with the upcoming cybersecurity regulation in Germany and Europe
- **Co-regulation may be expected** in certain fields, e.g. consumer declarations
- **Consumer trust and transparency** are key elements of EU cyber politics in the next years, and necessary for future products and services
- **(Informed) self determination of the end user** not only with regard to data protection, but IT security as well
- Companies should start **as soon as possible** with the political as well as the technical/organizational **follow-up**

Vielen Dank für Ihre Aufmerksamkeit!

Wir gestalten die e-diale Zukunft.
Machen Sie mit.

Ihr Ansprechpartner:

Dr. Dennis-Kenji Kipker

CERT@VDE & Cybersecurity

Tel. +49 421 218-66049

Dennis-Kenji.Kipker@vde.com

DKE

VDE DIN