The EU NIS Directive Compared to the IT Security Act – Germany is Well Positioned for the new European Cybersecurity Space

Dr. Dennis-Kenji Kipker is Research Managing Director of the Institute for Information, Health and Medical Law at the University of Bremen, Germany, and a Member of the Board of the European Academy for Freedom of Information and Data Protection (EAID) in Berlin.

Since 2015, two legislative measures concerning the IT-security of Critical Infrastructures have been introduced by the European Union and the Federal Republic of Germany: The EU NIS Directive and the German IT Security Act. This paper aims at providing essential information to promote the understanding of the NIS Directive while also taking into account the German key regulations in this field. Finally, both legislative measures will be taken into comparison.

1. Milestones, history and key points

Following the *Commission's* proposal for a "Directive concerning measures to ensure a high common level of network and information security across the Union" (NIS Directive) as a key element of the EU Cybersecurity Strategy in February 2013, the European legislative procedure has recently been completed by the adoption of the legislative act by the *European Parliament* on 6th July 2016. The legislative procedure was characterized by a number of substantial and procedural difficulties. Therefore, it is now to be welcomed that, having been published in the Official Journal of the EU on 19th July 2016, the directive entered into force as intended on 8th August 2016. In the course of the legislative procedure even the title of the EU legislative act has changed and the updated version reads as follows: "Directive concerning measures for a high common level of security of network and information systems across the Union" – however, the abbreviation remains the same. The NIS Directive provides various implementation deadlines, so-called milestones. Hereafter the most important milestones are briefly mentioned:

- 9.2.2017: Deadline for the representation in the Cooperation Group and in the CSIRTs (Computer Security Incident Response Teams) network.
- 9.5.2018: Deadline for the implementation of new legal and administrative regulations required by the directive in EU Member States.
- 10.5.2018: Application of the new Member State regulations for NIS.
- 9.11.2018: Deadline for the identification of operators of so-called "essential services".
- 9.5.2019: Deadline for the consistency report about the identification of operators of essential services.
- 9.5.20202: First progress report of the *European Commission* about the implementation of NIS.

For all obligations set out in the directive, their legal nature has to be taken into account: According to Art. 288 TFEU the directive is binding for each Member State in terms of the result to be achieved, but leaves the choice of form and methods to the national authorities. This means the NIS Directive is primarily addressed to the Member States' bodies which must establish a national act to implement the NIS Directive. In Germany, some of the individual laws, previously amended by the IT Security Act, probably need to be revised once again. When implementing the Member States' obligations regarding the NIS Directive, the principle of a

minimum harmonization has to be kept in mind: it follows that Germany can also provide by law for a higher level of IT security than the directive prescribes.

The NIS Directive is based on several considerations in terms of current legal policy: For one thing, the growing importance of network and information security as a key factor for a functioning community and the European economy is emphasized, yet it is conceded that scope, frequency and consequences of security issues increase. Additionally, an EU-wide coordinated cybersecurity strategy requires a minimum level of IT security in all Member States. It is argued that the existing provisions of the Member States are not overall sufficient to ensure a high level of NIS across the EU. On these grounds the NIS Directive has been designed as a "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", as stated in the recitals of the directive.

2. Subject matter and scope, Art. 1, 2 and 3

As noted above, the NIS Directive is not directly addressed to individuals or operators, but to EU Member States which must fulfill several legal implementation obligations to increase national IT security. These are:

- 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 to support the operational cooperation in IT security between Member States.
- Determining security and notification requirements for operators of essential services and digital service providers.
- Designating national competent authorities, single points of contact and CSIRTs.

Several exceptions to the scope of the directive are made 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).
- The Processing of personal data according to EU data protection law.

In addition, it is generally defined as a "lex specialis" that sector-specific requirements of EU law take precedence. However, the scope regarding micro-enterprises is not restricted by the directive itself, but by thresholds to determine the operators of essential services (Art. 5 (2), Art. 6).

3. Definitions, Art. 4

The NIS Directive contains a comprehensive directory that defines the used terms. According to Art. 4, the term "Network and information systems" covers electronic communications networks (cable; radio; optical, electromagnetic equipment; satellite networks; "internet"; power lines as far as used for signal transmission; sound broadcasting; television) and devices that, pursuant to a program, perform automatic processing of digital data as well as digital data processed in the above-mentioned entities. The term "operators of essential services" includes both public and private entities. From this point of view, the scope of the NIS Directive seems to be significantly extended as compared to the German IT Security Act, however, Annex II of the

directive (which Art. 4 refers to as well) does not mention the sector "government and administration". A "digital service" is defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. An "incident" means any event having an actual adverse effect on the security of network and information systems. Additional technical definitions can be found for IXP, DNS, TLD, online marketplace, online search engine and cloud computing service. These definitions are further specified by Annexes I to III of the NIS Directive.

4. Protection of essential services, Art. 5, 6, 14, 15

One of the key objectives of the NIS Directive is the protection of operators of so-called "essential services". Although a different term is used, according to their general meaning these services correspond to Critical Infrastructures in the German IT Security Act. It is a Member States' obligation to identify the operators of such essential services with an establishment on their territory by 9th November 2018. The relevant sectors and subsectors of the essential services are designated in Annex II – compared to the IT Security Act practically as a "quality criterion" of a specific industry. The differences between the NIS Directive and the IT Security Act are apparently rather small at this point and will presumably become more concrete within the fine adjustment during the period of implementation into national law. Essential services according to the NIS Directive are located in the following sectors:

- 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).

Going beyond the scope of the NIS Directive, the IT Security Act supplements the sectors of Critical Infrastructures by Food and Insurance in Section 2 § 10 BSIG. While the determination of essential service sectors as a quality criterion initially defines the general criticality of a certain industry, the further classification of a service determined like this as "essential" is made by three criteria which – compared to the IT Security Act – reflect the quantity of the service:

- The service is essential for the maintenance of critical societal/economic activities.
- The provision of the service depends on network and information systems.
- A potential security incident causes significant disruptions, inter alia measured by the number of users, domino effects, market share and alternative means.

Based on the aforementioned criteria, the Member States compile a list of essential services; in Germany this task of concretisation is assumed by the "Kritis-Verordnung" (BSI-KritisV) of the *Federal Office for Information Security*. The list of operators thus determined has to be checked at least every two years in order to achieve an EU-wide harmonized evaluation standard for determining Critical Infrastructures.

Operators of essential services must meet specific security requirements. Therefore, the NIS Directive states that operators must take appropriate and proportionate technical and organisational measures (so-called TOM), having regard to the state of the art by the integration of standards and technical guidelines of *ENISA* (Art. 19). Even though the term

"having regard to the state of the art" describes a weaker requirement than the IT Security Act which in Section 8 a BSIG (Act on the Federal Office for Information Security) requires to "comply with" the state of the art, the principle of a minimum harmonisation takes effect. That is why the national legislator may also prescribe higher requirements. The aim of the prescribed protective measures is to promote a maximum of service availability.

Along with the establishment of TOM, a content-related notification requirement for operators in case of incidents with a significant effect on service availability is established. Again, the IT Security Act is more far-reaching than the NIS Directive because according to German law a potential impairment of service is already sufficient for causing a notification requirement. The NIS Directive defines different criteria for the activation of a notification requirement:

- Number of users affected,
- duration of the incident,
- its geographic spread,
- besides, the NIS Directive provides an opportunity to determine EU-wide criteria for the activation of the notification requirement.

The respective notification is then included in a transnational, EU-wide exchange of information. Moreover, the competent national authority – in Germany the *Federal Office for Information Security (BSI)* – can provide instructions for the reporting persons to manage the incident. Apart from that, it is possible to officially inform the public in individual cases.

Art. 15 (1) of the NIS Directive should also be interesting for the segment of essential services: Member States shall ensure that the competent authorities have the powers to assess whether operators actually fulfill their obligations regarding TOM and notification. In practice, the question arises how firstly, this provision can be effectively implemented considering that – as calculated by the *Federal Government* – approximately 2.000 operators are affected, and secondly, if random checks are adequate for this purpose. Finally, regarding essential services, it is laid down that Member States shall guarantee appropriate official capabilities to control the predefined security requirements. Member States shall further ensure that authorities have the powers to issue instructions for operators in case security deficiencies are identified.

5. Protection of digital service providers, Art. 16, 17, 18

Another major focus of the NIS Directive is the protection of digital service providers. A digital service is defined as an Information Society service, which means any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. As specified by Annex III of the directive, these digital services include online marketplaces, online search engines and cloud computing services. In comparison, the IT Security Act determines provisions for digital services in Section 13 § 7 of the Telemedia Act (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 and protection against data breaches and external attacks is provided. On the other hand, the NIS Directive prescribes that service providers must provide appropriate and proportionate TOM to manage risks for network and information security, taking into account the state of the art. According to Art. 4 no. 9 a risk is "any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems". TOM are determined by the integration of standards and technical guidelines of *ENISA* (Art. 19). At first sight a comparison of national and European IT Security law only reveals few differences: The

NIS Directive seems to imply a slightly broader definition of the protective aim, but then again sets a restriction limiting the scope to Annex III, whereas the TMG refers to any telemedia.

The NIS Directive prescribes notification requirements for digital service providers in case of incidents with significant effects on the provision of the service, just as stated for essential services. Criteria similar to those for essential services are thus taken into account for assessing the significance. Likewise, a notification requirement applies if essential services and digital services are combined and an incident relating to the digital service implicates a restriction of continuity at the essential service. Official information of the public is possible in cases where the incident is a matter of public interest. Exceptions from the notification requirement apply for those providers who do not have access to the information relevant for the assessment of the incident as well as for micro-enterprises, defined by EU law as enterprises with less than ten employees and an annual balance up to € 2 million. If a failure to comply with TOM and the notification requirement is indicated, the NIS Directive opens the possibility of a subsequent official review. A special regulation can further be found in Art. 18: Accordingly, 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.

6. Notification by uncritical entities, Art. 20

Whereas a notification is mandatory for operators of essential and digital services, this turns into a voluntary notification for uncritical entities. In addition, the voluntary notification is restricted to incidents with significant effects on the availability of service. The administrative processing for these voluntary notifications is carried out in accordance with the processing for operators of essential services, but it is specified that voluntary notifications shall only be processed if this does not constitute a disproportionate burden. Voluntary notifications are necessarily of subordinate priority in terms of processing as compared to mandatory notifications. The directive expressly declares that this voluntary option does not result in any obligations for the notifying entity.

7. National regulatory framework, Art. 7, 8, 9, 10

The NIS Directive does not only determine obligations for operators and service providers, but also establishes a comprehensive national regulatory framework for IT security. Thus it is specified that each Member State has to provide a national strategy for network and information security. Germany is already well prepared due to the "National Plan for Information Infrastructure Protection" (NPSI) from 2005 which was replaced by the extensive Cybersecurity Strategy of the *Federal Government* in 2011. The NIS Directive constitutes an obligation to designate an authority competent for NIS and a single point of contact. In Germany, the *BSI* is capable to perform these tasks, acting as a liaison department for cross-border cooperation and for cooperation with national law enforcement authorities and national data protection authorities. The Member States have to communicate their national strategy on NIS and the designation of the national competent authorities to the *European Commission* which then publishes an EU-wide list.

Moreover, it is a duty of all Member States to designate their own national CSIRTs (Computer Security Incident Response Teams), also known as CERTs (Computer Emergency Response Teams). In Germany, the "*CERT-Bund*", located at the *BSI*, is capable to fulfill this role since it already meets the relevant requirements of Annex I of the NIS Directive. The *European Commission* has to be informed about the work of the national CSIRTs and annual interim reports at EU-level about national IT security incidents must be submitted.

8. European and international regulatory framework, Art. 11, 12, 13

Since the NIS Directive aims to establish a uniform European Cybersecurity Strategy, it necessarily includes extensive requirements to create a European – and moreover an international – regulatory framework for network and information security. For this purpose, an EU-wide Cooperation Group for strategic cooperation and the development of trust and confidence concerning NIS among Member States is set up. This Cooperation Group is composed of Member States' representatives, the *European Commission* and *ENISA*, along with the possibility of involving external stakeholders. It is intended to incorporate the Cooperation Group into international conventions concerning IT security and data protection. The following key tasks of the EU-wide Cooperation Group are determined by the NIS Directive:

- 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 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.

While the individual national CSIRTs are set up as part of the national strategies on NIS, the NIS Directive at European level strives to establish a CSIRTs network to promote a supranational, operational cooperation, consisting of representatives from the national CSIRTs, the CERT-EU and, supportively, *ENISA*. The CSIRTs network prepares periodic reports about the results of the cooperation among Member States. Essentially, it has the following tasks:

- Planning the operational cooperation of the national CSIRTs.
- Exchange of information among the individual CSIRTs.
- Identifying a coordinated response to security incidents.
- Supporting Member States in addressing cross-border incidents.
- Informing the Cooperation Group.
- Analysing exercises relating to network and information security.

9. Penalties, Art. 21

Finally, Art. 21 of the directive determines a Member States' obligation to lay down rules on penalties applicable to an infringement against the national requirements based on NIS, provided that these penalties are "effective, proportionate and dissuasive".Concerning German law, it can be assumed that regulations appropriate to these requirements are already defined within the IT Security Act by Section 14 BSIG (Act on the Federal Office for Information Security) and Section 16 TMG.

10. Conclusion, outlook and recommendations

Though the NIS Directive proves to be extensive, it cannot be assumed that it implicates a considerable need for action particularly for the operators of Critical Infrastructures in Germany: According to the current state of knowledge, a modification or even an extension of Critical Infrastructure sectors is not to be expected. Significant modifications in terms of TOM and the notification requirement for operators are unlikely as well. Concerns regarding a

"double effort of implementation" due to parallel national and European legislation therefore turn out to be unfounded, only a fine adjustment is to be expected. Operators of Critical Infrastructures are recommended to implement the requirements of the IT Security Act as originally planned. For the national legislator and the authorities the implementation of the enhanced European cooperation framework for cybersecurity entails a greater effort. Nevertheless, due to its previous efforts in terms of legal policy in IT security, Germany is well positioned for the new European cybersecurity space.

Weiterführende Links

This article is a result of the research project „IT security for Critical Infrastructures" promoted by the *German Federal Ministry of Education and Research* as part of the High-tech Strategy of the *Federal Government*. Vgl. auch zu Kritis, *Kipker*, ZD-Aktuell 2016, 05261; *Voigt/Gehrmann*, ZD 2016, 355; ZD-Aktuell 2016, 04945 und *Mehrbrey/Schreibauer*, MMR 2016, 75.