CORE®

# IT SECURITY ACT

## New Requirements for Critical Infrastructure Operators

Dr. Waldemar Grudzien

20. May 2016
COREtechmonitor | Blogpost

## Key Facts

- The IT Security Act (IT-SiG) has been in force since July 25, 2015 and stipulates two key requirements of operators of critical IT infrastructure: Maintaining a minimum security threshold and setting up regulatory reporting.
- Critical sectors include energy, information technology and telecommunications, transport, healthcare, water, food, as well as finance and insurance (financial sector). A detailed description of which institutions, systems or parts thereof fall under the IT Security Act is determined by way of a regulation.
- The regulation for the first four sectors (information technology and telecommunications, energy, water and food) came into force on May 3, 2016. The amending regulation for the sectors of transport, healthcare, and finance and insurance is due to be published in December 2016.
- In addition to bilateral auditing by the supervisory authority, operators can also prove their conformity with IT-SiG by implementing industry-specific security norms and monitoring their implementation.
- Fulfilling legal requirements will also pose challenges to the financial sector: Regulatory reporting for IT incidents is new and compliance with a minimum security level must be proven.

## Report

If we consider that 40 percent of global value creation is already based on information and communications technology, it is clear that secure and sound IT infrastructures will be an important factor in selecting a business location in the future. With Germany's cyber security strategy, the German government is pursuing the goal of guaranteeing cyber security at the highest level, establishing Germany as one of the most secure digital locations in the world.

The IT Security Act (law to increase the security of IT systems) is part of this strategy. Other elements of the strategy include a National Cyber Defense Center and effectively combating cyber crime. The law requires operators of critical infrastructure from the fields of energy, information and telecommunications technology, transport, healthcare, water, food, and finance and insurance to maintain a minimum standard of IT security and to notify the Federal Office for Information Security (BSI) of any significant IT security issues.

The legislation procedure for the IT Security Act pursues both the aim of creating one of the most secure digital locations as well as the obligation to adopt an IT Security Act resulting from the initiative to create a European network of information security guidelines (NIS-RL). The NIS-RL will be enshrined in national law within 18 months of being passed, and can be expected to come into force in summer 2016. The IT Security Act passed in July 2015 can be seen as a precursor to the NIS-RL.

As an omnibus bill law, the IT-SiG will change various laws pertaining to critical infrastructures: Article 1 amends the BSI Act, Article 2 the Atomic Energy Law, Article 3 the Energy Industry Act, Article 4 the Telemedia Act and

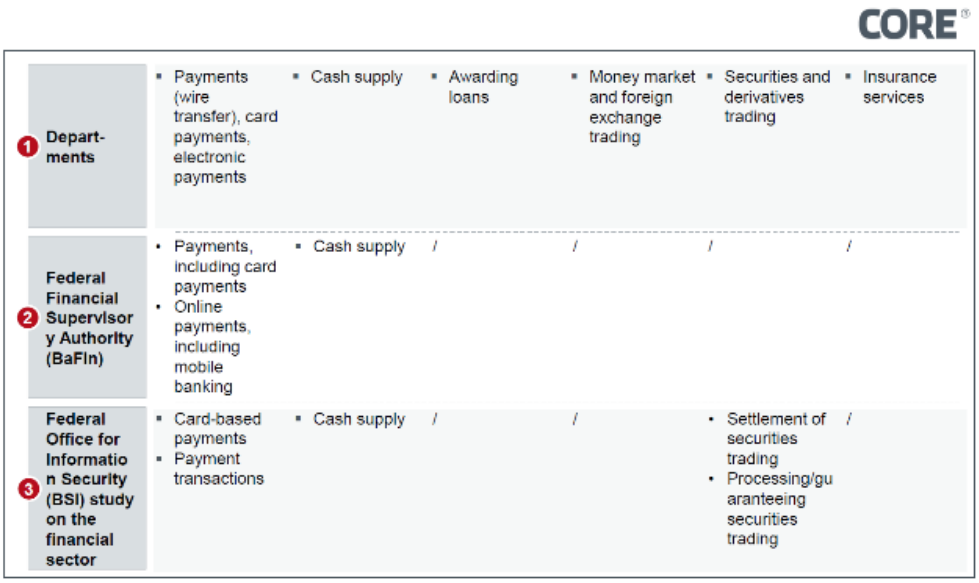


*Figure 1: Critical infrastructures in the financial sector according to government departments, BaFin and BSI prior to the amending regulation coming into force*

Article 5 the Telecommunications Act. For the operators of critical infrastructures, Article 1 is of the most interest, amending or adding various sections to the BSI Act, thus formulating requirements for critical infrastructures.

Critical infrastructures are defined in Section 2 of the BSI Act as institutions, systems or parts thereof that belong to the above-mentioned seven sectors and are of major significance to the functioning of society because their breakdown or restriction would result in major supply bottlenecks or jeopardize public safety or security.

An ordinance on the matter will determine which institutions, systems or parts thereof should be viewed as critical infrastructures. Whether or not an infrastructure is viewed as critical is based on the number of people supplied by the infrastructure. For the sectors in what is known as the “first basket” – energy, information technology and telecommunications, water and food – this ordinance al

ready came into force on May 3, 2016. A threshold of 500,000 people supplied was determined for these four sectors. The ordinance does not list the infrastructure operators affected as was expected in the early phases of drafting the legislation. Instead, an operator must check independently whether or not his or her business falls within the threshold stipulated by the ordinance and, if this is the case, should contact the BSI. The amending regulation should identify the operators of the three sectors of transport, healthcare, and finance and insurance (“second basket”) by the end of 2016. A threshold value of 500,000 is deemed too low for the finance and insurance sector in particular because this field, unlike the “first basket” sectors, already features substitution options for its critical infrastructures. For example, cash can be used instead of card payments, and vice versa. Cash can also be obtained from various independent sources, including ATMs, cashback and from the bank itself. Additionally, most bank customers also have more than one bank card available for mak

ing payments. These substitution options are not a feature of other sectors. For example, households only have one water, gas or electricity supplier. These conditions should be taken into account by the legislator in the form of a higher threshold value for the amending regulation for the "second basket".

By way of example, the table compares the critical infrastructures in the financial sector on the left according to the German government departments (when agreeing on the IT-SiG) with those of the Federal Financial Supervisory Authority (BaFin) as a professional supervisory body in the center, and in accordance with the sector study by the BSI on the right. All details represent the status prior to the end of talks on the amending regulation anticipated for December 2016.

It remains to be seen which critical infrastructures are finally identified as such in the amending regulation. Starting in May 2016, under the aegis of the BMI and BSI, expert talks were carried out with core teams within the three sectors, also incorporating industry associations and operators affected.

The core requirements of the operators of critical infrastructure – minimum security and regulatory reporting – are defined in the new sections 8a to 8d.

Section 8a "Security in Information Technology of Critical Infrastructures" Paragraph 1 requires operators to adopt appropriate organizational and technical precautions to avoid restrictions to the availability, integrity, authenticity, and trustworthiness of those information technology systems, components or processes that play a key role in the proper functioning of the critical infrastructures the operator provides no later than two years after the legislation has come into force. In doing so, the operators must also actually comply with the state of the art, rather than merely "observing" it. Several operators of critical infrastructures and their industry associations may develop an "Industry-Specific Security Standard" (B3S) and submit it to the BSI for recognition. In consultation with the Federal Office of Civil Protection and Disaster Assistance (BBK) and the relevant government supervisory bodies – such as BaFin for the financial sector – the BSI must check whether B3S is suitable for fulfilling the requirements of IT-SiG. The operators must provide evidence that they still fulfill all requirements every two years (Paragraph 3). This proof may take the form of security audits, tests or certifications. If any security weaknesses are detected, the BSI may

1. request that it receives the results of all audits, tests or certifications and
2. with the consent of the relevant government supervisory bodies, request the resolution and remedying of the security weaknesses.

Regulatory reporting, as the second core requirement, is regulated by Section 8b "Central Point of Contact for the IT Security of Critical Infrastructures". An operator must name a point of contact responsible for such matters to the BSI within six months of the legislation coming into force. Any significant restrictions to the availability, integrity, authenticity, and trustworthiness of those information technology systems, components or processes provided by the operator (Paragraph 4), which may lead to, or have already led to, the failure or loss of function of the critical infrastructures the operator provides and for which the operator has to provide an immediate notification to the German federal

authorities via the point of contact. In such circumstances, the operator only needs to named if the fault has actually led to a failure or loss of function. Operators within the same sector may name a single point of contact (SPOC). One major innovation is the option for the BSI to request that the manufacturer help to remedy or avoid a fault. It remains to be seen whether the BSI can also assert itself and bring its authority to bear on very large suppliers from abroad.

The BSI act also now includes Section 14 “Provisions on the Payment of Fines”, according to which infractions of the requirement to remedy security weaknesses can be met with a fine of up to EUR 100,000 and infractions of the requirement to submit audit, test and certification results may result in a fine of up to EUR 50,000.

As mentioned above, the IT-SiG can be seen as a precursor to the implementation of the European NIS guidelines, which will have to be implemented in all EU states within 18 months, i.e. by the end of 2017, according to the EU Commission’s current timeline. It will implemented in Germany in the form of the “IT Security Act 2”. We can assume that the NIS guidelines will not result in any major changes to the current “IT Security Act 1”.

With regard to the financial sector, the implementation deadlines are shown below provided that the amending regulation enters into force by the end of 2016:

- Ability to notify: July 1, 2017
- Compliance with a minimum security level: January 1, 2019.

Experts think it likely that there could be a delay to the timelines of up to six months.
Although the financial sector is seen as being well-prepared from an IT point of view in a comparison of the seven critical sectors, regulatory reporting of IT incidents is new for this sector too. This regulatory reporting must be established or integrated, implemented and operated into an existing reporting system – for example, one resulting from the legislation on the Guidelines on internet payments security (MaSI). The minimum level of IT security should already be guaranteed by the banking supervisory body; however, evidence will once again have to be provided. This proof is best provided through the implementation of a documented IT security framework, either for each bank or as B3S for several institutes. The legally compliant implementation of the framework will then need to be checked. The auditing process remains undecided. Ideally, it would be integrated into the existing auditing processes, so that IT-SiG conformity could be audited internally, for example, or via the annual financial audit. This would enable the additional costs resulting from banks implementing the IT Security Act to be kept to a minimum wherever possible.

## Sources

LITERATURE:

Waldemar Grudzien: *IT-Sicherheitsgesetz: Regulierungsarbitrage muss vermieden werden*, die bank, May 2016, pp. 46–51

INTERNET:

European Commission, Network and Information Security (NIS) Directive, 2015

https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-nis-directive

Security (NIS) Directive, 2015
Heise, Erste Verordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten, 2016
http://www.heise.de/newsticker/meldung/Erste-Verordnung-zur-Umsetzung-des-IT-Sicherheitsgesetzes-in-Kraft-getreten-3196234.html?wt_mc=nl.ho.2016-05-04

**Dr. Waldemar Grudzien** is Transformation Engineer at CORE and focused on the security regulations of the financial industry and their technological effects on IT infrastructures. During his work at a national federation of the financial industries he was a specialist for retail banking and banking technologies.

**Mail: waldemar.grudzien@coretransform.com**

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
www.coreinstitute.org
Phone: +49 30 16344 020
office@coreinstitute.org

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
www.coretransform.de
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
www.coretransform.ch
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
www.coretransform.co.uk
Phone: +44 203 319 0356
office@coretransform.co.uk