WATSON FARLEY
&
WILLIAMS

BRIEFING

THE NEW GERMAN IT SECURITY ACT

FEBRUARY 2016

- COMPANIES ARE OBLIGATED TO IMPROVE IT SECURITY
- VIOLATIONS MAY BE SUBJECT TO PENALTIES OF UP TO EUR 100,000

Seldom has the passage of a bill had such current relevance. While the draft IT Security Act was being debated in Parliament, the IT security department of the Bundestag and the Federal Office for Information Security ("**BSI**") were debating how to regain control over the Bundestag's internal network following a cyber attack.

"WHAT THE NEW IT SECURITY ACT AIMS TO PREVENT IS THE LOSS OF CONTROL OVER IMPORTANT IT SYSTEMS – WHICH IS PRECISELY WHAT HAPPENED TO THE BUNDESTAG."

That being said, what the new law for improving security of IT systems ("**IT Security Act**") aims to prevent is the loss of control over important IT systems – which is precisely what happened to the Bundestag.

The IT Security Act comes with an increase in requirements especially for website operators, service providers, telecommunications companies and operators of critical infrastructure.

WHAT DOES THE ACT AIM TO ACHIEVE?

The act entered into effect on July 17, 2015. Its aims are:

- to significantly **improve IT security** in Germany with regard to its availability, integrity, confidentiality and authenticity,
- to **improve the IT security of companies** and provide greater protection for citizens using the Internet, as well as
- to **protect critical infrastructure** that is of pivotal importance for the functioning of the community.

WHO DOES THIS ACT AFFECT?

The IT Security Act particularly applies to:

- Website operators and others considered as service providers according to the German Telemedia Act; (see below under A respectively),
- Telecommunications companies (see below under B respectively); as well as
- Critical infrastructure operators (see below under C respectively) in the following sectors:
  - Energy
  - IT and telecommunications
  - Transportation and traffic
  - Healthcare
  - Food and water
  - Finance and insurance.

A. Website operators and other service providers

The requirements recently included in the Telemedia Act by the IT Security Act apply for all operators offering telemedia on a commercial basis. This also includes all companies that operate their own website and it even applies if the company itself does not directly offer goods or services but only refers to these.

B. Telecommunications companies

Telecommunications companies are providers that offer commercial telecommunications services or are involved in providing such services (e.g. Internet service providers (ISPs) and other access providers, such as companies operating fixed and mobile phone networks).

"... THE FAILURE OR IMPAIRMENT OF CRITICAL INFRASTRUCTURE CAN SIGNIFICANTLY CONSTRAIN OR ENDANGER PUBLIC SAFETY."

C. Critical infrastructure operators

The Act defines critical infrastructure as those whose failure or impairment would significantly constrain or endanger public safety and therefore are highly important for the community to function.

A statutory ordinance still to be issued will define in detail specifically which companies will be categorized as critical infrastructure operators. The Federal Ministry of the Interior is currently preparing this statutory ordinance, and it is expected to take effect in two parts:

- "Basket 1" for the sectors of energy, IT and telecommunications, food and water by the end of the 1st quarter of 2016 and
- "Basket 2" for the sectors of finance and insurance, healthcare, transportation and traffic by the end of 2016.

"IN THE COURSE OF THIS YEAR A STATUTORY ORDINANCE WILL BE ISSUED THAT WILL SPECIFICALLY DEFINE WHICH COMPANIES WILL BE CATEGORIZED AS OPERATORS OF CRITICAL INFRASTRUCTURE."

In this statutory ordinance the Federal Ministry of the Interior will use branch-specific threshold values to determine the supply levels for every service deemed critical. For instance the market share of energy and food supply in a specific region necessary to reach the threshold value.

Companies that achieve the stipulated threshold values must meet the state-of-the-art security measures and comply with special reporting obligations vis-à-vis the BSI. The reasoning behind the act is that the law will affect approximately 2,000 companies operating critical infrastructures in the regulated sector.

WHAT ACTION DO THE AFFECTED COMPANIES NEED TO TAKE?

A. Website operators and other service providers

Website operators and other service providers must make sure that no one can access the IT systems they use without authorization and that their systems are secured against unauthorized access to personal (customer) data and against disruptions caused by external attacks. To this end they must implement the relevant state-of-the art technical and organizational measures, which include using secure encryption procedures.

However, a service provider will only be required to implement the corresponding measures insofar as this is "*technically possible and can be reasonably expected*" of the provider.

The statutory regulation has been intentionally designed to be flexible, which makes it difficult to assess specifically which measures are expected from which providers. Hence, some votes have considered the regulation as unconstitutional on the grounds of its indeterminate obligations. Here it is particularly important to keep an eye on further development, especially on how responsible state authorities will be in terms of implementing the Act in practice.

It is also not yet clear whether this new statutory regulation is intended to regulate market conduct, in other words it is as yet not known whether warnings can be issued to competitors and/or consumer protection associations for violating the law.

B. Telecommunications companies

In addition to the already existing obligation of sufficiently securing their systems and facilities against cyber attacks, now telecommunications companies have to inform their customers about any disruption to and abuse of their connections as well as about suitable and available defensive measures.

C. Critical infrastructure operators

The IT Security Act not only obligates critical infrastructure operators to protect their websites, but also to protect their other IT systems as well. As such they are obligated **to provide adequate state-of-the-art security** for the IT necessary for providing their services **within two years after the statutory ordinance has taken effect** and to have this security checked at least every two years.

"CRITICAL INFRASTRUCTURE OPERATORS ARE OBLIGATED TO PROVIDE ADEQUATE STATE-OF-THE-ART SECURITY FOR THE IT NECESSARY FOR PROVIDING THEIR SERVICES WITHIN TWO YEARS AFTER THE STATUTORY ORDINANCE HAS TAKEN EFFECT AND TO HAVE THIS SECURITY CHECKED AT LEAST EVERY TWO YEARS ..."

The law does not define what is to be considered specifically as state-of-the art in which branch. With regard to the methodology, the BSI states on its website:

"What the state-of-the-art is at a specific point in time can be determined, for instance, based on existing national or international standards like DIN or ISO standards or based on examples successfully proven in practice for the respective sector."

Critical infrastructure operators and their industry associations may propose branch-specific security standards that will be recognized by the BSI upon request as the state-of-the-art in a specific area if said standards are suitable for preventing disruptions and guaranteeing the availability, integrity, authenticity and confidentiality of the relevant infrastructure.

General and branch-specific best-practice recommendations can already be obtained via the Internet platform shared by the BSI and the German Federal Office for Civil Protection and Emergency Aid ("**BBK**").

In agreement with the BSI, the Federal Network Agency already published an IT Security Catalogue in August 2015 for energy supply companies that have their own grid operation. The catalogue provides specific guidelines for implementing IT security requirements.

In addition, within six months of the ordinance taking effect, critical infrastructure operators are required to set up an internal reporting structure that makes it possible for the companies to report IT-security incidents to the BSI. The BSI shall then provide the findings obtained from these reports as well as from other diverse information to all companies concerned so that these companies can readjust their IT on an on-going basis where necessary.

Currently this reporting obligation only applies to operators of nuclear power stations and telecommunications companies.

WHAT ARE THE CONSEQUENCES FOR VIOLATIONS?

The supervisory authority for website operators and other service providers are the respective competent state supervisory authorities. Telecommunications companies will essentially be subject to the supervision of the Federal Network Agency, the critical infrastructure operators will be subject to BSI supervision.

A. If website operators and other service providers fail to comply with their obligation to install state-of-the-art technical and organizational measures to protect their IT systems and customer data, they may be subject to **fines of up to EUR 50,000**.

B. If telecommunications companies fail to comply with their reporting obligations to their customers they may likewise incur **fines of up to EUR 50,000**.

C. **Fines of up to EUR 100,000** may be imposed on critical infrastructure operators that cause IT security incidents by failing to implement IT security measures. Violations of reporting obligations will be sanctioned with lesser fines.

"VIOLATIONS AGAINST STATUTORY OBLIGATIONS MAY INCUR FINES OF UP TO EUR 100,000 ..."

Since critical infrastructure operators have been granted an **implementation period of two years** after the ordinance takes effect, fines will not apply to these companies until this period expires.

WHAT HAS TO BE DONE NOW?

A. Website operators and other service providers

Website operators and other service providers, insofar as they operate the server themselves (for instance, they have their own data processing center or server housing), must ensure that any security gaps and weaknesses that become known are immediately closed by installing updates and patches and that the installed software is updated with the most recent release.

Companies that rely on host providers for operating their websites should review the underlying contracts as to whether the host provider is obligated to comply with the current state-of-the-art for IT security and adjust the contracts if necessary, because even companies that do not technically operate their website themselves are nevertheless still responsible vis-à-vis the supervisory authorities and must pay any fines incurred.

B. Telecommunications companies

Through their internal process organization, telecommunications companies must ensure compliance with the disclosure and reporting obligations newly created by the IT Security Act vis-à-vis the Federal Network Agency and their customers.

C. Critical infrastructure operators

With the creation of legally stipulated IT security and the establishment of reporting structures, critical infrastructure providers are faced with considerable financial and human resource challenges.

In addition the period scheduled for setting up internal reporting structures and implementing new IT security requirements is quite tight.

It will be important for these companies to quickly contact the respective branch associations to have the technical status and the security of their IT systems reviewed and to start rectifying any deficits. Efficient structures should be just as quickly set up in order to fulfill the legal reporting obligations in good time.

CONTACTS

Should you like to discuss any of the matters raised in this briefing, please contact Axel Löhde, Dr. Torsten Rosenboom, Torge Rademacher, Sebastian Ens, Ursula Staab, or your regular contact at Watson Farley & Williams.

AXEL LÖHDE
Partner
Hamburg
+49 40 800 084 314
aloehde@wfw.com

DR. TORSTEN ROSENBOOM
Partner
Frankfurt
+49 69 297 291 250
trosenboom@wfw.com

TORGE RADEMACHER
Senior Associate
Hamburg
+49 40 800 084 314
trademacher@wfw.com

SEBASTIAN ENS
Senior Associate
Frankfurt
+49 69 297 291 220
sens@wfw.com

URSULA STAAB
Associate
Hamburg
+49 40 800 084 449
ustaab@wfw.com

Publication code number: 57767815v1