KNOW-HOW

Gleiss Lutz

31.05.2021

TMT

IT SECURITY ACT 2.0 – PROHIBITION ON THE USE OF CRITICAL COMPONENTS TO PROTECT PUBLIC SECURITY

The Second Act to Increase the Security of Information Technology Systems (*Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*, "IT Security Act 2.0") came into force at the end of May 2021 (BGBl. I 2021, S. 1122 and Bundesrat document 324/21). The new legislation will make it possible to prohibit the use of certain IT components by operators of critical infrastructures if it is to be assumed that the use of these components is likely to adversely affect Germany's public order or security.

1. Background

With an ever-increasing rate of digitalisation and the resulting dependency on information technology, the use of IT as part of governments' foreign and security policies has become a hot topic in recent years. It is becoming ever more apparent that there is a risk of foreign governments gaining indirect control of particularly important infrastructures such as the financial system, the energy supply network or the telecommunications network. In light of this, the use of IT components from the manufacturer Huawei and other Chinese companies for the expansion of the 5G network in Germany was the subject of criticism in particular, as the possibility cannot be excluded that these companies might design their components in such a way that the Chinese government and its security agencies could, if need be, control them.

The amendment to the IT Security Act is aimed at countering this risk by increasing the requirements to be met for the use of IT components in areas of critical infrastructure. The IT Security Act also strengthens the current system of investment protection controls, which aims to prevent dependency on foreign governments resulting from the acquisition of infrastructure.

2. Current legal situation

Certain restrictions already applied to operators of critical infrastructures when purchasing IT components even before the amendment came into force. Since 23 December 2020, operators of telecommunications networks are obliged to use certified critical components based on the new list of security requirements under section 109 Telecommunications Act (*Telekommunikationsgesetz*). In addition, operators of public telecommunications networks and providers of publicly available telecommunications services with an increased level of criticality (5G networks) must check that the sources from which they obtain their components – not only manufacturers but also, where applicable, sellers or suppliers – are trustworthy.

Components are considered to be critical if they wholly or partially fulfil critical functions. A list of critical functions is still being drafted.

According to this, a function is critical in particular if, when technically compromised, it may result in significant data protection violations, systematic analysis of telecommunications or substantial security breaches pursuant to section 109(5) Telecommunications Act (i.e. especially unauthorised access or restrictions in availability). In relation to certain function categories the draft provides very precise definitions of their criticality. Critical components are to be identified and documented by operators within one year of the list being published.

Components used from 31 December 2025 onwards must be certified by a recognised certification body and reviewed by a recognised IT review body. Should the certification schemes required for this not be available, other suitable and appropriate measures to avert risks must be taken.

Previously used components must be replaced by no later than 31 December 2025 if they are not certified. However, if two suitable, correspondingly certified products from different manufacturers become available on the market prior to this, it must be documented, with accompanying substantiation and proof, that the continued use is not expected to lead to any risks or relevant security breaches. Otherwise, the components must be replaced by the alternative models that are available.

Operators must ensure that their sources of supply are trustworthy by obtaining a self-declaration from the supplier in question. This declaration includes obligations relating to information security, cooperation, transparency, and reviewing the security of the product and the production process.

In addition, the operator must be able to check the integrity of the components at any time after having taken delivery of the product concerned.

3. Expansion of critical infrastructures and introduction of the term critical component

First of all, the amendment slightly expands the list of critical infrastructures. In addition to the previous sectors, energy, information technology and telecommunications, transport and traffic, health, water, food, as well as finance and insurance, municipal waste management is now also included. The exact requirements are further specified in the Critical Infrastructures Ordinance (*KRITIS-Verordnung*).

The term "critical components" has now also been introduced into the Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik*) (section 2(13)). Critical components are IT products used in critical infrastructure in respect of which malfunctions can lead to significant impairments of the functionality of the critical infrastructure or to threats to public security. Furthermore, they must have been designated as critical components on the basis of a law with reference to the new section 2(13) Act on the Federal Office for Information Security or realise a function that has been designated as critical on the basis of a law. In this regard, the list of security requirements can be used for the area of telecommunications. The list of critical functions is however currently still in the draft stage (see 2.). Further provisions on critical components "on the basis of a law" do not exist yet. Moreover, critical components need not necessarily be identified in all sectors.

4. Introduction of a review procedure

In future, any use of critical components by operators of critical infrastructures must be notified to the Federal Ministry of the Interior and such critical components may not be put into use before the expiry of a review period of in principle 2 months, which can be extended to a maximum of 4 months, unless the use of a component of the same type had already been notified in the past and was not prohibited (section 9b(1) Act on the Federal Office for Information Security).

The notification must be accompanied by a manufacturer's guarantee in which the manufacturer must provide information on its organisational structure and describe how it has ensured that the component does not have technical features that specifically make it susceptible to misuse for the purpose of sabotage, espionage or terrorism. The details of the guarantee are yet to be determined by way of general decree by the Federal Ministry of the Interior.

The Federal Ministry of the Interior will take into account in its examination whether the *first-time* use of the component is likely to affect public order or security, in particular:

- whether the manufacturer is directly or indirectly controlled by the government of a third country,
- whether the manufacturer has already participated in activities that had an adverse effect on public security in Germany, an EU Member State or a NATO member,

or

- whether the use conflicts with security policy goals of the Federal Republic of Germany, the EU or NATO.

This review applies in addition to and in principle independently of the certification requirements based on the list of security requirements that came into force on 23 December 2020 (see 2.).

5. Possibility of subsequent prohibition

The *further* use of critical components can also be *subsequently* prohibited if the manufacturer proves to be untrustworthy (section 9b(4) and (5) Act on the Federal Office for Information Security). The subsequent determination that a manufacturer is untrustworthy can be based in particular on a false guarantee or violations of obligations contained therein, insufficient security checks on the component, non-transparent communication of vulnerabilities or the component's susceptibility to misuse.

Instead of the prohibition, which may be accompanied by an appropriate transitional period and which may also refer to further critical components of the manufacturer, it is also possible, as a milder means of enforcement, for the Federal Ministry of the Interior to issue subsequent orders with regard to the critical components in question.

Where a manufacturer is deemed to be extremely untrustworthy, the use of *all* its critical components may be prohibited (section 9b(7) Act on the Federal Office for Information Security).

6. Significance for companies

The amendment of the Act on the Federal Office for Information Security may have significant consequences not only for foreign manufacturers of IT components, but also for the operators of critical infrastructures as their customers, even leading to a ban on the use of these components. This affects the entire telecommunications sector.

The newly introduced review procedure, which must now be carried out before each new use of a critical component (see 4 above), must be taken into account in this regard. Added to this is the possibility that use can be prohibited subsequently (see 5 above).

This far-reaching consequence of the legislative changes gives rise to considerable uncertainty about the use of critical components from foreign, and especially Chinese, manufacturers for a large number of important network expansion projects in Germany.

The fact that the use of components may be prohibited even after they are already being used – theoretically, even if the relevant components themselves do not give rise to any security risks – creates the significant risk that operators may at any time find themselves having to replace components within an extremely tight timeframe. Should this risk arise, it may result in the disruption of business processes as well as significant costs, including for the procurement of replacement components.

EXPERTISE

Digital Future

TMT

EXPERTS

Dr. Hannah Bug

Dr. Christian Hamann

Dr. Moritz Holm-Hadulla

Dr. Andreas Neun

Simon Clemens Wegmann