White paper on the discussion about the security of Huawei network technology:

1. Introduction: the current situation

While the auctioning of 5G infrastructures is still under way/coming to an end, the German government has determined – in line with the European Commission – that the Federal Republic will not exclude Huawei from the development of 5G infrastructure. This decision was preceded by months of discussions as to whether critical telecommunications infrastructure could be operated with network equipment from China and, in particular, from Huawei. This discussion attracted particular attention when, on the very same day that the Bundesnetzagentur, Germany's telecommunications regulator, had proposed new security regulations for network operators, US ambassador Richard Grenell announced the stance of the United States on the issue. In a letter to German Minister of Economic Affairs Peter Altmaier, he threatened to significantly reduce the amount of intelligence shared with Germany if it continues dealing with Huawei.

Behind this are two problem areas supposedly associated with Huawei: Firstly, a fear of the network operator carrying out espionage because of Chinese laws and on behalf of Chinese intelligence services, thus enabling it to provide sensitive data to Chinese authorities. Secondly, there are concerns that if the Chinese government were to face an international crisis, Huawei could be compelled to disrupt or even paralyse foreign networks. Sabotage is the keyword. A so-called "kill switch" would shut down the entire infrastructure from one moment to the next, so the theory goes.

To identify such functions, it would be necessary to inspect the supplier's source code. Great Britain obliged Huawei to allow such insight and in the course of the inspection criticised the company for poor engineering work and possible security gaps in the supply chain. However, British security experts do not believe that the problems identified were the result of state interference. Consequently, the British government does not intend to exclude the Chinese telecommunications provider from the construction of the country's 5G mobile network. However, only parts subject to a low risk of espionage or sabotage may be supplied. This includes, for example, base stations, antennas, and certain transmission technology. Nevertheless, the most important and sensitive areas of the network infrastructure will be operated without Chinese equipment. There remains, therefore, a certain degree of mistrust.

The German government and the competent authorities, such as the Bundesnetzagentur and the Federal Office for Information Security (BSI) as well as the German Informatics Society (Gesellschaft für Informatik - GI), assess the situation somewhat differently to Great Britain. Berlin strengthened security requirements in March, but for all suppliers. A new catalogue of security criteria will have to be met in future. Essentially, it is a kind of reversal of the burden of proof. Network operators must prove that any telecommunications technology used in critical infrastructures is trustworthy.

Jochen Homann, the president of the Bundesnetzagentur, told the Financial Times in an interview: "The Bundesnetzagentur has not received any concrete indications against Huawei. Nor are we aware of any other body in Germany that has received any reliable indications."[1] Back in November 2018, Arne Schönbohm,

[1] https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a

president of the BSI, explained that his agency had no evidence of potential risks from Huawei products. On the contrary, at the opening of a Huawei security laboratory in Bonn, Schönbohm expressed his desire for other manufacturers to carry out similar activities. At the laboratory, customers can, among other things, examine the source code of Huawei products. Schönbohm also took the opportunity to emphasis that his security specialists had procured Huawei components around the world in order to inspect them – independent of the company's own laboratory.

The telecommunications provider and mobile phone manufacturer has repeatedly rejected the allegations. In an interview, Richard Yu, CEO of the Consumer Business Group, which the smartphone business belongs to, told German newspaper Die Welt: “That is nonsense, as it is not technically possible. And we would certainly not allow it. We have very high security standards for our hardware and software.”[2]

In a comprehensive white paper on the subject, Huawei underlined the importance of cyber security and data privacy: “In the digital world of ones and zeros, security is a necessary prerequisite that makes everything else possible. Cyber security and data privacy have the highest priority at Huawei. They are part of our DNA, encoded in all of our workflows, audits, processes, guidelines, products, and services. We have developed and implemented a global cyber security system that covers every process from end to end.”

Similar sentiments were expressed by the German Informatics Society, which believes that the allegations against Huawei are ideologically driven and which demands a selection of 5G network providers strictly based on technical and economic parameters. The allegations made against Huawei could also be made against Cisco, Nokia, and Ericsson.

The spokesperson for the GI’s working group of the executive committee, Professor Hartmut Pohl, commented: “Even if an IT system has already been inspected, and security gaps have been identified, more and more can become apparent in future. It cannot fundamentally be proven that an IT system is free of security gaps and therefore also free of points of attack. The same applies to back doors that are deliberately installed in IT systems by providers, enabling unauthorised access.”[3]

There therefore remains a certain residual risk, a residual security threat. What if a manufacturer of network equipment, Cisco or Huawei for example, actually wanted to misuse data from critical infrastructures? What if a kill switch were installed? Is that really possible or preventable?

Anyone who is somewhat more intensively involved in IT security knows that complete security is impossible. So such attacks would, in fact, be theoretically possible. Anyone intending to prevent this to the greatest possible extent must contemplate the company's internal security process. If it is designed to exclude any misuse, such alleged security threats can also be prevented: Segmenting and a firewall at the application level that blocks any malicious outgoing data traffic by means of an IDS/IPS are the methods of choice here. A multi-vendor environment and additional security measures guard against a kill switch.

[2] https://www.welt.de/wirtschaft/article190034791/Huawei-Manager-zu-Spionagevorwurf-Das-hat-politische-Gruende.html
[3] https://www.golem.de/news/huawei-informatiker-gegen-ausschluss-aus-politischen-gruenden-1903-140259.html

2. Security in critical infrastructures

According to the two CIP (Critical Infrastructure Protection) regulations of 3rd May 2016 and 3rd June 2017, operators of critical infrastructures are obliged to demonstrate their adherence to a minimum standard of IT security. In light of this obligation and the particular responsibility for the operation of their installations, which are important for the supply of the general public in the Federal Republic of Germany, they have to pay special attention to these additional measures. This includes encryption, monitoring, or also security by design. They can thus design the network infrastructure to be as secure as possible and, in particular, prevent the described – potential – risks.

And this is where telent – a company of the euromicron Group – comes into play. Together with its subsidiary KORAMIS, telent provides comprehensive security solutions and services to guarantee this protection. The system integrator takes a holistic approach to this task. telent experts will gladly recommend a vulnerability assessment for the operation of critical infrastructures. The assessment identifies points of attack both in the physical infrastructure and the organisational structure of a company's security strategy. In the process, experts analyse the security of the technical facilities, the awareness of employees, and processes, and thus determine the actual level of security of the IT and telecommunications infrastructure.

System hardening measures, for example, help to preclude the potential risks posed by network technology and associated software. At the same time, such measures prevent risks that are caused by the misconduct of employees or external companies.
What is the exact nature of the additional security measures?

The telent security guideline - (1st measure)

telent subjects the products of all providers of network equipment to a meticulous inspection. A checklist contains the technical requirements for the network provider. The guideline is provider-independent and applies equally to Cisco, Huawei, Nokia, and other partners/providers. telent employees work through this list point by point before putting a system into operation and, in the process, inspect certain security functions/settings. This includes questions such as: Is the default password deleted as soon as the device is connected? Are open ports deactivated, and does a firewall matrix exist for the system? It is also examined whether there are specific restrictions for the individual systems. Using the checklist, security experts can set the components so that they follow best practice examples.

telent performs a security check on all suppliers as part of the application of these guidelines. Among other things, questions concern how they handle security issues in general, including internally. Is a secure code review firmly established with regard to how security is taken into account in work processes? In addition, there are checklists for individual technologies such as directional radio, DWDM, and access and carrier systems, each containing different requirements. Here too, the checklists are aimed at hardening security settings by implementing best practices ("secure hardening"). The defaults applied are based on telent's past experience as well as that of the providers. Measures such as switching off unused interfaces, the use of the latest systems in the latest software version, and ensuring that the default password is not preset became an integral part of the inspection after telent employees repeatedly noticed that there was a need for this. They also pay attention to how the system is to be put into operation and which functions it has. These checklists are specifically adapted to the respective systems. The majority of cases recorded in the checklist revolve around the issues of default

passwords, open communication connections, and unused services that run alongside different operating systems but are not required.

Segmenting networks (2nd measure)

telent uses firewalls to segment networks. These days, traditional network firewalls on layer 3 are no longer used, with preference being given to next-generation firewalls on layer 7 of the OSI model. In the process, the software can examine the contents of the data packages in great detail with regard to what is actually happening at the application level. In this way, telent enhances security. Should a provider such as Huawei experience data leaks, it would be apparent thanks to these firewall technologies, since traffic would be made visible that otherwise remains hidden with traditional firewalls. Segmenting makes it possible to inspect the network traffic as to whether unauthorised connections are being established from the company network.

Whitelisting and sandboxing:

Targeted attacks from organisations with the necessary resources require highly sophisticated security strategies. System hardening measures help to avert such threats and, at the same time, safeguard against risks that can also be caused by the misconduct of employees or external companies. Simply put, system hardening involves establishing rules regarding who has access to which systems and who does not. In particular, it is necessary to define which critical application are to run in a sandbox. Sandboxing is a technique whereby software is operated in a runtime environment that is isolated from the other system resources. All activities in this isolated area have no impact on the external environment; conversely, intruders have no chance of reaching the software in the sandbox and causing damage.

The multi-vendor strategy (3rd measure)

Similarly to the guidelines of the Bundesnetzagentur (BNetzA), which were updated in early March 2019, all operators of critical infrastructures should make sure, when planning and building communication networks, that they plan and operate these using network and system components from different providers. This can be arranged differently for core and access networks. Such a multi-vendor approach is not an indication of a fundamental distrust towards a particular supplier, rather a statement of forward-looking infrastructure. All operators of critical infrastructures should pursue this approach irrespective of whether they do not – or no longer – trust a provider. The architecture could be designed, for instance, so that the company uses Huawei equipment in the access network and, for example, Cisco equipment in the transport network. Where appropriate, the design should be construed so that changes in vendor are possible in individual sections.

“Sleeper” programs, which are repeatedly mentioned in the media, cannot be detected by familiar security technologies, as the programs are inactive until they are awoken. In this regard, telent recommends examining the state of the company’s security measures within the framework of the continuous improvement process and thus avoid possible security threats. Monitoring is an extremely important task in cyber security. Security officers must repeatedly assess whether the methods used to monitor the company’s own networks are state-of-the-art. They should also analyse whether what they are having monitored is working as it should. telent recommends security event management in line with the current standard SIEM (security information and event management) process. In this way, all security-related events can be comprehensively and clearly monitored.

3. Moving methodically towards secure networks

Using the described methods, telent enables its customers to efficiently and securely network processes and infrastructures and successfully pave the way to a digital future. Operators of critical infrastructures and industrial companies trust in our expertise. Due to our focus on critical infrastructure protection (CIP), telent not only has extensive practical experience as a system integrator, but is also the specialist for planning, building and operating secure networks and systems.

As telent critically evaluated the suspected security threats from Huawei on the basis of its own security guidelines and found no cause for complaint, telent also markets, implements and operates the solutions for next-generation telecommunications networks. Through security audits, personal discussions, and tests, we have established a relationship of trust with Huawei.

telent and Huawei have built a dedicated joint innovation lab at telent's headquarters in Backnang. Here, systems are extensively tested with regard to their functions, interoperability, and security. The lab offers our customers best possible service in the event of hardware or software problems, warranty questions, or queries about the general handling of Huawei equipment. In addition, on-site training is conducted to optimally prepare employees for service provision on the customer's premises. This principle applies not only to Huawei systems, but in general to the systems technology of other providers in the telent portfolio.

Therefore, as things stand, we can – in good conscience – recommend the equipment of the global market leader and look forward to your reactions to this white paper. Please contact us by telephone at any time for further information.

Author and contact

Nico Werner
Head of Cyber Security
telent GmbH - a company of the euromicron Group
Phone_ +49 7191 900-0
E-mail: info.germany@telent.de
Web: www.telent.de

About the author

Nico Werner has been enthusiastic about computers from an early age, especially about technologies and IT infrastructures.
His interest was rounded off by training as an IT specialist with a focus on cybersecurity.
The subject of IT and OT security has shaped his career to date.

Since 2012, he has been involved in cybersecurity at various well-known companies including Audi, SimonsVoss and NATEK Technologies. Since January 2017, he has been in charge as "Head of

Cybersecurity" at telent GmbH, true to his motto "cybersecurity is a matter for the boss". His goal: communicating the importance of the security topic to the key players.

He is involved in the committees of several associations such as Bitkom, TeleTrust, PMeV and IEC 62443. Furthermore, Nico Werner has certifications and experience in many areas, including ISO 27001 and BSI §8a (auditing of mission critical infrastructures operators (KRITIS)).