The Cyber Security Transparency Centre in Brussels

23

THE CYBER SECURITY TRANSPARENCY CENTRE IN BRUSSELS

Christoph Hugenschmidt, Switzerland[312]

"You will be disappointed," Wang Liangchen warns me. In fact: what's interesting about a few almost empty, cramped offices in a rather nondescript building in Brussels? After all, the entrances to the offices on the first floor are well secured, and the alarm triggered accidentally is really loud. In the windowless rooms themselves there is a desk, one or two office chairs, one or two screens and a PC, sometimes even just an internet connection.

What Wang Liangchen showed me in Brussels in January 2022 is actually completely unspectacular. But not what happens in these rooms.

---

[312] Original text published in German: Christoph Hugenschmidt, Wie Huawei Cybersecurity praktiziert und wie transparent das wirklich ist – Ein Besuch im Cyber Security Trasnparency centre in Brüssel, in Marc Furrer (Ed.), Selbstbestimmt. Sind souveräne Kommunikationsnetze in der Schweiz möglich?, Stämpfli Verlag, Bern, 2022, 89-95. Published in English with permission of the publisher. | DOI: 10.58863/20.500.12424/4276057 |

Because in the Brussels Huawei Cyber Security Transparency centre, more precisely in these windowless, narrow rooms, customers and partners from the security ecosystem can view and check the source code. Namely the source code of the programs that are in Huawei's network, data centre and other components. However, the source code itself is not stored on the PCs and servers in Brussels. It is – in all likelihood extremely well secured – in a data centre in Shenzhen and can be viewed from Brussels. And, as Wang assures, for as long as the customer needs. There is no time limit.

Wang Liangchen is a cybersecurity specialist. For nine years he has been working for the Chinese technology group Huawei, one of the world's three largest providers of infrastructure for telecommunications and, in particular, fifth-generation mobile networks. There, Wang was responsible, among other things, for so-called "penetration tests" as part of the company's independent security laboratory. They are more important than ever in the IT and telecom industry; Because this is how manufacturers and operators of computer and network infrastructures try to find out whether their systems are protected against attacks from outside. And that is exactly what cybersecurity is all about: Can outsiders penetrate my systems? Can they steal or manipulate data? Can they cripple systems or cause them to do something other than what they were built to do?

The fact that customers or their security teams can view the source code of an operating system or applications of commercially marketed network products is exceptional. It indicates that the Chinese telecom equipment supplier trusts its own software and, conversely, is dependent on customers trusting their software. In the background of Huawei's transparency offensive is the accusation, expressed above all by the USA, that Huawei is building back doors into its software on orders from the Chinese secret services or the army. These backdoors would allow Chinese intelligence agencies to penetrate networks using Huawei machines.

Another suspicion, expressed primarily by the United States, is that Huawei is secretly installing additional chips in its devices. These would monitor or manipulate the data traffic. That's why Huawei even allows customers to physically analyse its hardware. However, if you want to do this, you have to travel to Shenzhen in China. There is no Huawei hardware in Brussels.

23.1 "We love processes"

Yoann Klein is my second interviewee at Huawei's Cyber Security Transparency centre in Brussels. The Frenchman can look back on a long career in the European IT security industry. He worked for the French high-tech and armaments group Thales and before that for Airbus. According to Klein, Huawei has come a long way in developing cybersecurity. While the focus before 2005 was still on product security, company founder Ren Zhengfei defined cybersecurity as an absolute priority at every level in an open letter to employees at the end of 2011. The open letter from the charismatic industry veteran was probably intended as a wake-up call to employees and the outside world to really and always take the issue of security seriously. Since then, software development processes at Huawei have been and continue to be redefined in terms of security, and the entire organisation of the giant corporation has been aligned with security, from management to the individual in sales.

The European market is enormously important for Huawei, emphasises Klein in an interview. On the one hand, it is large with well over 400 million inhabitants. The level of industrialization is high, and investments in telecommunications are correspondingly massive. In addition, the EU defines the standards worldwide when it comes to data protection. Huawei itself implements the standards of the European General Data Protection Regulation across the group. In addition to the centre in Brussels, Huawei operates three other such centres in Europe

and employs a total of 13,000 people in the EU area, 2,400 of them in research and development.

Klein takes the time to explain in detail how the Chinese technology group intends to ensure the security of its network products. What he explains is reminiscent of the process obsession of US technology companies. “It is true. We love processes, certifications and standards. We also learned from IBM,” says Klein. In fact, in the 1990s, Huawei sought advice from the then leading IT group, among others, and was inspired by its methods and best practices for its product development processes.

23.2 Traceability, Tests, Standards

Rules and processes are of little use if they are not enforced. Every employee at Huawei is regularly tested for security awareness. Those who fail must be detained. "I've never had to take exams as often in any company as I do at Huawei," says security specialist Klein.

Another important principle in all security systems is traceability. Which customer uses which version of the software in which devices? Which software components from open source libraries are used where and in which version? Huawei can say within an hour exactly which software version is being used by which customer. Hardware can be identified within one tag if it is affected by a gap.

A current case, which has occupied the IT industry worldwide, shows how important sophisticated vulnerability management that customers can reliably understand is. In December 2021 it became known that the software components Log4J contained a security gap. Log4J is used to record logins in certain software systems. Over the years, it has become a de facto standard in many places. After the vulnerability in the open source component became known, it was up to the manufacturers to inform their customers immediately and patch the software. Not all manufacturers were able to do this. In some cases, attackers managed to exploit the vulnerability.

Huawei is not only obsessed with processes and rules, but also with standards and recognized regulations. The group participates in the development of safety standards in international bodies such as the industry association 3GPP. The GSMA, together with 3GPP, has developed the security program NESAS (Network Equipment Security Assurance Scheme). People in Brussels are audibly proud that Huawei was the first telecoms supplier to have its first network products tested according to NESAS. The Chinese technology giant also attaches great importance to having its processes checked and evaluated externally. Huawei had the software of the central unit of a 5G network, the Unified Distributed Gateway, checked for quality by the independent German security company ERNW. The inspection took place – how could it be otherwise – in the windowless, well-secured offices in Brussels mentioned at the beginning. ERNW checked the quality of the source code, the handling of open source components and compliance with security rules in the programming process.

23.3 Additionally: Independent Safety Laboratories

Altruism: All rules, standards and processes are useless if they are not followed. For example, because a development department is under time or cost pressures, or if anyone in Huawei's massive workforce wants to take the path of least resistance. That is why there is an additional level within the organisation of the tech company: the independent cyber security laboratories (ICSL). These have their own budget, are organisationally located outside of the development departments and therefore have different bosses. Even the goals that are given to the employees of the ICSL are different. Because they should find as many gaps and errors as possible and communicate them consistently. The independent labs have the right to stop the development of a product or a new software version and send a product back to Huawei's software

factories. Around 200 security specialists tap Huawei's software for gaps.

It is one thing to ensure the security of network components, such as those built by Huawei for 5G networks, among other things. Demonstrating to customers and the public that devices and software are secure is another thing. For each product, one can prove which methods and systems it was tested with, says Wang. He doesn't just say it, he lets me take a look at a huge "workbench". Information on Huawei products and their individual components and their sub-components is collected in the database. When were they tested, by whom, using what methods, and what comments did the testers and their supervisors make? Has further development been approved or stopped? Wang clicks through the database and ends up at a product whose further development has been stopped. Apparently it's a smartphone. "The customer must be able to deactivate the microphone himself," it says. According to the database, the man who passed the death sentence on the product or component is John Suffolk, who is responsible for security and transparency at Huawei group-wide.

23.4 Who is in Control of the Data?

But what about remote maintenance? Who should prevent Huawei from remotely accessing network infrastructures and tapping data? Klein emphasises that a distinction must be made between the infrastructure supplier and the network operator: “As suppliers of the hardware for 5G networks, we know nothing about data traffic. The operators of the networks have full control over what we do with the equipment." Huawei has no access to the networks of the network operators (e.g. Sunrise) if they do not consciously allow and monitor it. In addition, Huawei fully implements the European Data Protection Regulation (GDPR). Huawei maintains, repairs and disposes of network equipment in Europe and has a production facility in Hungary.

You can feel the urgency of security when speaking to the experts at Huawei's Brussels centre. “Cybersecurity is the top priority at Huawei. That has to be the case if we want to survive as a company,” says Klein more than once. He has never seen a company that invests so much in transparency.