Cybersecurity – a Challenge and an Opportunity for Germany

Security in a world that is more and more interconnected is a challenging topic, both for people privately and for the society. Germany, with one of the strongest and high-tech economies in Europe, is often a target for hackers and industrial espionage. Hacking attacks pose a real threat to power grids, industrial facilities, computers and smartphones. In Germany, there is a great awareness of the issue of data protection because of Germany's historical background. There is a prevailing scepticism towards governmental surveillance. How is Germany facing those challenges?

In 2011, the German Ministry of Internal Affairs initiated the Cyber Security Strategy. This strategy includes the national Cyber Defense Center and the national Cyber Security Council. This Council advises companies as well as the government on how to improve their IT security. Simultaneously, the strategy covers critical infrastructure, which will be explained later on. There is also an IT-Planning Council which aims at giving political guidance for a voluntary cooperation between federal and state authorities in this field.

Cyber-Attacks

German companies are frequently targeted out of either political or commercial intent. For one thing, know-how is often stolen. It can be difficult to distinguish between espionage and reverse engineering. Reverse Engineering is a practice for analyzing a (commercial) product in order to uncover its unknown features. Sometimes it is not clear whether construction data was stolen or the product was copied via Reverse Engineering. It takes on average 243 days to discover Advanced Persistent Threats. APT is the name for a continuous hacking process. Those occur often, especially targeting companies in order to steal their knowledge. This is difficult for companies as they don't know immediately whether their system has been hacked. Yet it poses a major problem to companies because it is unclear how to protect their expertise. It is estimated by the Federal Criminal Police Office that cyber espionage costs the German industry 42.5 million EUR every year.

The Federal Office for Information Security plays a central role in organising security strategies. In cooperation with the BITKOM it supports e.g. also the Alliance of Cybersecurity. BITKOM is the association of the ICT industry. Also, companies and organisations from the critical infrastructures sector have to report attacks to the office for Information Security.

But not only companies are targeted by hackers. An estimated 40 per cent of computers in Germany are affected by malicious software. The government and associations are trying to inform citizens on how they can protect their computers from being hacked by giving advice on internet pages such as https://www.buerger-cert.de/ and https://www.botfrei.de/.

The other important federal institution concerning security is the Federal Ministry of Research and Education (BMBF). The BMBF initiated several research programs. Firstly, "Autonomously and safely in the digital world", with 190 million EUR. Running from 2015 until 2020, it focuses upon new Hightech-Technologies for IT security, data protection and secure ICT-systems. This program is also part of the

Hightech-Strategy for Germany from the federal government. Furthermore, the BMBF initiated three competence centers for cybersecurity, with an amount of 17.2 million EUR.

Securing the world of interconnected Devices

More and more sensors are used in products and devices. This makes the production more connected and flexible and thus individualised because companies have the possibility of reacting immediately. On the other hand, the "Internet of Things" represents a possible danger because they make a company or a private user vulnerable to cyber-attacks.

Data security and know-how protection is partly addressed in transnational panels.

- Fit4sec is a center for security and technology which is supported by the Federal Ministry of Education and Research is a part of the "German Applicants fit for Europe" program. It aims at pooling expertise in the German security sector to successfully form German-European research alliances together with end users and academic partners. The core team of fit4sec is composed of the IABG in Ottobrunn and Berlin, the Brandenburg Institute for Society and Security in Potsdam, Fraunhofer FOKUS in Berlin and the University of the Federal Armed Forces in Munich. http://www.fit4sec.de/

Securing Clouds is important because more companies are using clouds to store their data online. By using external data centers you draw less from the company's own resources. Another advantage is that companies have world-wide access to their data. Since clouds are getting more and more essential for companies, there is also research done in that field. Three examples are:

- The Fraunhofer Institute for Secure IT, the SIT in Darmstadt, is developing *OmniCloud*. OmniCloud encrypts Data before they are being uploaded to a Cloud. http://www.omnicloud.sit.fraunhofer.de/index_de.php

- Also, the SIT developed *Hash Guard*, a product providing protection from Advanced Persistent Threats. https://www.sit.fraunhofer.de/de/hashguard/

- One of the local clusters in Nord Rhine-Westphalia is the ICT Cluster NRW. It funds amongst others the CPS.HUB NRW with 2 Mio. EUR from 2012 until 2015. This Hub is doing research on security challenges in the connected world.

The Federal State Bavaria is also important to mention, since it is one of the strongest industrial areas in Europe. In addition, experts say that the conservative Bavarian State Government is investing traditionally more money in security.

There are many security clusters with different focuses located in Bavaria.

- Bavarian IT-Security cluster: http://www.it-sicherheit-bayern.de/
- The Bavarian cluster for ICT: http://www.bicc-net.de/
- Bavarian IT-Logistics Cluster: http://www.it-logistik-bayern.de/it-logistik/
- The Bavarian association for Security in the industry: http://www.bvsw.de/

Moreover, other trade associations such as the chambers of commerce (IHKs) and the association of Bavarian industry (http://www.vbw-bayern.de/vbw/Home/) are also working on IT-Security-related topics.

Critical Infrastructures

Critical infrastructures, such as power grids and telecommunications, are becoming increasingly complex. They are interdependent and their reliable operation is essential for many aspects of our lives. Because of ICT they are getting smarter and more flexible, but also more complex and vulnerable.

One of the key instruments of the federal German government regarding critical infrastructures is the implementation plan Critical Infrastructures, launched by the federal office for information security and is a part of the Cyber Security Strategy. It brings together companies from the critical infrastructure sector with governmental institutions. The public-private cooperation is aiming at promoting information exchange, protecting vital processes of the ICT-components and setting up a crisis management.

Most of the technology programs are supported by the Federal Office for Information Security, or the Federal Ministry of Research and Education. The program “Research for civil security’’ is being government-sponsored with 400 million EUR; 100 million EUR are added by the industry. Two examples are:

- CamInSens, promoted by the Ministry of Research and Education within their program ‘’Research for civil security”, is measuring data of movement by the use of cameras in order to detect potentially dangerous situations immediately and not only after they happened. http://www.caminsens.org/
- The Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS in Sankt Augustin in NRW is developing several tools which can be introduced for securing critical infrastructures: The physical infrastructure, such as the airport and stations for instance, as well as the “Cyber-infrastructure”.

Drones

Privately used drones are strictly limited by law in Germany. They have to stay in sight of the person controlling the drone; they aren't allowed to fly near airports, preserved areas, a crowd of people, power plants and many more. However, the government is thinking of how to deal with illegally used drones. With the new satellite system Galileo it is possible to detect even drones that weigh less than two kilograms. The Galileo Satellites are using PRS, the European pendant to the military GPS, and is therefore better protected against cyber-attacks. In Germany, the general public mainly disapproves of drones.

Research in this field, also on civil and not only military used drones is essentially done by the University of Federal Armed Forces in Munich. Their focus lays on human-machine-system integration and autonomous drones. Research is done on the ideal division of labour between the drone and the person in control: Drones aren't developed to fly entirely autonomously, only to a certain degree. The person controlling the drone mustn't be unchallenged whereas this can lead to boredom and thereby to negligence. The extent of technical support should be guided by not only the technical possibilities, but primarily by the human need for technical assistance.

Smart Grids

Climate change, the rapid surge in energy demand and scarce natural resources present Germany with challenges in the field of energy supply. The answer to the problem is the implementation of smart grids. The term smart grids describes power grids. Smart grids distribute energy intelligently and independently. A computer program checks where how much energy is produced and consumed.

Because of the energy transition (*Energiewende*) smart grids are a very important matter for Germany. Many people produce energy on their own, with solar panels for example. Those are called prosumers. In 2013, 25.5 percent of the gross electricity consumption comes from producers of renewable energy. The delocalisation makes the distribution of energy in Germany more complicated. Transporting the energy produced with windmills from the north of Germany to the industrial centers in the south is a difficult task. Protecting smart grids is also one of the challenges. A study in the U.S. finds that power grids are attacked every four days, online or in person.

- The IAEW, a RWTH Aachen institute focusing on electrical systems, is doing for instance research on modern smart grids in Germany, supported by the Ministry of Research and Education. The objectives of the study are to quantify the required network expansion in German distribution networks as a result of the renewable energy systems and evaluating smart grid technologies. http://www.iaew.rwth-aachen.de/

- Germany, Austria and Switzerland formed together DACH security. The transnational research cooperation focuses on ICT-based energy systems. That includes the development and testing of implementation strategies for smart grids. This cooperation is supported among others by the Federal Ministry for Economic Affairs and Energy in their supporting program of E-Energy. http://www.syssec.at/dachsecurity2014/

Secure Cities

Regarding the fact that securing cities is a great challenge for our society, it is worthwhile to take a look at these two examples:

- The Fraunhofer cluster ''Future Urban Security'' develops products protecting city residents from growing threats such as terrorism, climate change and crime. Fraunhofer EMI, the Ernst-Mach-Institut in Freiburg, is also participating. The EMI dedicates one entire department to research on critical infrastructures and secure cities. It is for example commissioned to carry projects by the German Federal Office of Civil Protection and Disaster Assistance. http://www.future-security.org/

- VITRUV is a tool by the Fraunhofer EMI for risk analysis in urban areas. The software integrates security measures directly into the urban planning process. http://www.vitruv-tool.eu/

Predictive Policing

There is a software testing project called Precobs (Pre Crime Observation System) in Bavaria, led by the superintendent of Bavaria. The software is developed to support and direct police operations. Based on past data of housebreaking, it predicts which areas are vulnerable for burglaries in the future. More police officers can be sent to those critical areas. The method itself is called Near Repeat Prognostic and is used in the U.S. and the U.K.

The project runs from October 2014 until March 2015 in Bavaria, more specifically in Munich and in Middle Franconia. Those two areas were chosen for their representativeness: Munich as a urban region and Middle Franconia as a rural region. If the project is successful, it will be rolled out in those areas. The results of the project will be presented to the Bavarian Ministry of Internal Affairs soon. The figures are said to be similar to the ones in Zürich: in Zürich the number of burglaries dropped by 30 per cent.

Baden-Wuerttemberg will soon use the software Precobs as well. Nord Rhine-Westphalia is also busy with starting a Predictive Policing project. However, they are approaching it with different software. The other federal states are attentively observing the pilot project in Bavaria before they implement it.

Meer informatie:

Julia Klein

BLN-TWA@minbuza.nl