

## 2012 Cyber Security Summit

On September 12, 2012, the first Cyber Security Summit (CSS) took place in Bonn. Its initiators, the Munich Security Conference and Deutsche Telekom, intended that the event would provide new stimuli for Germany as a secure cyber-location. The summit brought together 75 leading personalities from the fields of industry and politics to initiate discussions of the threat level and structures of cross-functional and cross-sector collaboration. The discussions of the various working parties have been summarized in a series of articles.

### Report on the Finance workshop

#### **“Umbrella organization as point of contact”**

*In the financial sector, the age of classic hacker attacks by individuals is past. IT attacks now threaten from various directions. Although there are a number of established standard technologies for IT security, there will still be a need for further action in the future, because cyber-attacks are constantly changing in quality and quantity.*

The big difference between the financial sector and other sectors is that in this area, a successful hack brings a cash reward. This makes the financial sector a particularly attractive target for attacks, as participants in the working group for Finance declared. A small selection of incidents from the very recent past: The attack by a group of hackers calling themselves GhostShell, which published about a million user data and passwords from banks and consultancy companies<sup>1</sup>. The data theft by an employee of the Swiss private bank, Julius Bär<sup>2</sup>. Or the state-initiated attack on bank customers in Lebanon<sup>3</sup>.

#### **Cyber-attacks in different dimensions**

These examples show the directions from which cyber-attacks currently threaten the financial sector in particular – and how these have developed. The hacker attack by GhostShell was a classic cyber-crime – although there is a striking increase in the professionalism of the attacks.

<sup>1</sup> <http://www.zdnet.de/88120879/hacker-stehlen-daten-von-einer-million-nutzern/>

<sup>2</sup> <http://www.spiegel.de/wirtschaft/soziales/julius-baer-schweizer-bankangestellter-wegen-datenklau-festgenommen-a-852189.html>

<sup>3</sup> <http://www.computerwoche.de/index.cfm?pid=332&pk=2519955>

It is no longer individual actors, but well-organized, large groups of hackers which attack banks or insurance systems together – and thus at the same time more vehemently.

Attacks coming from within the company itself are also difficult to prevent. In order to defend itself against internal data theft and insider trading, such as took place for example at the Swiss bank Julius Bär, stricter control mechanisms, that is, more “eyes and ears” within the system are necessary, as several participants in the discussion stressed.

A completely new dimension to the attacks on IT security is shown by the case in the Middle East, where apparently a government commissioned malware programs that were supposed to spy on bank transfers. When states initiate cyber attacks, completely new motives and objectives are involved: redistributing wealth, geo-political expansion or weakening the economy of a state. Classic cyber-crime then develops into international cyber-war.

### **Consistent cyber-defense strategy desired**

Faced with threats which will grow in both quantity and quality, the financial sector sees the necessity for closer collaboration and better exchange of information, both within the industry and going outside the sector and beyond regional boundaries. Instead of diversifying cyber-defense strategy into many small individual initiatives, an umbrella organization is desired which will act as a central point of contact to collect and exchange information and lead all the initiatives in the sense of “guidance.” In the long term, reliable international cooperation is also to be established.

Nevertheless, the participants believe that the financial sector is already well equipped to cope with cyber-attacks today, especially in a direct comparison with other sectors. A number of instruments and technologies exist for the security of the IT infrastructure, and innovations and system updates take place regularly. This is on the one hand because the sector, if only on account of the strict data protection provisions and the sensitive nature of its business, traditionally relies on highly secure structures and is constantly adjusting and improving them. In addition, services such as online banking or mobile payment have been on the market for a considerable time. In recent years the sector has been able to establish many functioning and reliable basic features within IT security.

It is now important to develop further innovative features for these standard technologies in Germany, which will enhance security. This also includes driving forward and supporting more research programs on the subject.

**Focus on the end customer**

Finally, the focus is also on consumer-centric developments. Customers can now use all the core processes, such as online banking or mobile payment on their mobile devices as well.

This means that the sector is also responsible for end-to-end security. For even the best in-house IT security systems cannot offer full protection against attacks if the customer's (mobile) device is not secure against viruses or Trojans. At the moment, the financial sector regards it as a challenge to create the right technologies to ensure comprehensive, end-to-end security.