Cyber Security Summit 2013 – Working party 2

New threat scenarios for the economy

The threats from cyberspace are not only increasing, they are becoming ever more targeted and more specific. Every day around 200,000 new variants of viruses, Trojans and worms appear. Up to 800,000 attacks on the early warning systems of Deutsche Telekom take place every day. In addition to espionage and sabotage activities, it is mainly organized economic crime that is playing a large and growing role in this context. Overall, people's trust in the digital world is being hugely affected. We must regain this trust. For this purpose, a valid, real-time picture of the Internet attacks is required.

Major companies were normally well aware of the danger of cyber attacks, the working party agreed. With small and medium-sized enterprises things looked very different. The greatest worry for all companies is economic espionage.

Against this background, more and more companies were very suspicious of suppliers of technical components from all over the world. There was a fear that some manufacturers could leave backdoors in programs or hardware components which allowed access to the relevant systems without the user companies being able to discover these backdoors. Nevertheless, most German companies were dependent on products coming from outside Europe, since up to now the home market only had a few alternatives to offer.

Supporting innovations

In the view of some participants in the discussion, one possible way to counter backdoors would be for their manufacturers to be fined. For example, companies whose products had demonstrably contained these backdoors could be required to pay heavy fines amounting to between two and five percent of the revenue.

In the first instance, an even more intensive and open exchange of information between companies and the authorities could contribute to identifying black sheep among manufacturers more quickly, and thus to reducing security risks.

However, even better than the identification of malicious products and possibilities of forbidden access would be a switch to trustworthy products "made in Germany." But up to now, Germany was an also-ran in this environment. The U.S. and Asia were so far ahead in terms of innovation that it would be very hard to catch up. Nevertheless, the members of the workshop agreed that there was potential for achieving this. The aim should therefore be to

drive innovations forward and to support small and medium-sized enterprises with their ideas as well. Because the market for IT security was still growing, and there was a big demand internationally for products based on German security standards; so this could open up interesting competitive opportunities. The accompanying investment requirements could only be borne jointly by companies and the state.

An "IT safe" remained the stuff of dreams

Despite all the efforts of companies and the authorities: Anyone working in cyberspace had to be aware that there was no such thing as 100 percent security and there probably never would be. The "IT safe" in which companies would be able to keep their business secrets secure will even in the future remain the stuff of dreams. Every company was therefore required to take responsibility for its own data, carefully weigh up possible risks and then proceed, taking the risks fully into account. In individual cases, this could even mean cutting particular information or processes off from the Internet completely – if necessary, even if this made them less user-friendly. Parallel to this, staff awareness of the risks had to be increased.

Whilst major corporations were already largely sensitive to the dangers from cyberspace, the discussion group believed that some small and medium-sized enterprises were still in need of enlightenment. Here too, a greater exchange of information between the major players and the smaller companies was just as desirable as even stronger cooperation between companies and the state. The Alliance for Cyber Security in the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) was giving a good example. At the moment, more than 340 players in the cyber security field in Germany were members. The aim of the Alliance was to provide across-the-board current and valid information on the subject of IT security.

There was also agreement on a second issue. The subject of cyber security should be on the agendas of company boards and should not just be a task for the experts.