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 Trade and Logistics

"Danger for on-board computers and traffic routes"

The trade and logistics sector bears particular responsibility for protecting the lifeblood – streams of goods and traffic – against cyber attacks. Here the highly complex and connected control systems in the sector offer an abundance of attack targets.

Every day, tens of thousands in Germany travel by plane, rail and other public transport systems. Germany as an export nation exports goods every year with a value of more than one trillion euros. The most important transport route within Europe is by road. In addition, there is rail and ocean and air freight for intercontinental traffic. Highly complex control systems, which are increasingly interconnected, ensure smooth logistical processes and their manipulation can have a direct impact on people.

The working group for Trade & Logistics therefore first discussed the issue of whether it was possible to use stolen or forged employee data to access sensitive control instruments. Or can cyber-criminals find a weak point to penetrate the networks of an airport and interrupt both aviation and non-aviation processes? In December 2011, hackers demonstrated how dangerous access to the transport systems of providers could be. For two days they interrupted the signaling system of a rail route in the north-west of the USA. Fortunately no accidents took place, the hackers merely brought about some delays.

Some participants alluded to risks in aircraft construction. If bogus hardware and software components were installed in a particular aircraft type, for example, it would be possible to control all aircraft of a specific series remotely. Even satellite navigation data can be manipulated. Here the great danger emanates from internal offenders who can cause very great damage to their company from within.

Take your own precautions and exchange information

According to the participants, companies tackle this threatening scenario in very different ways. Whereas a high degree of security is prescribed for airlines because of the terrorist threat, hardly any cyber-security provisions exist for travel by ship as the most significant means of transport for German exports overseas.

Effective precautions are vital. Gaps in security must be recognized early and then closed. But which technology and processes do we need for this purpose? For example, companies should allocate responsibilities for security mechanisms as part of their risk management. But companies, sectors and institutions today approach the issue of cyber-security in very different ways – each one setting up its own cyber-center. The experts compared the problem of cyber-security with an elephant, which could only be drawn correctly if all the actors worked together and combined their analyses, experiences and insights.

Clear recommendations for action to the German Federal Ministry of the Interior (BMI)

This will succeed by using institutionalized methods of exchange at multiple levels: Public authorities still do not communicate enough with other public bodies. Private companies often do not exchange information intensively enough either. For example, it is not ideal that individual sectors speak independently of one another with the Federal Ministry of the Interior. The Ministry needs clear statements from the trade and logistics sector about where the government should introduce tougher regulation. At the moment, regulations are too strict in some areas and too lax in others. The slow processes in the public sector and differing provisions within the EU also make things difficult.

In the opinion of the working group, it is essential to intensify continuous communication between the public and private sectors of the economy. The BMI's cyber-defense center needs the private sector, which is keen to get involved.

This exchange must be characterized by transparency and openness, in order to create a better infrastructure for rapid reactions. At the moment, around 90 percent of cyber-attacks are not made public. In the future, attacks must be analyzed every day and information must flow in both directions. Insights from the prosecutor's office should be made available to private industry.