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 Energy workshop

"Digital GSG9 Special Forces for the protection of critical infrastructure"

By launching cyber attacks on the energy suppliers' critical infrastructure, hackers can manipulate power stations, blackmail the operators and take entire regions off the grid.

In the U.S., unknown perpetrators attacked the operators of natural gas pipelines with sophisticated phishing attacks for several months at the end of 2011. If employees had clicked on one of the malicious links, malware would have automatically installed itself on the systems. As a consequence, hackers would have gained access to secret documents or would have been able to manipulate gas compressors control systems. Between 2000 and 2011, an Israel-based energy supplier registered a 17-fold rise in attempts to penetrate its IT systems. By now, cyber criminals start attacks on the supplier up to 20,000 times a day.

Critical infrastructure increasingly networked

Such cyber attacks are now experienced by companies in any industry. However, participants in the CSS working group for Energy stress that in the energy sector, successful attacks from cyberspace have an impact far beyond the companies themselves, because the economy and society are dependent on a functioning energy supply process. For now, critical infrastructure in the energy sector is still hardly networked, which means that cyber attacks would only hit individual power stations. In an energy industry that will be highly networked via smart grids in the future, however, the risk of successful attacks on energy providers having a direct impact on entire cities, regions or states will be growing.

For example, the early smart meters offered on the market could have been used to switch off the power supply for an entire house via the grid. With a seamless

smart meter infrastructure, a blackout could, in effect, hit entire districts – and result in the well known consequences.

Risk of sabotage is higher than risk of espionage

According to the participants in the discussion, this is why risk minimization plays a very important role in the energy sector. However, in contrast to the production industry, for utility companies, cyber espionage plays a less significant role than sabotage intended for blackmail. An additional potential risk is posed by activists who attack power stations specifically to assert their interests. In 1994, for example, saboteurs threatened the operator of a nuclear power station in Lithuania that they would blow it up. This blackmail attempt shows how dangerous cyber attacks in the energy industry can be. It doesn't bear thinking about what disasters successful cyber criminals could trigger if they were to hack into the control systems of a power station. However, as with most companies, external criminals are not the biggest problem for IT security. Risks are frequently lurking within the companies themselves, for example if internal staff are too careless or have not been informed about the risks involved in handling IT infrastructure and how to protect themselves.

Internal risks and risks from third-party companies

Third-party companies are also a source of danger which needs to be taken seriously. While many companies also take into account security aspects in the selection and control of in-house staff, subcontractors or third-party companies frequently have open access to buildings. In addition, controls are frequently much more lax than within the company. Such externals could knowingly or unknowingly infiltrate their customers' systems with viruses, worms and Trojans. Or they pick up documents from desks which can be used by criminals to obtain access to the IT systems more easily. Even telephone and e-mail lists could be used for this. An easier way for better control would be if external companies had to submit a police certificate of good conduct for their employees. A brief summary of the fundamentals of risks which could be used to eliminate most of the sources of danger would also be helpful.

Standardization and pooling of forces

In the energy industry, too, costs are a key problem for increasing IT security in companies. Security costs money, and costs for IT security are continually on the rise Cross-company, standardized security procedures could be used to close security gaps more cost-effectively.

The participants in the Energy workshop expect support from the world of politics in this area. Political action should be more harmonized, ensure more standardization and result in specific action recommendations. This would make it necessary, in their view, to pool the variety of responsibilities and organizations in

the form of a central institution and a kind of digital GSG9 Special Forces.

However, companies do accept responsibility themselves as well. According to the workshop participants, management must act as a role model and demonstrate awareness of cyber security: “The topic belongs at C-level.” Companies should also strengthen collaboration with each other and with governments. Otherwise the state would be faced with the problem of being responsible for security at the national level but having no direct access to other countries. This would make it impossible to ensure whether security issues are sufficiently looked after in all energy grids. What is needed is a relationship between companies and governments based on trust.