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 Production Workshop

"Attack on production lines"

IT-supported economic sabotage is evolving into a growth market. Tailor-made cyber weapons generate completely new options for interfering with the control of production lines and, consequently, of manipulating the value creation of industrial enterprises. The number of known cases is still small. But one thing is for certain: a lot is at stake. While the users worry about their company's value and the trust of their business partners, technology providers do not want to be suspected of needing to catch up on security management issues.

Participants in the working group agreed that a crucial topic was the availability of the systems. To ensure this, it is necessary to find ways to adjust control systems much more quickly to the changing risks. The real crux is that the speed of innovation in the ICT environment is much higher than in machine control systems.

Warranty endangered

Since production lines go through lifecycles of several years, effective patch management is only possible to a very limited extent. Every security-relevant update therefore exposes companies to the risk of losing the warranty for their equipment. Collateral damage may be particularly high where a large number of stand-alone solutions are in place.

In relation to attacks from outside, the view of the working group for Production was that manufacturing industry had done its homework. 85 to 90 percent of attacks can be warded off successfully by using best practices. On the other hand, many companies are still nearer the beginning of the learning curve when it came to criminal acts from within.

Detecting security-related issues

There is a particular lack of systematic procedures with which anomalies can be recognized as soon as they occur. Frequently, it is left to chance whether security-related events are discovered. Since communications are encrypted in security-critical areas, the observation of unusual data transfers is often the only way to trace that there is anything wrong. In view of this inequality of weaponry, those in responsible positions are demanding additional methods to recognize problems at an early stage.

Industrial companies face even greater headaches because of the increasingly common use made by employees of their own ICT devices on company premises. The same applies to the use of company equipment outside the company. This opens the door for introducing malware via employee equipment.

As the discussion revealed, problems were much more serious among foreign subsidiaries than on the home market. For example, many Asian employees can be seen to maintain social networks dating from their time at university. As soon as companies impose effective central BYOD guidelines, the employees affected leave to join competitors who do not regulate access as strictly. From the perspective of headquarters in Germany, this is an intercultural problem that has not yet been solved.

Managing the security of suppliers

Industrial companies look on their suppliers as an internal part of their value creation. It is therefore far more important than before to develop processes allowing producers to ensure that the upstream products supplied are hardened in security terms. Since small and medium-sized enterprises (SMEs) do not have sufficient resources for effective cyber-security, a greater degree of knowledge transfer is essential.

The participants in the Cyber Security Summit confirmed that they exchange security-relevant information, largely via personal networks.

In order to involve small and medium-sized companies more, they consider it urgently necessary to set up an overarching platform for the systematic exchange of knowledge. Only then will information be able to be fed into the supply chain quickly enough to enable SMEs to build up effective protection against cyber-attackers.