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 Health workshop

"People's lives are at stake"

The healthcare sector is facing a radical change. More and more health data is being digitized. Whilst this is improving processes within the industry, it is also making them more susceptible to cyber attacks and IT downtimes.

The two Tel Aviv hospitals, Assuta and Scheba, are far ahead of their time - unfortunately. In January 2012, the two hospitals were attacked by Cyber warriors with an Islamist background. Hackers sent large numbers of requests to the hospitals' computers until they failed under the increased load.

Overall, however, cyber-attacks still play a minor role in the healthcare sector. According to U.S. statistics, 489 data protection violations were registered in hospitals in the U.S. over the past three years. Only very few of these – around six percent – were cyber-attacks. Most offenses could be traced back to lost files and equipment, the unauthorized forwarding of data or employee negligence.

The CSS working group for Health believes that employee training is what is most needed right now. It claims that although awareness of data protection and data security has increased overall, employees still require intensive training on this topic, particularly because doctors and nursing staff often have a low awareness of risks.

Digital processes are changing the healthcare sector

IT is both a curse and a blessing in the healthcare industry. On the one hand, the increasing use of technology is improving the way in which hospitals can network with each other, exchange data, develop new approaches and reduce costs through better processes. On the other hand, this is associated with a growing dependency on technology.

A large amount of data (such as x-rays) is no longer available in paper form, only in a digital format. Even data such as a patient's temperature curve, which is traditionally written down and maintained on paper, is increasingly being digitized. In the event of a power failure, doctors can no longer access this data. In the case of a patient's temperature curve, this is a particularly serious matter as this data record is used, for example, to determine the patient's medication. A member of the working group summed up the problem: If the servers at a company in a different industry go down, the loss amounts to several million euros, depending on the duration. If servers and IT in hospitals go down, people's lives are at stake.

Obsolete medical technology

This means that hospitals bear a high level of responsibility when it comes to IT security. Many hospitals are aware of this and are installing their own infrastructure such as combined heat and power plants or emergency generators. Despite the hospitals' efforts, however, the workshop participants believe that the performance of emergency drills and the development of emergency plans are being neglected.

Some hospitals have now set up two physically separate networks (for internal and external communication) as an additional security measure, but this solution does not appear to be future-proof in light of the increasing digitization in the healthcare sector. Another preventive strategy is the use of protection software such as virus scanners. However, many medical devices are obsolete in terms of security and therefore do not offer sufficient protection. Upgrading security standards can often be done at great expense only, if at all.

Conflicting interests

So, how can the healthcare sector become better organized in order to jointly tackle such risks? At this point, the discussion quickly focused on the conflicting interests of different stakeholders.

Health insurance providers, different medical associations and political representatives often do not agree on any level and therefore block many developments. The healthcare sector has suffered as a result of this lack of agreement for many years.

An example of this is the introduction of the health card in Germany, which is still not being used to the extent originally intended, despite many years of preparation.

Some participants expect that the topic could gain in significance with the arrival of younger doctors in hospitals. Younger doctors, in particular, are much more aware of and open to the topics of process optimization, data protection and data security.

The working group for Health also sees the lack of resources as a critical issue. Due to high cost pressure, the healthcare sector is unable to achieve sufficient revenue to invest in cyber security. The problem will become even more critical in the future because the public sector is increasingly withdrawing its funding of the healthcare sector.

Large number of measures required in order to succeed
According to the participants, the diversity in the healthcare sector means that there will be no *single* measure to remedy the situation, but that a large number of activities are required. However, such a bundle of measures will not be coordinated from one central point, but from multiple areas, i.e., politics, the industry and employees.

The participants do not believe that minimum standards are the solution and also have a skeptical attitude toward a national coordinator. Instead, they argue that the industry participants should voluntarily undertake to comply with standards. They claim that whilst better technology (such as single sign-on) offers more security, progress can be achieved by involving and raising the awareness of employees in a more effective manner. However, the fear remains that “something major will have to happen before anything changes,” i.e., for a serious incident to shake the industry into action.