Cyber Security Summit 2013 – Working party 1

Rebuilding trust in the digital society

The revelations by the American whistle-blower, Edward Snowden, have led to an extreme loss of trust in the digital world. The highest priority must now be to win back this trust. In order to do this, all players in the digital world must focus more strongly on social values.

"No security without trust and no trust without security." This is how Prof. Stock, Vice President of the Federal Criminal Police [Bundeskriminalamt], summed up the formidable mandate for the digital society in his keynote speech. A life with interpersonal relations is not conceivable without a certain level of trust. Trust helps us to work with systems that we neither entirely control nor fully comprehend. Trust thus enables us take actions in risky situations, whether these involve road traffic or the Internet.

Trust logically requires the existence of risks. It is still the case that society clearly underestimates the threats posed by cyber criminality. The approximately 20 high-ranking participants in the discussion in the "Trust in the digital society" working party agreed on this point. All the institutions from politics and industry and the companies themselves had to therefore do their utmost to sensitize companies even more strongly than before to the risks posed by criminal cyber attackers. Effective protection – like trust – requires knowledge of risks and possible protective measures.

Here, the media reports on the subject of the U.S. NSA secret service agency (National Security Agency) and the British counterpart GCHQ (the Government Communications Headquarters) might even have provided a genuine stimulus to

make people more sensitive: By now everyone had to be aware of where the dangers lay in cyberspace.

Sensitization concepts that are viable in the long term also require clarification in the vocational and professional environment. We also need an awareness of the fact that data in the digital society is increasingly being retained for life. Here we must develop reliable consumer protection rules that are in line with the times, such as putting into practice a "digital right to forget."

Greater transparency and cooperation

As early as the morning plenary session of the second Cyber Security Summit, the desire for greater transparency regarding cyber attacks was expressed. Companies should notify a central body of attacks on their IT systems, networks and databases far more frequently than has been done up to now. The more and more professional attacks are no individual phenomenon. In the long run, they can only be prevented by people working together. For this purpose, the companies and public authorities affected should bundle and draw together their know-how. However, the working party agreed that we are some distance away from this type of open cooperation. Companies that have been damaged by cyber attacks and fear a considerable loss of image and customers still dominate this field. We still need to develop a true culture of trust here.

Most members of the working party therefore welcomed the idea of a duty to notify of cyber attacks. This would lead to a transparent picture of the situation and thus form the basis for effective and sustainable defensive measures against cyber attacks. As a result, products to protect against attacks could be developed and distributed more quickly.

Some participants in the discussion went beyond demands for transparency and urged new international alliances and collaborations, since the individuals affected

were still too wedded to a silo mentality. At the same time, there were already a number of parallel initiatives for increased cyber security, but these were not properly coordinated with one another. Thus a great deal of time was lost in duplicating work, time that could be used in a more targeted way.

No consensus was reached on the question as to whether the state should try harder, through additional regulation, to create more security and transparency. Whilst one side regarded regulation as unavoidable, the other feared too serious an intervention in events on the market. Is it even possible to get the large number of different and sovereign states to come to an agreement on a standardized global regulatory framework? A discussion that is not confined to the topic of cyber security.

No compromises in data protection

The parties to the discussion were skeptical on the issue of joint, international data protection, applying across borders and specifying uniform norms in order to ensure people's trust in products and services in the network in the future too. They claimed that one global single view of ethics and a uniform value system as regards data protection and data security remained a distant goal. Therefore defining and implementing global rules would be all but impossible.

Voluntary agreements would prove futile if nobody kept to the results of these. That makes it very difficult to build up trust. However, the aim must be to reach the maximum possible consensus. The classic negotiation strategy of finding the lowest possible common denominator did not go far enough: there can be no compromises when it comes to data protection. There was no mutual consensus that trust is the central category for the future and acceptance of the digital world. It is for this reason that high data protection is not available for European citizens.

The re-negotiation of the Safe Harbor Agreement is indispensable since the requirements it makes in terms of data protection and the possibilities for

enforcement in the U.S. obviously do not comply with European law. One participant described how different the understanding of data protection is in Europe and in the U.S. In a conversation with a high-ranking politician in the U.S. the latter had made his own standpoint crystal clear: Edward Snowden had betrayed secrets, and therefore deserved to be found guilty of treason. He had little understanding about the excitement over PRISM in Europe because the U.S. president had a clear responsibility: protecting the U.S. took priority over protecting any single individual.

Making better use of technical opportunities

In addition to the absence of uniform norms and standards, the lack of user awareness as regards cyber risks and possible protective measures was also addressed. The outcome was that existing technologies were not being used enough, particularly by small and medium-sized enterprises. For example, those who consistently employed encryption procedures were able to protect their data far better against cyber attacks.

All measures to increase the level of security without restricting the achievements of a free and global Internet were important. Statutory regulations for routing to Schengen and the national storage of call data were able to make a valuable contribution here. Certifications were also able to offer crucial orientation for users and were being promoted.

To summarize the discussion: the age of naive Internet use is past. Everyone – whether from the political, industrial or academic worlds – is required to point out the dangers of the digital society to a greater extent, but without demonizing it. However, we urgently need greater discussion on values and ethics in a digital world. That is the only way to regain trust in an increasingly networked world.