CyberSecurity
Summit

First 2012 Cyber Security Summit in Bonn

Summary

The first Cyber Security Summit, held in 2012, sets the course for Germany as an innovative and safe place to do business. Modern information and communication infrastructures are increasingly developing into a location-related advantage in international competition. At the same time, state-of-the-art technology has now penetrated every aspect of our lives. With this development, the network becomes critical infrastructure and a target for attacks. The common goal of industry and the state must therefore be to provide the best possible protection. Nowadays, security in cyberspace cannot be achieved if it is treated as the task of a few IT specialists or as a technical challenge for individual companies. Security instead requires concerted action by industry, politics and society at all levels.

The latest top-level meeting initiated jointly by the Munich Security Conference and Deutsche Telekom has for the first time brought together leading personalities in order to initiate the discussion regarding threat situations and structures of a cross-area and cross-sectoral cooperation. The Cyber Security Summit thereby creates valuable synergy effects between industry and security policy. No state, company or citizen can provide effective protection on his own. We will only win the battle against criminality, industrial espionage and sabotage from the Internet with comprehensive cooperation. Here, eight key points describe the relevant areas of action.

1. Virtually all areas of political, industrial and social life now depend on functioning IT and Internet structures. Business processes between companies almost exclusively use the Internet as the central infrastructure. For German industry, cyber security is therefore a long-term success factor – not only for information technology and telecommunications companies but across all sectors. The Cyber Security Summit has shown a significant need for discussion and action. Cyber security should be on the agenda of every company and their management – and this is where it has arrived today. **"Industry wants to see continuous exchange at the highest executive levels** and establish regular high-level meetings, simulation exercises and workshops in Germany.

2. We see cyber security as a global task which requires international solutions as well as national measures. The international exchange which is already taking place between individual national *Computer Emergency Response Teams* (CERT) at a technically pragmatic level must also be extended to the international political and industrial levels. The **creation of legal and institutional instruments for an international dialog** on behavioral norms and confidence-building measures must therefore be vigorously pursued in order to broaden the international cooperation for cyber security.

3. As part of this, Germany needs a cyber security alliance with participation from all sectors. Previous activities must be more closely integrated and the actors from industry, politics and society must be better networked across sectors. An urgent task for such an alliance—ideally under the guidance of the Federal Government and as a joint initiative of industry associations – is **to set up a platform in which all branches of industry and companies of all sizes can get involved**. Such a forum will allow findings, e.g., on attack scenarios, to be transferred openly and quickly between the

members.

4. We want to promote **open exchange on attack scenarios on a voluntary basis**. With this willingness, we create a climate in which measures for protecting against cyber attacks are developed and shared more quickly. The overall system will only be strengthened by handling attacks from cyberspace in a bolder, more transparent way which the companies want to implement. A corresponding initiative by industry must also be allowed to freely develop. We support the integration of industry in the national cyber security strategy of the federal government and the European Commission.

5. The number of actors and experts involved in cyber security is also insufficient. In particular, small and medium-sized enterprises require access to capacities and know-how as well as support in order to network with other companies. **A secure information society requires a growing community of contacts** in companies which, as a “cyber defense force”, is capable of safeguarding the information flow and introducing and carrying out measures in the event of a security incident. In the public sector, contacts must also be named who supplement information from industry with knowledge from government offices and intelligence services. In addition, suggestions must be developed on how to strengthen cyber security as a discipline for initial and ongoing training within companies as well as at universities.

6. We are committed to **maintaining technological sovereignty in Germany**. A secure overall system requires the security of fully developed hardware components and their supply chains. For example, unauthorized access to information and communication systems, e.g., via built-in “backdoor technologies,” must be prevented. The introduction of products which are not market ready due to the negligent tolerance of subsequent

defect rectification (updates, patches) must not be the order of the day.

7. It must be a priority for every company to be prepared to provide increased cyber security. With information and awareness-raising campaigns, German industry also contributes to a secure information society. Experts estimate that 90 percent of security problems can be resolved if companies, the public sector and the population keep their systems well maintained and up-to-date at all times. For this reason, we are committed to **raising awareness among employees of companies, institutions and organizations**. Further cyber security will be additionally achieved in companies through the introduction of standardized security guidelines and the creation of security architectures.

8. In order for people to be informed of and brought along on this highly important path for Germany, we also propose **suitable media measures for raising the public's awareness**. As for the state and industry, cyber security should also be of high importance for private individuals. Every computer user should take his own measures for cyber security in order to protect himself and his personal environment against digital attacks.

The popularity of the first Cyber Security Summit in Bonn in 2012 encourages us to consider also holding the high-level meeting in 2013. In addition, the action areas mentioned should be further specified in comprehensive working groups, workshops and beacon projects.

Bonn, September 12, 2012

www.cybersecuritysummit.de
www.twitter.com/CYSS2012