Cyber Security Summit 2014 – Documentation

Panel discussion:
ICT Companies and Industry: Expectations and Responsibilities

What kind of support does private industry need in order to be able to address the explosive growth in cyber threats? This question was at the center of the panel discussion on "ICT Companies and Industry: Expectations and Responsibilities." The participants in the discussion, which was moderated by Klaus Schweinsberg (Managing Director, Centrum für Strategie und Höhere Führung), included Siegfried Russwurm (Member of the Managing Board of Siemens AG), Ingrid-Helen Arnold (Chief Information Officer, SAP), Ciaran Martin (Director-General, Government & Industry Cyber Security, GCHQ) and Elmar Theveßen (Deputy Editor-in-Chief / Head of News, ZDF German Television).

Russwurm: Equipment suppliers need to watch the process level

For transnational companies, regional models such as "Shengen routing" are unsuited, explained Siegfried Russwurm, member of the managing board of Siemens, at the beginning of the discussion. Instead, governance solutions are needed that can function across all economic areas and cultural spheres. His own company is doubly challenged in this area, Russwurm explained: As a supplier of industrial equipment, Siemens not only has to protect its own processes, it also has to enable its customers to provide adequate security in their own companies. Russwurm explicitly cited the process level: "We need to make the entry hurdles high, and yet we will still live with the paranoia that intruders will always be able to scale our walls. We thus need to make it as difficult as possible for intruders to use those golden nuggets." A range of effective measures is available at the process level, he added. One good idea, for example, is to undo product data packages and store their various components in separate network infrastructures. That makes it very difficult for attackers to reconstruct the packages. For Siemens and its customers, the

resulting time savings are the decisive factor. In practice, the key is to keep attackers busy for so long that they can no longer derive economic benefits from the restructured data.

Arnold: Attackers' imaginations know no bounds

With more than 260,000 corporate customers in over 180 countries, SAP sees itself as sharing much responsibility for the functioning of the world's economy. In this context, SAP's Chief Information Officer, Ingrid-Helen Arnold, noted that a great many customer systems run in business-critical environments. For this reason, she added, IT security is an integral part of overall solutions. SAP aims for the very highest security standards in product development, she noted. "In general, we find that along with a strong quantitative increase, the quality of attacks has also been growing," Arnold noted, and added, "attackers' imaginations seem to know no bounds." In addition, she added, the number of points of attack has been increasing. The key reason for this, she explained, is that the supply and sales networks in which SAP customers operate keep becoming more and more complex. Furthermore, in keeping with growing amounts of worksharing, supporting IT networks are becoming more and more permeable. From the perspective of network defenders, she noted, it is thus more and more important to be able to work in real time. The aim must be to keep shortening the time between an attack's occurrence and the time at which the attack is successfully warded off. In light of such challenges, Arnold expressed support for the idea of a global framework for Internet security: "a global solution is the only solution that will move us forward."

Martin: Trustworthy cooperation with private industry

Along with industry and policy makers, intelligence services are also called on to help develop suitable protection. This was the opinion of Ciaran Martin, who heads up the area of Government & Industry Cyber Security at the British intelligence service GCHQ. "I know you are concerned that we are tapping your communications and stealing your data,", Martin conceded to the

participants of the Cyber Security Summit. "If such concerns are actually confirmed, the digital industry will collapse like a house of cards. We are working together with private industry to counter such concerns." The GCHQ has a direct role in supporting private industry and has been fully accepting this role, Martin added. The fact that industry cooperates better with intelligence services in the U.S. and the UK is a good thing, he emphasized. In addition, exchanges take place with a number of international companies that only have locations in Great Britain. All of this takes place via voluntary alliances, Martin declared. All in all, many private industry partners find it very important to speak with GCHQ about cyber security and pending measures. His service believes in open markets and free societies, he added. The government for which he works has clearly stated that security is vitally important for the functioning of economies. In this connection, Martin called for exchanges at the European level: "To protect our economic interests and the interests of our allies and partners, we need to work together within the EU."

Theveßen: Don't focus only on protective measures

From the perspective of Elmar Theveßen, Deputy Editor-in-Chief at ZDF German Television, policy makers tend to consider cyber security issues first and foremost in terms of national interests. They use transnational instruments in order to promote such interests, he added. Among other things, this makes it possible for globally operating companies to become "victims and vehicles" for attacks at any time. This results in a loss of trust and enormous economic damages, he added. "In both parts of the world, people believe we are already in a cyber war and that economic warfare is permissible and necessary in order to move national prosperity forward," Theveßen added. For this reason, an open public discussion and, ultimately, clear rules, are needed. This also applies to the same extent for companies, he noted. In this area, Theveßen called for international conventions that would clearly define what user data companies may access, and for what purposes. To restore trust in state institutions and in the network industry, a digital narrative is needed, he stated, that is based on the principle that

national laws, international law and human rights apply to everything that takes place in cyber space. "We have not yet cracked this nut. And we need to crack it soon, instead of just thinking about protective measures," Theveßen concluded.