Region NRW

The Growing need for Cyber Security

Guy Street
Chairman

Generously co-hosted and sponsored by Stadtsparkasse Düsseldorf (SSKD) BCCG hosted a panel discussion „The Growing need for Cyber Security“ at the premises of SSKD on 5 September.

After welcome speeches by Guy Street, regional chair of the BCCG, and Frau Karin-Brigitte Göbel, the CEO of SSKD, Sebastian Tischer, Regional Director Europe of the Information Security Forum (ISF), an institution that follows Cybercrime for the last 30 years, introduced the different standards and emphasized „Define/Implement/Evaluate/Enhance“ as the methods to approach cybercrime. He noted we should always have in mind that cyber criminals ramp up at least as fast as any organization can. Cybercrime is meanwhile a business model and money driven. No one should believe to be safe. You can buy any cyber-attack in the dark net.

Markus Hartmann, Head of the Cybercrime Department (ZAC NRW) of the Prosecutor's office in Cologne urged the audience to file a case with the authorities in case of any attack. Often attacks are identified only afterwards and companies are shy about filing a complaint. Never forget: Criminals know who you are and what you do. Time is of the essence. The Prosecutor's Office is able to give valuable advice and even to identify and successfully chase criminals.

Sarah-Jill Lennard of Deloitte UK insisted on a holistic and strategic approach, which shall identify the measures needed both internally and externally. Very often data is lost just due to inappropriate behavior of people, mostly the own staff. Any conversation in public or trains can be easily nowadays be publicly recorded. The human factor is decisive as most persons do not reflect that the data is not theirs but property of the company and that even printed paper or unlocked doors may lead to the disclosure of business secrets.

Oz Alashe of CybSafe, based in London, highlighted the need for training and education of people. Changing behavior is triggering change. Most helpful are examples of lessons learned. Tick boxes training would not be helpful. Just the consciousness of knowing not to share emails from unknown senders would reduce the distribution of malware significantly.

Stefan Bange, Country Manager Germany of Digital Shadows again reemphasized the need for a holistic approach but also the difficulties to achieve this. Usually there are many stakeholders in your own organization making it very difficult to set up a „perfect“ system. As an example, he used how many third parties are involved just to construct a building. A further issue is IoT (Internet of Things) which increases access points for hackers within an organization. He advised to „control your pool temperature“ and increase the awareness of everyone involved.

An interesting discussion followed. The overriding message was be aware of developments, never stand still and adjust your systems and processes continually. Do not believe that you can control everything but increase the awareness of your staff and understand the value of your key data in defining your defense strategy.