ENISA Workshop “EU Threat Landscape”
24th February 2015, Brussels

Concluding remarks (non-exhaustive, non-prioritized)

- Impact of delivered information should be measured by the degree of uptake: the more implementations are based on the delivered material, the bigger the impact.
- Less information exchange is needed, not more. But the RIGHT information needs to be found.
- While more and more threat intelligence tools are entering the market, the challenge is to discover, correlate and properly display relevant information. It is expected that some work will be done in this area, leading to various types of apps that support users in this task.
- Though it seems that separate intelligence for operational, tactical and strategic information do exist, one has to acknowledge the risks behind separating related collection and analysis life-circles.
- Threat analysis/intelligence is currently a forward looking activity. While this is quite natural, one should recognize/encounter the role of historic threat data in this process.
- While collecting threat information, it should be clear that open source intelligence (OSINT) has limitations, in particular regarding information from Darknet.
- Current practices on risk management, risk assessment, security policy definition, selection of controls, etc. will need to take into account threat and vulnerabilities information. This will increase speed of adaption to new attack methods and exploits.
- A policy framework for sharing threat related information/intelligence will be necessary.
- Discussions on various data management issues when sharing data (e.g. anonymity, retraction, persistency, deletion, retention, etc.).
- A standardized way for referring to threats, threat categories and threat terminology is necessary.
- An important role for reduction of exposure to cyber threats is seen outside big organizations. These are merely SMEs, often lacking the means (financial, skills) to successfully manage cyber threats.
- Lacking training and – to an extend education – regarding awareness and management of cyber threats is seen as one of the roots of today’s problems. Security training/education needs to be lined up with developments of the threat landscape.
- The speed of reaction to cyber threats is an issue that deserves further consideration. Currently, most of cyber threat information/intelligence involves human interfaces.