European Research and Innovation

A Structured Approach to Defence Simulation Training

by Peter Kieseberg

The Austrian SCUDO project is developing a training kit enabling an easy-to-use setup simulation environment for training personnel in the defence of critical infrastructures against IT security incidents.

Modern IT systems are heavily integrated into critical infrastructures and attached to vital parts of operative core components. Many organizations have contingency plans in case of attacks on their critical systems. Post-mortem reviews of the contingency plans indicate that the plans are often outdated or even completely unknown to key players [1]. Problems are further compounded when the contingency plan of an organization relies on establishing communication with parties outside the administrative boundaries of the organization under attack. The lack of updates in the partners' structure results in loss of vital information, outdated assumptions, and an inability to establish appropriate paths of communication and information exchange in the case of an attack.

Regular training focusing on different attack scenarios can facilitate detection of weaknesses, and thus help to overcome them. While table-top exercises are quite popular within some industries, we still lack standardized training methods. In particular, we need to work on developing: efficient setup of training; metrics for measuring readiness and progress; and the availability of tools for preparing and developing the exercises, including an appropriate environment for their execution and analysis.

The SCUDO research project addresses the following research questions:

- The development of an iterative training process yielding quantifiable results, including the required metrics (see Figure 1).
- The construction of different classes of scenarios with respective training environments.
- The development of a training kit that allows the further development of practical scenarios based on the iterative training process.
- Providing tool and visualization support for training execution.

The main aim of the SCUDO project was to generate a training kit that facilitates the straightforward tailoring of predefined basic scenarios into suitable and diverse training scenarios by non-experts in the field of simulation training or table-top exercises. To this end, it included:

- A set of practical basic scenarios, based on three different incident classes.
- A repertoire of easy to deploy inline events.
- Guidelines for the adaption and tailoring of scenarios to fit the training partners and environment.
- Guidelines for efficient execution and operation of training, including recommendations for observers.

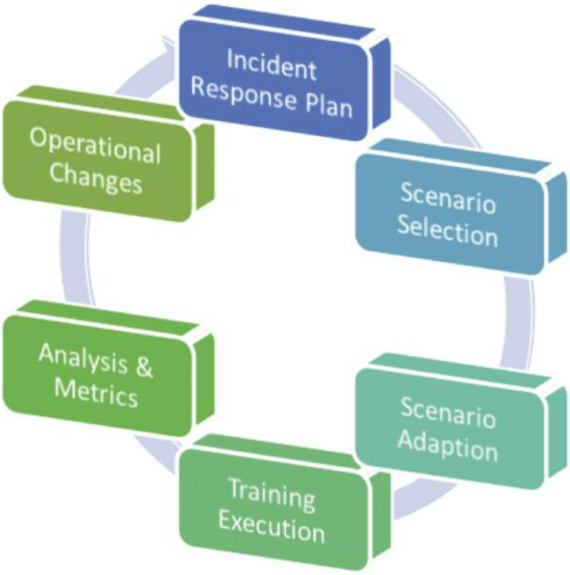

Figure 1: Iterative training process.

Figure 2: Tool support.

- Metrics for the measurement of the readiness level.
- Templates for the documentation of readiness and progress.

An emphasis was placed on generating exercises that involved several related institutions (e.g. supplier-customer) or competing companies, since conflicting contingency plans were identified as a major obstacle [1]. In order to enable the trainers to select the right exercise environment from the basic scenarios and the set of inline events, three fundamental incident classes were defined. The first class (IC1) is concerned with a local disruption of vital IT service business operations (e.g. DNS), while IC2 deals with attacks against the availability and integrity of data transfer and (secured) IT-based communications. Finally, IC3 covers the worldwide disruption of integral IT services that are vital for business continuity, e.g. zero day exploits in the backbone router infrastructure. For each incident class different responses are required from the trainee response team, for example: in regard to communication obligations with governmental departments and the general public, down to liabilities and other legal and regulatory issues.

The SCUDO project has developed support tools for training execution, including support for the players, operators, and observers of an exercise. This set of tools is based on open source technologies and features on-site training for the players, in case of several different companies, as well as the automated collection of training data for the calculation of different metrics in the course of a subsequent analysis.

SCUDO also delivered preliminary results on developing a Situational Awareness Centre [2], monitoring data streams that can lead to the detection of the attacks. This functionality may be added transparently to the exercise scenarios. Thus, the same exercise can serve both the traditional training setup and for identifying the needs and gaps in a potential Situational Awareness Centre.

The SCUDO tools were evaluated in practical exercises attended by major players in Austria with emphasis on important providers for critical infrastructures and the respective governmental partners and ministries [3]. The simulated scenarios within training sessions helped to dramatically increase the readiness of all participants, leading to a better response by their response teams, as well as updates to their contingency plans. Furthermore, the project has raised the collective situational awareness of these issues to a higher level. This direction will be further pursued in a follow-up project regarding the development of Situational Awareness Centres.

The SCUDO project, which was supported by the KIRAS programme of the Austrian Research Promotion Agency (FFG), concluded in February 2015. The project consortium was led by Thales Austria and was carried out by a team of ten partners, ranging from (governmental) stakeholders to scientific and industrial partners.

References:

[1] L. Zechner, P. Kieseberg, E. Weippl: “INMOTOS: Extending the ROPE-methodology”, in Proc. of the 14th International Conference on Information Integration and Web-based Applications & Services (pp. 272-277), ACM, 2012.
[2] M. R. Endsley, W. Jones: “Situation awareness: The Oxford Handbook of Cognitive Engineering, 88-108”, 2013.
[3] B. Riegler: “Cyber-Großangriff in Österreich nur Frage der Zeit”, in Der Standard, 15.01.2015 (in German).

Links:

The official SCUDO project homepage:
http://www.sba-research.org/scudo

Please contact:

Peter Kieseberg
SBA Research, Austria
E-mail: pkieseberg@sba-research.org