Chapter 47
Holistic and Law Compatible IT Security Evaluation:
Integration of Common Criteria, ISO 27001/IT-Grundschutz and KORA

Daniela Simić-Draws
Universität Koblenz-Landau, Germany

Philipp Richter
Universität Kassel, Germany

Stephan Neumann
Technische Universität Darmstadt, Germany

Rüdiger Grimm
Universität Koblenz-Landau, Germany

Anna Kahlert
Universität Kassel, Germany

Melanie Volkamer
Technische Universität Darmstadt, Germany

Alexander Roßnagel
Universität Kassel, Germany

ABSTRACT

Common Criteria and ISO 27001/IT-Grundschutz are well acknowledged evaluation standards for the security of IT systems and the organisation they are embedded in. These standards take a technical point of view. In legally sensitive areas, such as processing of personal information or online voting, compliance with the legal specifications is of high importance, however, for the users' trust in an IT system and thus for the success of this system. This article shows how standards for the evaluation of IT security may be integrated with the KORA approach for law compatible technology design to the benefit of both – increasing confidence IT systems and their conformity with the law on one hand and a concrete possibility for legal requirements to be integrated into technology design from the start. The soundness of this interdisciplinary work will be presented in an exemplary application to online voting.

DOI: 10.4018/978-1-4666-8473-7.ch047

INTRODUCTION

Embedding IT in everyday life, brings not only many advantages, but also increases risks. For example, in case of malfunction economic damages or – in the worst case – damages for life and health are possible. IT security plays a key role in preventing these risks. In order to make IT security measureable and comparable, different standards for the evaluation of IT Security have been developed. As an internationally accepted standard, the Common Criteria are used for the evaluation of IT related products. This evaluation only includes security objectives, directly related to the IT product. However, security objectives concerning the product environment are also of importance when analysing IT security. A broader approach is chosen by ISO 27001/IT-Grundschutz with its organisational perspective: Here, organisation, infrastructure, applications and employees are considered. In combination they constitute the so called *information domain to be protected*. Thus ISO 27001/IT-Grundschutz aims at enforcing and evaluating a basic protection level for complete organisations. Usually, IT security evaluation standards, such as Common Criteria or ISO 27001/IT-Grundschutz consider system security from a technological and organisational point of view and do not specifically integrate legal requirements for the system in different contexts. A fixed integration of national law into internationally applicable standards would be impractical. Integrating legal evaluation of IT security is crucial, however, for systems to be designed in a law compatible way. This might lead to higher acceptance and increasing trust by users. Integration with IT security evaluation standards would provide the law with an effective option to accomplish its normative requirements in IT environments. Legal requirements should be integrated with such standards in an easy and flexible way, in order to be able to adjust them to different jurisdictions and application areas. Thus, IT security evaluation and assertion of legal requirements would both benefit from integration.

Therefore, we proceed to show how the approach for law compatible technology design KORA (Konkretisierung rechtlicher Anforderungen/ concretisation of legal requirements), Common Criteria and ISO 27001/IT-Grundschutz may be integrated into an evolving interdisciplinary approach for the design and evaluation of secure and law compatible IT systems. After presenting the state-of-the-art of related work, the article will first give an extended overview of the applied approaches and standards. Then it will be shown how these approaches and standards may be integrated into one evolving interdisciplinary approach for law compatible IT-security evaluation. We first describe possible interfaces between the presented approaches and standards and illustrate possible combinations. Afterwards, application of our concept will be shown by way of an example from online voting: ballot secrecy in remote online voting systems. Finally, a conclusion will be given on the results of the interdisciplinary work and an outlook on necessary future work.

RELATED WORK

As IT security engineers and lawyers have a different professional background, difficulties often arise when working together on a topic. Even if both strive for the same goal, they usually operate by means of different approaches and different terms or the same term indicates slightly or even totally different concepts. In order to be able to operate effectively, a mutual basis must be found. Already several works have been conducted considering the question of how to enhance security evaluation approaches with legal aspects.

Breaux et al. (Breaux & Antón, 2005a; Breaux & Antón, 2005b; Breaux & Antón, 2008; Breaux, Vail, & Antón, 2008) address the challenges of highly regulated domains, in their case the U.S.