NETWORKED IT-SECURITY FOR CRITICAL INFRASTRUCTURES – THE RESEARCH AGENDA OF VESIKI

Sandra Bergner[1], Benedikt Buchner[2], Sebastian Dännart[1], Albrecht Fritzsche[3], Andreas Harner[4], Sophia Harth[4], Max Jalowski[3], Dennis-Kenji Kipker[2], Ulrike Lechner[1], Kathrin Möslein[3], Andreas Rieb[1] and Martin Riedl[1]

[1] *Lehrstuhl für Wirtschaftsinformatik, Universität der Bundeswehr München*

[2] *Institut für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen*

[3] *Lehrstuhl für Wirtschaftsinformatik I, FAU Erlangen-Nürnberg*

[4] *VDE|DKE, Frankfurt*

Abstract

In order to evaluate and to improve IT security of critical infrastructure that considers also aspects beyond technical ones, the project VeSiKi accompanies various projects from different critical infrastructure backgrounds to establish a collaborative research process among these projects. It serves as a platform which allows research institutions and providers to access results derived within this collaborative process.

Keywords: IT-Security, Critical Infrastructure, Research Project

1 INTRODUCTION AND PROJECT BACKGROUND

IT systems of a critical infrastructure (CI) are never completely isolated from their environment due to interaction, in terms of data exchange, maintenance, software updates and manual input to control and change the operation of the system. These interfaces make CIs vulnerable, in particular when individual human interaction is involved. Technical measures to increase the protection of infrastructures against external attacks increase the pressure on other aspects of security, regarding employee behaviour, institutional culture and procedural routines of daily work etc. [1]. To ensure functional IT security architectures, it is necessary to consider technical, human and organizational aspects at the same time as well as legislation, norms and standards. In order to address the above aspects and to establish new approaches for evaluating and improving IT security of CIs, the BMBF research program “IT-Security for Critical Infrastructures” has been initiated as part of the “High Tech Strategy 2020” of the German Federal Government. Hereby, the Project “Networked IT-Security of Critical Infrastructures” (Vernetzte IT-Sicherheit Kritischer Infrastrukturen, acronym “VeSiKi”; FKZ:16KIS0214) is the accompanying research project beside other selected projects carrying out a collaborative research process. VeSiKi started in January 2015 and runs for a period of 3.5 years.

2 RESEARCH ACTIVITIES AND APPLIED METHODS

VeSiKi´s research perspective is trans-sectoral and will engage the other projects in a collaborative research process and reach out to the IT security community as well.

As depicted in Figure 1, all collaborative research activities of the project VeSiKi, which will be detailed in the following section, will result in a framework of reference processes for IT security of CIs. Hereby, also the communication of researchers and practitioners in the project, including various stakeholders will get a common foundation

by means of a reference model for IT security. In long-term, this reference model will address small and medium sized providers of CIs as an ontology-based tool which allows them to identify suitable procedures and technology to assess and improve IT security for their CIs and align with legislation and governmental regulations.

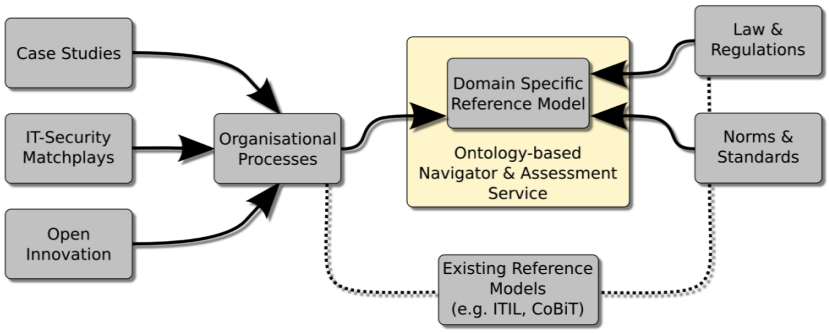

Figure 1: Research Activities

2.1 Case Studies and IT-Security Matchplays

Identifying all relevant requirements specific for IT security of CIs will be a key factor for delivering a valid and practical framework in this domain. In order to learn how CI providers currently ensure security of their information systems and which processes are implemented, we will conduct two approaches in close cooperation with the joint projects within the research program. On one side, we invite IT service operators of CIs to contribute case studies, either concerning established IT security relevant processes, measures and ongoing or finished projects in the organization. Beyond delivering workshops, templates and guidelines, we will accompany the partners during the development of their case studies and carry out a cross-case analysis afterwards which will help us identify best practices and common criteria for the design of a domain-specific framework. On the other side, we will perform IT-Security Matchplays with project partners to challenge leadership processes as well as resilience and business continuity measures in a setting which enable us to see trans-sectoral influences and common issues.

2.2 Open Innovation

Various authors like Hawkey et al. distinguish a variety of different factors and dimensions of IT security and IT security management [2]. IT security is accordingly not only a matter of individual competencies and capacities, but also has strong connections to all aspects of interaction in communities and networks of knowledge and information [3]. Community and network-related activities across institutional boundaries are reflected in open approaches to innovation [4] which intensify the use of knowledge and allow flexible setups and targets of research and development. Open innovation, however, also means that internal knowledge is conveyed to the outside. In an area as sensitive as CIs, open innovation activities therefore have to be designed very carefully. Security concerns of all stakeholders require special attention. Individual interests have to be weighed against each other in order to reach a satisfactory solution for everyone and a suitable overall result. We propose a framework for open innovation based on a representation of IT security for CIs as a service system. Systemic structures allow identification of different instances of value creation on different levels, which can then be addressed individually by specific open innovation activities reflecting the requirements of each instance individually.

2.3 Legislation and Regulations

The IT security of CIs is not only a technical challenge. Legal aspects for the realization of IT security can not be ignored, rather they have to be integrated into the development of IT security measures on from the beginning during the design phase of new technical infrastructures. Likewise, this kind of integration is essential to guarantee the practical character of the IT security law [5]. As a result, an authority which sets legally binding standards has to be in cooperation with the institution which implements these standards. Only under these circumstances, it is possible to realize a coherent, systematic and in a sufficient manner made concrete IT security law. To achieve these research goals, the Institute for Information, Health and Medical Law (IGMR) at the University of Bremen follows a research agenda which can be structured into two different parts. The first part addresses legal questions arising from CI providers that are partners within the research program. For example, solutions to up to date legal problems will be presented in seminars or workshops during visits of enterprises or industrial plants. The second part of the research agenda is focused on the evaluation and classification of applicable laws for CI regarding the different sectors. Besides these two research focuses and on a long dated basis, the IGMR will also develop new legislative proposals for the IT security of CIs. These proposals will mainly be focused onto the results of the dialogue between the researchers and the operators of CIs so that their wishes and complaints can be integrated into future regulations as far as it is possible. To reach this goal, the IGMR seeks the contact to legislative institutions during the complete duration of the VeSiKi research project.

2.4 Norms and Standards

Norms and standards are important for the sustainability and transferability of research results as they bring together interested parties of industry and science. They also guarantee the transfer of the research results into the market. To give the joint research projects the opportunity to work on this topic together, the VDE|DKE will host a working group “norms and standards” (Fachgruppe “Normung und Standardisierung”). The aim is to achieve a common view on standardization of IT security for CIs. As there are a lot of standards and guidelines concerning this topic, it is important to simplify the applicability of those documents so that small providers can easily use those standards. On one hand, the working group will produce recommendations for new standards resulting from the outcome of the research projects, on the other hand it will identify and close gaps in already existing standards. Furthermore it will categorize those existing standards for IT security for CIs. The aspects of norms and standards in general and especially for IT security will be presented and discussed in workshops as and when required by the joint research projects. In the end of the process the VDE|DKE will take care that the derived results find their way into the relevant standardization-committees, even beyond the project duration.

3 INTENDED PROJECT ARTEFACTS

Besides accompanying the joint research projects, a major output will be our own artifacts, derived from the research activities described above. In the following section we will address exemplary deliverables in more detail.

3.1 Reference Model IT-Security for Critical Infrastructures

Since governments more and more recognize the importance of CIs, regulations and legislation, in particular focusing their IT security systems, are increasing. Due to the fact, that many providers of CI are small or medium enterprises, they simply don’t have the resources to develop and implement their own concept of conform IT security.

Current IT-Management frameworks and reference models, such as ITIL or COBIT do consider IT security, but they don't focus it, far less taking CI in account. Based on identified best practices, processes and special requirements of CI, derived from the case studies and IT-Security Matchplays as well as open innovation activities, we will deliver a reference model for the Management of IT security for CI. This will enable organizations to adopt proved processes and align their IT-Security management to both reliable IT security and their duties towards governmental demands. In order to standardize and simplify the adoption we aim at delivering a framework, which is either based on, extending or at least compatible to common de-facto standards. Since many organizations yet are conform and aligned to these standards, the change and approach will be well known and easy to handle.

3.2 Ontology-based Navigator and Assessment Tool as a Platform Deployed Service

The derived reference model as well as the classification of applicable laws, regulations, norms and standards will be made accessible via an ontology-based webservice in order to simplify and accelerate CI assessment. Such a service may be the first, fast and easy to gain reference point for every legal assessment of a CI even for non-jurists. This service applies for sectoral norms and standards in the field of IT security of CIs as well. It is further planned to eventually support CI providers to assess their organization by denoting the infrastructure type, processes and assets. This may give hints on how to improve their current situation based on the reference model serving as a framework for implementing relevant norms and to conform to legislation, best-practices and state-of-the-art methods as developed within the joint projects of this research program.

4 CONCLUSION

Beyond the exchange between the joint projects of the research program via conferences, workshops and the developed platform to allow project partners to share research results and to establish public visibility, VeSiKi carries out its research agenda. Therefore, CI providers are included to carry out case studies, perform IT-Security Matchplays and to use open innovation as a tool for improving information security. A cross-sectoral analysis and classification of common practices and processes, applicable laws, regulations, norms and standards is performed in order to derive a common knowledge model accessible via an ontology based service integrated as part of the provided webplatform.

REFERENCES

[1] Halliday, S., Badenhorst, K., and von Solms, R. (1996). *A Business Approach to Effective Information Technology Risk Analysis and Management*. Information Management & Computer Security 4(1), pp. 19-31.

[2] Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A., & Beznosov, K. (2008). *Human, organizational, and technological factors of IT security*. CHI'08 Extended Abstracts on Human Factors in Computing Systems (ACM), pp. 3639-3644.

[3] Fenz, S., Parkin, S., & Van Moorsel, A. (2011). *A community knowledge base for IT security*. IT Professional 13(3), pp. 24-30.

[4] Chesbrough, H.W., West J & Vanhaverbeke W (eds) (2006) *Open Innovation: Researching a New Paradigm*. Oxford: Oxford University Press.

[5] Spindler, G. (2008). *IT-Sicherheit – Rechtliche Defizite und rechtspolitische Alternativen*. MMR 11(7), pp. 7-12.