

Design and Application of a Security Analysis Method for Healthcare Telematics in Germany (HatSec)

Ali Sunyaev

Technische Universität München
D-85748 Garching, Germany
sunyaev{at}in.tum.de

Purpose: The goal of this work is to provide a method for organisational and technical analysis of security issues in health care (using tools, methods and processes in a structured and traceable way). On the basis of this method the current security status of health care telematics in Germany is evaluated and valuable hints for future developments in the health care sector are derived.

Findings: During the planning stage of designing such an IS security analysis method specific to healthcare industry [Ka04], it is advisable to base the design procedure on established standards and best practice approaches, so that the security analysis method relies on previously approved frameworks [SBH04]. Based on the PDCA (Plan/Do/Check/Act) model [De86] the HealthcAre Telematics SECurity - HatSec - analysis method is built in a compositional manner. This means that the HatSec method was designed from existing IS security analysis approaches (like ISO 27001 and IT-Grundschutzhandbuch), which were subdivided into method fragments. These method fragments were used to construct the HatSec security analysis method. The identified method fragments of selected IS security analysis approaches were methodically composed into the following seven steps: (1) scope identification, (2) asset identification, (3) basic security check, (4) threat identification, (5) vulnerability identification, (6) security assessment and (7) security measures. These steps represent at least one part of an IS security approach that fits best to the current situation.

The application of the HatSec method identified 24 deficiencies around the current status of the German health care telematics (including weaknesses, inconsistent and conflicting development documents and violation of security demands) and provided solutions for discovered vulnerabilities accordingly.

Practical implications: Based on the outcome of this research project, a broader understanding of analyzing healthcare security is expected. The created method is designed for chief information security officers (CISO) to analyze forthcoming or already implemented healthcare information systems. A further contribution to practice is the identification of security problems in the current concept of the German healthcare telematics.

References

- [Ka04] Katsikas, S.K.: *Health care management and information systems security: awareness, training or education?* International Journal of Medical Informatics, Vol. 60 (2000), pp. 129-135.
- [SBH04] Siponen, M., Baskerville, R. and Heikka, J.: *A Design Theory for Secure Information Systems Design Methods*. Journal of the Association for Information Systems, Vol. 7 (2006) Nr. 11, pp. 725-770.
- [De86] Deming, W. E.: *Out of the Crisis*. MIT Center for Advanced Engineering Study, Mit Press (1986).