Ali Sunyaev

Lehrstuhl für Wirtschaftsinformatik Prof. Dr. Krcmar
Technische Universität München

15.09.2009
Design and Application of a Security Analysis Method for Healthcare Telematics in Germany (HatSec)

Ali Sunyaev
Technische Universität München
Fakultät für Informatik
Lehrstuhl für Wirtschaftsinformatik (I17)
Overview

• Introduction
• Research Questions
• Results
Electronic Health Card (eHC)

- General practitioners
- Hospitals
- Pharmacists
- Rehabilitation institutions
- Other care providers
- Insured person
- Electronic health card

Quelle: in Anlehnung an www.gematik.de

- 300 Health insurances
- 2,200 Hospitals
- 21,000 Pharmacies
- 188,000 Medical specialists/dentists
- and...
- 80 Million Insurants!
Importance of Research

- „Bei der Mehrheit der gesetzlich Krankenversicherten (73%) bestehen zumindest geringe Bedenken, dass die Daten auf der eGK von unberechtigten Personen eingesehen und missbraucht werden könnten – ein gutes Drittel der Versicherten äußert sogar große Bedenken“ (Forsa, 2008)

- handling of these new electronic patient cards
- business process reorganisation
- technical dependability
Overview

Problem

„Research shows insufficiencies with the … current analysis methods lacking the techniques to analyse technical and social aspects of information security in a health environment.“ (Brooks, 2004)

The goal of this project is to provide a method for the analysis of security issues in health care

Whom

• domain: health care / health care telematics
• chief information security officers
• results: patients, physicians, pharmacists, hospitals, health insurance companies

Why

• in order to evaluate the current security status of health care telematics in Germany and give valuable hints for future developments in the health care sector
What are special Characteristics of Health Care with Respect to Security?

- Trade-off between availability (securing of an ideal treatment) and confidentiality (privacy)
- Strong regulations by law
- Local and heterogenous it-systems (not standardizied it-components)
- Contextual access rights
- Ad hoc and dynamic information exchange
- Physical property
Research approach

• Literature review based upon the approach by Webster and Watson (2002)

• Examination of healthcare IS security issues currently receiving attention in the literature.

• Spanning the IS security, information management, information systems, healthcare informatics, risk- and security analysis and management literature

• Identification of relevant journals

• Examination of appropriate articles

• Full-text electronic search - > analyzed articles 1007

• Total number of 145 relevant articles

• In-depth review of 25 articles
<table>
<thead>
<tr>
<th>Journals</th>
<th>Abstract</th>
<th>In-Depth Review</th>
<th>Of Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM Computing Surveys</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>ACM Transactions on Information and System Security</td>
<td>38</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Bank Accounting &amp; Finance</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Communications of the ACM</td>
<td>54</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>Computers &amp; Security</td>
<td>92</td>
<td>32</td>
<td>2</td>
</tr>
<tr>
<td>European Journal of Information Systems</td>
<td>4</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>HMD Praxis der Wirtschaftsinformatik</td>
<td>7</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>IEEE Security &amp; Privacy</td>
<td>21</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>IM Information Management &amp; Consulting</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Information and Organization</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Information Management &amp; Computer Security</td>
<td>33</td>
<td>9</td>
<td>1</td>
</tr>
<tr>
<td>Information Systems Journal</td>
<td>13</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Information Systems Management</td>
<td>12</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Information Systems Security</td>
<td>41</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>Information Security Management</td>
<td>29</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Internal Auditor</td>
<td>21</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>International Journal of Network Management</td>
<td>28</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>International Journal of Medical Informatics</td>
<td>9</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Journal of Computer Security</td>
<td>7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Journal of Management Information Systems</td>
<td>4</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Journal of Research and Practice in Information Technology</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Strategic Finance</td>
<td>7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Andere</td>
<td>11</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total Journals</strong></td>
<td><strong>441</strong></td>
<td><strong>95</strong></td>
<td><strong>10</strong></td>
</tr>
</tbody>
</table>

| Articles of organizations and authorities  | 19       | 19             | 2           |
| Dissertations/ Master's/- Bachelor Theses/ Working Paper | 39       | 39             | 5           |
| Conferences/ Workshops                     | 13       | 4              | 1           |
| **Total**                                  | **512**  | **157**        | **18**      |

IS Security Analysis Approaches

Checklists
- SAFE
- AFIPS
  - Computer Security Handbook

Assessment Approaches
- Risk Assessment Approaches
- Security Control Assessment Approaches
  - Questioning Techniques
    - Expert Interviews
    - Stochastic Methods
    - VaR
    - Indicator Approaches
    - Key Indicator Approaches
    - Causal Methods
    - Bayesian Networks
  - Financial Ratios
    - ROSI
    - Static Investment Appraisal Approaches
    - Cost Comparison Method
  - Dynamic Investment Appraisal Approaches
  - Stochastic Decision Analysis Approaches
    - Gordon/Loeb 2002
  - Game Theory Approaches
    - Cavusoglu et al. 2004

Risk Analysis Approaches
- Classic Approaches
  - CRAMM
  - ISRAM
- Process-Oriented Approaches
  - Attack Trees
- Tree-Based Approaches

IT Security Management Approaches
- Standards
  - NIST SP-800-30
  - ISO/IEC 2700x
- Best Practice Models
  - COBIT
  - ITIL

Legislation Accommodations
- Basel II
- KonTraG
- SOX
- HIPAA

Caption:

Approach provides parts of a security analysis
IT security analysis approach
Approach provides more than a security analysis
Approaches from class A can contain none, one or several approaches from class B and/or class C
**Found Approaches**

- Checklists: 5
- Assessment Approaches: 33
- Risk Analysis Approaches: >100
- IT Security Management Approaches: 32
- Legislations: 12
Characteristics of IS Security Approaches with Respect to Healthcare

Three different types:

- Healthcare Specific IS Security Approach Characteristics
- General IS Security Approach Characteristics with Reference to Healthcare
- General IS Security Approach Characteristics
Important Aspects

• Focus on the healthcare sector;
• Provision of detailed information which identifies the IS security approach and could be used to create an approach identity card;
• Creation of information packages for healthcare organizations to help them select suitable methods for performing a security analysis;
General IS Security Approach Characteristics

• Basic Information

• Identification and Personalization of the profile of the researched IS security approach

• establish the relationship between the approaches and the different characteristics.
General IS Security Approaches Characteristics with Reference to Healthcare

• Provide a better understanding of the specifics of healthcare.

• Similar to those of the first classification area but

• Could also be interpreted in a context that is applicable to the healthcare domain.
Healthcare Specific IS Security Approaches Characteristics

- Considers the special requirements such as the importance of protecting patient health information.

- Takes the uniqueness of the medical environment (ISO 2007, V) into consideration.

- Takes the specific laws concerning the security and privacy of health-related data into consideration
<table>
<thead>
<tr>
<th>Fokus/Zielsetzung</th>
<th>Brooks-Evaluation</th>
<th>HIPAA</th>
<th>ODESSA</th>
<th>CRAMM</th>
<th>IT-Grundschutzhandbuch</th>
<th>ISO/IEC 17799</th>
<th>NIST SP 800-30</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>- Implementierung geeigneter Sicherheitsmaßn.</td>
<td>- Ableitung und Bewertung passender Sicherheitsmaßn.</td>
<td>- Ableitung geeigneter Sicherheitsmaßnahmen</td>
<td>- Ableitung geeigneter Sicherheitsmaßnahmen</td>
<td>- Ableitung geeigneter Sicherheitsmaßnahmen</td>
<td>- Ableitung geeigneter Sicherheitsmaßnahmen</td>
<td></td>
</tr>
<tr>
<td>Vollständigkeit</td>
<td>Nein</td>
<td>Ja</td>
<td>Ja</td>
<td>Nein</td>
<td>Nein</td>
<td>Ja</td>
<td>Ja</td>
</tr>
<tr>
<td>Aufwand/Umsetzungskosten</td>
<td>Mittel – Hoch</td>
<td>Hoch</td>
<td>Mittel</td>
<td>Mittel</td>
<td>Mittel</td>
<td>Mittel – Hoch</td>
<td>Hoch</td>
</tr>
<tr>
<td>Methodik der Informationsgewinnung</td>
<td>Befragungstechniken</td>
<td>Befragungstechniken</td>
<td>Befragungstechniken</td>
<td>Befragungstechniken</td>
<td>Analyse der IT-Landschaft</td>
<td>Hinweis auf ISO/IEC 13335</td>
<td>Befragungstechniken</td>
</tr>
<tr>
<td>Updates</td>
<td>Nicht bekannt</td>
<td>Nein</td>
<td>Nicht bekannt</td>
<td>Ja</td>
<td>Ja</td>
<td>Ja</td>
<td>Nein</td>
</tr>
<tr>
<td>Internationalität</td>
<td>Keine Informationen verfügbar</td>
<td>Keine Informationen verfügbar</td>
<td>Keine Informationen verfügbar</td>
<td>Ja</td>
<td>Ja</td>
<td>Ja</td>
<td>Keine Informationen verfügbar</td>
</tr>
<tr>
<td>Zertifizierungs möglichkeit</td>
<td>Ja</td>
<td>Keine Informationen verfügbar</td>
<td>Keine Informationen verfügbar</td>
<td>Ja</td>
<td>Ja</td>
<td>Ja</td>
<td>Keine Informationen verfügbar</td>
</tr>
<tr>
<td>Toolunterstützung</td>
<td>Keine Informationen verfügbar</td>
<td>Nein</td>
<td>Ja</td>
<td>Ja</td>
<td>Ja</td>
<td>Ja</td>
<td>Nein</td>
</tr>
</tbody>
</table>
Relationship between Method Fragments

- Process fragment precedes Product fragment
- Product fragment produces Process fragment
- Process fragment requires 0...n
- Product fragment produces 0...m

Ali Sunyaev, Department of Informatics, Technische Universität München
Granularity levels
HatSec Method

- Seven steps:
  
  1. scope identification
  2. asset identification
  3. basic security check
  4. threat identification
  5. vulnerability identification
  6. security assessment
  7. security measures
HatSec Method

Security Analysis Context and Preparation

1. Scope Identification
2. Asset Identification

Security Analysis Process

3. Asset Identification
4. Threat Identification
5. Vulnerability Identification
6. Security Assessment

Security Analysis Product

7. Security Measures

Security Analysis

- Asset based
- Process based
- Standard based
- Policy based

Hazard list relevant to health care

- Likelihood determination
- Impact analysis
- Security determination

Security Analysis Context and Preparation

1. Scope Identification
2. Asset Identification

Security Analysis Process

3. Asset Identification
4. Threat Identification
5. Vulnerability Identification
6. Security Assessment

Security Analysis Product

7. Security Measures

Security Analysis

- Standard based
- Policy based

Security Analysis Context and Preparation

1. Scope Identification
2. Asset Identification

Security Analysis Process

3. Asset Identification
4. Threat Identification
5. Vulnerability Identification
6. Security Assessment

Security Analysis Product

7. Security Measures

Security Analysis

- Standard based
- Policy based

Security Analysis Context and Preparation

1. Scope Identification
2. Asset Identification

Security Analysis Process

3. Asset Identification
4. Threat Identification
5. Vulnerability Identification
6. Security Assessment

Security Analysis Product

7. Security Measures

Security Analysis

- Standard based
- Policy based

Security Analysis Context and Preparation

1. Scope Identification
2. Asset Identification

Security Analysis Process

3. Asset Identification
4. Threat Identification
5. Vulnerability Identification
6. Security Assessment

Security Analysis Product

7. Security Measures

Security Analysis

- Standard based
- Policy based
PDCA Mapping

1. Plan
2. Do
3. Check
4. Act

- Scope Identification
- Asset Identification
- Basic Security Check
- Threat Identification
- Security Assessment
- Security Measures
- Vulnerability Identification
- Scope Identification
Security Analysis

Identification by:
- Legal basis
- Specifications
- Engineering documents
- Basic goals of IT security
- ...

Methodical analysis by:
- Penetration tests
- Tools for analysis
- Exploitation frameworks
- Attack-Trees
- Metrics
- ...

Actions by:
- Selection from activity catalogue
- New development

Scope Identification
Asset Identification

Threat Identification
Basic Security Check

Vulnerability Identification

Security Assessment

Security Measures

Security Analysis Context and Preparation

Security Analysis Process

Security Analysis Product
A safe freeway with insecure on-ramps?

- The connection between the primary systems and the connector should be encrypted
- Security specifications for primary systems should be defined
- Backup processes for essential health care telematics processes and services should be defined
- Long-term confidentiality of encrypted medical data
- Handling of electronic health cards and of health professional cards especially in hospitals
Design and Application of a Security Analysis Method for Healthcare Telematics in Germany (HatSec)

Ali Sunyaev
Technische Universität München
Fakultät für Informatik
Lehrstuhl für Wirtschaftsinformatik (I17)
References


