SECURE IT/TELCO ENVIRONMENT PLANNING MADE EASY
A Concept of a Tool for Planning Secure IT/Telco Infrastructure and Applications

Wolfgang Haidegger
SECUDE Global Consulting GmbH, Lassallestrasse 7b, 1021 Wien, Austria

Keywords: e-Business, ISMS, ISO/IEC 27001, ISO/IEC 17799, ISO/IEC 15408, Risk Analysis, Information Security Policies, Security Guidelines and Procedures, Evaluation Assurance Level.

Abstract: This paper first motivates the necessity of a planning tool for IT infrastructure and applications, which allows the inclusion of security measures in an automated way. Then the author summarizes the requirements coming from legal and technical standards, which serve as a framework to assure the compliance of the results of planning activities with the respective applicable regulations. Next, a rough concept for realizing the planning tool is presented and finally conclusions are presented.

1 INTRODUCTION

The IT/Telco industry supports e-commerce with a selection of electronic business applications aimed at commercial transactions. The following list enumerates some of the better known business applications, but is by no means exclusive:

- electronic funds transfer,
- supply chain management,
- e-marketing,
- online marketing,
- online transaction processing,
- electronic data interchange (EDI),
- automated inventory management systems, and
- automated data collection systems.

From a technical point of view this paper distinguishes between the network services (also called "infrastructure") and the application services, which are necessary to implement business applications as listed above. This distinction is important, as it mandates different technical and procedural security measures.

In addition to distinguishing the type of service necessary (infrastructure or application) to put together a business application, one is very often faced with a converged IT/Telco landscape concerning both types of services. This means one has to accommodate for the security needs of both circuit switched and packed oriented networks with their different transport and control planes, management protocols and application service philosophies.

The last two paragraphs show that security issues pertaining to information stored of transferred within networks for the purpose of doing electronic business can get arbitrarily complex both on a technical and a procedural level. At the same time the need for security grows as more and more personal (and sometimes very private) data is involved in e-commerce transactions. This is also reflected by the fact that compliance requirements to national and international regulations concerning confidentiality, availability and integrity of information become stricter.
Taking the complex surroundings just described into account, then in order to carry out a proper analysis of security requirements and planing of the according security measures a comprehensive tool (or tool chain) needs to be developed, which guarantees

- technical correctness,
- compliance to all relevant regulations and
- proper tailoring to the business needs

for the solution found.

A final remark: The author of this paper does not distinguish between Greenfield analysis and analysis of existing infrastructure and applications concerning the capabilities of the planning tool, as this does not seem to be relevant for a preliminary treatment of the topic.

Haidegger W. (2008).
SECURE IT/TELCO ENVIRONMENT PLANNING MADE EASY - A Concept of a Tool for Planning Secure IT/Telco Infrastructure and Applications.
In *Proceedings of the International Conference on e-Business*, pages 107-110
DOI: 10.5220/0001913501070110

2 THE NORMATIVE FRAMEWORK

The following paragraphs show the steps necessary for risk analysis and mitigation. These have been described in different level of detail but with the same general intention in ISO/IEC FDIS 27001, ISO/IEC 15408 and ASIS.

Figure 1 gives an overview over the procedure the steps are embedded in.

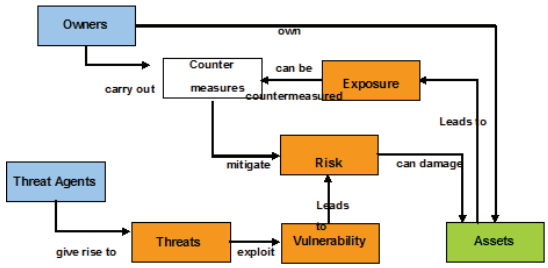

Figure 1: Process, which the tool has to support.

Step 1: Risk Analysis

- Assets, their value and their owners are identified.
- Vulnerabilities of the assets as well as threat agents, which might exploit the vulnerabilities, are identified.
- For the resulting risks possible countermeasures are identified and the appropriate ones are selected.

Step 2: Definition of Mitigation Measures

- Development of security policies
- Analysis of relevant international, national and corporate legal and technical standards relevant for the situation.
- Development of procedures and guidelines, designing the way the security policies shall actually be realized.

Step 3: Integration into Service/Infrastructure architecture (not shown in figure 1)

- Design of infrastructure with selected security measures
- Design of applications according to selected security measures

Step 4: Verification (not shown in figure 1)

- Selection of appropriate Assurance Level
- Development of Evaluation Assurance Level Criteria corresponding to the Assurance Level selected

The following subsections give an idea about the legal and technical recommendations the tool (or tool-set) will have to be able to abide to. They represent additional, project external constraints.

2.1 International Legal, Procedural and Technical Standards

There are many international legal standards, which have to be considered as important when treating IT/Telco security. Some examples are:

- Treaties of the European Union,
- European Convention for the Protection of Human Rights and Fundamental Freedoms,
- European Directives

To show one important European standard in the area of Identity Management:

The European Directive 95/46/CE: deals with data protection, is aimed at giving to the data subject (owner of data) the most control possible on its own identity and personal data, posing a series of requirements on recipients, controllers, processors and even third parties. Art. 2, letter a), giving a definition of "personal data", says: "identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".

There are also quite some procedural (non-technical) international standards, which will play a role when planning security measures. Two examples are:

- ISO/IEC FDIS 27001: This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an IT security management plan focussing on the overall business risks of the organization the plan is made for.
- COBIT: The Control Objectives for Information and related Technology (COBIT) provides a set of generally accepted measures, indicators, processes and best practices to assist
    - in maximizing the benefits derived through the use of information technology and
    - developing appropriate IT governance and control in a company

International technical standards will come from ISO, IETF, ITU-T, OMA, TMF, W3C and other international standardization bodies or industry forums.

2.2 National Legal Standards

Every nation will have a set of national legal standards, which have to be considered as important in addition when treating IT/Telco security. This time the examples are selected from the USA, again with the focus on relevance to Identity Management:

- Privacy Act of 1974: all government agencies - federal, state and local - which request social security numbers are required to provide a disclosure statement on the form;
- Family Educational Rights and Privacy Act (FERPA, also known as the "Buckley Amendment," enacted in 1974, 20 USC 1232g): social security numbers fall within the scope of personally identifiable information that is restricted from disclosure by schools that receive federal funding under the Family Educational Rights and Privacy Act;
- Children's Online Privacy Protection Act (COPPA) - 15 U.S. Code 6501 et seq.: The act's goal is to place parents in control over what information is collected from their children online;
- Financial Services Modernization Act, Gramm-Leach-Bliley (GLB), Privacy Rule - 15 USC 6801-6827: The 1999 federal law permits the consolidation of financial services companies and requires financial institutions to issue privacy notices to their customers, giving them the opportunity to opt-out of some sharing of personally identifiable financial information with outside companies;

2.3 Corporate Standards

Finally, organizations whose security needs to be planned or evaluated and updated will probably have additional regulations, which need to be taken into account. For example it might be necessary for every employee to wear a badge with her or his photo id on it to guarantee an additional possibility to identify her or him.

3 CONCEPT FOR THE REALIZATION OF THE PLANNING TOOL

The threat analysis will be based on a database that holds information about known threats to the specific system components, their architecture, protocols. This database will also be filled with the results of the tasks dealing with risk assessment. There are tools today, which do this on a very general level (e.g. COBRA). The main challenge will be to drill down to implementation level if possible and/or necessary.

Furthermore a network/application planning tool will be developed based on the threat database above, which is capable of identifying threats to a planned network, suggesting methods to mitigate the threats according to a specific Evaluation Assurance Level and including the results into the network plan, a threat model document and a test specification. Here two issues will be of main concern:

- Developing solution variants, which really fit the topic and providing guidance for the selection of the “right” solution.
- Using the selected Evaluation Assurance Level as the driving parameter for the automated solution development

The tool will be capable of tracking the changes to the planned network, the according changes in the threat model, and the changes in the security measures to be taken and finally, track the changes in the documentation (network plan, test specification).

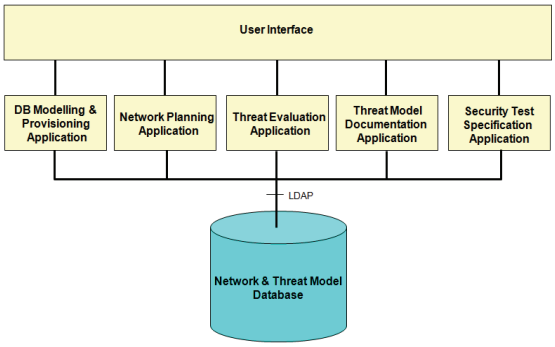

Figure 2: General architecture of the tool (tool chain).

Figure 2 give a first impression of how the tool chain shall be designed. The main part will be an intelligent central data base, which will serve all planning applications likewise.

4 CONCLUSIONS

The paper shows the necessity of a general IT/Telco security planning tool (or tool chain) as a consequence of heightened complexity concerning the infrastructure and the applications as well as tightened security and compliance regulations.

The regulatory framework, which such a tool chain has to accommodate, is dealt with conclusively concerning the types of regulations, but only exemplary concerning the actual recommendations.

Finally a first idea of a possible realization is given together with the crucial points to solve.

Next steps will be the collection of the technical ingredients of the database (protocols, HW architectures, SW architectures, SW frameworks, ...) and a first design of the database itself. This will have to happen in the light of the applications, which will use the database.

REFERENCES

ISO/IEC FDIS 27001: "*Information technology — Security techniques —Information security management systems — Requirements*" Final Draft 2007

ISO/IEC 17799: "*Information technology — Security techniques — Code of practice for information security management*" 2005

ISO/IEC 15408: *Common Criteria for Information Technology Security Evaluation* Version 3.1, Revision 1, September 2006 (Part 1 – Part 3)

ASIS: *The General Risk Assessment Guidline*, ASIS International, November 13-th 2002, ASIS GLCO 01 012003, Sean Ahrens et al