Bundesamt
für Sicherheit in der
Informationstechnik

Supplement to BSI-Standard 100-3, Version 2.5

Application of the Elementary Threats from the IT-Grundschutz Catalogues for Performing Risk Analyses.

03. August 2011

Ferderal Office for Information Security
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
Email: grundschutz@bsi.bund.de
Internet: http://www.bsi.bund.de

Table of Contents

Index of Tables

1 Introduction

The BSI-Standard 100-3 [BSI3] describes a methodology for how to apply the threats defined in the IT-Grundschutz catalogues [GSK] to perform a simplified risk analysis for information processing. In doing so, the following questions stand in the foreground:

- Which threats to information processing have not yet been sufficiently, or not at all, taken into account by implementation of the relevant IT-Grundschutz modules?
- Is there a need for possible additional security safeguards, which go beyond the IT-Grundschutz model, to be scheduled and implemented?

The threats defined in the catalogues T 1 to T 5 from [GSK] serve as a starting point for the methodology described in [BSI3]. Meanwhile, these five risk catalogues identify approximately 450 individual threats. This complicates the analysis and evaluation of all threats when performing risk analyses. Therefore, the BSI has summarised the general aspects of the sometimes very specific individual risks, and developed 46 generic threats. These *elementary threats,* as they are referred to, were published in the course of the 12th supplementary release of the IT-Grundschutz catalogues in the threats catalogue T 0.

The objective of this document is to show how the elementary threats can be used for performing risk analyses based on BSI-Standard 100-3. The adaptations to the procedures presented in [BSI3] necessary for this will be described.

During practical implementation of the BSI-Standards, the users thus have the choice of whether to perform risk analyses using the specific threats defined in the threats catalogues T 1 through T 5 or using the new elementary threats from the catalogue T 0. The BSI recommends the use of elementary threats for performing new risk analyses since this, compared to using the specific threats, usually requires less overhead without consideration of sacrificing the attainable level of security.

2 Overview of the Elementary Threats

The elementary threats were developed to pursue the goals described in the following. Elementary threats are:

- optimised for use in a risk analysis,
- product-independent (always),
- technology-independent (whenever possible – certain technologies dominate the market so strongly, that they also influence abstracted threats),
- compatible with comparable international catalogues,
- integrated seamlessly into the IT-Grundschutz approach.

Since the elementary threats should primarily ensure performing a risk analysis efficiently, the focus is on identifying real threats. Threats which focus on insufficient or missing implementation of safeguards and hence refer to indirect threats, were intentionally avoided.

During development of the elementary threats, it was also taken in consideration which basic parameter of the information security (confidentiality, availability, integrity) is affected by each threat. Since this information may be of interest at various stages of the security concept, they are included in the following table. Not all threats correspond to exactly one basic parameter, rather various threats affect several basic parameters. In the interpretation, each threat directly affects the basic parameter listed in the table next to the corresponding threat. In the case of many threats it is namely controversial to which extent all three basic parameters are affected due to indirect effects which can be derived from it. Thus, for example, in T 0.1 availability is mentioned as the only basic parameter affected by fire. A fire could certainly result in the fact that storage media suffer only minor damage, so that files are still there at first glance, but there has been loss of integrity. In another scenario, during a fire and related rescue measures confidential documents were suddenly disclosed to unauthorised persons – both cases had however indirect effects on the basic values of confidentiality and integrity, only availability was affected directly.

The following table gives an overview of the elementary threats. Here, A stands for Availability, C stands for Confidentiality, and I for Integrity.

	Threat	***Basic Parameter***
T 0.01	Fire	I,A
T 0.02	Unfavourable climatic conditions	I,A
T 0.03	Water	I,A
T 0.04	Pollution, dust, corrosion	I,A
T 0.05	Natural disasters	A
T 0.06	Environmental disasters	A
T 0.07	Major events in the environment	C,I,A
T 0.08	Failure or disruption of the power supply	I,A
T 0.09	Failure or disruption of communication networks	I,A
T 0.10	Failure or disruption of mains supply	A
T 0.11	Failure or disruption of service providers	C,I,A
T 0.12	Interfering radiation	I,A
T 0.13	Intercepting compromising emissions	C
T 0.14	Interception of information / espionage	C
T 0.15	Eavesdropping	C
T 0.16	Theft of devices, storage media and documents	C,A
T 0.17	Loss of devices, storage media and documents	C,A
T 0.18	Bad planning or lack of adaptation	C,I,A
T 0.19	Disclosure of sensitive information	C
T 0.20	Information from an unreliable source	C,I,A
T 0.21	Manipulation of hardware and software	C,I,A
T 0.22	Manipulation of information	I
T 0.23	Unauthorised access to IT systems	C,I
T 0.24	Destruction of devices or storage media	A
T 0.25	Failure of devices or systems	A
T 0.26	Malfunction of devices or systems	C,I,A
T 0.27	Lack of resources	A
T 0.28	Software vulnerabilities or errors	C,I,A
T 0.29	Violation of laws or regulations	C,I,A
T 0.30	Unauthorised use or administration of devices and systems	C,I,A
T 0.31	Incorrect use or administration of devices and systems	C,I,A
T 0.32	Abuse of authorisations	C,I,A
T 0.33	Absence of personnel	A
T 0.34	Attack	C,I,A
T 0.35	Coercion, extortion or corruption	C,I,A
T 0.36	Identity theft	C,I,A
T 0.37	Repudiation of actions	C,I
T 0.38	Abuse of personal data	C
T 0.39	Malicious software	C,I,A
T 0.40	Denial of service	A
T 0.41	Sabotage	A
T 0.42	Social Engineering	C,I
T 0.43	Replay of messages	C,I
T 0.44	Unauthorised entry to premises	C,I,A
T 0.45	Data loss	A
T 0.46	Loss of integrity of sensitive information	I

Table 1: Overview of the elementary threats

3 Preparing the Threat Summary

To use the elementary threats when performing a risk analysis, the methodology described in [BSI3] can be applied almost without any changes. Content-related adaptations are only necessary at the step *Preparing the Threat Summary* (see Chapter 3 in [BSI3]). The following section describes how to produce a summary of the threats for which the target objects under review are subject.

The starting point for preparing the threat summary is a list of target objects or groups of target objects which should be reviewed in the risk analysis. This list is available as the result of the supplementary security analysis (see Chapter in 4.6 of [BSI2] and Chapter 2 of [BSI3]). The list is supplemented by the superordinate target object *Entire information domain*, provided that the target object has not already been included in the list.

Example: (Excerpt)

Number	***Description***
IV	Entire information domain
M.723	Server room
M.811	Technical infrastructure room
S3	Communications server
C4	Client
N3	Router
N7	Switch

Table 2: List of the target objects under review (Excerpt)

In the treats catalogue T 0 of the IT-Grundschutz catalogues, the BSI published the elementary threats optimised for use within a risk analysis. Using the catalogue T 0, each target object under review, one by one, is assigned the elementary threats which can in *principle* incur *considerable* damage to this target object. Thereby, it does not matter how high the potential for damage is exactly. This aspect is dealt with in a later step. As well, the safeguards already planned or implemented for the target object reviewed should *not* be considered in the assignment of the elementary threats. This aspect is also discussed in a later step.

Altogether, the assignment of elementary threats to the relevant target objects is based on the assumption that no security safeguards are implemented, for example from the IT-Grundschutz catalogues or other sources.

In practice, it is the type of target object which has a significant influence on what elementary threats are applicable to it at all.

For instance the threat T 0.28 *Software vulnerabilities or errors* will hardly be relevant for an office room, but rather for the workstations operating inside it. Threats which do not relate to specific technical components, such as T 0.29 *Violation of laws or regulations*, are usually suitable for target objects of the type *application*, *business process* or *entire information domain*.

As a result, a table has been produced in which each target object is assigned a list of relevant elementary threats.

In order to facilitate the subsequent analysis, the table should include the protection requirement for each target object, which was identified in the course of assessment of protection requirements in relation to the three basic parameters: confidentiality, integrity and availability. For the superordinate object *entire information domain*, this assignment is not necessary.

This table presents a *threat summary* for the target objects under review. It serves as a starting point for the subsequent *determination of additional threats*.

Example: (Excerpt)

Communications server S3	
Confidentiality:	normal
Integrity:	high
Availability:	high
T 0.8	*Failure or disruption of the power supply*
T 0.22	*Manipulation of information*
T 0.23	*Unauthorised access to IT systems*
T 0.24	*Destruction of devices or storage media*
T 0.25	*Failure of devices or systems*
etc.	

Table 3: Threat summary for the target object S3 (Excerpt)

Room M.811	
Confidentiality:	normal
Integrity:	normal
Availability:	high
T 0.1	*Fire*
T 0.3	*Water*
T 0.24	*Destruction of devices or storage media* (e.g. air-conditioning system)
T 0.41	*Sabotage*
T 0.44	*Unauthorised entry to premises*
etc.	

Table 4: Threat summary for the target object M.811 (Excerpt)

4 Creating User-Defined Modules

Often during the risk analysis, it becomes necessary to create a user-defined module for a subject area, which has not yet been adequately covered by the IT-Grundschutz catalogues to allow modelling of the information domain being reviewed. On the other hand, the IT-Grundschutz catalogues are so comprehensive that at least for parts of these areas, existing modules from the IT-Grundschutz catalogues can be used as a basis during the risk analysis. In doing so, one should on one hand stick to the existing materials as far as possible to avoid unnecessary overhead, but on the other hand discuss potential new or enhanced threats as often as possible, in order to avoid overlooking threats.
For the subject under consideration, a risk analysis must first be performed.

For this purpose, the elementary threats from the elementary threats catalogue T 0 should be studied carefully for the subject area under review. It should be considered carefully whether they are relevant for each target object, that is whether they could in principle cause considerable damage to it. To achieve this, every elementary threat must be evaluated in terms of whether it affects the target object in a direct or indirect way, or not at all.

For example, if a specific server operating system is reviewed, the elementary threat T 0.25 "Failure of devices or systems" is a relevant risk, against which specific security safeguards have to be implemented. At first glance it may, besides the aforementioned, seem necessary to classify the elementary threat T 0.1 Fire as relevant for this target object, with the justification that "A fire causes a failure of the server". Here, however, the server failure is a consequence of the fire, so an indirect effect on the hardware. What causes the failure is generally irrelevant for the selection of the necessary security safeguards. An operating system provides no specific preventive measures against fire. Examination of threat T 0.1 Fire would bring no new aspects into the analysis as compared to T 0.25 "Failure of devices or systems".

Threat	Basic Parameters	Effect & Relevance	Comments
T 0.01 Fire	**Availability, Integrity**	**Indirect effect / Irrelevant**	The threat for an operating system due to fire is indirect, examination of threat T 0.1 *Fire* covered no new aspects in the analysis as compared to T 0.25 *Failure of devices or systems*. The indirect threat due to T 0.1 *Fire* is, among other threats, covered by T 0.25 *Failure of devices or systems*.
T 0.09 Failure or disruption of communication networks	**Availability, Integrity**	**Indirect effect / Irrelevant**	The threat for an operating system due to failure or disruption of communication networks is indirect, examination of threat T 0.9 brought no new aspects in the analysis as compared to T 0.26 *Malfunction of devices or systems*. An operating system provides no specific preventive measures against T 0.09, the threat is thus not relevant. No specific safeguards are necessary.
T 0.25 Failure of devices or systems	**Availability**	**Direct Effect / Relevant**	The threat T 0.26 *Malfunction of devices or systems* has a direct impact on an operating system. Therefore, safeguards against T 0.26 *Malfunction of devices or systems* have to be examined.
T 0.26 Malfunction of devices or systems	**Confidentiality, Availability, Integrity**	**Direct Effect / Relevant**	The threat T 0.25 *Failure of devices or systems* has a direct impact on an operating system. Therefore, safeguards against T 0.26 *Failure of devices or systems* have to be examined.

Table 5: Example for identifying supplementary elementary threats

In a subsequent brainstorming session, it should be checked whether all relevant threats have been identified this way, i.e. a completeness check carried out as described in BSI Standard 100-3 in Chapter 4, "Determination of additional threats." For this purpose, it is helpful to gather all relevant information about the audited subject e.g. from the Internet. It is also worthwhile to look up in the IT-Grundschutz catalogues, which existing modules cover subjects or approaches similar to those which need to be defined in a new module and how they do this. In addition, auxiliary materials on the IT-Grundschutz web pages should be consulted, to check whether similar issues are discussed in materials available there. On this basis, the threats described in the relevant existing modules should be viewed as well.

Subsequently, the elementary threats identified as relevant have to be consolidated with the threats from other modules or other sources, and summarised in a threat overview as clearly and accurately as possible.

5 Further Work Steps

According to [BSI3] the steps following Preparing the Threat Summary include the following further steps:

- *Determination of additional threats*
- *Threat assessment*
- *Handling risks*
- *Consolidation of the security concept*
- *Feedback to the security process*

To use the elementary threats, no methodological changes in these steps are required. When executing these steps, the elementary threats replace the specific threats. The examples previously presented in [BSI3] are tailored to the use of the specific risks but these can easily be replaced by the basic threats.

6 Bibliography

[BSI1] BSI-Standard 100-1: Information Security Management Systems (ISMS), Version 1.5, May 2008, *https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html*

[BSI2] BSI-Standard 100-2: IT-Grundschutz Methodology, Version 2.0, May 2008, *https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html*

[BSI3] BSI-Standard 100-3: Risk Analysis based on IT-Grundschutz, Version 2.5, May 2008, *https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html*

[GSK] IT-Grundschutz catalogues – Standard Security Safeguards, BSI, reissued annually, *https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html*