- **Module catalogue**
- **Threat catalogue**
- **Measures catalogue**

- **Module catalogue**
  - Generic Aspects
  - Infrastructure
  - IT-Systems
  - Networks
  - Applications
- **Threat catalogue**
  - Basic threats
  - Force Majeure
  - Organisational shortcomings
  - Human Error
  - Technical Failure
  - Deliberate Acts
- **Measures catalogue**
  - Infrastructure
  - Organisation
  - Personnel
  - Hardware and software
  - Communication
  - Contingency Planning

- **Module catalogue**
  - Generic Aspects
    B 1.0
    B 1.1
    B 1.2
    B 1.3
  - Infrastructure
  - IT-Systems
  - Networks
  - Applications
- **Threat catalogue**
  - Basic threats
    G 0.1
    G 0.2
    G 0.3
    G 0.4
  - Force Majeure
  - Organisational shortcomings
  - Human Error
  - Technical Failure
  - Deliberate Acts
- **Measures catalogue**
  - Infrastructure
    M 1.1
    M 1.2
    M 1.3
    M 1.4
  - Organisation
  - Personnel
  - Hardware and software
  - Communication
  - Contingency Planning

B 1.2 Personnel

Description

This module illustrates the generic IT-Grundschutz safeguards that should be implemented as standards in the area of personnel. A number of safeguards are necessary starting from the time the employees are hired and continuing until they leave the organisation. Adequate security safeguards also need to be implemented to handle external personnel such as visitors or maintenance technicians. Personnel recommendations that are linked to a specific role such as the appointment of a system administrator for a LAN are provided in the modules dealing with the corresponding topic.

Method recommendation

To secure the information system examined, other modules will need to be implemented in addition to this module. These modules are selected based on the results of the IT-Grundschutz modelling process.

A series of safeguards need to be implemented for the personnel employed at a company or a government agency, starting with proper training for new employees and further training and continuing right up to until an employee leaves the organisation. The steps to be followed in this case as well as the safeguards to be taken into consideration in the respective steps are listed in the following.

Sort by

Threats
Measures

Threats

- **Force majeure**
  - G 1.1 *Loss of personnel*
    - M 2.226 (A) *Procedures regarding the use of outside staff*
    - M 3.51 (Z) *Appropriate concept for assignment and qualification*
  - G 1.2 *Failure of the IT system*
- **Organisational shortcomings**
  - G 2.2 *Insufficient knowledge of rules and procedures*
  - G 2.7 *Unauthorised use of rights*
- **Human error**
  - G 3.1 *Loss of data confidentiality or integrity as a result of user error*
  - G 3.2 *Negligent destruction of equipment or data*
  - G 3.3 *Non-compliance with IT security measures*
    - M 3.4 (A) *Training before actual use of a program*
    - M 3.50 (Z) *Selection of employees*
  - G 3.8 *Improper use of the IT system*
  - G 3.9 *Improper IT system administration*
  - G 3.36 *Misinterpretation of events*
  - G 3.37 *Unproductive searches*
    - M 3.11 (A) *Training of maintenance and administration staff*
  - G 3.43 *Inappropriate handling of passwords or other authentication mechanisms*
  - G 3.44 *Carelessness in handling information*
  - G 3.77 *Insufficient acceptance of information security*
- **Deliberate acts**
  - G 5.1 *Manipulation or destruction of equipment or accessories*
  - G 5.2 *Manipulation of information or software*
  - G 5.20 *Misuse of administrator rights*
  - G 5.23 *Malicious software*
  - G 5.42 *Social Engineering*
  - G 5.80 *Hoax*
  - G 5.104 *Espionage*

G 3.3 Non-compliance with IT security measures

It is a relatively common occurrence that, due to negligence and insufficient checks, people fail to implement the security measures, either completely or in part, that have been recommended to them or that they are required to implement. This can cause damage which otherwise could have been prevented or at least minimised. Depending on the function of the person in question and the importance of the safeguard ignored, the resulting damage could even be very serious. Security safeguards are frequently disregarded due to the lack of awareness of security issues. A typical indicator of a lack of awareness is the ignoring of recurring error messages after a certain time once the users become accustomed to the error messages.

- Storing documents, DVDs, USB sticks or other information media in a locked desk does not adequately protect them against unauthorised access when the key is kept in the same office, e. g. on top of a cabinet or under the keyboard.
- Although it is widely known that the purpose of data backups is to minimise potential damage, it is still common for damage to be caused by the unintended deletion of data that subsequently could not be restored due to inadequate backups. This is indicated in particular by the cases of damage caused, for example, by malicious software reported to the BSI.
- Access to a computer centre is only supposed to be possible through a door protected by an access control system (e. g.authentication using a chip card reader, PIN or biometric procedures). However, the emergency exit door, which is not equipped with security mechanisms, is used as an additional entrance and exit even though it is only supposed to be opened in an emergency.
- In a z/OS system, batch jobs were run on a daily basis to back up the RACF database. The correct execution of these procedures was required to be checked daily by the responsible administrators. However, since the backups ran for several months without any problems, no one checked the backup procedure any more. Only after the RACF databases of the production system were defective and they wanted to restore the databases using the backups was it established that these batch jobs had not run for several days. The result was that there were no up-to-date backups available and the changes made during the last few days had to be entered subsequently by hand. In addition to the considerable amount of additional administrative work, this incident also introduced an uncertainty factor since it was impossible to reconstruct all definitions with certainty.
- In an organisation, it is prohibited to connect third party USB devices to the organisation's IT infrastructure. An employee does not find an official USB stick and instead connects his smartphone to the PC. However, this mobile IT was infected with malicious software (malware), resulting in unauthorised data leaks.

B 1.2 Personnel

Description

This module illustrates the generic IT-Grundschutz safeguards that should be implemented as standards in the area of personnel. A number of safeguards are necessary starting from the time the employees are hired and continuing until they leave the organisation. Adequate security safeguards also need to be implemented to handle external personnel such as visitors or maintenance technicians. Personnel recommendations that are linked to a specific role such as the appointment of a system administrator for a LAN are provided in the modules dealing with the corresponding topic.

Method recommendation

To secure the information system examined, other modules will need to be implemented in addition to this module. These modules are selected based on the results of the IT-Grundschutz modelling process.

A series of safeguards need to be implemented for the personnel employed at a company or a government agency, starting with proper training for new employees and further training and continuing right up to until an employee leaves the organisation. The steps to be followed in this case as well as the safeguards to be taken into consideration in the respective steps are listed in the following.

Sort by

Threats
Measures

Measures

- **Planning and design**
  - M 2.226 (A) *Procedures regarding the use of outside staff*
    - G 1.1 *Loss of personnel*
  - M 3.51 (Z) *Appropriate concept for assignment and qualification of employees*
  - - G 1.1 *Loss of personnel*
  - M 3.83 (Z) *Analysis of security-relevant personnel factors*
- **Procurement**
  - M 3.50 (Z) *Selection of employees*
    - G 3.3 *Non-compliance with IT security measures*
- **Implementation**
  - M 3.1 (A) *Well-regulated familiarisation/training of new staff with their work*
  - M 3.10 (A) *Selection of a trustworthy administrator and his substitute*
  - M 3.33 (Z) *Security vetting of staff*
  - M 3.55 (C) *Non-disclosure agreements (NDAs)*
- **Operation**
  - M 3.3 (A) *Arrangements for substitution*
  - M 3.4 (A) *Training before actual use of a program*
    - G 3.3 *Non-compliance with IT security measures*
  - M 3.5 (A) *Training on security safeguards*
  - M 3.7 (Z) *Point of contact in case of personal problems*
  - M 3.8 (Z) *Avoidance of factors impairing the organisation climate*
  - M 3.11 (A) *Training of maintenance and administration staff*
    - G 3.37 *Unproductive searches*
- **Disposal**
  - M 3.6 (A) *Regulated procedure for when employees leave the organisation*