**Annex D**

(informative)

## Vulnerabilities and methods for vulnerability assessment

### D.1 Examples of vulnerabilities

The following table gives examples for vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The lists can provide help during the assessment of threats and vulnerabilities, to determine relevant incident scenarios. It is emphasized that in some cases other threats may exploit these vulnerabilities as well.

|  |  |  |
| --- | --- | --- |
| **Types** | **Examples of vulnerabilities** | **Examples of threats** |
| Hardware | Insufficient maintenance/faulty installation of storage media | Breach of information system maintainability |
| Lack of periodic replacement schemes | Destruction of equipment or media |
| Susceptibility to humidity, dust, soiling | Dust, corrosion, freezing |
| Sensitivity to electromagnetic radiation | Electromagnetic radiation |
| Lack of efficient configuration change control | Error in use |
| Susceptibility to voltage variations | Loss of power supply |
| Susceptibility to temperature variations | Meteorological phenomenon |
| Unprotected storage | Theft of media or documents |
| Lack of care at disposal | Theft of media or documents |
| Uncontrolled copying | Theft of media or documents |
| Software | No or insufficient software testing | Abuse of rights |
| Well-known flaws in the software | Abuse of rights |
| No 'logout' when leaving the workstation | Abuse of rights |
| Disposal or reuse of storage media without proper erasure | Abuse of rights |
| Lack of audit trail | Abuse of rights |
| Wrong allocation of access rights | Abuse of rights |
| Widely-distributed software | Corruption of data |
| Applying application programs to the wrong data in terms of time | Corruption of data |
| Complicated user interface | Error in use |
| Lack of documentation | Error in use |
| Incorrect parameter set up | Error in use |
| Incorrect dates | Error in use |

|  |  |  |
| --- | --- | --- |
|  | Lack of identification and authentication mechanisms like user authentication | Forging of rights |
| Unprotected password tables | Forging of rights |
| Poor password management | Forging of rights |
| Unnecessary services enabled | Illegal processing of data |
| Immature or new software | Software malfunction |
| Unclear or incomplete specifications for developers | Software malfunction |
| Lack of effective change control | Software malfunction |
| Uncontrolled downloading and use of software | Tampering with software |
| Lack of back-up copies | Tampering with software |
| Lack of physical protection of the building, doors and windows | Theft of media or documents |
| Failure to produce management reports | Unauthorised use of equipment |
| Network | Lack of proof of sending or receiving a message | Denial of actions |
| Unprotected communication lines | Eavesdropping |
| Unprotected sensitive traffic | Eavesdropping |
| Poor joint cabling | Failure of telecommunication equipment |
| Single point of failure | Failure of telecommunication equipment |
| Lack of identification and authentication of sender and receiver | Forging of rights |
| Insecure network architecture | Remote spying |
| Transfer of passwords in clear | Remote spying |
| Inadequate network management  (resilience of routing) | Saturation of the information system |
| Unprotected public network connections | Unauthorised use of equipment |
| Personnel | Absence of personnel | Breach of personnel availability |
| Inadequate recruitment procedures | Destruction of equipment or media |
| Insufficient security training | Error in use |
| Incorrect use of software and hardware | Error in use |
| Lack of security awareness | Error in use |
| Lack of monitoring mechanisms | Illegal processing of data |
| Unsupervised work by outside or cleaning staff | Theft of media or documents |
| Lack of policies for the correct use of telecommunications media and messaging | Unauthorised use of equipment |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Site | | Inadequate or careless use of physical access control to buildings and rooms | | Destruction of equipment or media | | | |
| Location in an area susceptible to flood | | Flood | | |  |
| Unstable power grid | | Loss of power supply | | |  |
| Lack of physical protection of the building, doors and windows | | Theft of equipment | | |  |
| Organization | | Lack of formal procedure for user  registration and de-registration | | Abuse of rights | |  |  |
| Lack of formal process for access right review (supervision) | | Abuse of rights | |  |  |
| Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties | | Abuse of rights | |  |  |
| Lack of procedure of monitoring of  information processing facilities | | Abuse of rights | |  |  |
| Lack of regular audits (supervision) | | Abuse of rights | |  |  |
| Lack of procedures of risk identification and assessment | | Abuse of rights | |  |  |
| Lack of fault reports recorded in  administrator and operator logs | | Abuse of rights | |  |  |
| Inadequate service maintenance response | | Breach of  maintainability | | information | system |
| Lack or insufficient Service Level Agreement | | Breach of  maintainability | | information | system |
| Lack of change control procedure | | Breach of  maintainability | | information | system |
| Lack of formal procedure for ISMS documentation control | | Corruption of data | | |  |
| Lack of formal procedure for ISMS record supervision | | Corruption of data | | |  |
| Lack of formal process for authorization of public available information | | Data from untrustworthy sources | | | |
| Lack of proper allocation of information security responsibilities | | Denial of actions | | | |
| Lack of continuity plans | | Equipment failure | | | |
| Lack of e-mail usage policy | | Error in use | | | |
| Lack of procedures for introducing software into operational systems | | Error in use | | | |
| Lack of records in administrator and operator logs | | Error in use | | | |
| Lack of procedures for classified  information handling | | Error in use | | | |
| Lack of information security responsibilities in job descriptions | | Error in use | | | |
|  | | Lack or insufficient provisions (concerning information security) in contracts with employees | | Illegal processing of data | | | |
| Lack of defined disciplinary process in case of information security incident | | Theft of equipment | | | |
| Lack of formal policy on mobile computer usage | | Theft of equipment | | | |
| Lack of control of off-premise assets | | Theft of equipment | | | |
| Lack or insufficient 'clear desk and clear screen' policy | | Theft of media or documents | | | |
| Lack of information processing facilities authorization | | Theft of media or documents | | | |
| Lack of established monitoring  mechanisms for security breaches | | Theft of media or documents | | | |
| Lack of regular management reviews | | Unauthorised use of equipment | | | |
| Lack of procedures for reporting security weaknesses | | Unauthorised use of equipment | | | |
| Lack of procedures of provisions  compliance with intellectual rights | | Use of counterfeit or copied software | | | |