Information Security Management as a basis for data breach prevention

Isabel Münch
Bundesamt für Sicherheit in der Informationstechnik

EDPS/ENISA Data breach seminar
23 October 2009

Agenda

- Short overview BSI
- IT-Grundschutz approach
- Data Protection and IT-Grundschutz

The Federal Office for Information Security (BSI)

- Independent and neutral
- Founded in 1991 – unique as a public agency in comparison to other European institutions
- In the area of responsibility of the Federal Ministry for the Interior
- Staff: ~ 500 employees
- Budget: 64 million Euro (2009)
- R&D: 14 %

Bundesamt für Sicherheit in der Informationstechnik

BSI - The Information Security Service Provider for the German Government

15 Jahre IT-Grundschutz

In 2005, the Federal Cabinet passed an overall IT-security strategy, the “National Plan for Information Infrastructure Protection”

National Plan
for the Protection of Information Infrastructures

- **National Plan** Implementation Plan Federation
- **National Plan** Implementation Plan KRITIS

Secure Information Technology for our Society

Mission Statement

BSI

Positioning / Costumers:

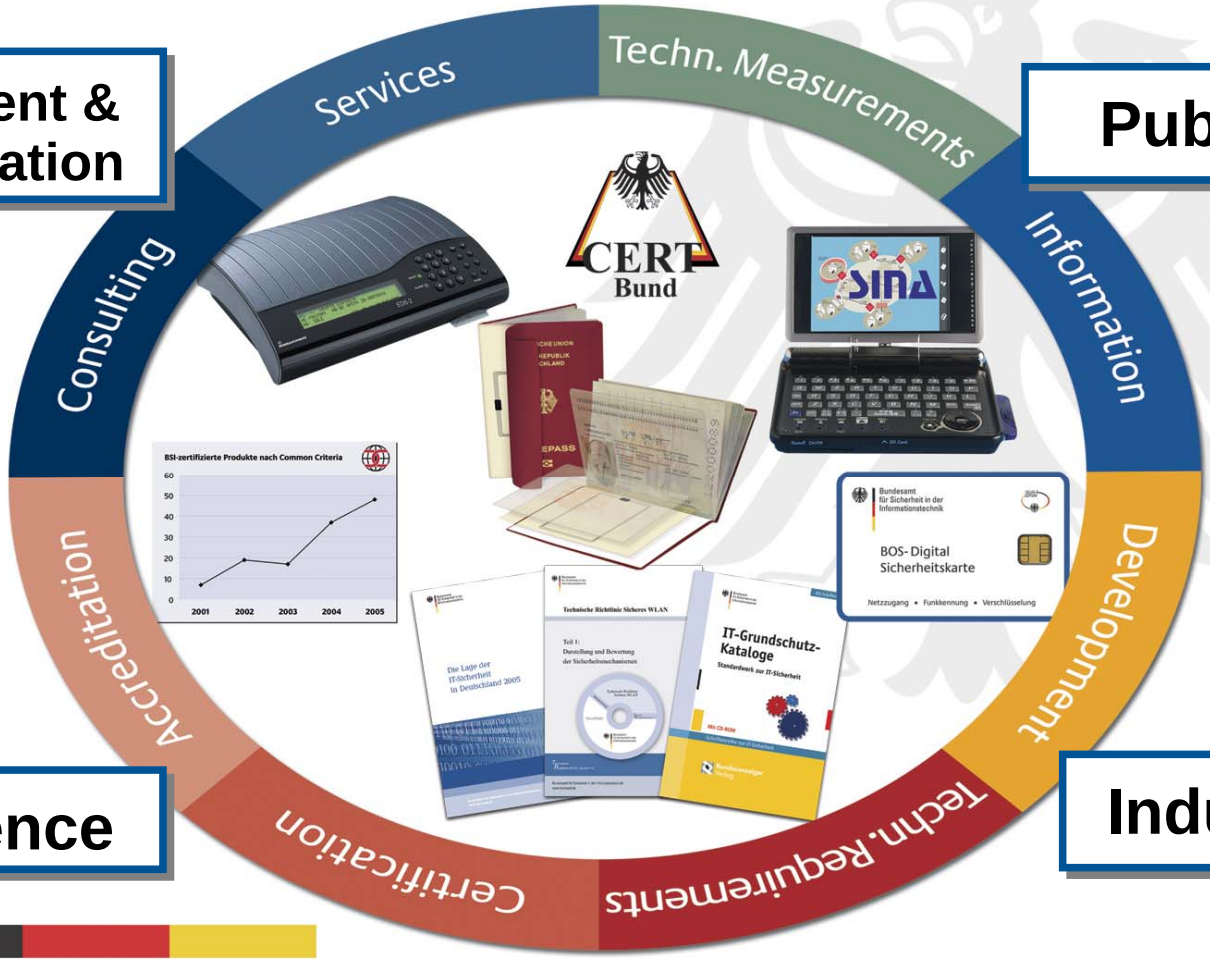
- Operational: federal authorities
- Cooperative: industry, science
- Informative: general public

Prevention **Reaction** **Sustainability**

Products and Services – Overview and Target Groups

Government & Administration

Public



Science

Industry

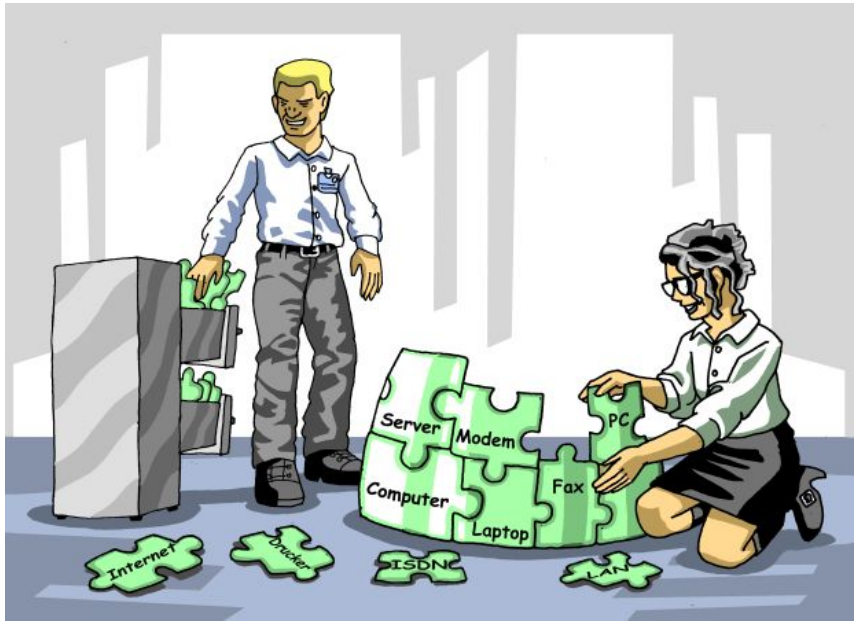
Information Security Management with IT-Grundschutz

The Challenge

- Increasing dependence on information processing.
- Ubiquitous and nomad computing.
- Decreasing time scales and zero-day exploits.
- Increasing complexity of information systems.
- Convergence of networks and technologies.

The Need

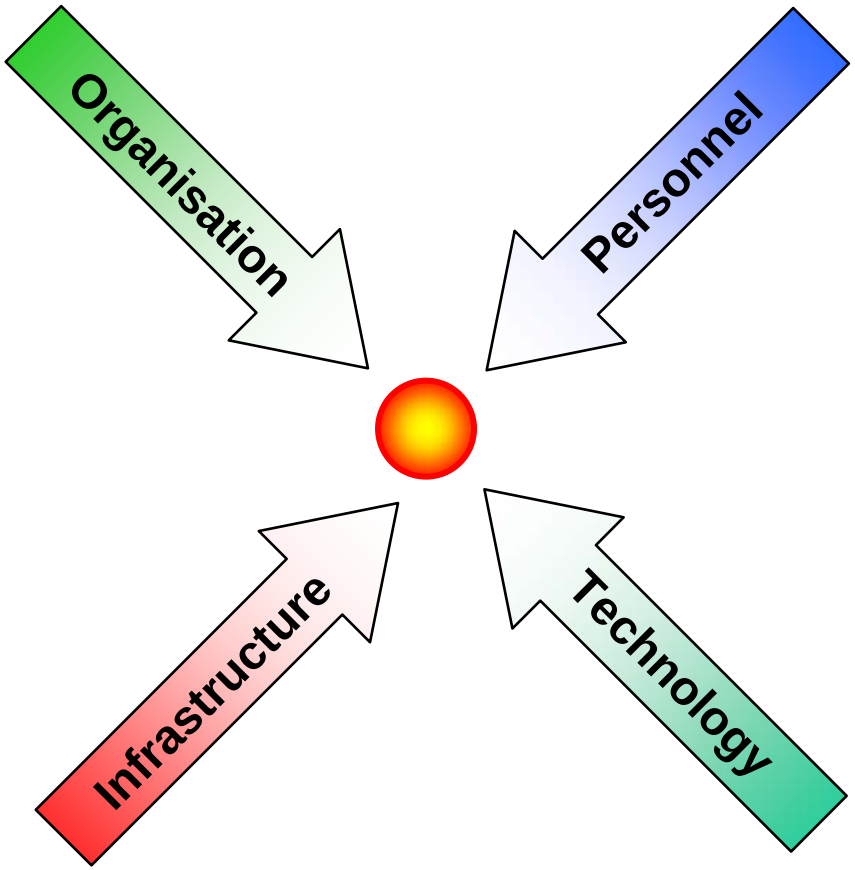
- We need ...
  - efficient
  - flexible
  - working
  - practical
  - potent
  - quick
- ... information security and risk management
- plus data protection management



IT-Grundschutz
- Basic Principles -

- Concentrate on typical components of business processes and information technology.
- Consider typical threat scenarios to determine the protection requirements.
- Provide catalogues of standard safeguards as countermeasures ("best practice").
- Cover technical as well as non-technical aspects ("holistic approach").
- Provide in-depth and reusable guidelines and recommendations.

IT-Grundschutz
- Different Aspects -



- Methodology for information security management.
- Holistic approach.
- Practical help for developing security concepts.
- Collection of typical threats and countermeasures.
- Standard for information security.
- Standard for risk analysis.

The Structure

BSI Standards on information security

BSI Standard 100-1:
Management Systems for Information Security (ISMS)

BSI Standard 100-2:
IT-Grundschutz Methodology

BSI Standard 100-3:
Risk Analysis based on IT-Grundschutz

BSI Standard 100-4:
Business Continuity Management

IT-Grundschutz Catalogues

Chapter 1: Introduction
Chapter 2: Layer model and modelling
Chapter 3: Roles
Chapter 4: Glossary

- **Catalogues of Modules**
  - Chapter B1 "Generic aspects"
  - Chapter B2 "Infrastructure"
  - Chapter B3 "IT systems"
  - Chapter B4 "Networks"
  - Chapter B5 "Applications"
- **Catalogues of Threats**
- **Catalogues of Safeguards**

IT-Grundschutz Catalogues

More than 70 Modules in 5 tiers:

B 1.0 Information security management

B 1.1 Organisation

B 1.2 Personnel

B 1.3 Business Continuity management

B 1.5 Data protection

B 1.6 Malware Protection

B 1.8 Incident Management

…

B 2.9 Data Centres

B 3.101 General Server

B 3.203 Laptop

…

IT-Grundschutz and Data Protection

Information Security Management and Data Protection Management: workflows and processes are very similar

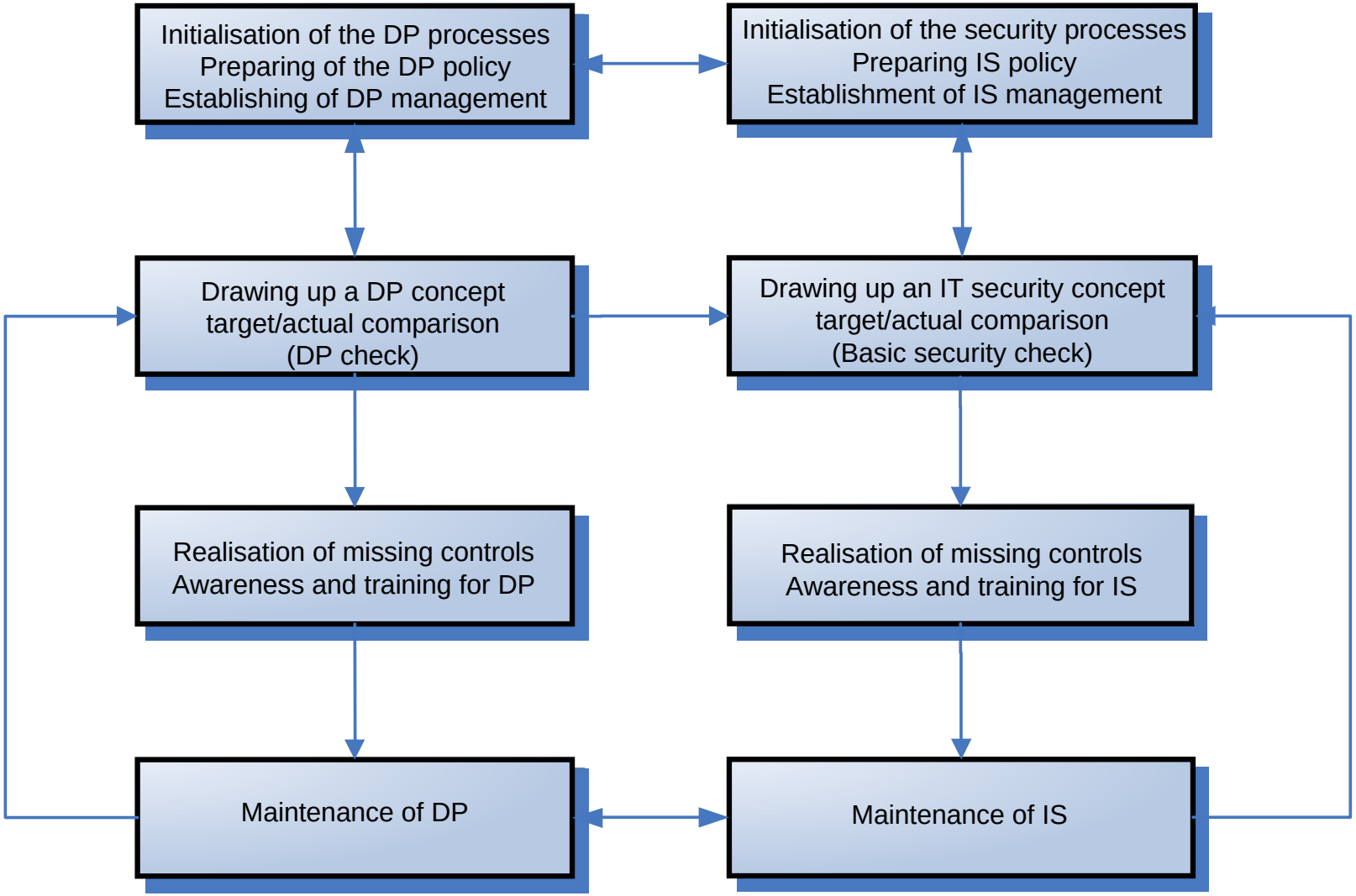
Core: data protection concept

- plus: registration requirements for the processing of personal data
- Determination of the legal framework and preliminary checks for the processing of personal data
- Selection of appropriate (organisational and technical) measures

Integration of data protection and data security management is possible

- e.g. in small organisations
- Take differences in the goals and the tasks into account

Data Protection and IT-Grundschutz



IT-Grundschutz and Data Protection

- Module "Data Protection" for the IT-Grundschutz Catalogues
- Created in Co-operation with the German Federal DP Commissioner, DP Commissioners of the Federal States and the DP Regulatory Agencies for private enterprises
- based on German law
- Integration of Data Protection aspects also in the BSI-Standards
- Module + Materials available on BSI website
- www.bsi.bund.de/grundschutz/baustein-datenschutz
- Thanks to Malta there is an english version!

Data Protection Module

Description and references to legal bases

Threat scenario:

- T 6.1 Missing legal grounds for the processing of personal data
- T 6.2 Violation of the purpose for which the data originally was collected / Violation of the "purpose binding principle"
- T 6.3 Violating the "necessity" principle of collecting only personal data when it is needed for the business process

...

- T 6.13 Missing or insufficient Data Protection auditing

Data Protection Module

Recommended safeguards:

Planning and Design

- S 7.1 (C) Management of Data Protection
- S 7.2 (B) Definition of Roles and Responsibilities Data Protection
- S 7.3 (A) Elements of a Data Protection Concept
- S 7.4 (A) Determination of the legal framework and preliminary checks for the processing of personal data
- S 7.5 (A) Establishment of state-of-the-art of technical-organisational controls when processing personal data

Data Protection Module

Recommended safeguards:

Implementation

S 7.6 (A) Declaration by / awareness training of personnel involved in the processing of personal data

S 7.7 (A) Organisational Procedures to protect the rights of the data subject during the processing of personal data

S 7.8 (A) Registration of procedures and fulfilment of registration requirements for the processing of personal data

...

Data Protection Module

Recommended safeguards:

Operations

- S 7.13 (A) Documentation of the Data Protection acceptability of the processing of personal data
- S 7.14 (A) Maintenance of Data Protection during operation
- S 7.15 (A) Data Processing-compliant disposal/destruction
- S 2.110 (A) Data privacy guidelines for logging procedures

Products and Services – IT-Grundschutz

- De-facto standard for information security in Germany and other countries
- Normal security requirements; basis for high level security requirements
- Applied by industry and administration as best practice

15 Jahre IT-Grundschutz

- **IT Grundschutz Catalogues**
- **BSI Standards (100-1 to 100-4)**
- **Web Based Training**
- **GSTOOL (Software)**
- **IT-Grundschutz Profiles**
- **IT Security Guidelines**
- **ISO 27001 Certificate**

Contact

Federal Office for Information Security (BSI)

Isabel Münch

Godesberger Allee 185-189
53175 Bonn
Germany

Phone: +49 228 99 9582 5367
E-Mail: isabel.muench@bsi.bund.de

IT-Grundschutz-Hotline:
Tel: +49 228 99 9582 5369
grundschutz@bsi.bund.de