IT-Sicherheitsmanagement als Unterstützung des DSB

Frank Reiländer, Berater IT-Sicherheit/Datenschutz
- Lizenzierter IT-Grundschutz-Auditor des BSI -
INFODAS GmbH, Rhonestr. 2, 50765 Köln
☎(0221) 70912-85 f.reilaender@infodas.de www.save-infodas.de

Überblick

Datenschutz im Unternehmen

- Welches IT-Sicherheitswissen sollte der DSB besitzen?
  - Datensicherheit = IT-Sicherheit?
- Anforderungen zur IT-Sicherheit gemäß BDSG und EU-Datenschutzrichtlinie
  - Legaldefinitionen und Ableitungen
- Effektive Umsetzung der notwendigen Datensicherheits-Anforderungen
  - Praxis der Aufsichtsbehörden
- Nutzung des IT-Grundschutzhandbuchs
  - Methodik und Werkzeugunterstützung
- Fallbeispiel Verfahrensverzeichnis
  - Transparenz und Darstellung

Was ist eigentlich Sicherheit?

- Beispiele aus dem Alltag:
  - Arbeitssicherheit → Schutz von Arbeitnehmern
  - Verkehrssicherheit → Schutz von Verkehrsteilnehmern
- Sicherheit beschreibt die Bemühungen zum Schutz vor nachteiligen Veränderungen
- **IT-Sicherheit** (Informationssicherheit) beschreibt den Schutz von Informationen („Inhalte eines IT-Systems“)
- **Datensicherheit** beschreibt den Schutz von spezifischen Informationen (personenbezogene Daten im Sinne des BDSG)

Zielsetzung der IT-Sicherheit

- Minimierung der Beeinträchtigung von Systemen, verarbeiteten Daten (Informationen) sowie der Datenverarbeitung (Funktionen und Prozesse) selbst hinsichtlich Bestand, Nutzung oder Verfügbarkeit
- Minimierung der Risiken, die beim Betrieb des IT-Systems entstehen.

„IT-Sicherheit ist der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.“ *

- Datensicherheit lässt sich mit Mitteln der IT-Sicherheit erreichen

* IT-Sicherheitshandbuch, Version 1.0, BSI 1992

Verlässlichkeit des IT-Systems – die technische Sicht

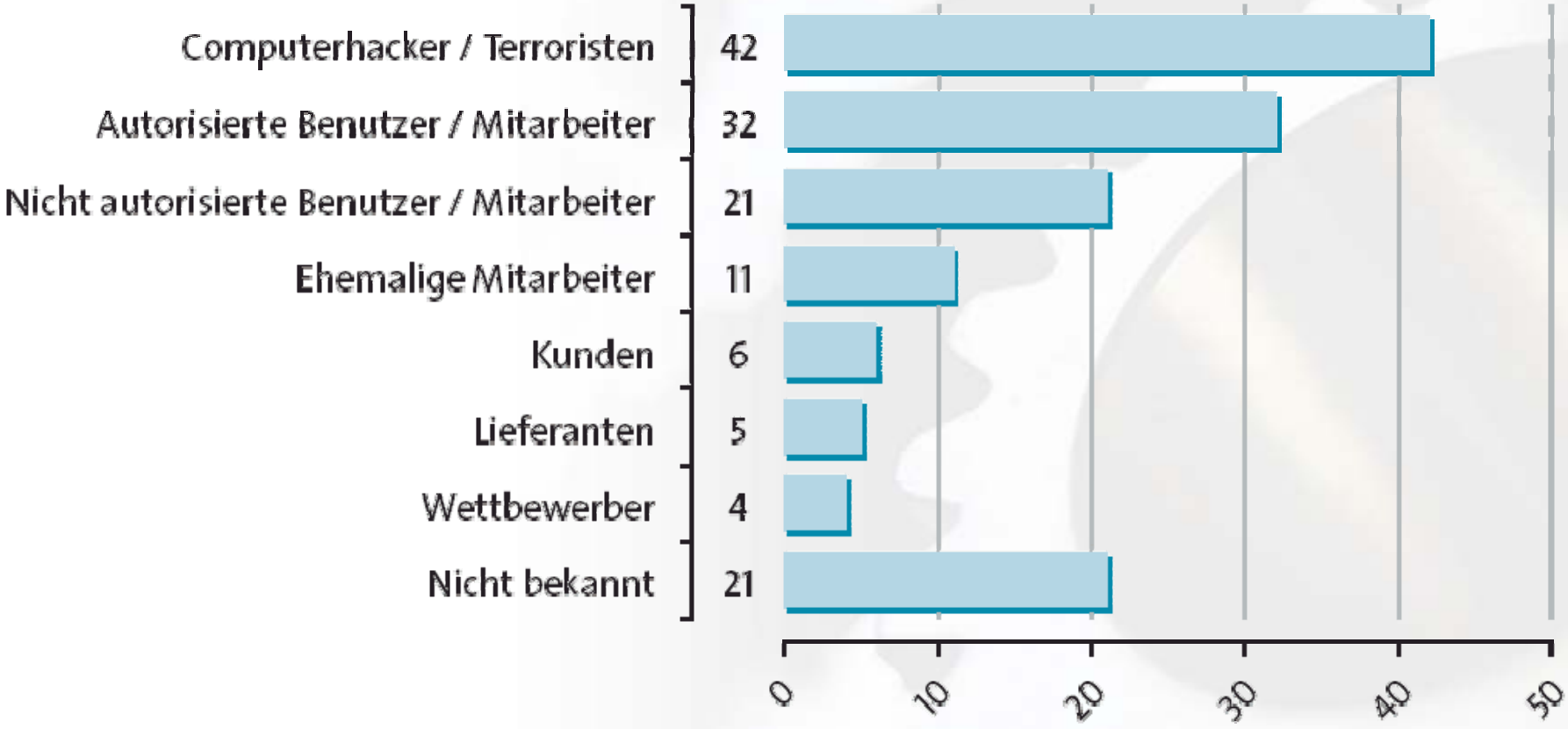
- Vertraulichkeit (confidentiality)
  - keine unbefugte Einsichtnahme in Daten
  - kein unbefugtes Erschließen von Daten
- Integrität (integrity)
  - keine unbefugte / unbemerkte Veränderung von Daten
  - keine unbefugte Veränderung von Funktionen des Systems
- Verfügbarkeit (availability)
  - Ausführung der Prozesse (Funktionen) des Systems zum vorgegebenen Zeitpunkt
  - Ablauf im vorgegebenen Zeitrahmen

Beherrschbarkeit des IT-Systems – die Sicht des Betroffenen

- Zurechenbarkeit (accountability)
  - Von jedem Prozess (jeder Funktion) und dessen Ergebnissen muss während seines Ablaufes oder danach feststellbar sein, welcher Instanz er zuzurechnen ist,
  - d. h. welche Komponente – u. a. auch welche Person – ihn ausgelöst oder verursacht hat.
- (Rechts-)Verbindlichkeit ((legal) liability)
  - Von jedem Prozess (jeder Funktion) und dessen Ergebnissen muss auch Dritten gegenüber beweiskräftig nachweisbar sein, welche Instanz ihn zu verantworten hat.

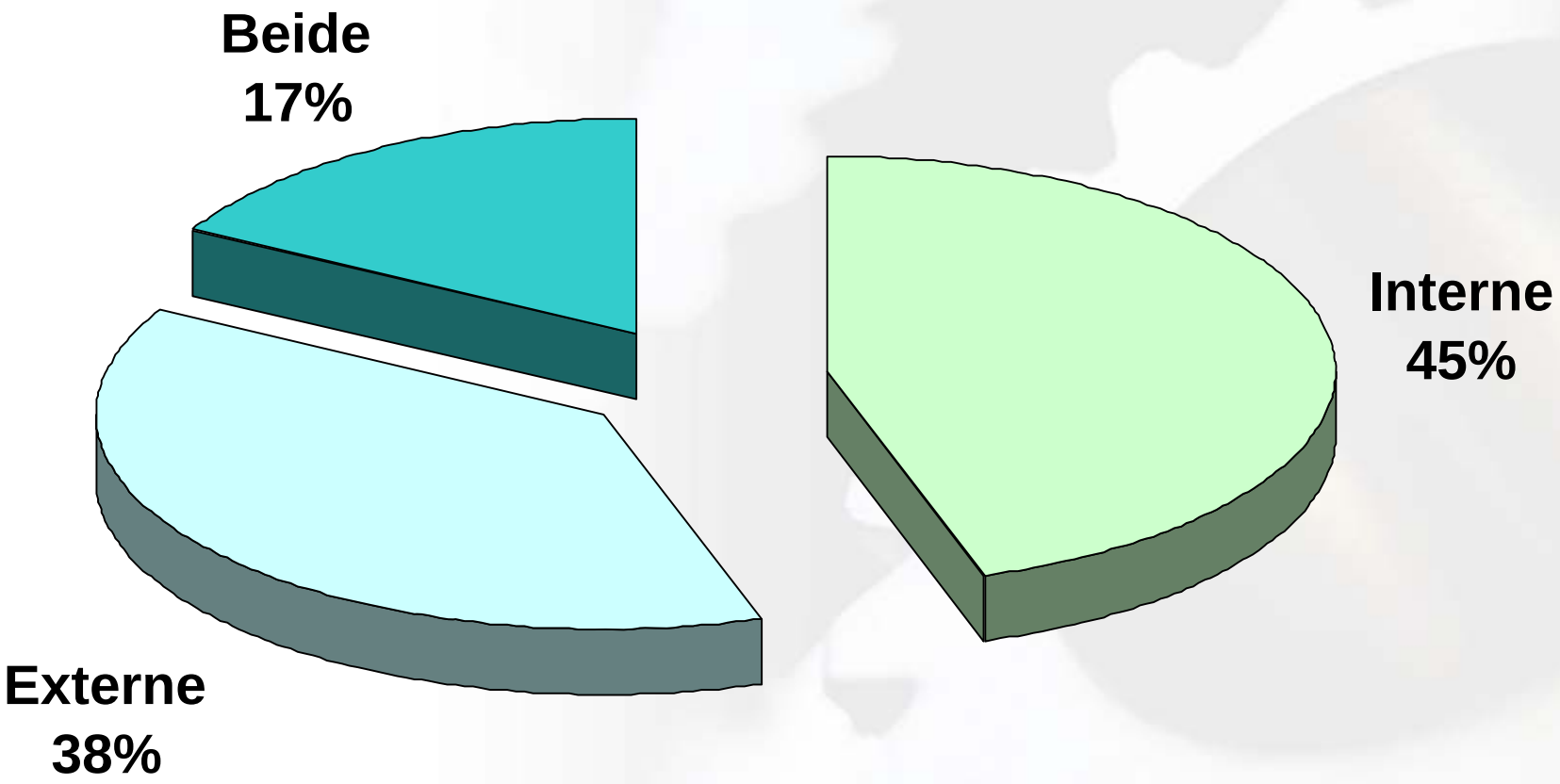
Verlässlichkeit und Beherrschbarkeit sind komplementäre Sichten des Begriffs IT-Sicherheit (duale Sicherheit*).

Verstöße – beabsichtigt/ungewollt



Quelle: Informationweek, IT Security 2002, Prozentwerte

Verstöße – Täterkreis



IT-Sicherheitswissen für den DSB

- Grundwerte der IT-Sicherheit
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Verbindlichkeit (Authentizität, Nicht-Abstreitbarkeit)
- IT-Sicherheit ist ein Prozess
  - Ganzheitliche Sicht auf die Systeme
  - Integration der Sicht des Betroffenen
  - Nutzung von Standards

Überblick

Datenschutz im Unternehmen

- Welches IT-Sicherheitswissen sollte der DSB besitzen?
  - Datensicherheit = IT-Sicherheit?
- Anforderungen zur IT-Sicherheit gemäß BDSG und EU-Datenschutzrichtlinie
  - Legaldefinitionen und Ableitungen
- Effektive Umsetzung der notwendigen Datensicherheits-Anforderungen
  - Praxis der Aufsichtsbehörden
- Nutzung des IT-Grundschutzhandbuchs
  - Methodik und Werkzeugunterstützung
- Fallbeispiel Verfahrensverzeichnis
  - Transparenz und Darstellung

Wer sagt mir, was zu tun ist?

- Betriebswirtschaftliche Vorgaben
  - Grundsätze ordnungsgemäßer DV-gestützter Buchführung (GoBS)
  - Handelsgesetzbuch (HGB) / Wirtschaftsprüfer
  - Aktiengesetz (AktG) bzw. GmbH-Gesetz (GmbHG)
- Risikomanagement
  - KonTraG / BASEL II
- Datenschutzrechtliche Vorgaben
  - EU-Datenschutzrichtlinie
  - Bundesdatenschutzgesetz (BDSG)
  - Landesdatenschutzgesetze
  - Sozial- und Kirchenvorschriften
  - Tele- und Mediendienste

Vorgaben der EU-Datenschutzrichtlinie

- Artikel 17 – Sicherheit der Verarbeitung
  - Maßnahmen zum Schutz der Daten
    - gegen zufällige oder unrechtmäßige Zerstörung
    - Unberechtigte Weitergabe
    - Unberechtigten Zugang
    - Jede Form der unberechtigten Verarbeitung
  - Auswahl des Auftragdatenverarbeiters unter Gesichtspunkten der technischen Sicherheitsmaßnahmen
  - Auftragsverarbeitung auf Weisung des Auftraggebers
  - Maßnahmen zur Beweissicherung
- Hierbei ist ein Höchstmaß an Schutz zu gewährleisten
  - Erwägungsgründe Nr. 10

Prinzipien des aktuellen BDSG

- Fokussierung auf elektronische Speicherung und Nutzung
- Aspekte der IT-gestützten Übermittlung
- Auftrags-DV und Outsourcing
  - technische/organisatorische Schutzmaßnahmen
- Prozesssicht
  - Dateiregister -> Verfahrensübersicht
- Systemdatenschutz
  - Datenvermeidung und -Sparsamkeit

Erweiterte Anforderungen BDSG2001

- Erweiterte Transparenz gegenüber dem Betroffenen
  - Erstellen einer öffentlichen Verfahrensübersicht
- Erweiterte Verarbeitungsbeschränkungen
  - Allgemeines Widerspruchsrecht
  - „Besondere Arten“ personenbezogener Daten
- Erweiterte Datenschutzkontrolle
  - Vorabkontrolle bei risikoreichen Verarbeitungen
- Einführung des Datenschutzaudits
  - Qualitätsmerkmal und –Kontrolle (freiwillig)

Stellenwert der IT-Sicherheits-Aspekte im Datenschutz

- Technische und organisatorische Maßnahmen (§9, Anlage zu §9 BDSG)
  - Datensicherungsmaßnahmen (BDSG 1990) -> Datensicherheitsmaßnahmen (BDSG 2001)
  - „Terminologie der IT-Sicherheit“ (Aussage BMI)
- Prozesssicht der Verarbeitung
  - Datei-Register -> Verfahrensübersicht
  - Widerspruchsrecht des Betroffenen
- Datenschutzkontrolle
  - Kontrolle der DV-Programme, Vorabkontrolle

Überblick

Datenschutz im Unternehmen

- Welches IT-Sicherheitswissen sollte der DSB besitzen?
  - Datensicherheit = IT-Sicherheit?
- Anforderungen zur IT-Sicherheit gemäß BDSG und EU-Datenschutzrichtlinie
  - Legaldefinitionen und Ableitungen
- Effektive Umsetzung der notwendigen Datensicherheits-Anforderungen
  - Praxis der Aufsichtsbehörden
  - Nutzung des IT-Grundschutzhandbuchs
  - Methodik und Werkzeugunterstützung
- Fallbeispiel Verfahrensverzeichnis
  - Transparenz und Darstellung

Anforderungen der Aufsichtsbehörden

- Prüfung der technischen und organisatorischen Maßnahmen
- Vorlage eines IT-Sicherheitskonzepts
  - Nicht nur bei Verankerung der Forderung im Gesetz (z. B. § 10, Abs. 3 DSG NRW)
- Erläuterungen zu den Sicherheitszielen
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Transparenz
  - Revisionssicherheit
- Empfehlungen zur Nutzung des IT-Grundschutzhandbuchs

IT-Grundschutzhandbuch

- Vorgehensweise zur Erstellung von IT-Sicherheitskonzepten
- Standard für IT-Sicherheit
- Maßnahmensammlung
- Nachschlagewerk

- www.bsi.bund.de/gshb

BSI Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutzhandbuch 2004

- 67 Bausteine
- 370 Gefährdungen
- 857 Maßnahmen
- 2909 Seiten

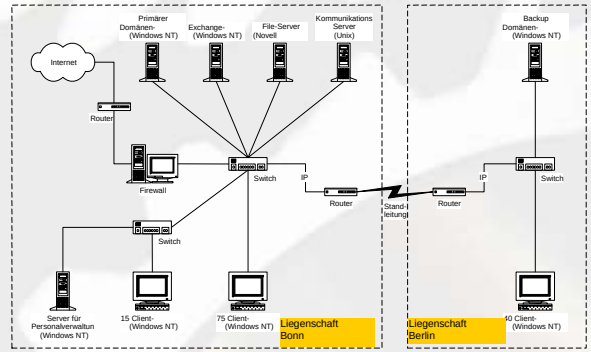
Bildquelle: BSI

Schritte zur IT-Sicherheit

- Schutzbedarfsanalyse
  - Analyse der IT-Struktur / Schutzobjekte
  - Analyse der zu schützenden Werte
- Bedrohungsanalyse und -bewertung
  - Analyse der Bedrohungssituation
  - Bewertung der Risiken
  - Entscheidung zur Abwehr von Bedrohungen
- Maßnahmenplanung
  - Auswahl geeigneter Maßnahmen
  - Bestimmung der Kosten
  - Bestimmung des Restrisikos

Ökonomische Vorgehensweise durch Soll-/Ist-Vergleich

IT-Grundschutz-Modell



Maßnahmen-empfehlungen

Soll-/Ist-Vergleich

Realisierte Maßnahmen

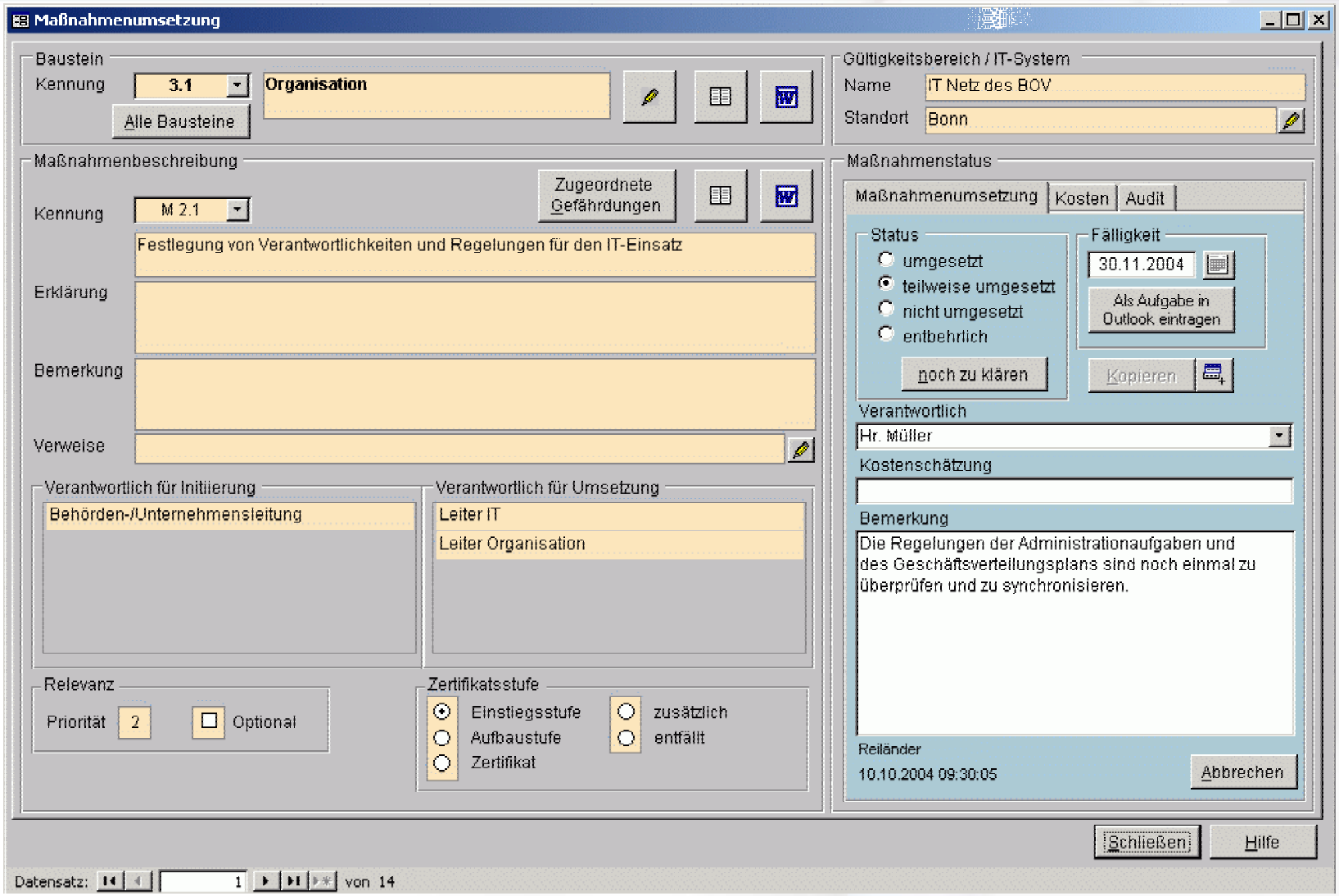
IT-Sicherheitskonzept:
defizitäre Maßnahmen

Quelle: BSI

Geeigneter Umgang mit Risiken

- Festlegung einer Grenze, bis zu der Risiko-Werte akzeptiert werden
  - genaue Festlegung der Grenzwerte in Abhängigkeit von der Werteverteilung
- Kategorisierung der bedrohten Objekte
  - Einteilung des Schutzbedarfs (niedrig/mittel <-> hoch/sehr hoch)
- Hauptrisiken müssen auf jeden Fall abgesichert werden
  - ggf. durch spezifische Schutzmaßnahmen
- Kombinierter Ansatz (combined approach)
  - Abdeckung der geringen Risiken durch Grundschutzmaßnahmen
  - oder auch Akzeptanz dieser Risiken

Werkzeugunterstützung im IT-Sicherheitsmanagement



Planung der Umsetzung (Plan ➢ Do ➢ Check ➢ Act)

Realisierungsplanung defizitärer Maßnahmen

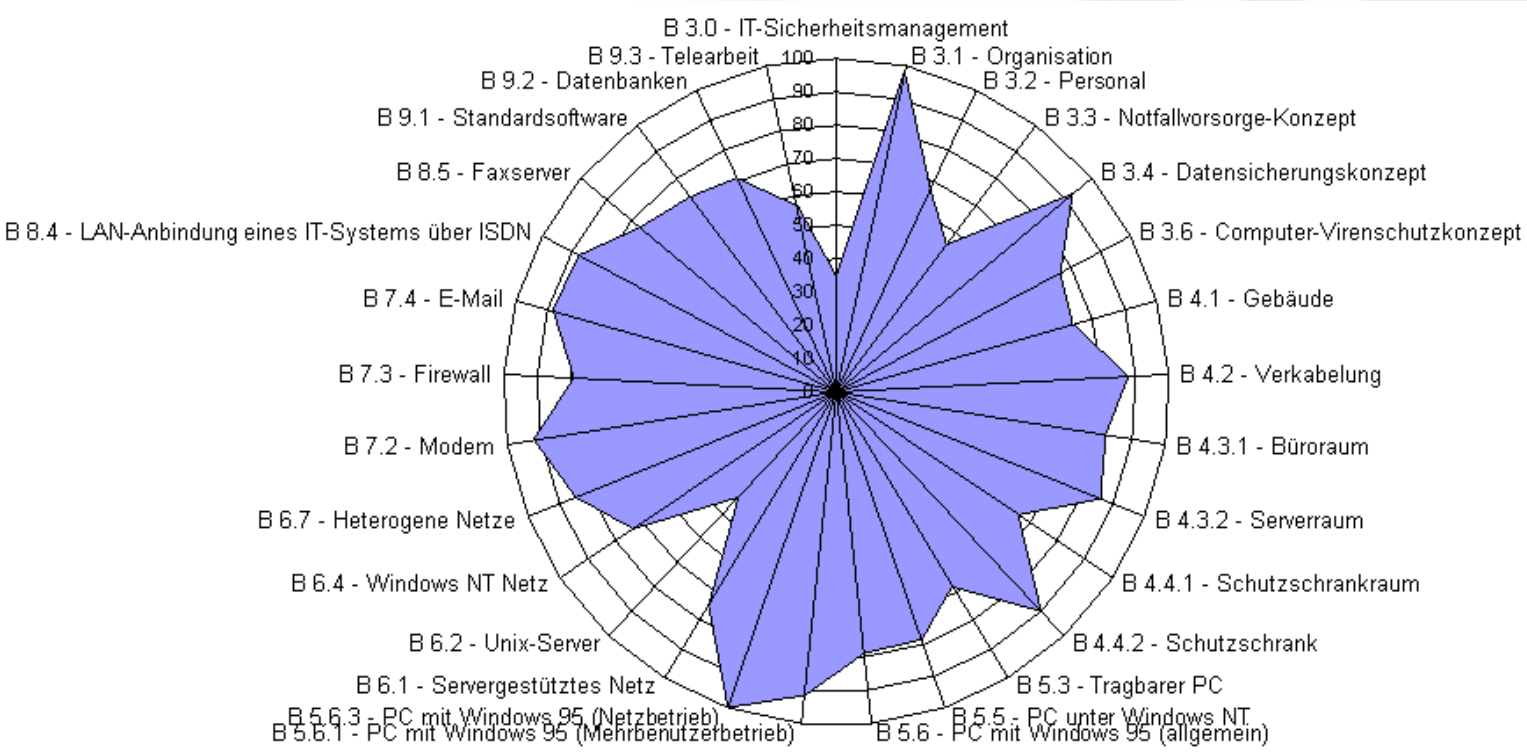
Datenbestand: Standort Bonn

Bundesamt für Organisation und Verwaltung (BOV)

Nr.	Beschreibung	Zertifikat	z.T.	Nein	fällig	verantwortlich	Bemerkungen	Kosten: Personalaufwand (PT) einmalig	Kosten: Personalaufwand (PT) pro Monat	Kosten: Sachkosten (€) einmalig	Kosten: Sachkosten (€) pro Monat
M 1.5	**Galvanische Trennung von Außenleitungen**										
4.1	Gebäude	zusätzlich	○	◉	30.04.2005	Hr. Lange	sollte über Elektro Müller realisert werden				€ 20.000,-
M 1.10	**Verwendung von Sicherheitstüren und -fenstern**										
4.1	Gebäude	zusätzlich	◉	○	31.03.2005	Hr. Assman	nur im Rechenzentrum, für Netzwerkräume nachrüsten				€ 8.000,-
M 1.13	**Anordnung schützenswerter Gebäudeteile**										
4.1	Gebäude	zusätzlich	○	◉			zu aufwendig				
M 1.14	**Selbsttätige Entwässerung**										
4.1	Gebäude	zusätzlich	○	◉			keine Wasserschäden zu erwarten				
M 1.17	**Pförtnerdienst**										
4.1	Gebäude	zusätzlich	○	◉	01.12.2004	Hr. Assman	Auftrag WuSG erweitern	3000 ,0		2.500 ,00	
M 1.18	**Gefahrenmeldeanlage**										
4.1	Gebäude	zusätzlich	○	◉			zurückgestellt				
M 1.19	**Einbruchsschutz**										
4.1	Gebäude	Aufbau	◉	○	31.03.2005	Hr. Assman	für Abt. I+K nachrüsten				€ 25.000,-
M 1.22	**Materielle Sicherung von Leitungen und Verteilern**										
4.2	Verkabelung	zusätzlich	○	◉	30.03.2005	Hr. Gebhart	Schließzylinder für Etagenverteiler				€ 5.000,-

Legende zur Maßnahmenumsetzung: "z.T.": teilweise umgesetzt - "Nein": nicht umgesetzt

Umsetzungsstand von IT-Grundschutzmaßnahmen



- Ergebnis eines Basis-Sicherheitschecks nach IT-Grundschutz-Handbuch (Praxisbeispiel)

Überblick

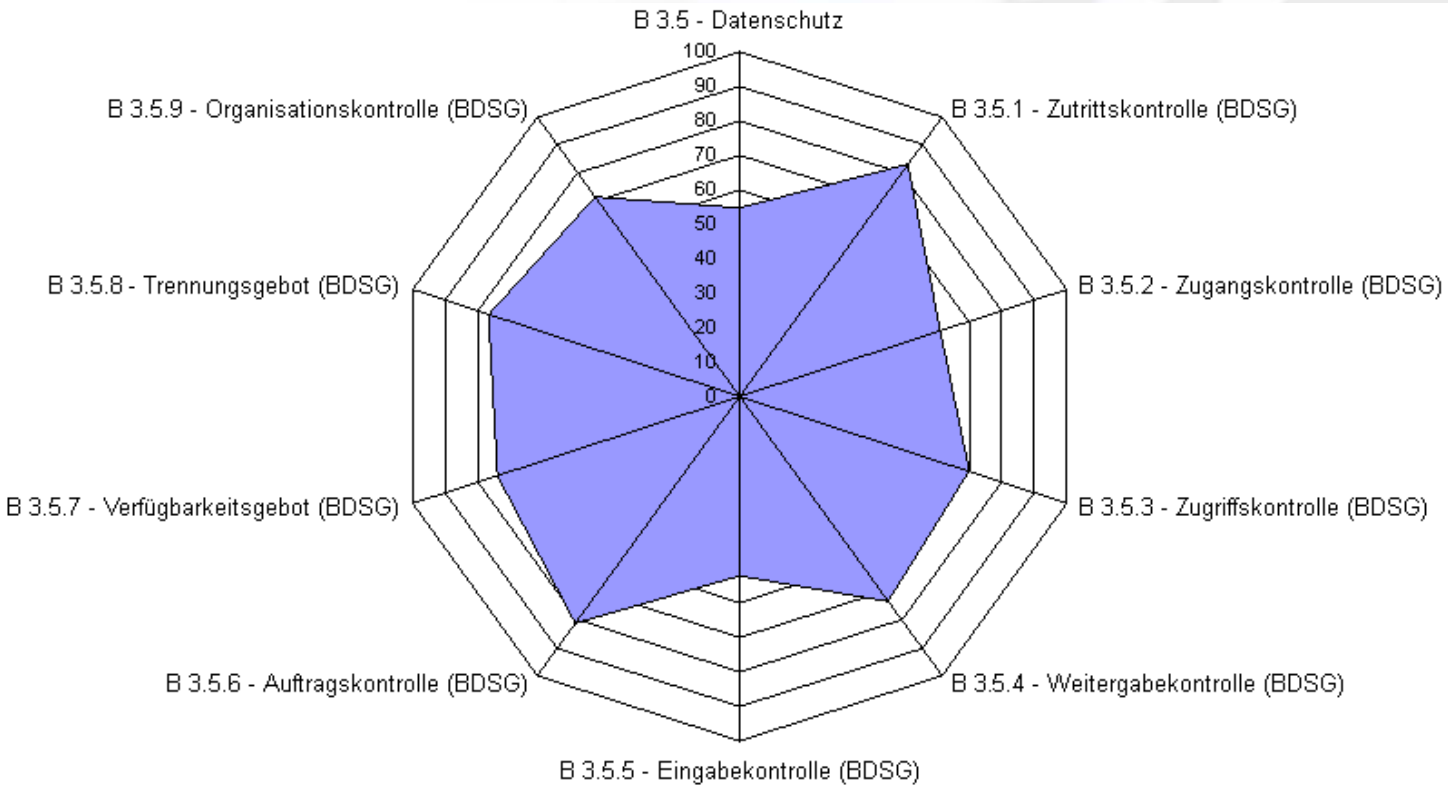
Datenschutz im Unternehmen

- Welches IT-Sicherheitswissen sollte der DSB besitzen?
  - Datensicherheit = IT-Sicherheit?
- Anforderungen zur IT-Sicherheit gemäß BDSG und EU-Datenschutzrichtlinie
  - Legaldefinitionen und Ableitungen
- Effektive Umsetzung der notwendigen Datensicherheits-Anforderungen
  - Praxis der Aufsichtsbehörden
  - Nutzung des IT-Grundschutzhandbuchs
  - Methodik und Werkzeugunterstützung
- Fallbeispiel Verfahrensverzeichnis
  - Transparenz und Darstellung

Abdeckung der Anforderungen des Verfahrensverzeichnisses

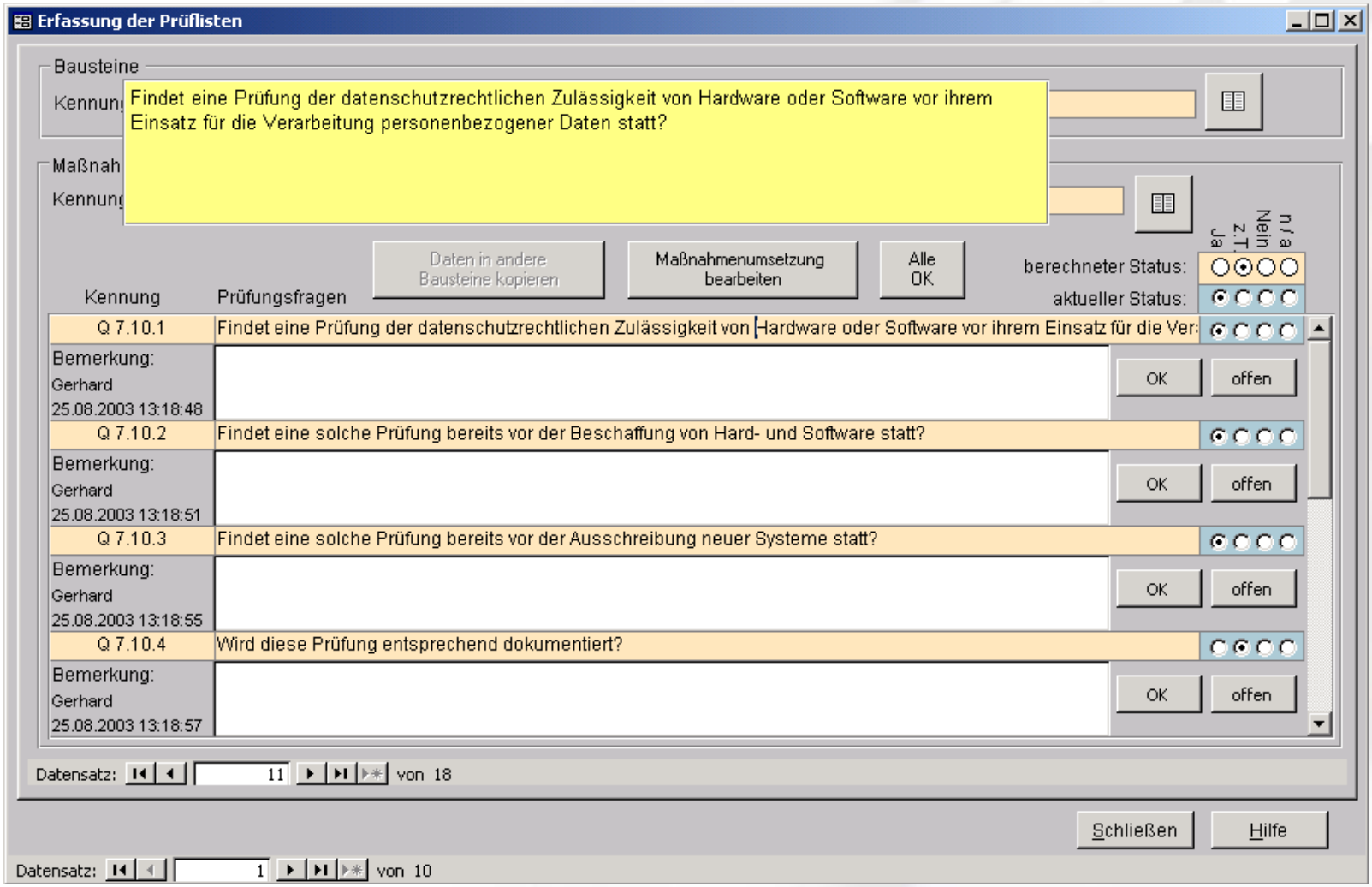
- Überblick über die Gesamtsituation der IT
  - Abdeckung durch die IT-Strukturanalyse im IT-Grundschutz-Vorgehen
- Meldepflicht gemäß § 4e BDSG
  - „allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach §9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind“
  - Bewertung des Schutzbedarfs (Schutzbedarfsanalyse)
  - Beschreibung der Umsetzung durch den Soll-Ist-Vergleich (Basis-Sicherheitscheck)
  - Übernahme der Sicht aus der IT-Grundschutz-Betrachtung

Datenschutz-Sicht als Ergänzung der IT-Sicherheits-Betrachtung



- Datensicherheitssicht auf Basis dieser Grundschutzerhebung (Praxisbeispiel)

Prüfung der Datenschutzorganisation



Fazit

- IT-Sicherheit und Datenschutz ergänzen sich in vielen Aspekten
- Synergiepotential gemeinsamer Bearbeitung
  - führt zu einheitlichen Bewertungsmaßstäben
  - erlaubt die Nutzung einer Werkzeugunterstützung
- Der Ansatz berücksichtigt gleichzeitig
  - Selbstkontrolle
  - Effizienz
  - Wirtschaftlichkeit
  - Transparenz

IT-Sicherheitsmanagement als Unterstützung des DSB

Vielen Dank für Ihre Aufmerksamkeit!

Ihre Fragen sind unsere Herausforderungen…

INFODAS GmbH, Rhonestraße 2, D-50765 Köln
info@save-infodas.de oder www.save-infodas.de