Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein

Anstalt des öffentlichen Rechts

Sommerakademie 2013

Datenschutz- und IT-Sicherheitsmanagement (ISMS)

als Grundlage für Big Data

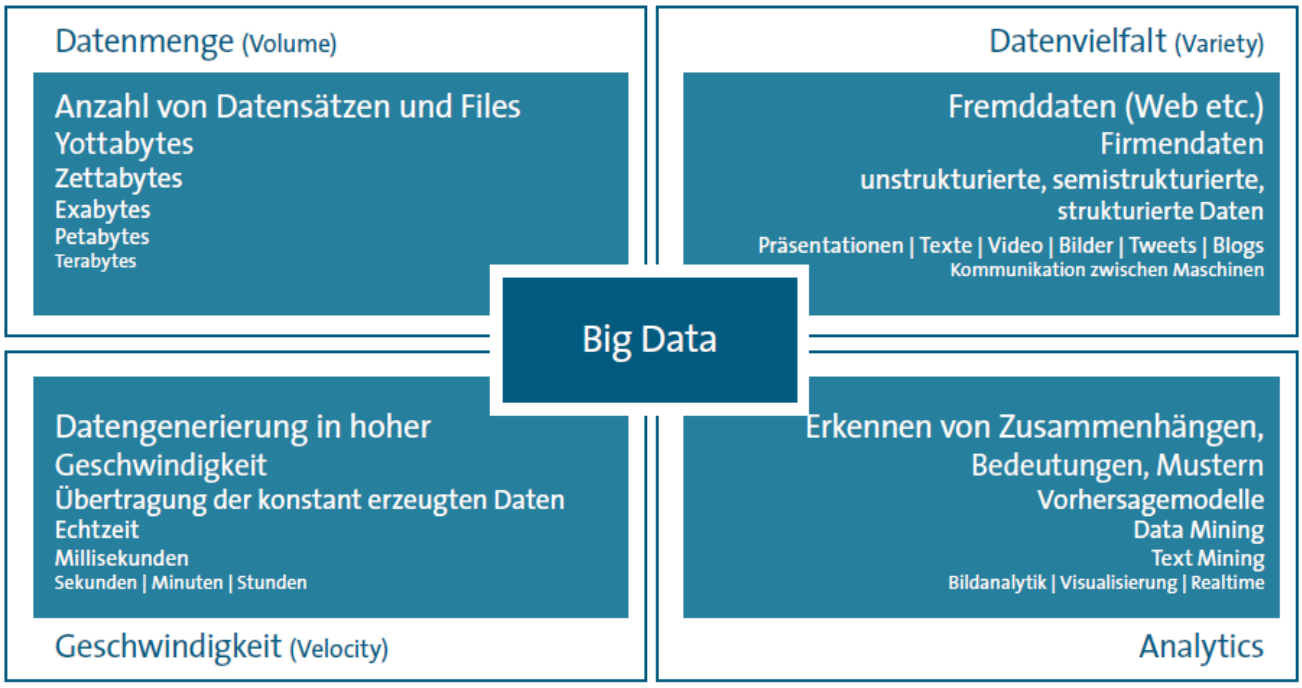
Heiko Behrendt
ISO 27001 IT-Grundschutzauditor
Fon: 0431 988 1212
Mail: behrendt@datenschutzzentrum.de
Web: www.datenschutzzentrum.de

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Themen

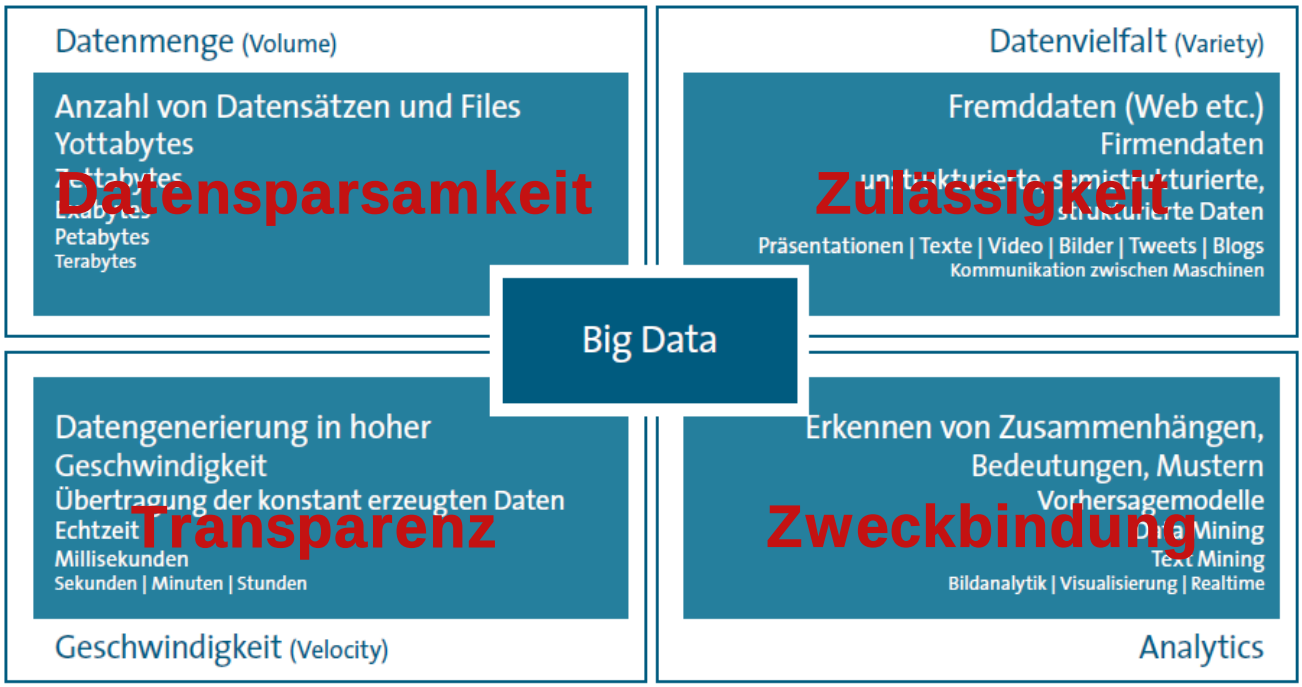
- Big Data? Aber bitte mit Datenschutz!
- Mit Methode zum Big-Data-Erfolg
- Ohne ISMS kein ausreichender Schutz der Daten
- Anforderungen für ein ISMS
- Aufgaben des Datenschutz- und IT-Sicherheitsbeauftragten
- Technische und organisatorische Maßnahmen
- Datenschutz-Audit
- Prüfpunkte für ein Big-Data-Verfahren

Big Data? Aber bitte mit Datenschutz!



Quelle: BITKOM Leitfäden Big Data im Praxiseinsatz, Management von Big Data Projekten

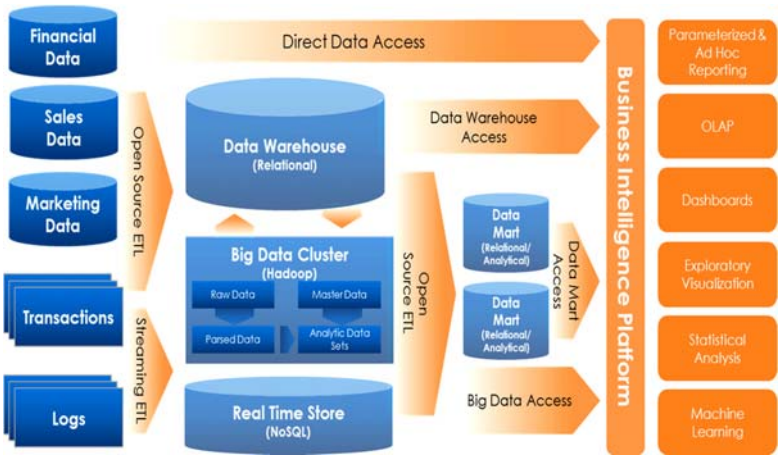
Big Data? Aber bitte mit Datenschutz!



Big Data? Aber bitte mit Datenschutz!

Big-Data-Verfahrensmodule

- Hard- und Software
- Dateisystem
- Datenquellen
- Datenbanken
- Datenflussplan
- Entwicklung
- Nutzer
- Auswertung



Quelle: www.openbi.com

IT-Infrastruktur, Sicherheitsstandard, Vorschriften, Verträge

www.datenschutzzentrum.de

Big Data? Aber bitte mit Datenschutz!

Big-Data-Merkmale

- Echtzeit
- Datenmenge
- Nicht verdichtete Daten
- Unstrukturierte Daten
- Datensegmentierung
- Muster-, Trenderkennung
- Vorhersagen, Prognosen
- Sofortergebnisse

Kundendaten auswerten und Echtzeitanalysen

Quelle: www.t-systems.de

Mit Methode zum Big-Data-Erfolg

Big Data wird nur zum Erfolg, wenn die rechtliche Zulässigkeit des Verfahrens gegeben ist.

- Phase 1: Planung **wenn okay, dann**
  - Anforderungen, Ziele
  - Pflichtenheft
  - Datenprofile
  - Datenquellen
  - Datenanalyse
  - Datenschutzkonzept
  - Betriebsrat
  - ...

Kontrolle

- Phase 2: Entwicklung
- Phase 3: Test und Freigabe
- Phase 4: Produktion
- Phase 5: Änderungen
- Phase 6: Außerbetriebnahme
- ggf. Audit, Zertifizierung

Mit Methode zum Big-Data-Erfolg

Die Rahmenbedingungen geben vor, in welcher Form die Datenverarbeitung ausgestaltet werden kann.

- Unternehmens- bzw. Geschäftswerte
- Ziele der Geschäftsführung
- Verantwortlichkeiten und Prozesse in der DV
- Transparenz über den Einsatz von Applikationen und Daten
- Interne Regelungen / Compliance
- Vertragsregelungen mit Kunden
- Gesetzliche Vorschriften

Ohne ISMS kein ausreichender Schutz der Daten

Schwachstellen in einem Unternehmen

1. Die Geschäftsführung ist nicht ausreichend sensibilisiert.
2. Ein Datenschutz- und IT-Sicherheitsmanagement ist nicht eingerichtet.
3. Datenschutz- und Sicherheitsvorfälle werden nicht erkannt.
4. Ein Datenschutz- bzw. IT-Sicherheitskonzept ist nicht vorhanden.
5. Die IT-Dokumentation ist unzureichend.

---

6. IT-Strukturen sind nicht nachvollziehbar.
7. Daten werden unstrukturiert verwaltet und nicht gelöscht.
8. Vergebene Berechtigungen auf IT-Komponenten sind nicht transparent.
9. Akten und elektronische Datenträger sind nicht ausreichend geschützt.
10. Dienstleister haben uneingeschränkten Zugriff auf interne Systeme.

ULD www.datenschutzzentrum.de

Ohne ISMS kein ausreichender Schutz der Daten

... noch mehr Schwachstellen!

11. Clients und Server sind nicht gehärtet.
12. Fachverfahren werden nicht ausreichend getestet und freigegeben.
13. Administrative Aktivitäten werden nicht protokolliert.
14. Beschäftigte sind in Bezug auf Datenschutz nicht geschult.
15. Sicherheitsrelevante Systemprotokolle werden nicht ausgewertet.
16. Für den Einsatz mobiler Geräte gibt es keine Sicherheitsvorgaben.
17. Die Netzstrukturen im Unternehmen sind nicht segmentiert.
18. Die Auftragsdatenverarbeitung wird ohne Kontrolle durchgeführt.
19. E-Mail und Web werden nicht ausreichend abgesichert.
20. Die Daten auf Digitalkopierern werden nicht ausreichend geschützt.
21. ...

Anforderungen für ein ISMS

Ein angemessenes Sicherheitsniveau ist in erster Linie abhängig vom systematischen Vorgehen.

- Datenschutz- und IT-Sicherheitsstrategie festlegen
- Zuständigkeiten für das ISMS definieren
- Bestandsaufnahme durchführen
- Sicherheitskonzept mit Sicherheitsmaßnahmen erstellen
- Datenschutz- und IT-Sicherheitsprozesse integrieren
- Sicherheitsmaßnahmen umsetzen
- Revision und Kontrolle durchführen

Anforderungen für ein ISMS

Aufgaben und Pflichten der Geschäftsführung sind Kernbestandteil des ISMS.

- Übernahme der Gesamtverantwortung für Informationssicherheit
- Informationssicherheit integrieren
- Informationssicherheit steuern und aufrechterhalten
- Erreichbare Ziele setzen
- Vorbildfunktion

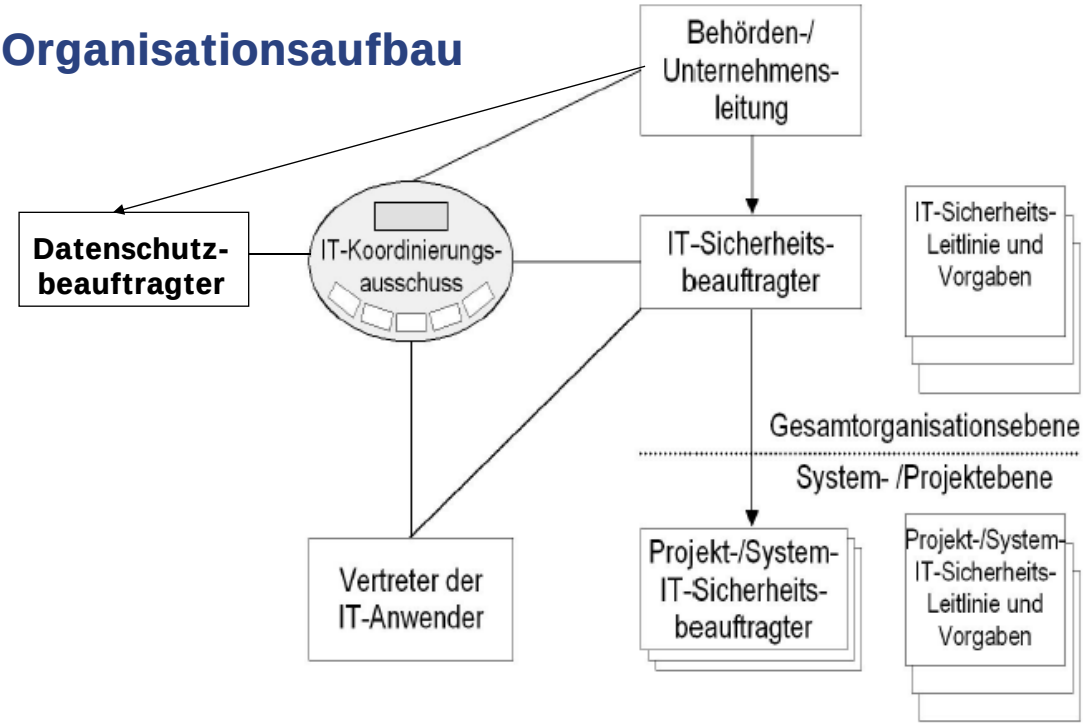
Anforderungen für ein ISMS

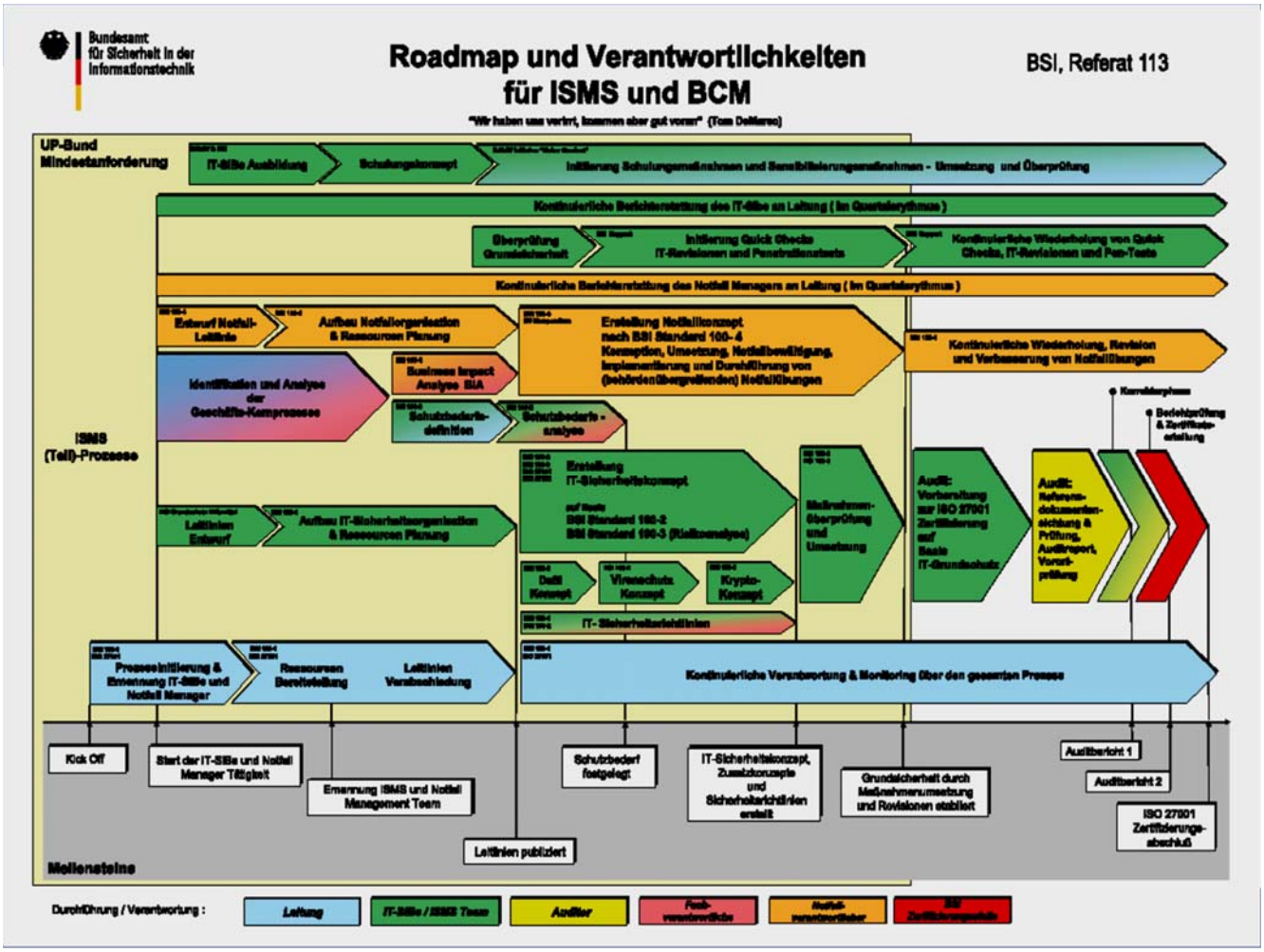
Die Unternehmensgröße und die Komplexität der Datenverarbeitung bestimmen die Parameter für die Ausgestaltung des ISMS.

- Geschäftsführung
- IT-Sicherheitsbeauftragter
- Datenschutzbeauftragter
- IT-Sicherheitsmanagement-Team
- Datenverantwortliche der Fachbereiche
- Fachbereichsbezogene IT-Sicherheitsbeauftragte

Anforderungen für ein ISMS

Organisationsaufbau





Aufgaben des Datenschutzbeauftragten

Der Datenschutzbeauftragte sorgt für die rechtliche Zulässigkeit der Datenverarbeitung im Unternehmen.

- Unterstützung und Beratung der Fachbereiche
- Überwachung und Kontrolle der Einhaltung der Vorschriften
- Unterrichtung der Beschäftigten über Datenschutz
- Mitwirkung bei der Umsetzung von Sicherheitsmaßnahmen
- Führung des Verfahrensverzeichnisses
- Durchführung der Vorabkontrolle
- ...

Aufgaben des IT-Sicherheitsbeauftragten

Der IT-Sicherheitsbeauftragte sorgt für die IT-Sicherheit der Datenverarbeitung im Unternehmen.

- Sicherheitsrelevante Projekte koordinieren
- IT-Sicherheitsprozess steuern
- Erstellung des IT-Sicherheitskonzepts
- Realisierung und Überprüfung der IT-Sicherheitsmaßnahmen
- Zusammenarbeit mit dem IT-Sicherheitsmanagement-Team
- Untersuchung von IT-Sicherheitsvorfällen
- ...

Aufgaben des IT-Sicherheitsmanagement-Teams

Das IT-Sicherheitsmanagement-Team unterstützt den Datenschutz- und IT-Sicherheitsbeauftragten bei der Umsetzung der Aufgaben.

- Datenschutz- und IT-Sicherheitsziele bestimmen
- IT-Sicherheitsprozess initiieren, steuern und kontrollieren
- Umsetzungsstand der IT-Sicherheit prüfen
- Maßnahmen für festgestellte Abweichungen entscheiden
- Datenschutz- und IT-Sicherheitsvorfälle bearbeiten
- ...

Technische und organisatorische Maßnahmen (TOM)

Sicherheitskonzept

Inhaltsverzeichnis

I. Grundlagen und Aufbau
1. Zielrichtung
2. Zuständig- und Verantwortlichkeiten
3. Überwachung
4. Fortschreibung

II. Schutzbedarf / Gefährdungen
1. Höhere Gewalt
2. Organisatorische Mängel
3. Menschliche Fehlhandlungen
4. Technisches Versagen
5. Vorsätzliche Handlungen

III. TOMs für die allgemeine Datenverarbeitung
1. Schulung der Mitarbeiter
2. Tür- und Fenstersicherung
3. Aktenführung und Aktenaufbewahrung
4. Archiv und Aufbewahrungsfristen
5. Reinigungspersonal
6. Publikumsverkehr
7. Auskünfte, Datenübermittlung

IV. TOMs für die automatisierte Datenverarbeitung
1. Zuständigkeiten
2. Betriebssicherheit
3. Server
4. Arbeitsstation
5. Datenbestände
6. Datensicherung
7. Externe Datenträger
8. Arbeitsumgebung
9. Nutzung der IT-Geräte
10. Nutzung der Verfahren
11. Systemprotokollierung
12. Verfahrensdokumentation
13. Externe Dienstleister

V. TOMs für die Internetnutzung
1. Allgemein
2. Firewall
3. E-Mail
4. WWW

VI. Restrisikoanalyse
1. Verfügbarkeit der Systeme
2. Integrität der Software und der Daten
3. Internet-Dienste

Datenschutz-Audit

Audits stellen sicher, dass das im IT-Sicherheitskonzept festgelegte IT-Sicherheitsniveau eingehalten wird.

- Überprüfung der Datenverarbeitung
- Durchführung von Stichproben
- Festlegung des Prüfbereichs
- Soll-Ist-Abgleich der Sicherheitsmaßnahmen
- Dokumentation der Ergebnisse
- Beseitigung von Abweichungen

- Öffentliche Stellen können ihr Datenschutzkonzept durch das ULD prüfen und beurteilen lassen

Prüfpunkte für ein Big-Data-Verfahren

Checkliste

1. Sind die Ziele von der datenverantwortlichen Ebene festgelegt worden?
2. Erfolgt die Datensammlung/-verarbeitung unter Berücksichtigung der einzuhaltenden gesetzlichen und/oder vertraglichen Regelungen?
3. Für welchen Zweck sollen die Daten genutzt werden?
4. Welche Sensibilität haben die Daten und wie viel Schutz ist erforderlich?
5. Sind die Daten anonymisiert und besteht keine Möglichkeit der Identifizierbarkeit von Personen?
6. Werden bei einer personenbezogenen Datenverarbeitung keine schutzwürdigen Interessen von Betroffenen beeinträchtigt?
7. Wie wird die Integrität des Verfahrens sichergestellt?
8. Gibt es ein Test- und Freigabeverfahren?
9. Wer prüft die datenschutzrechtliche Zulässigkeit?
10. Wer hat Zugriff auf die Daten; gibt es ein Berechtigungskonzept?

ULD www.datenschutzzentrum.de

Prüfpunkte für ein Big-Data-Verfahren

Checkliste

11. Welche IT-Komponenten (Hard- und Software) kommen zum Einsatz?
12. Wie sollen die Ergebnisse in die vorhandenen Geschäftsprozesse eingebunden werden?
13. Welche Datenquellen liefern welche Daten?
14. Ist der Datenabruf/die Datenauswertung einmalig oder kontinuierlich?
15. Werden die Daten aus den Datenquellen exportiert oder werden sie online abgerufen?
16. Sind Zuständig- und Verantwortlichkeiten festgelegt worden?
17. Wird protokolliert bzw. ist nachvollziehbar, wann welche Daten verwendet werden/wurden?
18. Welche rechtlichen Vorschriften und Vertragsregelungen gelten für die einbezogenen Fachverfahren/Datenquellen?
19. Wer administriert die Schnittstellen und die „Auswertungssoftware“?
20. Werden externe Dienstleister eingesetzt und/oder liegt eine Auftragsdatenverarbeitung vor?
21. ...

Leitfäden zum ISMS und zu Big Data

BSI: Managementsysteme für Informationssicherheit (ISMS)

BSI: Überblick IT-Grundschutz, Entscheidungshilfe für Manager

FUJITSU: White Paper Lösungsansätze für Big Data

IBM: Analytics - Big Data in der Praxis

BITKOM: Big Data im Praxiseinsatz – Szenarien, Beispiele, Effekte

BITKOM: Management von Big-Data-Projekten

TNS INFRATEST: Quo vadis Big Data

ULD: Big Data und Datenschutz

Vortrag: www.datenschutzzentrum.de

Begriffsdefinitionen

Das **Information Security Management System** (**ISMS)** ist eine Aufstellung von Verfahren und Regeln innerhalb eines Unternehmens, welche dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

business continuity management (BCM) bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden – zu schützen bzw. alternative Abläufe zu ermöglichen.

Die internationale Norm **ISO/IEC 27001** *Information technology – Security techniques – Information security management systems – Requirements* spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.

Unter **Data-Mining** versteht man die systematische Anwendung statistischer Methoden auf einen Datenbestand mit dem Ziel, *neue* Muster zu erkennen. Data Mining erlaubt das automatisierte Durchsuchen von Daten nach Mustern, Modellen oder Abweichungen.

Ein **Data-Warehouse** (**DWH**) ist eine Datenbank, in der Daten aus unterschiedlichen Quellen in einem einheitlichen Format zusammengefasst werden (Informationsintegration).

Apache Hadoop ist ein freies, in Java geschriebenes Framework für skalierbare, verteilt arbeitende Software. Es basiert auf dem bekannten MapReduce-Algorithmus von Google Inc. sowie auf Vorschlägen des Google-Dateisystems und ermöglicht es, intensive Rechenprozesse mit großen Datenmengen (*Big Data*, Petabyte-Bereich) auf Computerclustern durchzuführen.

Ein **Data-Mart** ist eine Kopie eines Teildatenbestandes des Data-Warehouse, die für einen bestimmten Organisationsbereich oder eine bestimmte Anwendung oder Analyse erstellt wird.

Extract, Transform, Load (**ETL**) ist ein Prozess, bei dem Daten aus mehreren ggf. unterschiedlich strukturierten Datenquellen in einer Zieldatenbank vereinigt werden. *Extraktion* der relevanten Daten aus verschiedenen Quellen *Transformation* der Daten in das Schema und Format der Zieldatenbank *Laden* der Daten in die Zieldatenbank.

Quelle: http://de.wikipedia.org

Das ISMS ist Grundlage für die gesamte Datenverarbeitung im Unternehmen!

Vielen Dank für Ihre Aufmerksamkeit!

Heiko Behrendt
ISO 27001 IT-Grundschutzauditor
Fon: 0431 988 1212
Mail: behrendt@datenschutzzentrum.de
Web: www.datenschutzzentrum.de