
Hochschule Niederrhein
University of Applied Sciences

Datensicherheit und Datenschutz

Prof. Dr. René Treibert

16.05.2018

Wirtschaftsförderung Viersen

Auftaktveranstaltung Digitalisierungsreihe der Stadt Viersen

Hochschule Niederrhein
University of Applied Sciences
Wirtschaftswissenschaften
Faculty of Business Administration and Economics

Vorstellung des Referenten
Prof. Dr.-Ing. René Treibert

- Studium: Mathematik & Wirtschaftswissenschaften Bergische Universität Wuppertal
- Wissenschaftler im Geschäftsbereich Sicherheitstechnologien am Battelle-Institut Europe in Frankfurt/Main
- Promotion im Fachbereich Sicherheitstechnik der Bergischen Universität Wuppertal
- Projektleiter PSI AG
- Leiter der Strategieabteilung, Anwendungssysteme der Stadtwerke Düsseldorf
- Zum Honorar-Professor an der der Bergischen Universität Wuppertal ernannt
- Seit 2003 Professor für Wirtschaftsinformatik, insbesondere Programm- und Systementwicklung an der Hochschule Niederrhein
- Leiter „Kompetenzzentrum für Informationssicherheit der Hochschule Niederrhein“ Clavis

Datensicherheit und Datenschutz

1. Informationssicherheit versus IT-Sicherheit
2. Prinzipien der IT-Sicherheit
3. Zeitachse der Regulative zum Datenschutz
4. Ausprägung personenbezogener Daten
5. Die acht Gebote technisch organisatorischer Maßnahmen
6. Anforderungsprofil an den Datenschutzbeauftragten
7. Handlungsbedarfe für Organisationen zur EU-DSGVO

Informationssicherheit versus IT-Sicherheit

IT-Sicherheit

[…] Zustand, in dem die Risiken, welche beim Einsatz von Informationstechnik aufgrund von Bedrohungen und Schwachstellen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß reduziert sind.

IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

(Def. gemäß BSI)

Informationssicherheit

Weiter gefasst als der Begriff IT-Sicherheit

Schutz aller (geschäfts-)relevanten Informationen und Informationsträger.

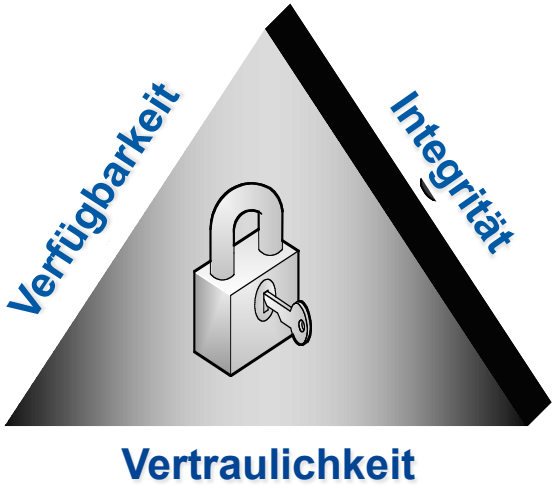
Dabei werden Infrastruktur und Geschäftsprozesse im Unternehmen mit einbezogen.

Keine rein technische Betrachtung!

Prinzipien der IT-Sicherheit

availability

Sicherstellen, dass Informationen (Daten) und IT-Dienstleistungen verfügbar sind, wenn sie gefordert werden



integrity

Schutz sensibler Informationen (Daten) vor ungewollter und unbemerkter Veränderung

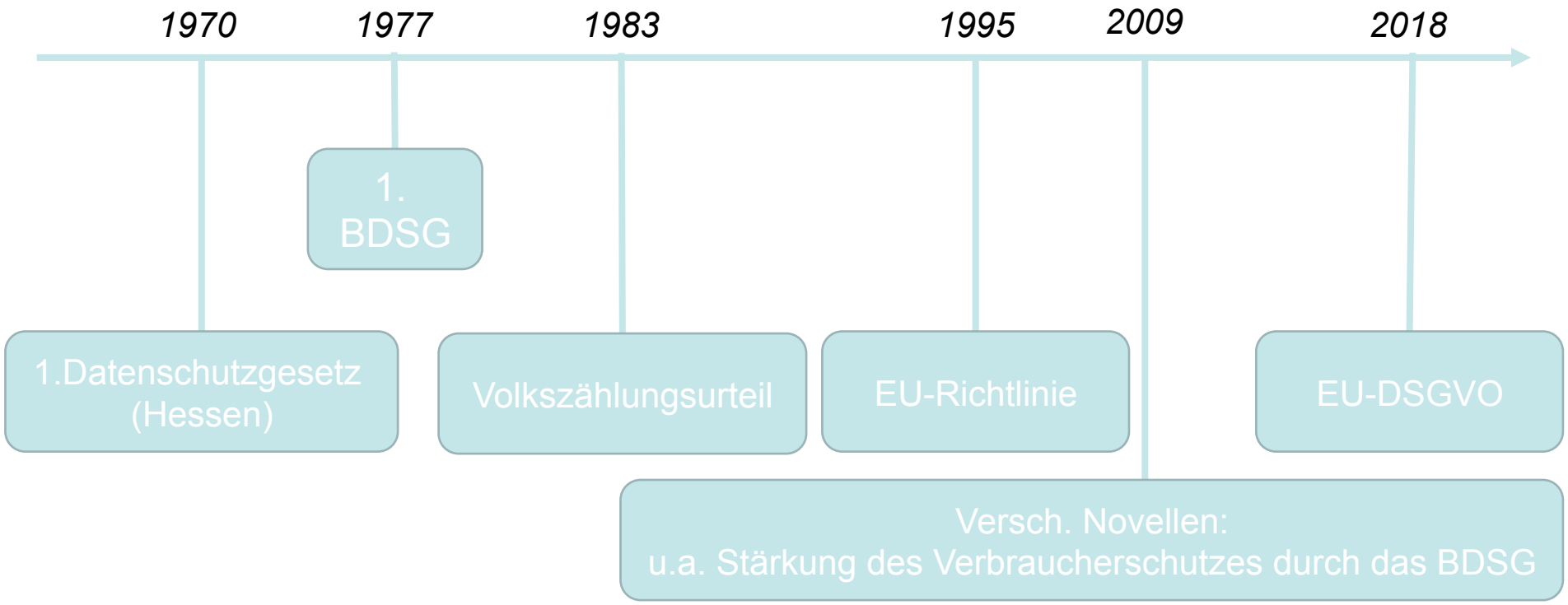
confidentiality

Schutz sensibler Informationen (Daten) vor unautorisierten Zugriffen

Weitere Prinzipien der IT-Sicherheit

- Authentizität
  Echtheit und Glaubwürdigkeit von Personen und Diensten müssen überprüfbar sein.
- Zurechenbarkeit (accountability)
  Informationen sowie Sender/Empfänger müssen eindeutig zugeordnet werden können.
- Verbindlichkeit (non-repudiation)
  - Informationen (Daten) dürfen bei Weiterleitung nicht verändert werden und nicht widerruf- oder abstreitbar sein.
  - Urheber von Veränderungen müssen erkennbar sein und dürfen Veränderung nicht abstreiten können.
- Revisionsfähigkeit (legal liability)
  Beweisbarkeit aller Informationen gegenüber Dritten
- Nicht-Anfechtbarkeit (Authentizität/Nachweisbarkeit)
  Sicherstellung von Nachweisen bzgl. Versand und Empfang von Daten
- Zugriffssteuerung
  Regulierung und Steuerung von Zugriffen auf IT-Systeme durch Personen und Dienste

Zeitachse der Regulative zum Datenschutz



Quelle: in Anlehnung an Zechel, Markus. Datenschutz in der Apotheke, Deutscher Apotheker Verlag, 2015

Ausprägungen personenbezogener Daten

Eigene Mitarbeiter:

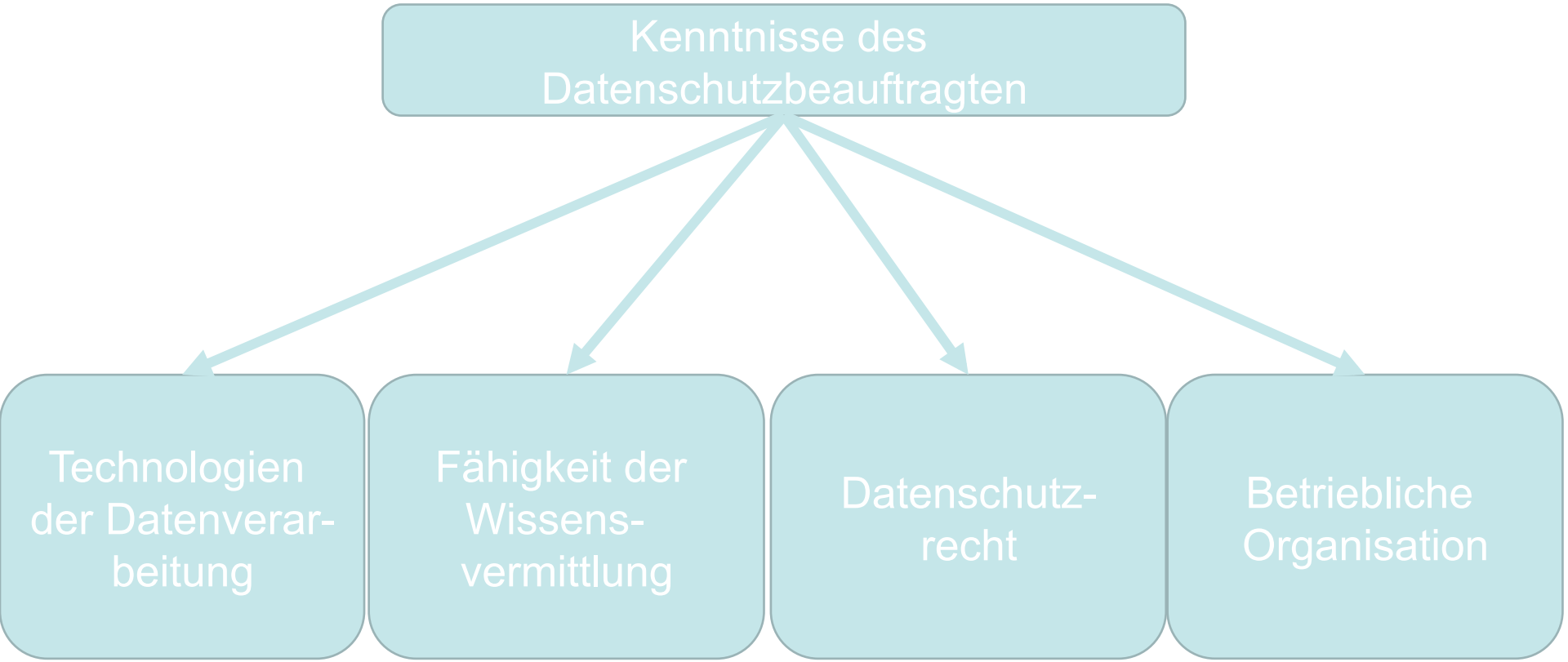
- Name, Vorname
- Anschrift
- Bankverbindung
- Telefonnummer/mobile Rufnummer
- Staatsangehörigkeit
- Familienstand
- Konfession
- Etc.

Die acht Gebote der technischen/organisatorischen Maßnahmen

1. Zutrittskontrolle
2. Zugangskontrolle
3. Zugriffskontrolle
4. Weitergabekontrolle
5. Eingabekontrolle
6. Auftragskontrolle
7. Verfügbarkeitskontrolle
8. Trennungskontrolle

Quelle: Zechel, Markus. Datenschutz in der Apotheke, Deutscher Apotheker Verlag, 2015

Anforderungsprofil an den Datenschutzbeauftragten



Quelle: in Anlehnung an: Kühnel, Patricia. Apotheke und Datenschutz, Govi-Verlag, 2015.

Handlungsbedarfe für Organisationen zur EU-DSGVO 1/3

- Als Erstes: Anwendungsbereich (Scope) festlegen!
- Bisheriges Verfahrensverzeichnis ergänzen und anpassen („Verzeichnis der Verarbeitungstätigkeiten“)
- Durchführung einer **Risikoanalyse** für alle Verfahren
  - Jeweils für alle Datenarten/-kategorien pro Betroffenenkategorie
- Durchführung der **Datenschutz-Folgenabschätzung** für Verfahren mit Risiko HOCH für die verarbeiteten personenbezogenen Daten der betreffenden Betroffenen-Kategorien
- Prüfung/Überarbeitung/Anpassung der **Auftragsdatenverarbeitungs-Vereinbarungen**
- Erstellung von Informationen/Anpassung vorhandener **Informationen an Betroffene**
- Einführung von **Privacy by Design und Privacy by Default**

Quelle: Baustein B.5.3 des BSI-Grundschutz

Handlungsbedarfe für Organisationen zur EU-DSGVO 2/3

- Verfahren zur **Etablierung der Rechenschaftspflichten** einrichten
- Etablierung von **Prozessen/Verfahren**, um den **Betroffenenrechten** nachkommen zu können
- Etablierung von **Prozessen/Verfahren** für **Meldungen bei Datenschutzverletzungen/ Datenschutzpannen**
- Anpassung der **Datenschutzerklärung auf der Homepage**
- Erfüllung aller Dokumentations-/Nachweispflichten nach EU-DSGVO durch Erstellung und Aufrechterhaltung der Aktualität der geforderten Dokumente

Quelle: Baustein B.5.3 des BSI-Grundschutz

Handlungsbedarfe für Organisationen zur EU-DSGVO 3/3

- **Explizite Nachweispflicht**:
  in der DS-GVO wird ausdrücklich ein „Nachweis“ gefordert
- **Implizite Nachweispflicht**:
  wenn Verantwortliche oder Auftragsverarbeiter den Prüfanforderungen einer Aufsichtsbehörde wohl nicht Rechnung tragen können, ohne über eine entsprechende Dokumentation zu verfügen.
- Die Dokumentation zum Nachweis besteht aus drei Teilen:

I. Dokumentation der Datenschutz-konformen Datenverarbeitung

II. Dokumentation der Sicherstellung der Betroffenenrechte

III. Dokumentation der Handhabung von Datenschutzverletzungen

Quelle: Baustein B.5.3 des BSI-Grundschutz

Impressum

Prof. Dr.-Ing. René Treibert
Clavis Kompetenzzentrum für Informationssicherheit der Hochschule Niederrhein

Fachbereich Wirtschaftswissenschaften (FB 08) der Hochschule Niederrhein
Wirtschaftsinformatik, insbesondere Programm- und Systementwicklung

Telefon +49 (0)2161 186-6343
Telefax +49 (0)2161 186-6313
Rene.Treibert@hs-niederrhein.de

Hochschule Niederrhein
University of Applied Sciences


Hochschule Niederrhein
University of Applied Sciences