



**TeleTrust**

*Pioneers in IT security.*

1989 25 Jahre 2014

## **TeleTrust-interner Workshop**

**Berlin, 05.06.2014**

# **Positionspapier „Big Data“**

**Oliver Dehning, antispameurope GmbH  
Leiter der AG Cloud Security**

## Definition „Big Data“

- Big Data bezeichnet
- große Datenmengen (Volume)
- unterschiedlichen Typs aus vielfältigen unterschiedlichen Quellen, sowohl strukturiert wie auch unstrukturiert (Variety),
- die automatisch mit hoher Geschwindigkeit (Velocity) erzeugt und verarbeitet werden, um daraus neue Informationen zu gewinnen und ggf. Entscheidungen abzuleiten.
- Eine weitere Eigenschaft von Big Data ist die unterschiedliche Qualität der Daten hinsichtlich Vertrauenswürdigkeit und Korrektheit (Varacity).

## Bedeutung

- Eine schnell wachsende Zahl von Systemen produziert immer mehr Daten:
  - automatische Abrechnungssysteme
  - bildgebende Diagnoseverfahren
  - digitale Motorsteuerungen
  - in Maschinen eingebaute Sensoren
  - Gebäudeautomation
  - Videoüberwachungen
  - Stichworte „Internet of Things“, „Industrie 4.0“ und „Smart Meter“.
- Rasant wachsenden IT-Kapazitäten (Rechenleistung, Speicher, Netzwerke) ermöglichen jetzt die Speicherung und Verarbeitung einer schnell wachsenden Menge dieser Daten.

## Chancen

Gewinnung neuer Informationen durch Kombination einer schnell wachsenden Datenmenge einerseits und schnell wachsender Fähigkeit zur Speicherung und Auswertung dieser Daten andererseits:

- Berechnung lokaler Wetterprognosen
- Aufdeckung geplanter terroristische Anschläge aus der Analyse von Kommunikationsdaten
- Vorhersage von Verkehrsspitzen und dynamische Verkehrslenkung durch Auswertung von Daten aus Navigationssystemen
- Rechtzeitige Maschinenwartung durch Analyse von Sensordaten
- Bedarfsgerechte Steuerung und Speicherung von Energie basierend auf aktuellen Verbrauchsdaten und kurzfristigen Verbrauchsprognosen
- Markt-, Meinungs- und Sozialforschung durch Auswertung von Social Media
- Nutzerprofilierung im Web, Retargeting

## Risiken / Gefahren

Gewinnbare Informationen gehen über das hinaus, was der Eigentümer der Daten mit der Erzeugung dieser Daten eigentlich bezweckt:

- Rückschlüsse auf das konsumierte Fernsehprogramm aus Schwankungen des Stromverbrauchs,
- Rückschlüsse auf eingesetzte Systeme aus statistischen Werten übermittelter Daten,
- Ermittlung und Verfolgung des Aufenthaltsortes von Personen aus Mobilfunkdaten,
- Erstellung eines sozialen Profils von Personen aus der Analyse öffentlich verfügbarer Daten (Wohnort, Arbeitgeber, soziales Netzwerk in Facebook, besuchte Webseiten, etc.)
- Problematisch: die nachträgliche Personalisierung zuvor anonymisierter Daten wird relativ einfach

# Forderungen von TeleTrust

- Gesellschaftlicher Dialog über Grundsätze von Big Data
  
- Forderungen von TeleTrust:
  1. Datensparsamkeit
    - Es dürfen nur solche Daten gespeichert werden, die für die Erledigung einer Aufgabe tatsächlich benötigt werden.
    - Daten dürfen nicht auf Vorrat gespeichert werden, im Hinblick auf einen später eventuell denkbaren Nutzen.
    - Für jede Erzeugung und Speicherung von Daten in größeren Mengen müssen Nutzen und Notwendigkeit dokumentiert werden.
  2. Verschlüsselung und Zugang
    - Die Speicherung von Daten muss, soweit irgend möglich, verschlüsselt erfolgen.
    - Der Zugang zu Daten durch Dritte muss eingeschränkt sein.
    - Die Übertragung von Daten mit potentiell Personenbezug in einen „unsicheren Drittstaat“ muss verboten sein.
  3. Verbot der nachträglichen Personalisierung
    - Eine nachträgliche Personalisierung von zuvor anonymen Daten muss generell verboten sein und darf nur unter gesetzlich genau geregelten Voraussetzungen ausnahmsweise erlaubt werden.