Unterschiedliche Ansätze

12. Symposium on Privacy and Security
Datenschutz und Informationssicherheit in die Prozesse integrieren
Die Herausforderung der Umsetzung

Dr. Bruno Porro
The Geneva Association

Rüschlikon, 6. November 2007

Wikipedia (Ist das eine zuverlässige Quelle?)

- Datenschutz
  - bezieht sich ausschließlich auf den Schutz personenbezogener Daten.
  - Datenschutz etabliert das Prinzip der informationellen Selbstbestimmung, wie sie auch im BVG-Urteil zur Volkszählung festgeschrieben wurde.
  - Privatsphäre: Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben.
  - Einhaltung des Bundesdatenschutzgesetzes

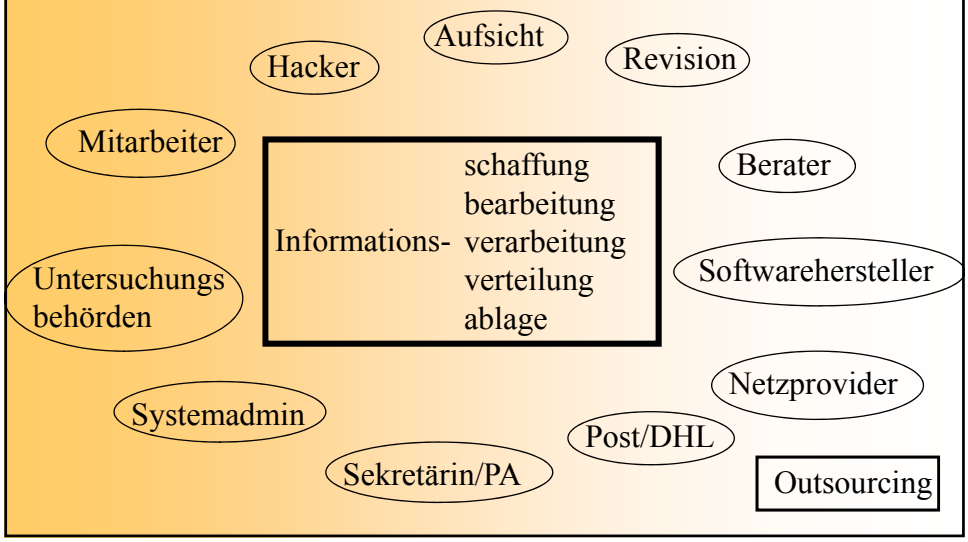
Wikipedia (Ist das eine zuverlässige Quelle?)

- **Informationssicherheit** (auch Datensicherheit); bezieht sich auf alle relevanten Informationen einer Organisation oder eines Unternehmens einschließlich personenbezogener Daten
  - Vertraulichkeit: Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.
  - Integrität: Daten dürfen nicht unbemerkt verändert werden, resp. müssen alle Änderungen nachvollziehbar sein.
  - Verfügbarkeit: Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden.

Wikipedia (Ist das eine zuverlässige Quelle?)

- IT-Sicherheit; Einrichtung und Aufrechterhaltung geeigneter betrieblicher und technischer Maßnahmen, um die Einhaltung der Schutzziele der Informationssicherheit bei IT-gestützter Verarbeitung von Informationen zu gewährleisten
  - Funktionalität: Hardware und Software sollen erwartungsgemäß funktionieren.
  - Einhaltung der betrieblichen Prozesse
  - Einrichtung geeigneter Sicherheitstechniken (Firewall, Zugriffschutz, Intrusion Detection, ...)
  - Vorsorgemaßnahmen zur möglichst reibungslosen Weiterführung bzw. Wiederaufnahme der Produktion nach Störungen

Objekte und Prozesse



Objekt- oder prozessorientiert, was ist besser?

Eher objektorientiertes Vorgehen:

- **Sicherheit von Gebäuden, Anlagen, Uebertragungs-systemen**
- **Klare Zuordnung der Verantwortlichkeit an eine Stelle (Funktion, Person)**
- **Ursache/Wirkung kann in der Regel ereignisbezogen evaluiert und es können Konsequenzen gezogen werden**

Eher prozessorientiertes Vorgehen:

- **Es muss ein neuer Weg beschritten und alte Routinen abgeschafft werden (change of mindset)**
- **Abläufe bleiben nach Einführung für gewisse Zeit stabil**
- **Klare Definition der Leistungen und Eskalationswege**
- **Outsourcing**
- **Schnittstellenproblematik**

Grundlegende Philosophie (1)

- Wertesystem(e) der Unternehmung. Definition der Ziele oder des Weges?
- Führung durch Stäbe oder internationale Arbeitsgruppen auf Zeit?
- Anreize und Widerstände
- Systematisches Risiko
- 100% oder ist 80/20 gut genug?
- Handbücher als Dokumentation oder Anweisung?
- Professionelles Projektmanagement

Grundlegende Philosophie (2)

- Was will die Unternehmung? (Frontrunner, best practice, Erfüllung der (gesetzlichen) Minimalerfordernisse)
- In weltweit tätigen Organisationen ist Abwägung der rechtlichen lokalen Besonderheiten ein Muss!
- Die inhaltliche Botschaft muss global die gleiche sein, die Umsetzung lokal – den kulturellen Besonderheiten angepasst.
- Falls es um grössere Investitionen an Zeit und Geld geht, muss ein Budget für diese Aktionen vorgesehen werden!
- Kosten/Nutzen Abwägungen sind schwierig, aber trotzdem notwendig.

Grundlegende Philosophie (3)

Burg

Schloss

Erfolgsfaktoren

- Der Chef
- Kongruenz von Absicht und Durchführung
- Machbarkeit, technisch und personell
- Detailliertes Projekt mit quantifizierten Risiken
- Schrittweise von Wegmarke zu Wegmarke
- Auch die dritte Version ist noch ein Pilot!?
- Integration in «normalen» Ablauf, nicht aufgesetzt
- Win-win, was liegt für die Leute drin?
- Kommunikation, immer wieder
- Messbarkeit der Leistung (KPI) über die Zeit
- Ein klarer Schlussstrich