

## Vertraulichkeit in (kleinen) Unternehmen (k)eine Frage der IT?

- Vertraulichkeit

die Eigenschaft von Daten, Worten oder allgemein gesprochen von Sachverhalten, nur für einen bestimmten Empfängerkreis vorgesehen und diesem exklusiv zugänglich zu sein

- Definition KMU in der EU

- kleiner 250 MA
- kleiner 50 Mio. Umsatz
- mehr als 99% der 3.600.000 Unternehmen Deutschland
- bis 10 MA: rund 96%

- im Innenverhältnis
  - Arbeitnehmer ↔ Arbeitgeber  
Treupflichten als „Nebenpflichten“ zum Arbeitsvertrag  
zusätzlich explizite Verschwiegenheitsverpflichtung
  - Arbeitnehmer ↔ Arbeitnehmer
- im Außenverhältnis
  - Grundsatz von „Treu und Glauben“
  - Culpa in contrahendo → Verschulden bei Vertragsschluß
  - Culpa post contractum finitum → nach Vertragsende
  - der „Ehrbare Kaufmann“ → modern ausgedrückt: CSR

# Vertraulichkeit im QM



- Beziehung Kunde  $\leftrightarrow$  Unternehmen
- Sicherstellen der Unternehmensleistung
- Verlässlichkeit des Unternehmens
- Umgang mit Kundendaten und -eigentum
  - Verantwortung der Leitung
  - Risikomanagement
  - Compliance
  - Sicherheit, Verfügbarkeit, Vertraulichkeit von Daten
- Datenschutz und -sicherheit

# in der Praxis...



- erst kommt der Betriebsablauf
  - gemeinsame Benutzerkonten und Passwörter
  - alle Räume und Ablagen sind frei zugänglich
  - wer steuert die Rechte der Dateiablage?
  - was befindet sich auf mobilen Geräten?
  - wer darf CD's, USB-Sticks beschreiben?
  - wer kontrolliert ausgehende Mails?
  - wie ist das im Heimbüro?
- **Komfort geht vor Vertraulichkeit!**

# einfach einfach anfangen...



im 2. Semester lernt man:

$$\ln \left[ \lim_{n \rightarrow \infty} \left( 1 + \frac{1}{n} \right)^n \right] + \sin^2 x + \cos^2 x = \sum_{n=0}^{\infty} \left( \frac{(\sinh x)}{(\sinh(2x))} \right)^n * \cosh^{n-1} x * \sqrt{1 - \tanh^2 x}$$

schon etwas einfacher:

$$\ln e + \sin^2 x + \cos^2 x = \sum_{n=0}^{\infty} \left( \frac{(\sinh x)}{(\sinh(2x))} \right)^n * \cosh^{n-1} x * \sqrt{1 - \tanh^2 x}$$

es geht aber auch so:

$$1 + 1 = 2$$

# einfach einfach anfangen...



- Stufen der Vertraulichkeit ermitteln
- Mitarbeiter klassifizieren
- Daten klassifizieren
- Mitarbeiter- und Datengruppen bilden
- Organisatorische Maßnahmen ergreifen
- Technische Maßnahmen ergreifen

# Beispiel LKW-Werkstatt 15 MA



- Betriebsleiter (1)
- Buchhaltung, Bürokraft (1)
- Bürokraft (1)
- Ersatzteilbeschaffung, Lagerleiter (1)
- Kunden- und Auftragsannahme, Werkstattmeister (2)
- Mitarbeiter Werkstatt (9)



# Beispiel LKW-Werkstatt Daten



- Personal- und Buchhaltungsdaten
- Finanzdaten, Kontodaten, Bankzugang, Zahlungen
- Kundenstammdaten
- Lieferantenstammdaten
- Fahrzeugstammdaten
- Auftragsdaten
- Warenbewegungen, Einkauf, Lieferungen

# Beispiel LKW-Werkstatt Gruppen



- Gruppe Betriebsleitung
  - wer: Betriebsleiter, Buchhaltungskraft
  - was: Personal- und Buchhaltungsdaten
- Gruppe Betriebsbüro
  - wer: Betriebsleiter, Buchhaltungskraft, Bürokraft
  - was: Finanzdaten, Kunden- und Lieferantenstammdaten
- Gruppe Lager
- Gruppe Werkstatt

- Organisatorische Trennung
  - Papier-Datenbestände nach Gruppen umsortieren
  - räumliche Trennungen vornehmen (Schränke, Ordner, ...)
  - Zugriffs- und Zutrittsschutz (Räume, Schlüsselgruppen)
- Tipps & Tricks
  - unterschiedliche Farben für unterschiedliche Datengruppen
  - Farben an Aufbewahrungsort und Ablagegut identisch
  - Achtung: Sehschwächen!
  - unterschiedliche Ablagearten für unterschiedliche Daten

- einfache Maßnahmen
  - Benutzergruppen bilden und MA zuordnen
  - Gruppenspezifische Programme und Daten in entsprechenden Verzeichnissen, gruppenbezogene Rechte
  - räumliche Trennungen (Fax Buchhaltung, Fax Werkstatt)
- technische Maßnahmen, z.B.
  - Thinclients, zentrale Datenhaltung
  - keine optischen Laufwerke, USB sperren
  - externe Zugriffe minimieren und absichern
  - Datenträger verschlüsseln

- freie Hardware?
  - Firmware-Löcher
  - BIOS
- proprietäre Software
  - direkte Kontrolle → unmöglich
  - indirekte Kontrolle über das Verhalten, z.B. Netztraffic
- freie Software
  - wer überschaut die Interna?
  - grundsätzlich möglich, aber... wer hat die Expertise?

# Fazit



- Vertraulichkeit ist technisch nicht sicher zu stellen!
- es fehlt an interner Expertise und Unterstützung
- ORGANISATION ist wichtiger als Technik
  - einfache Überlegungen
  - einfache Maßnahmen
  - Aufwand zur Umstellung
  - Aufwand der konsequenten, dauerhaften Umsetzung
- für Beratung und Hilfe gibt es für KMU Zuschüsse!
- Kontakt: siehe Fußzeile... :-)