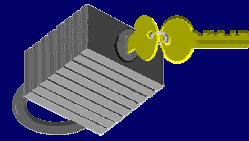


# Sicherheit und Schutz von Rechtsdaten

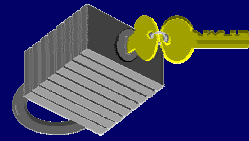
## Überlegungen zu Kosten und Nutzen

David Knöri  
Statistisches Amt des Kt. Zürich

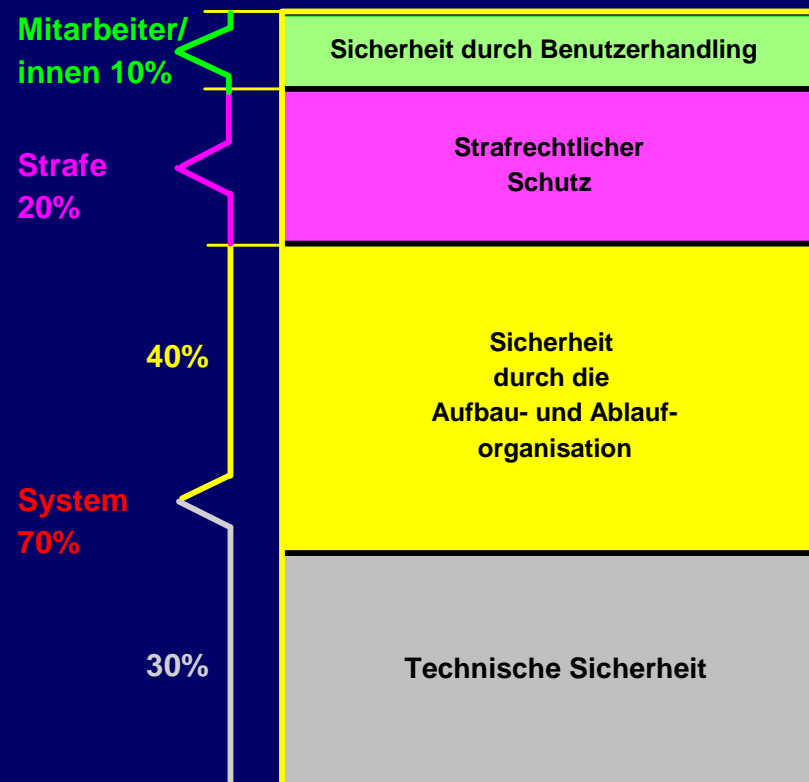


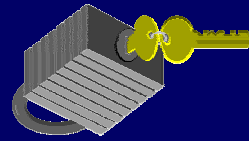
# Gefahren für die Sicherheit von (Rechts)daten

- Feuer, Wasser, Naturkatastrophen
- Technisches Versagen
- Kriminelle Handlungen
- Fehlmanipulationen
  - Systemwartung
  - Benutzer/innen
- Reinigungspersonal

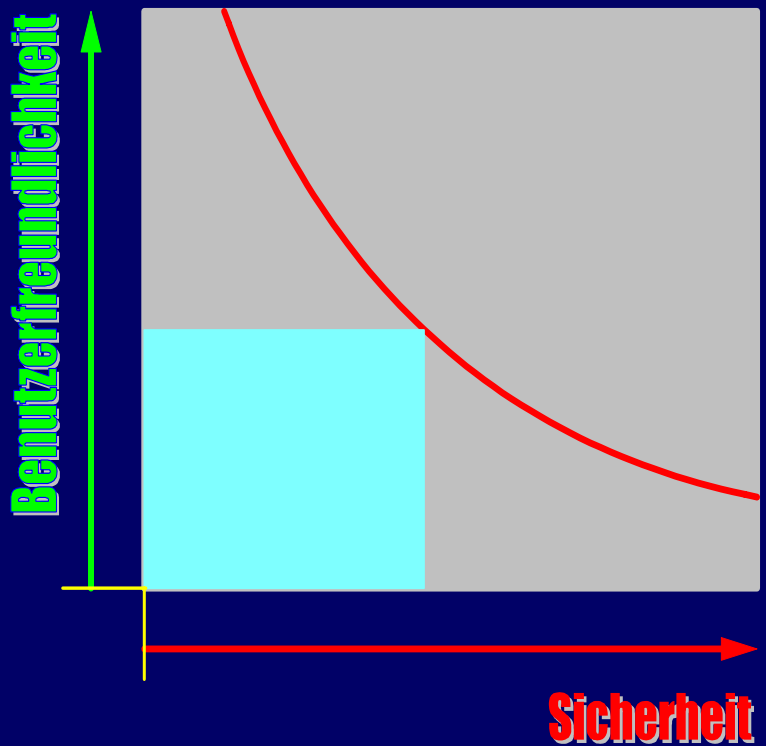


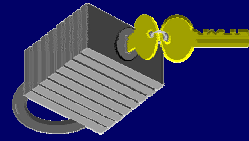
# Die vier Sicherheitsebenen zum Schutz von (Rechts)daten



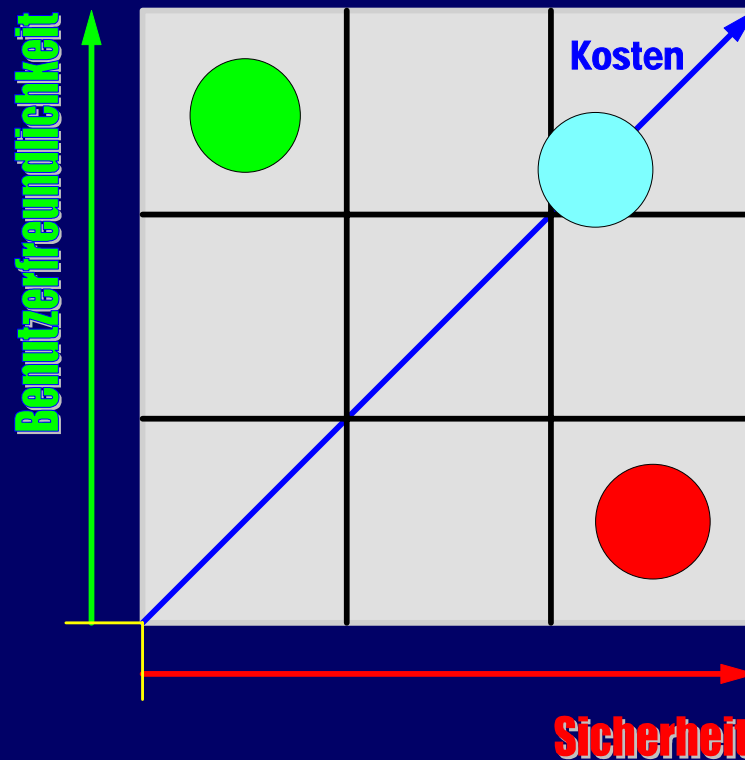


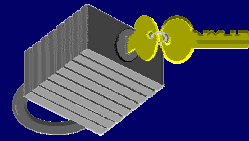
# Benutzerfreundlichkeit versus Sicherheit





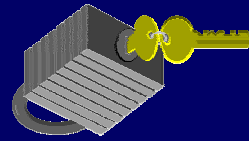
# Benutzerfreundlichkeit und die Sicherheit in Bezug auf die Kosten





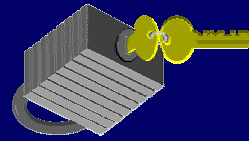
# Elemente zur Sicherheit und zum Schutz von (Rechts)daten

- Bauliche Massnahmen
- Logistik
- Organisation
- Systemstandort
- Systemauslegung
- Installation
- Systemzugriff



# Schutz durch kleine bauliche Massnahmen in EDV-Räumen

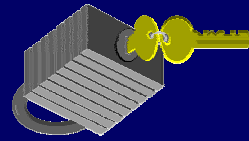
- Mit kleineren bauliche Massnahmen den Schutz erhöhen
  - Entfernen von brennbaren Materialien wie Teppiche, Vorhänge etc.
  - Einbau von Sicherheitsschlösser zum Beispiel: Kaba-Star
  - Einbau von Türschwellen (Brandschutz)
  - durch Einbau von Rollläden bei den Fenstern (Einbruchschutz)
  - Einbau von Raumklimageräten



# Sicherheit und Schutz durch Umbau von EDV-Räumen

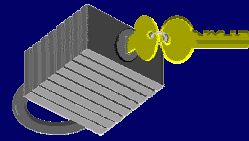
- Bei der Inbetriebnahme von EDV-Anlagen sind heute grössere Umbauten unumgänglich
  - durch einbauen von feuerhemmenden Türen und Durchgängen
  - durch einbauen von Feuermeldern
  - den Einbau einer Klimaanlage
  - den Einbau von Zutrittsschleusen
  - den Einbau elekt. gesicherten Türen
  - den Einbau Flutungsanlagen mit Halon





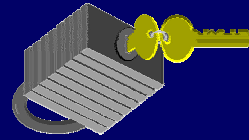
# Logistische Anforderungen

- Die Logistik hat besondere Anforderungen auf Sicherheit und Schutz der Daten/Datenträger zu erfüllen
  - bei der Verteilung von Datenträger in Bezug Gebäudezutritt, Räumung von Gebäude resp. Gebäudeteilen
  - Bereitstellen, Verpacken und Versand von Daten und Datenträger
  - Lagerung von Datenträger (Nässe, EMP, Hitze, Verfügbarkeit und Lesbarkeit)



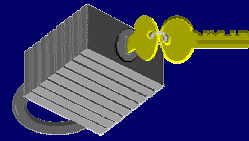
## Organisatorische Massnahmen (effizient und kostengünstig)

- Mit organisatorischen Massnahmen kann sehr flexibel auf Ereignisse Reagiert werden
  - Notverfahren erarbeiten und testen
  - Katastrophenplan dokumentieren
  - Verfahren für den Zugriffsschutz erstellen
    - ☐ Vergabe von User-ID und Passwort
    - ☐ Verfahren zum Rücksetzen von Passwörtern
    - ☐ Ein- und Austritte von Mitarbeiter/innen



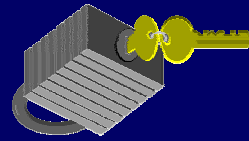
# Dokumentation und Schulung

- Einführung und Schulung der Benutzer/inne
  - genügend Zeit für die Schulung
  - praxisgerechte Handbücher
  - Helptexte in den Applikationen
- Einführung der Systembetreuer
  - Systemhandbücher abgeben
  - technische Abläufe durchspielen
  - Notverfahren dokumentieren



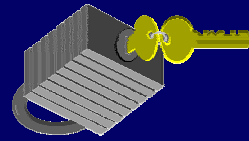
# Systemstandort

- Standort der Systeme resp. Server
  - Systeme in abschliessbare Räume
  - keine Hinweis auf EDV- od. Serverräume
  - Räume bleibt immer abgeschlossen
    - ▣ Sicherheitsschloss/Zutrittsbatch/Schleuse
- **Wichtige Typs**
  - Immer min. 10 cm ab Boden (Wasser)
  - Systeme ca. 20 cm von den Wänden
  - Kühlrillen nicht abdecken (Überhitzung)

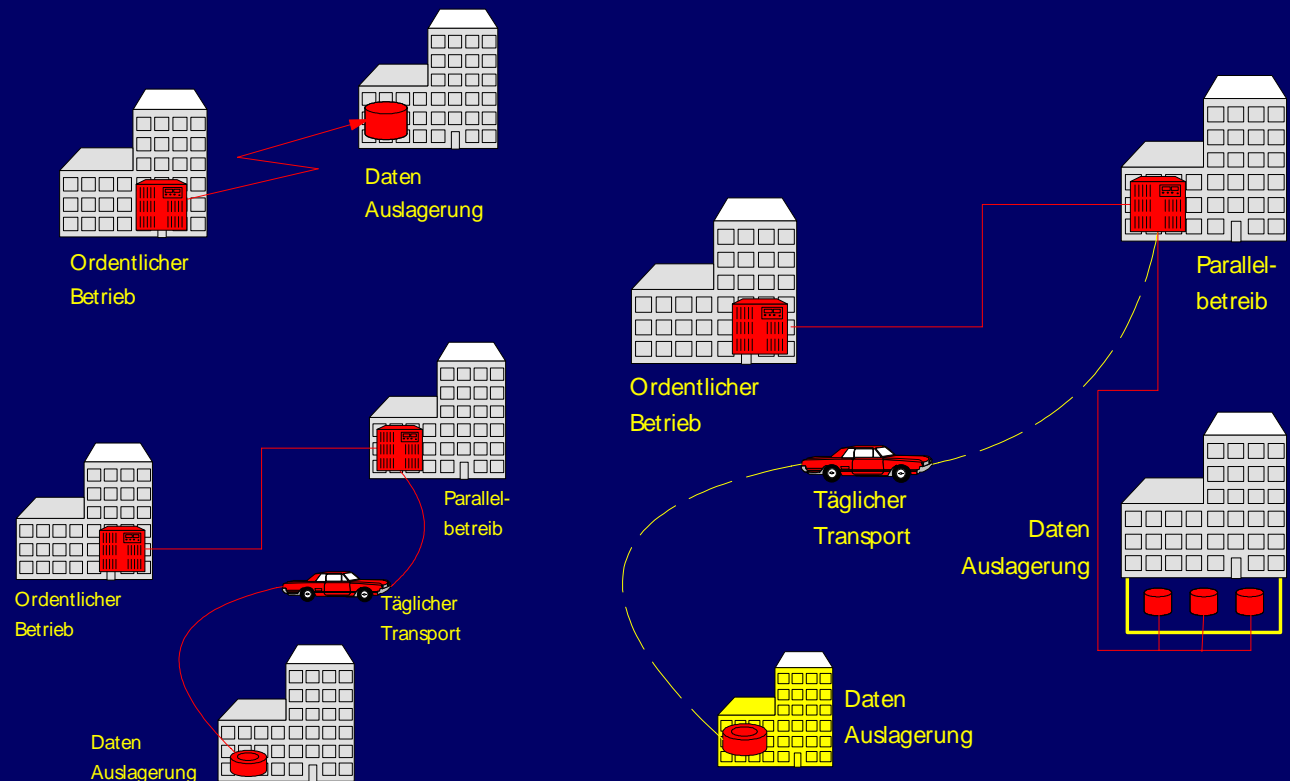


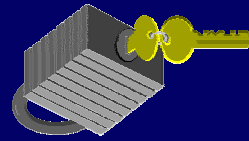
# Systemauslegung

- Sicherheit durch technisches Design
  - Backup-System (Strategie festlegen)
  - Fault Tolerance Systeme (Lavel)
  - auslagern von Backups an Roboter
  - Parallelbetrieb (Teil- oder Vollbetrieb)
  - UPS (Unterbruchsfreie Stromversorgung)
- **Wichtige Typs**
  - nur soviel wie nötig (komplexe)  
wird sehr schnell sehr teuer



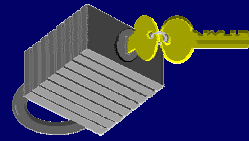
# Schematische Darstellungen von Systemauslegungen





# Installation

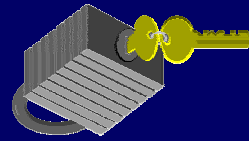
- Zur Vermeidung von Datenverlusten sind Vorkehrungen erforderlich
  - Installation sauber dokumentieren
  - Zugriffsrechte dokumentieren
  - Save- und Recoverkonzept erstellen
- **Wichtige Typs**
  - Save halbjährlich durch Recover testen
  - Speichermedium gehört in einen Tressor
  - Systempasswörter im Couvert in



# Systemzugriff

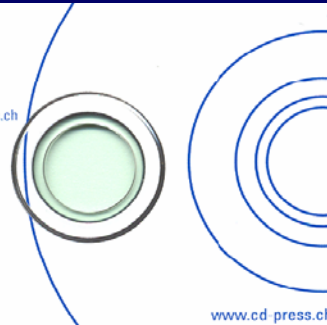
- Sicherheit und Schutz mittels Zugriffsverfahren beeinflussen
  - Zugriffssystem und -Konzept erarbeiten
    - ☒ User-ID und Passwort
    - ☒ CD-oder Smart-Cards und Passwort
    - ☒ PKI-Infrastruktur
    - ☒ biomechanische Verfahren
- **Wichtige Aussage**
  - Nur biomechanische Verfahren garantieren eine Authentizität (Finger, Iris, etc.)





# Systemzugriff mittels Hilfsmittel

CD Press AG  
Industriestrasse 48  
CH-8962 Bergdietikon  
Tel. +41 (0)52 202 55 60  
Fax +41 (0)52 202 55 61  
sandra.stauffer@cd-press.ch



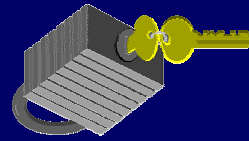
www.cd-press.ch

CD-Card



ID-Mouse





# Verschlüsselung

- In offenen Netzen müssen Rechtsdaten unbedingt verschlüsselt werden
  - Mail an falschen Adressaten
  - Mails sind herumliegende Postkarten
  - Böswillige Attacken
- Funktionsprinzip der Verschlüsselung

