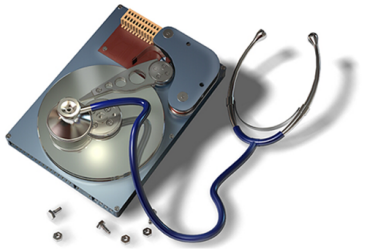
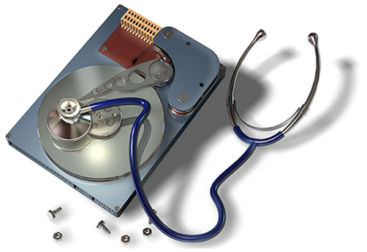
Datenwiederherstellung



Universität Hamburg

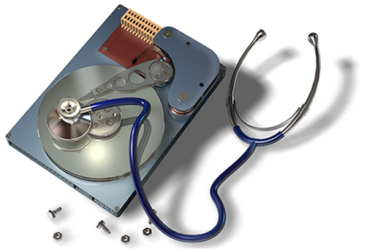
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Proseminar: Speicher- und Dateisysteme
Vortragender: Nicolas Petereit



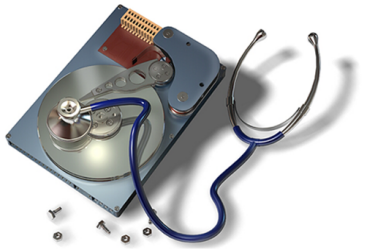
Daten-wiederherstellung

Datenwiederherstellung



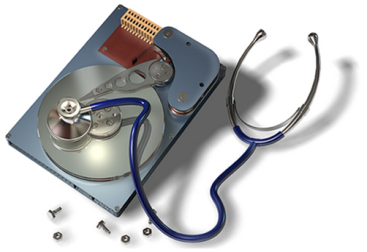
Gliederung

- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung



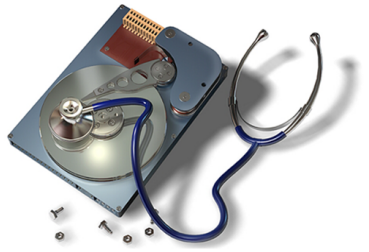
Gliederung

- Part 2: IT-Forensik
  - Was ist das?
  - Vorgehen
  - Schutzmechanismen
  - Demo
- Fazit
- Medien-/Quellenverzeichnis



Gliederung

- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung



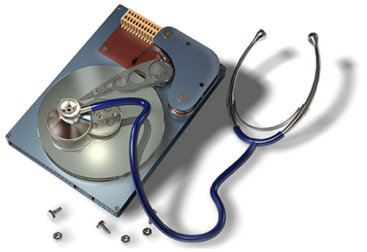
Einleitung

Table 1. **The Cisco VNI forecast: historical internet context**

Year	Global Internet Traffic
1992	100 GB per day
1997	100 GB per hour
2002	100 GB per second
2007	2,000 GB per second
2016	26,600 GB per second
2021	105,800 GB per second

Source: Cisco VNI, 2017.

[2]

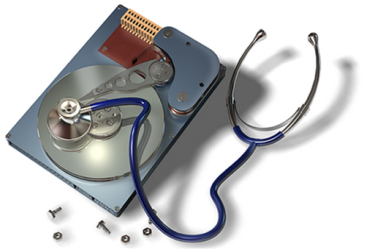


Einleitung

- Menge der Daten steigt ins Unermessliche
- Abhängigkeit von Daten steigt stetig

➔ Sicherheit von (wichtigen) Daten muss gewährleistet sein

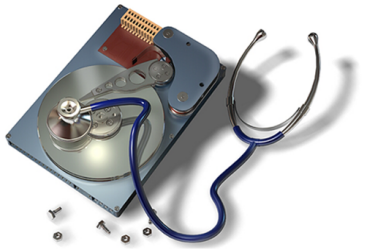
Datenwiederherstellung



Einleitung

"93% der Unternehmen, deren Datenbestand für zehn oder mehr Tage durch Datenverlust ausfiel, überlebten das darauf folgende Geschäftsjahr nicht."

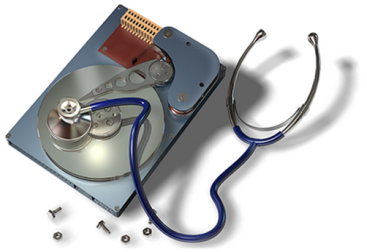
https://www.krollontrack.de/datenrettung/datenverlust/



Einleitung

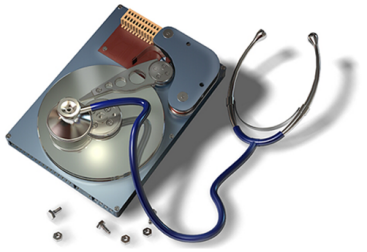
- Grundsätze von Datensicherheit:
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit

➔ Einhaltung dieser Grundsätze oberstes Ziel!



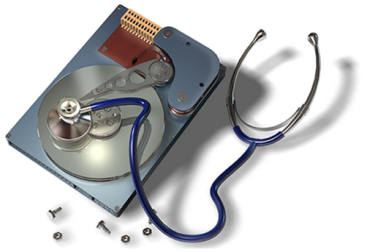
Gliederung

- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung



Grundsätzliches zur Datenwiederherstellung

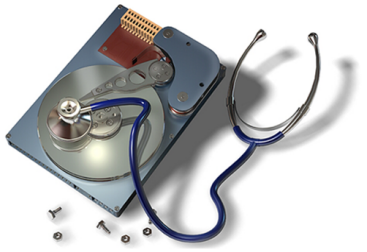
- Ziel: Einhaltung der Datensicherheits-Grundsätze
  - Besonders: Verfügbarkeit
- Enger Zusammenhang zu Präventivmaßnahmen



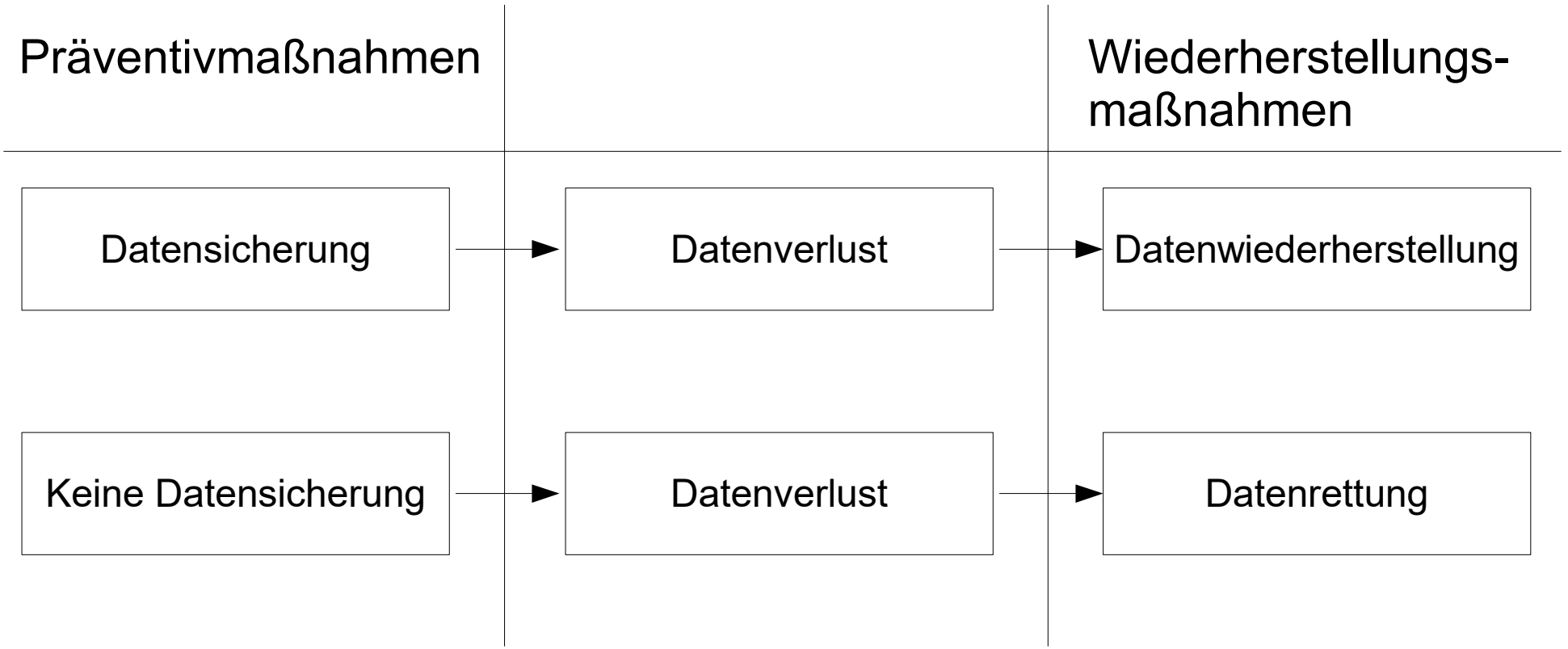
Grundsätzliches zur Datenwiederherstellung

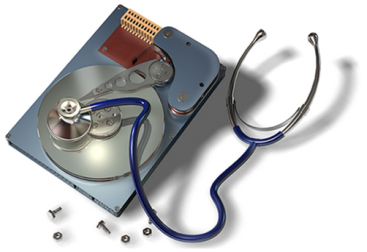
- Erfolgsrate abhängig vom Grad der Präventivmaßnahmen
- Unterscheidung: Datenwiederherstellung und Datenrettung

Datenwiederherstellung



Datensicherheit im Zeitverlauf

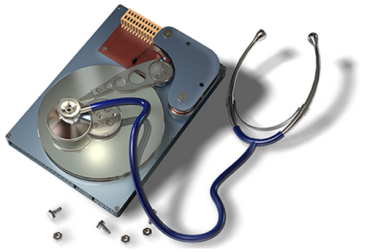




Grundsätzliches zur Datenwiederherstellung

- Grundsatz: "Es ist nicht die Frage ob, sondern wann Daten verloren gehen"
- ➔ Man sollte gut darauf vorbereitet sein

Datenwiederherstellung



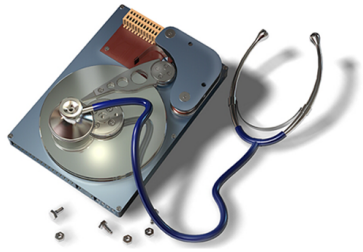
Grundsätzliches zur Datenwiederherstellung

- Theoretisch sind so gut wie alle Daten wiederherstellbar

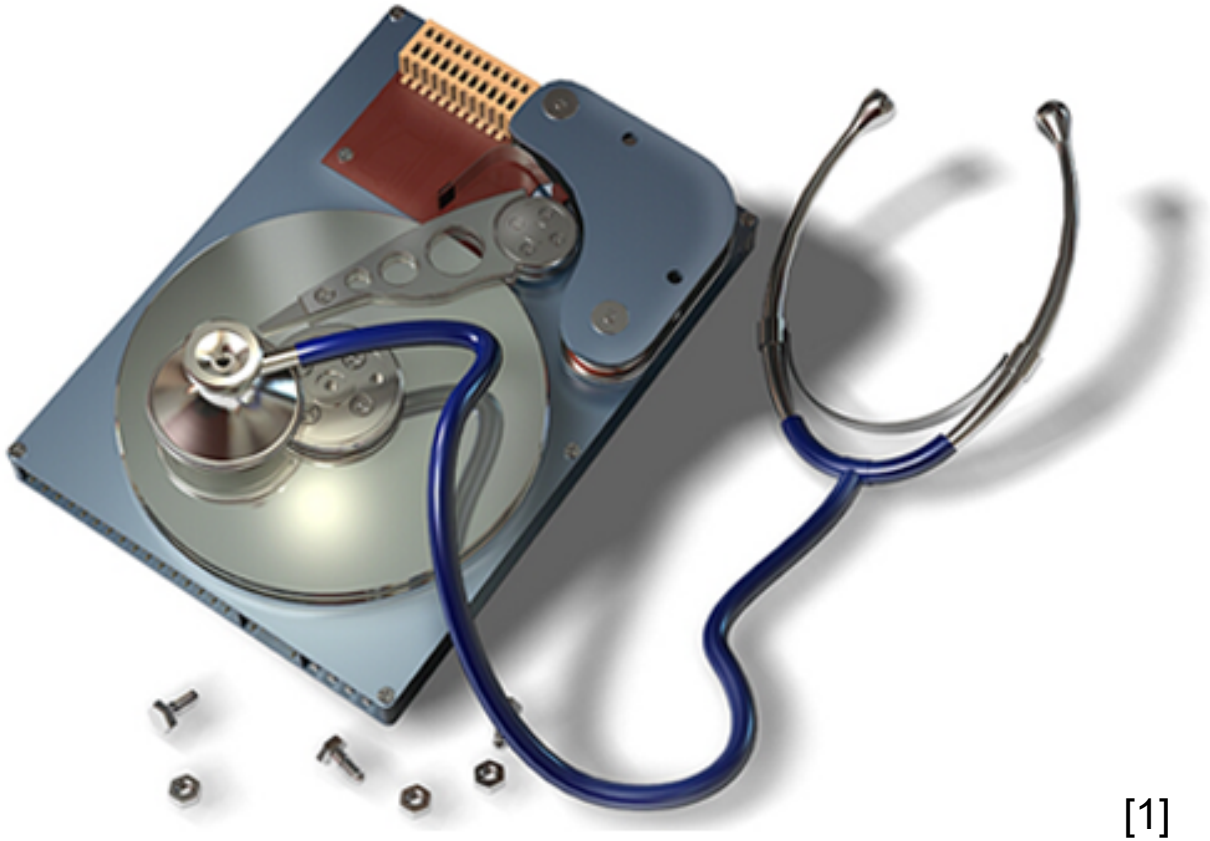
➔ Kosten bzw. Zeit sind begrenzende Faktoren

➔ Vergleich (Kosten-Nutzen-Analyse):

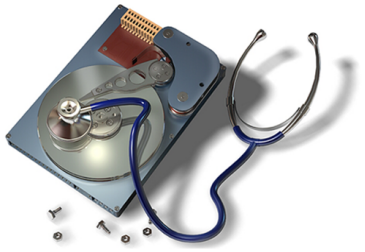
  - Wichtigkeit der Daten
  - Wiederherstellungs-/Sicherungsaufwand



Part 1: Datenwiederherstellung



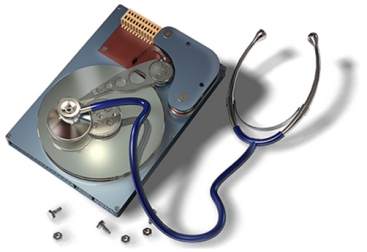
[1]



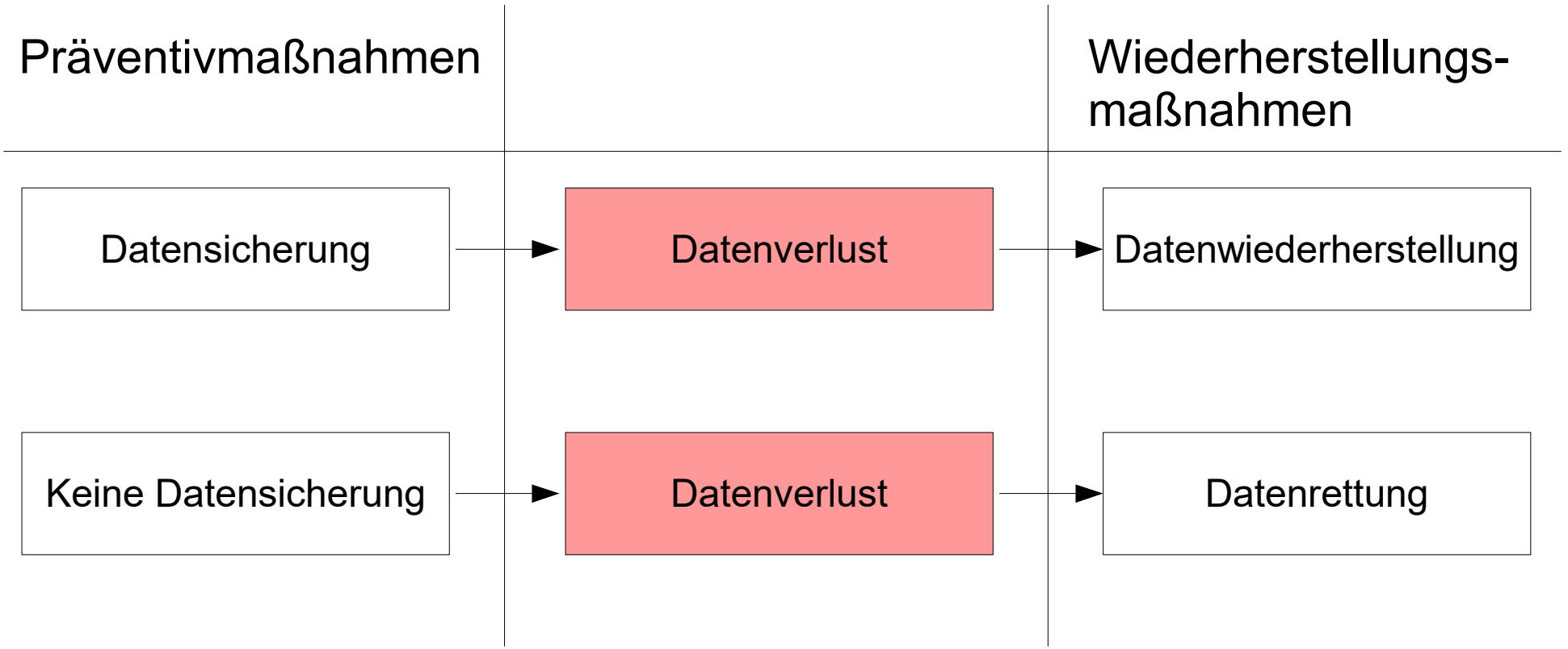
Gliederung

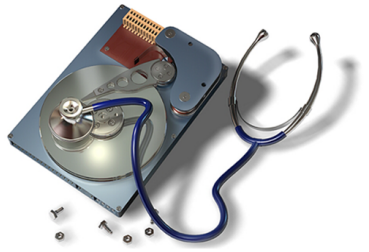
- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung

Datenwiederherstellung

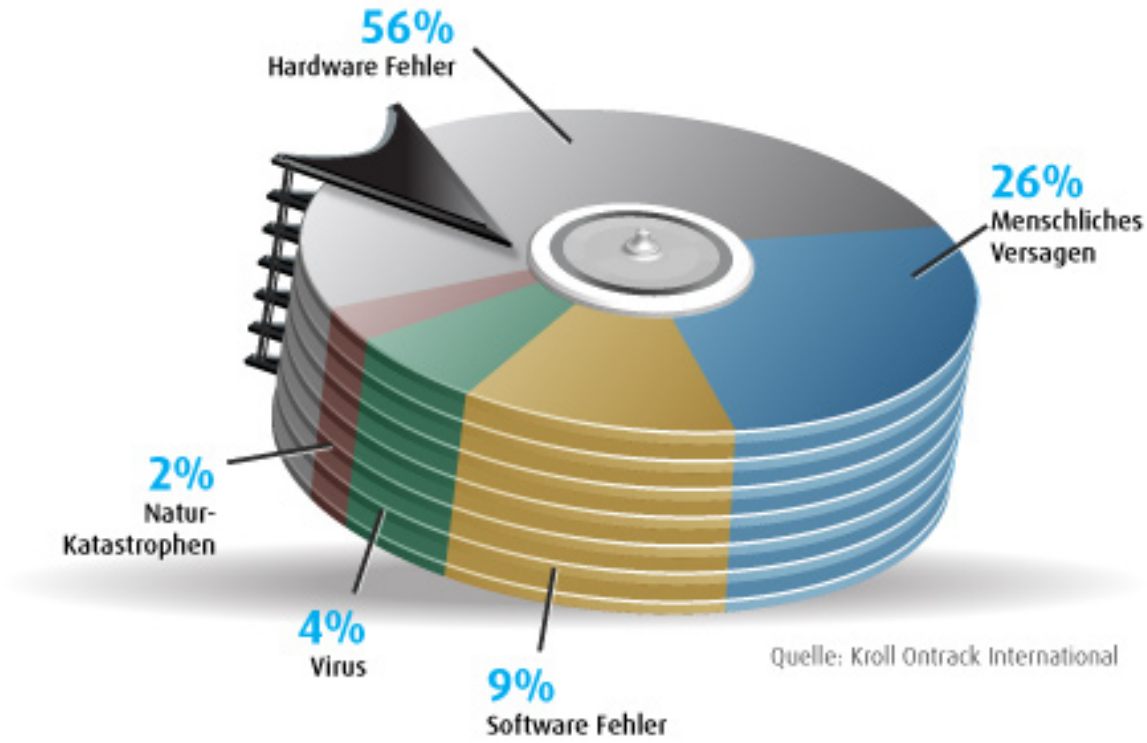


Datensicherheit im Zeitverlauf



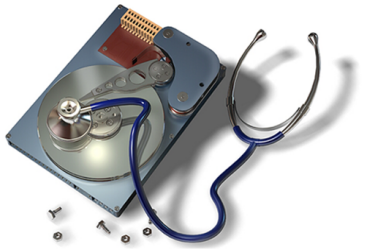


Wie gehen Daten verloren?



[3]

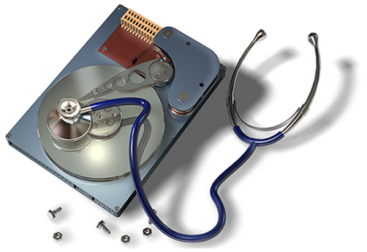
Datenwiederherstellung



Wie gehen Daten verloren? - Menschliches Versagen

- Simples Löschen von Daten
  - Beabsichtigt (aufgrund von Missverständnissen)
  - Unbeabsichtigt (unaufmerksam, "verklicken")
- Überschreiben von Dokumenten
  - z.b. "Speichern" anstatt "Speichern unter"

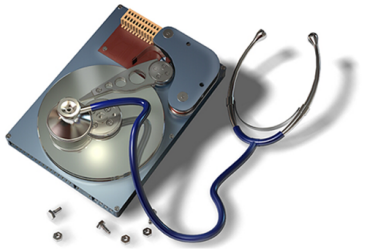
Datenwiederherstellung



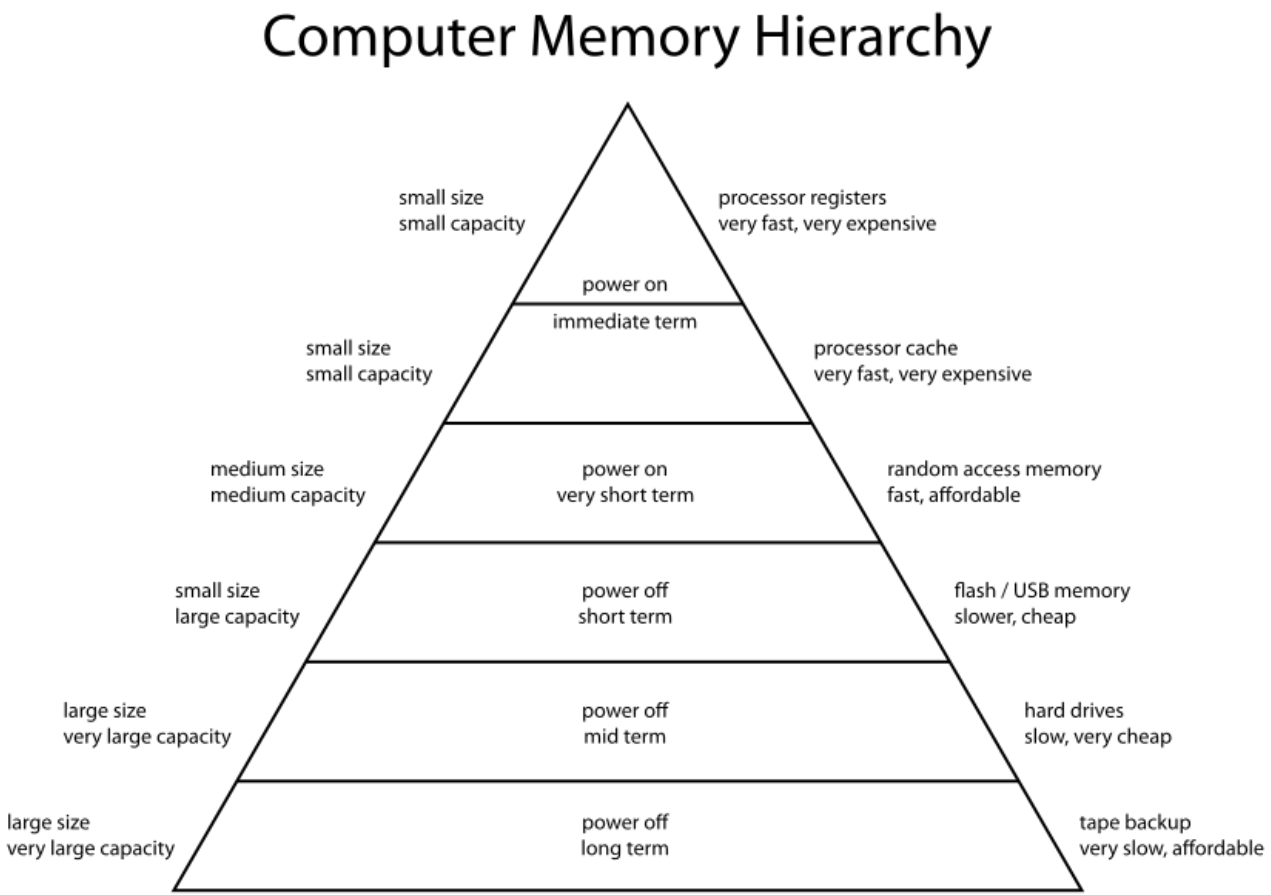
Wie gehen Daten verloren? - Hardwarefehler

- "Predictable Failures"
  - Vorhersehbar
  - Durch Abnutzung des Speichermediums
  - Abhängig von der Lebensdauer

Datenwiederherstellung

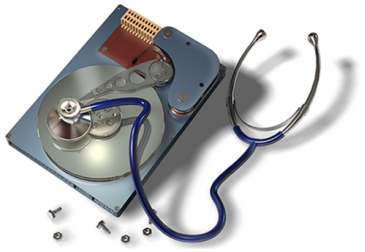


Wie gehen Daten verloren? - Hardwarefehler



[4]

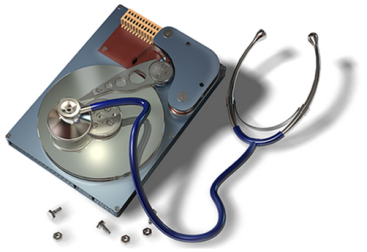
Datenwiederherstellung



Wie gehen Daten verloren? - Hardwarefehler

- "Unpredictable Failures"
  - Durch äußere Einflüsse oder Katastrophen
  - Nicht vorhersehbar

Datenwiederherstellung

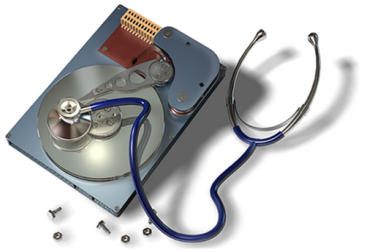


Wie gehen Daten verloren? - Hardwarefehler

- Unsachgemäßer Umgang mit Hardware:
  - Falsche Lagerung, Umweltbedingungen, ...
  - Falsches Herunterfahren, Entfernen von Speichermedien

➔ Ist Teilweise auch auf menschliches Versagen zurückzuführen

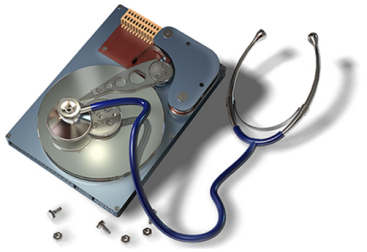
Datenwiederherstellung



Wie gehen Daten verloren? - Softwarefehler

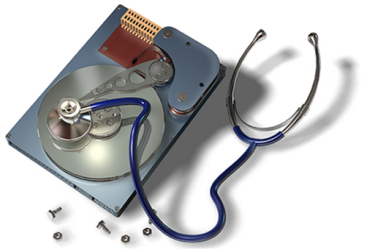
- Korruption von Daten durch:
  - Absturz von Programmen
  - Systemcrashes
  - ...
- Fehlende Rückwärtskompatibilität

Datenwiederherstellung



Wie gehen Daten verloren? - Manipulation von außen

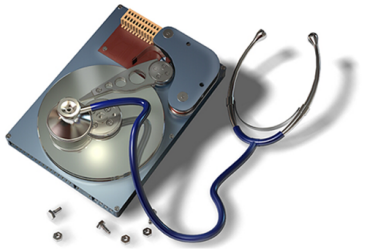
- Malware
- Hacker
- Mutwillige Zerstörung
  - Löschung
  - Zerstörung der Hardware



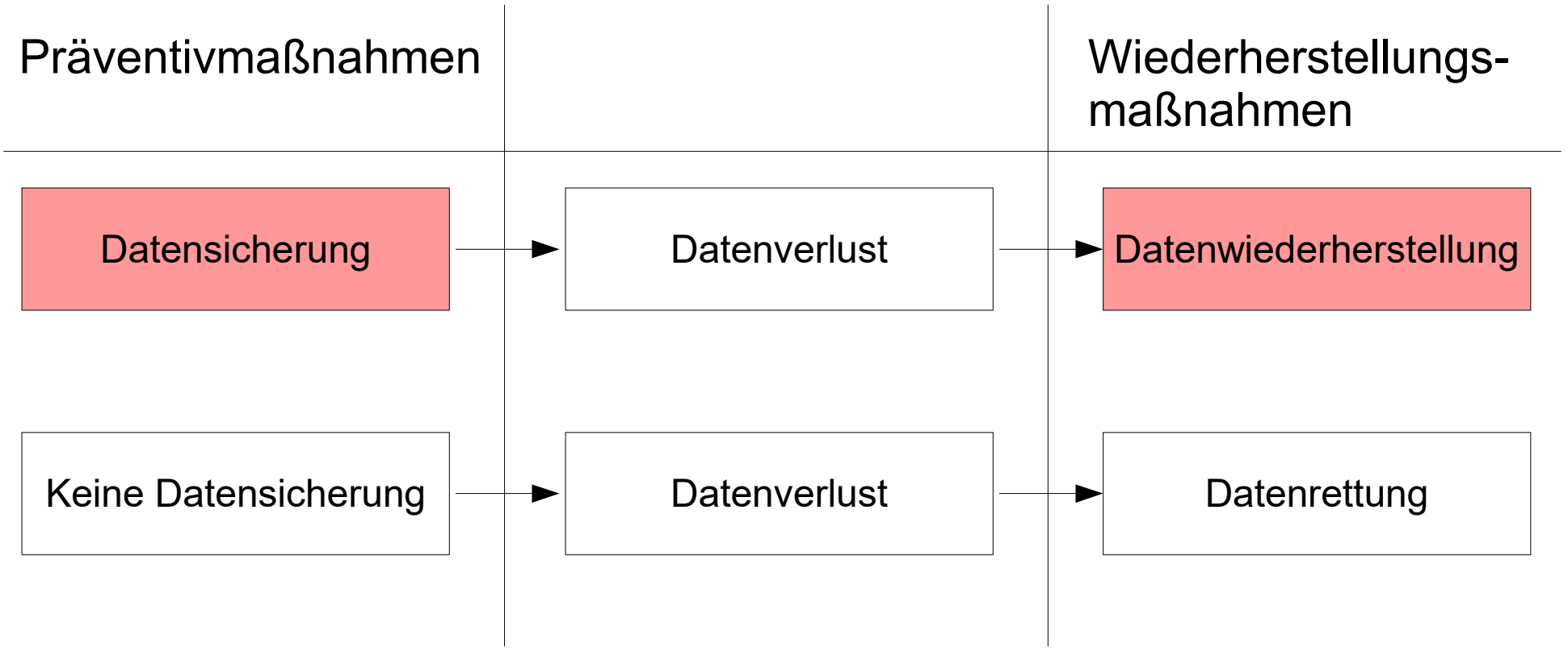
Gliederung

- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung

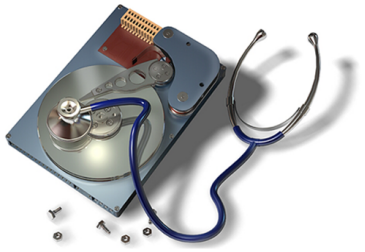
Datenwiederherstellung



Datensicherheit im Zeitverlauf



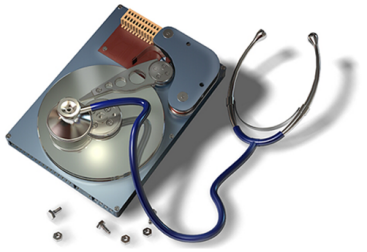
Datenwiederherstellung



Wiederherstellungs-/Präventionsmaßnahmen

- Datenwiederherstellung ist einfach, wenn Daten gut gesichert sind
- Ein gutes Datensicherungskonzept ist unumgänglich für eine vollständige Datenwiederherstellung!

Datenwiederherstellung

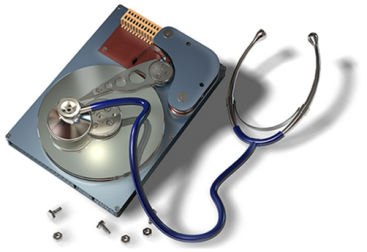


Wiederherstellungs-/Präventionsmaßnahmen

- Datensicherungskonzept umfasst:
  - Welche Daten
  - Frequenz
  - Art der Sicherung

➔ Wiederherstellungstests nicht vergessen!

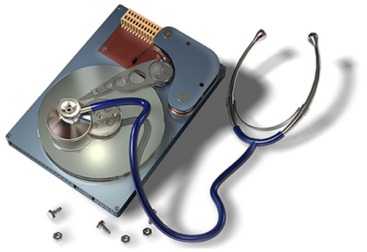
Datenwiederherstellung



Wiederherstellungs-/Präventionsmaßnahmen

- Im Unternehmen die richtigen Strukturen einrichten:
  - Incident Response Management
    - Wie geht man mit IT-Störungen um?
    - Wie stellt man die Daten möglichst schnell wieder her?
  - Security Information and Event Management (SIEM)
    - Zentrale Sammlung von sicherheitsrelevanten Daten
    - → Analyse von Mustern
    - → Früherkennung von Sicherheitsrisiken

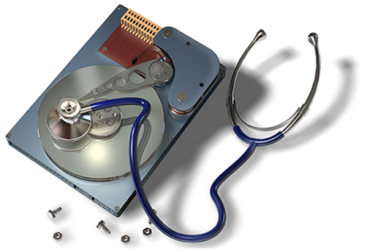
Datenwiederherstellung



Wiederherstellungs-/Präventionsmaßnahmen

- Methoden der Datensicherung:
  - Löschen/Manipulation erschweren:
    - Papierkorb einrichten
    - Zugangs-/Zugriffskontrolle
    - Verschlüsselung
    - Verstecken
  - Hardware-Instandhaltung

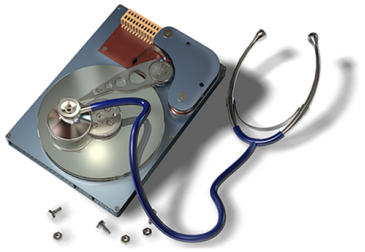
Datenwiederherstellung



Wiederherstellungs-/Präventionsmaßnahmen

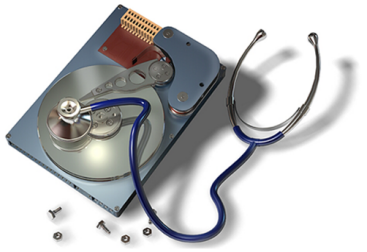
- Methoden der Datensicherung:
  - Katastrophenplan
  - Backup:
    - Mehrfach abspeichern
    - Separates Backup
  - RAID

Datenwiederherstellung

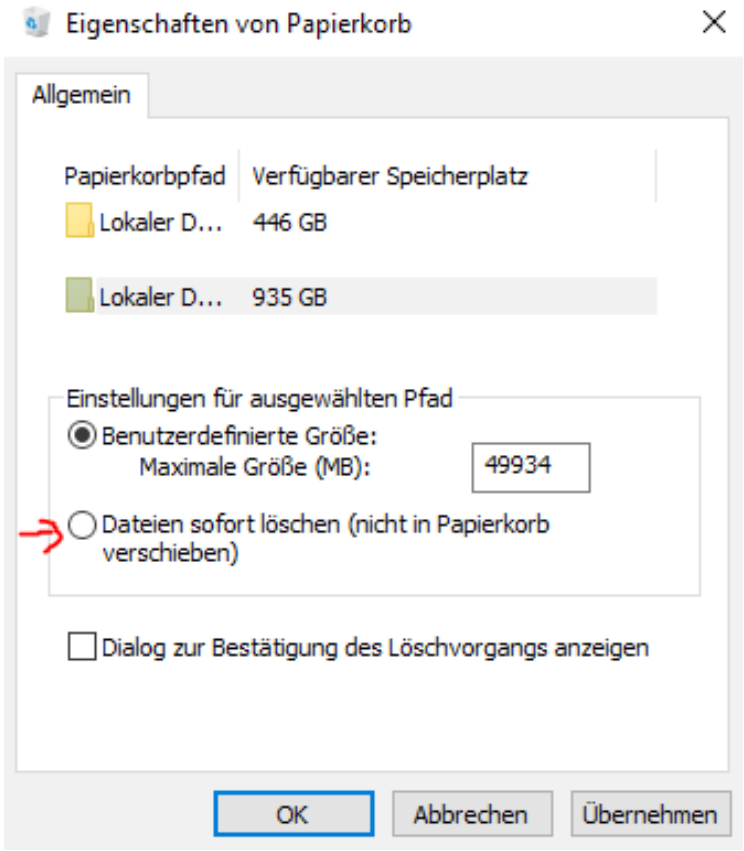


Papierkorb einrichten

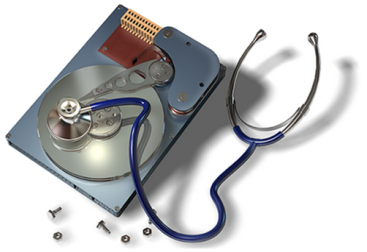
- Dient als Zwischenverzeichnis
- Daten werden nicht wirklich gelöscht
- Sind einfach wieder aus diesem Verzeichnis zurückholbar
- Funktioniert solange der Papierkorb nicht geleert wird
- Funktioniert nur auf lokalen Verzeichnissen



Papierkorb einrichten

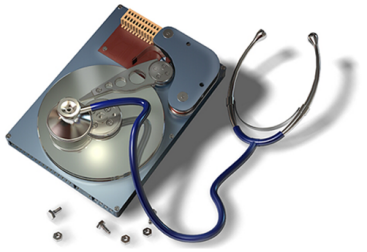


[5]



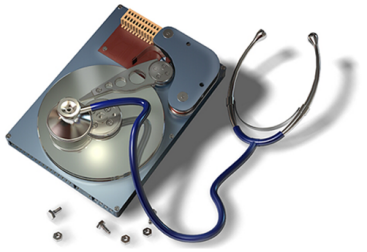
Papierkorb einrichten

- Hilft bei:
  - Menschlichen Fehlern
- Hilft nicht bei:
  - Katastrophen
  - Hardware-Defekten
  - Manipulation von außen
  - Softwarefehlern



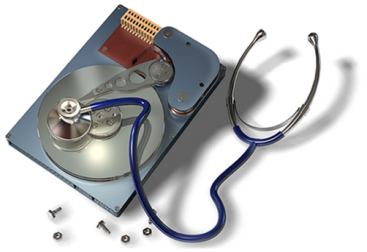
Zugangs-/Zugriffskontrolle

- Unbefugte von Nutzung vertraulicher Ressourcen abhalten
- z.B. durch:
  - Passwörter
  - Benutzerkonten, -gruppen, usw.
  - Rechtezuweisung



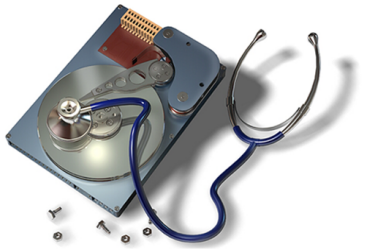
Zugangs-/Zugriffskontrolle

- Hilft bei:
  - Menschlichen Fehlern
  - Manipulation von außen
- Hilft nicht bei:
  - Katastrophen
  - Hardware-Defekten



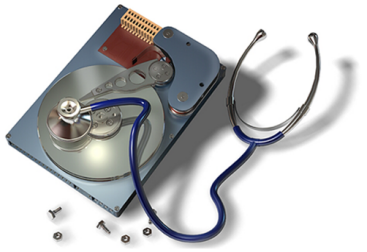
Hardware-Instandhaltung

- Durchschnittliche Lebensdauer des gewählten Speichermediums beachten
- Regelmäßiger Austausch der Hardware
- Bereitstellung von geeigneten Umweltbedingungen:
  - Temparatur
  - Feuchtigkeit
  - ...

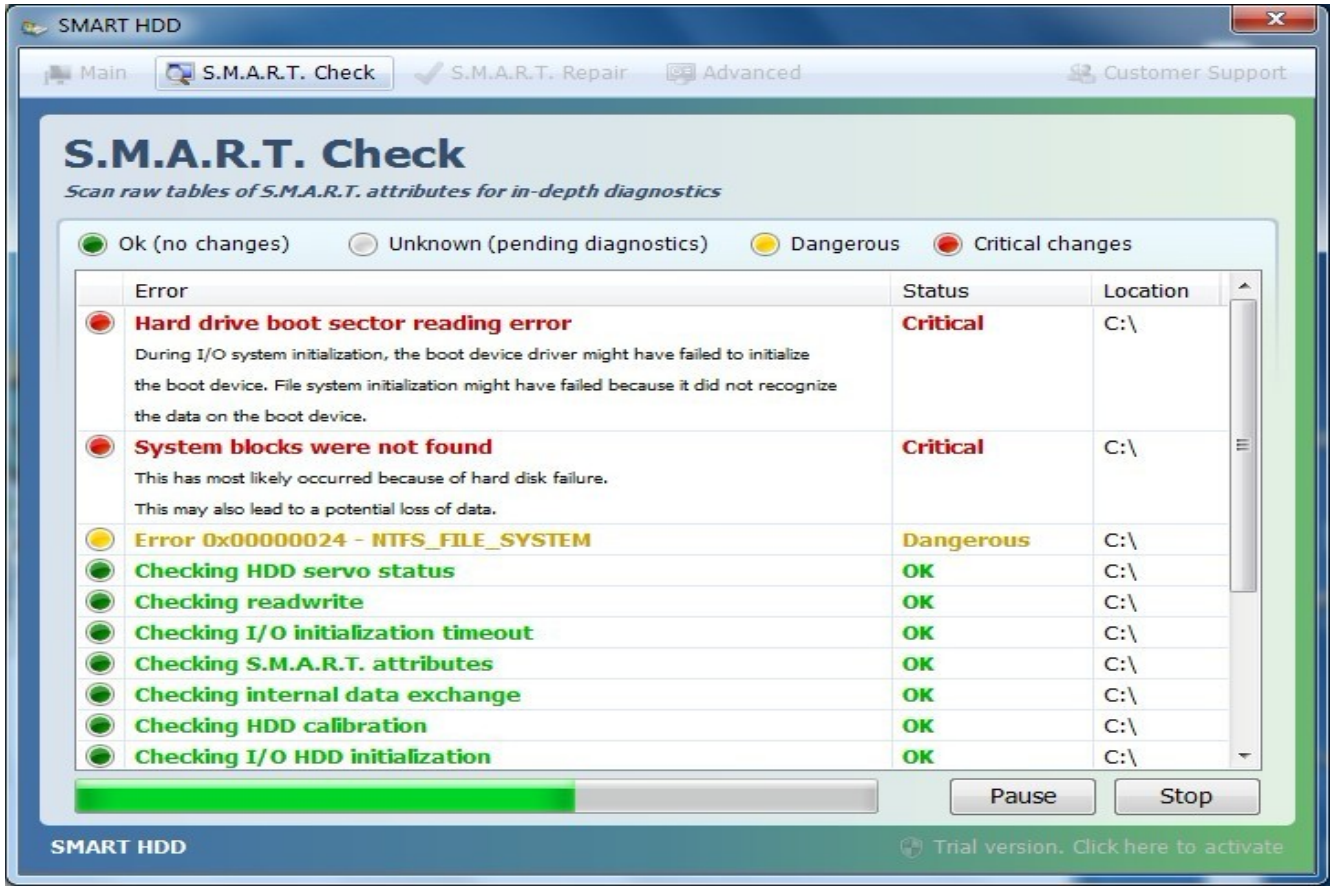


Hardware-Instandhaltung

- Verwendung von Überwachungstools
  - Auslesung verschiedener Sensoren
  - Frühzeitige Erkennung von möglichem Hardwareversagen

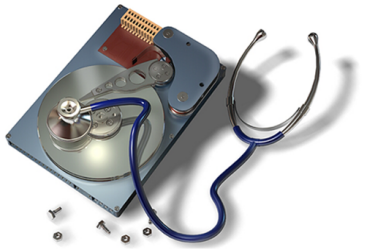


Hardware-Instandhaltung



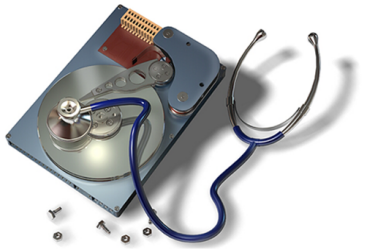
[6]

Datenwiederherstellung



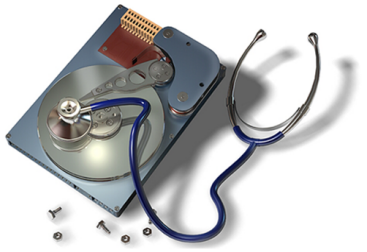
Hardware-Instandhaltung

- Hilft bei:
  - "Predictable Failures"
- Hilft nicht bei:
  - Katastrophen
  - Menschlichen Fehlern
  - Manipulation von außen
  - Softwarefehlern



Katastrophenplan

- Versuch, Auswirkungen von Katastrophen zu verringern
- Katastrophen sind sehr unwahrscheinlich, haben aber hohes Schadenspotenzial

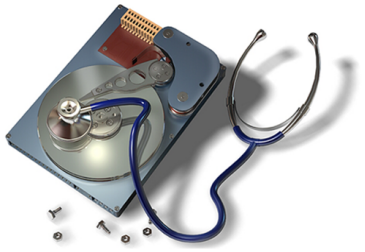


Katastrophenplan

Beispiele:

- Notstromversorgung
- Serverräume mit weniger Sauerstoffanteil

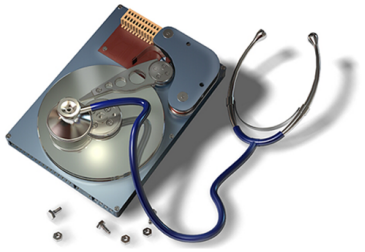
- Manche Katastrophen sind nicht vorhersehbar
  - z.b. Terrorismus



Katastrophenplan

- Hilft bei:
  - "Unpredictable Failures"

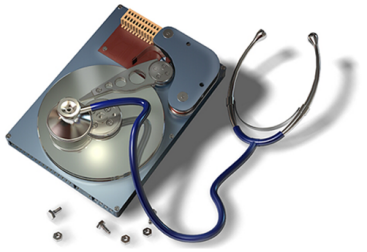
Datenwiederherstellung



Mehrfach abspeichern

- Nichts anderes als ein Backup in kleinerem Umfang
- Besonders hilfreich bei Office-Anwendungen o.Ä.
- z.B. bei:
  - Überschreibung eines Templates
  - Crash während des Speicherns

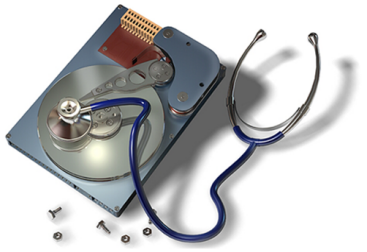
Datenwiederherstellung



Mehrfach abspeichern

- Passiert bei vielen Anwendungen automatisch
  - Für z.B. Autowiederherstellung
- Einfach aber effektiv
- ACHTUNG: Backup liegt meist auf selbem Datenträger!

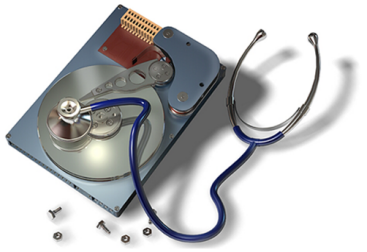
Datenwiederherstellung



Mehrfach abspeichern

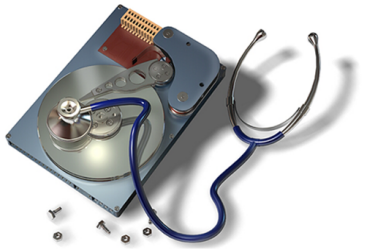
- Hilft bei:
  - Menschlichen Fehlern
  - Softwarefehlern
- Hilft nicht/selten bei:
  - Malware
  - Hardwaredefekten
  - Katastrophen

Datenwiederherstellung



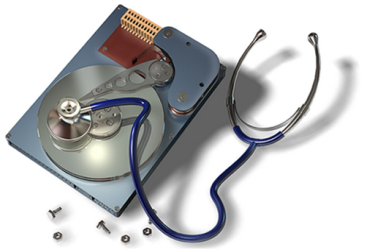
Backup

- Sicherung einzelner Daten oder gesamter Speichermedien auf separate Speichergeräte
- Je häufiger, desto effektiver
- Auf dafür geeigneten Speichermedien
  - Langlebig
  - Robust
  - Hohe Kapazität



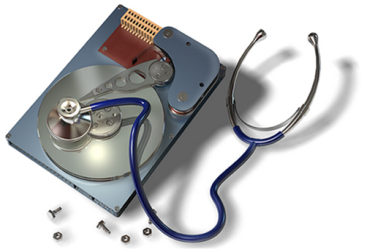
Backup

- Müssen sicher gelagert sein:
  - Separat, für den Katastrophenfall
  - Unzugänglich für Unbefugte
  - In geeigneten räumlichen Bedingungen
- Arten z.B.:
  - Speicherband
  - HDD (anstatt SSD)
  - Cloud



Backup

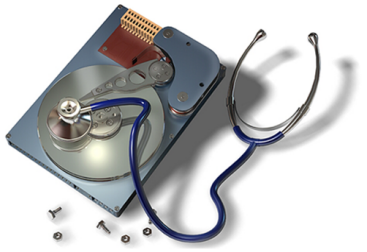
- Balance finden zwischen Verfügbarkeit und Vertraulichkeit
  - ➔ Mehr Backups = Höhere Chance, dass Unbefugte an sie herankommen
  - ➔ Je unzugänglicher, desto unhandlicher



Backup

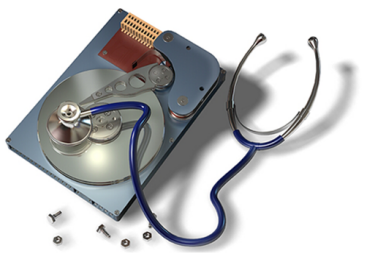
- Hilft bei:
  - Allem!
- VORSICHT: Bei Backups von schon korrumpierten Daten (durch z.B. Malware) kann es später zu größeren Problemen kommen!

Datenwiederherstellung



RAID

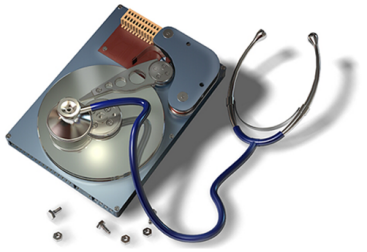
- **R**edundant **A**rrays of **I**ndependent **D**isks
- Mehrere Datenträger laufen parallel
- Durch mehrfaches abspeichern wird Verlustwahrscheinlichkeit bei Hardwaredefekt verringert
- Dem System erscheint es wie eine einzige Festplatte



RAID

- Verschiedene Typen von Arrays, z.B.:
  - RAID 1: Mirroring
    - Klonen der Daten
  - RAID 0: Striping
    - Verteilen der Daten → keine Redundanz!
  - Verschiedene Kombinationsmöglichkeiten

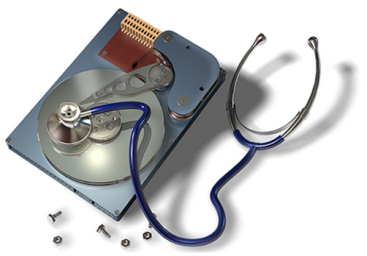
Datenwiederherstellung



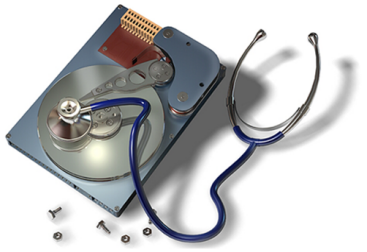
RAID

- Hilft (je nach Art) bei:
  - Hardwaredefekt
- Hilft nicht bei:
  - Malware
  - Menschlichem Versagen
  - Katastrophen
  - Softwarefehlern

Datenwiederherstellung

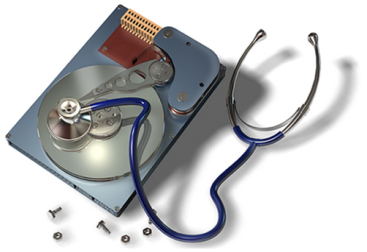


RAIDs sind kein Backup und ersetzen dieses auch nicht!



Verschlüsselung

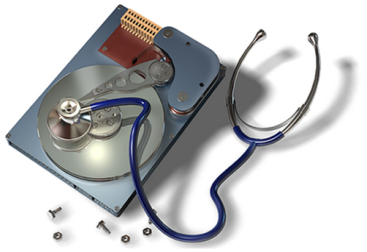
- Sichert nicht nur Vertraulichkeit
- Verhindert auch Verändern und Unzugänglichmachung von Daten (Integrität)



Verschlüsselung

- Hilft bei:
  - Malware
  - Hackern
- Hilft nicht bei:
  - Hardwaredefekten
  - Softwarefehlern
  - Katastrophen

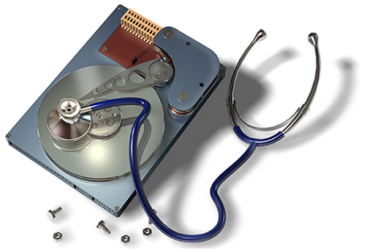
Datenwiederherstellung



Verstecken

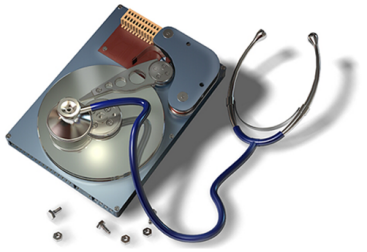
- Schütz vor allem bei gezielten Manipulationsversuchen
- Wenn man nicht weiß, dass Daten existieren, kann man sie nicht verändern
- Beispiel: Steganographie

Datenwiederherstellung



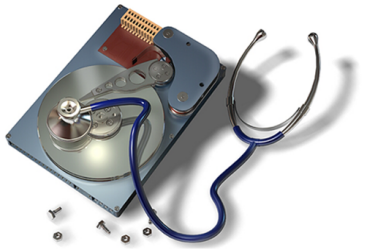
Verstecken

- Hilft bei:
  - Hackern
  - Manipulationsversuchen
- Hilft nicht bei:
  - Hardwaredefekten
  - Katastrophen



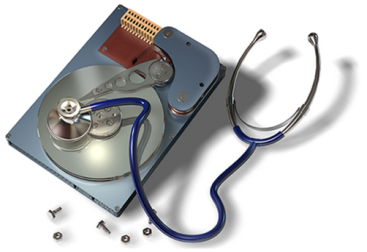
Datensicherung

Katastrophe	Hardwaredefekt	Menschliches Versagen	Manipulation	Softwarefehler
Backup				
Katastrophenplan	Instandhaltung	Zugangs-/Zugriffskontrolle		Mehrfach abspeichern
	RAID	Papierkorb	Verschlüsseln	
		Mehrfach abspeichern	Verstecken	



Datensicherung

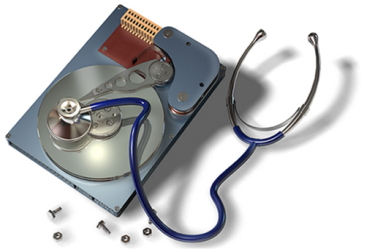
- Fazit:
  - Je mehr Methoden man verwendet, desto sicherer sind die Daten
  - ➔ Absicherung gegen verschiedene Verlustarten
  - ➔ Aufgrund von hohem Aufwand aber nur für sehr wichtige Daten zu empfehlen



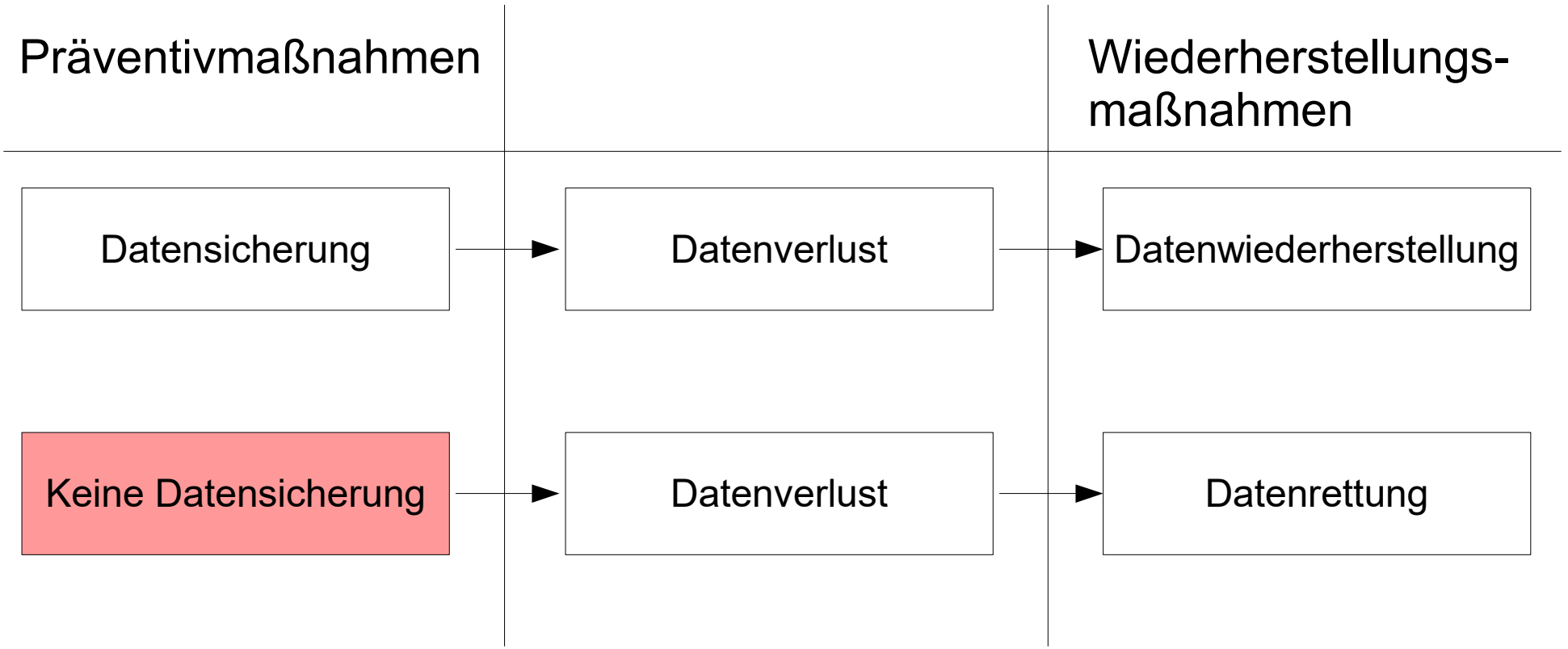
Gliederung

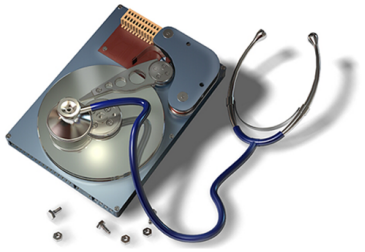
- Einleitung
- Grundsätzliches zur Datenwiederherstellung
- Part 1: Datenwiederherstellung
  - Wie gehen Daten verloren?
  - Wiederherstellungs-/Präventionsmaßnahmen
  - Datenrettung

Datenwiederherstellung



Datensicherheit im Zeitverlauf



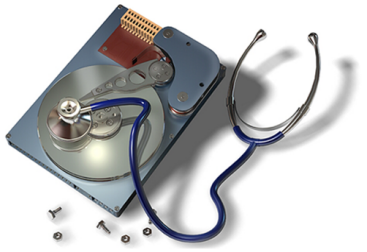


Datenrettung

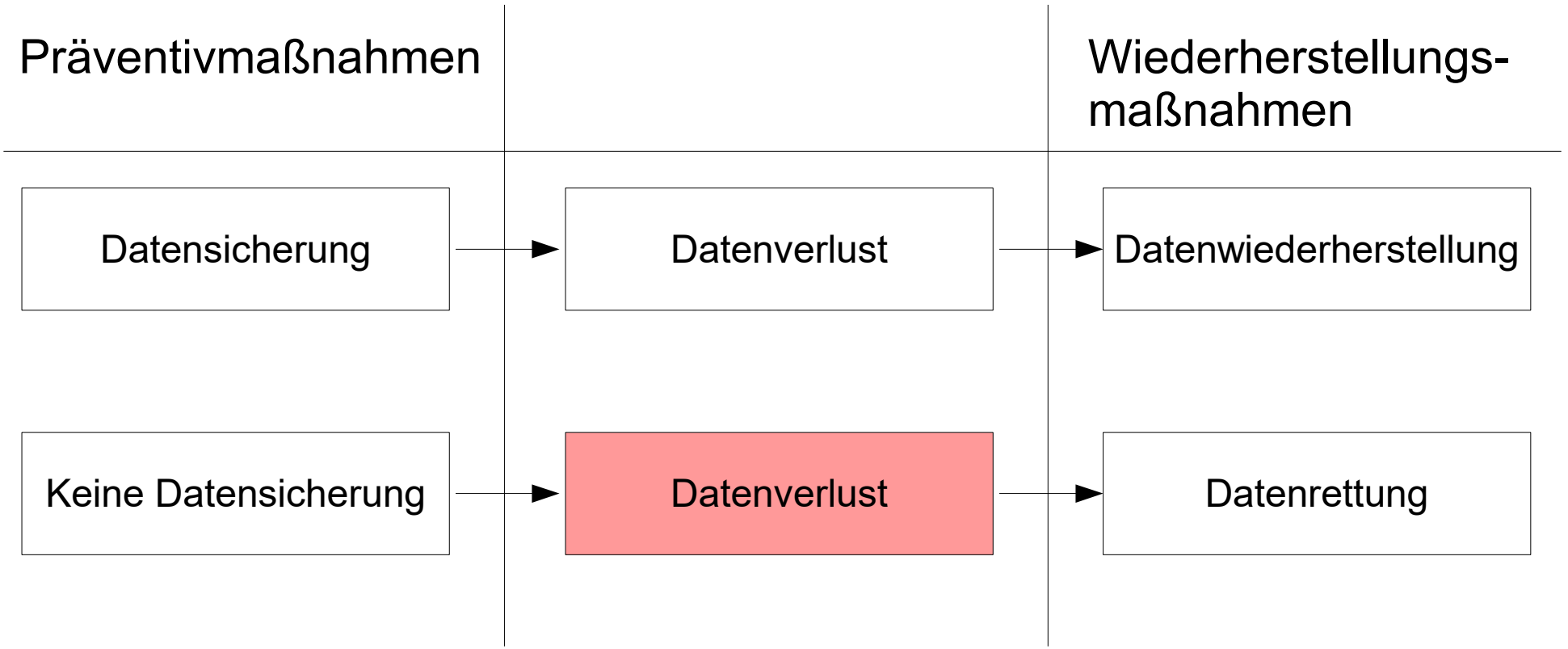
- Wenn kein ausreichendes Backup vorhanden ist, müssen Daten auf anderen Wegen gerettet werden
- Je nach Wichtigkeit werden unterschiedliche Methoden angewandt

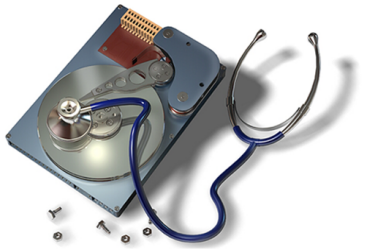
➔ Für wichtige Daten Experten beauftragen!

Datenwiederherstellung



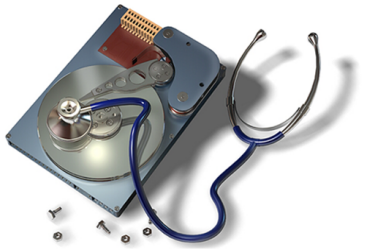
Datensicherheit im Zeitverlauf





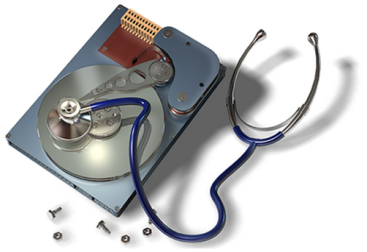
Datenrettung

- Verlustart:
  - Löschung
  - Hardwaredefekt



Datenrettung - Löschung

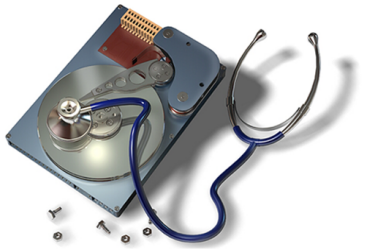
- Wie werden Daten gelöscht?
  - Werden in Master-File-Table (o.Ä.) markiert
  - Speicherort wird für neue Daten freigegeben
  - HDD:
    - Daten bleiben vorhanden, bis sie von anderen überschrieben werden



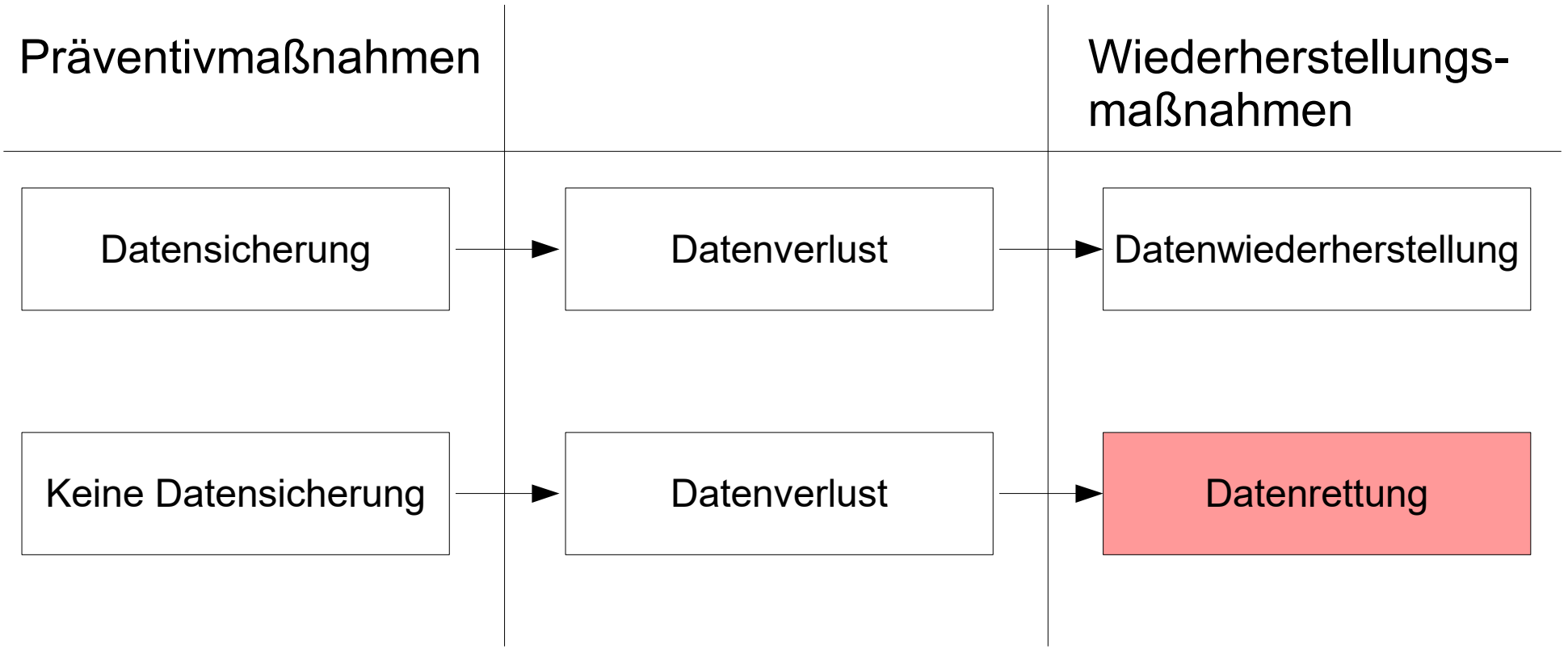
Datenrettung - Löschung

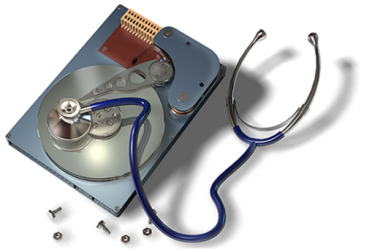
- Wie werden Daten gelöscht?
  - SSD:
    - Daten werden durch "Trimmen" vorzeitig gelöscht
    - ➔ Da Flashspeicher nicht auf vorhandene Daten schreiben können
    - Durch "Wear-Leveling" zerstört eine Datei bei SSDs meist mehr Dateien als bei HDDs

Datenwiederherstellung



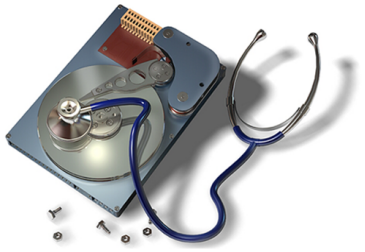
Datensicherheit im Zeitverlauf





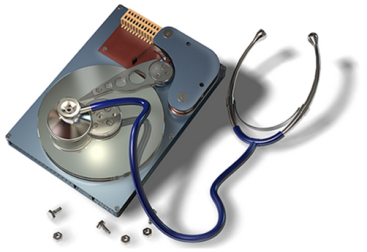
Datenrettung - Vorgehen

- Nach Feststellen des Fehlers sofort Speichermedium trennen/abschalten
  - Verhindert potenzielles Überschreiben gelöschter Daten
- Öffnen der Hardware unter Reinraum-Bedingungen
  - Sonst weiterer Datenverlust!



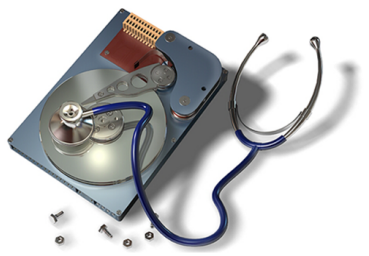
Datenrettung - Vorgehen

- Reparatur oder Auswechseln von kaputten Teilen
- Image des Datenträgers erstellen
  - Nicht davon ausgehen, dass ein betroffenes System zweimal hintereinander das gleiche tut!
- Nur auf Kopien vom Image arbeiten
  - Um immer ein funktionierendes Original zu behalten



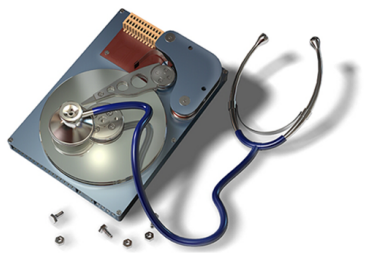
Datenrettung - Vorgehen

- Suchen nach markierten Dateien in MFT
- Auslesen des nicht zugewiesenen Speichers ("unallocated space")
- Findung von Datei-Anfängen (Headern)
  - Auslesen von Meta-Daten
- Auslesen von Datei-Inhalten



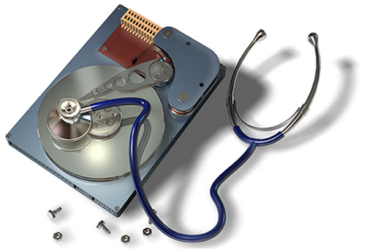
Datenrettung

[7]



Part 2: IT-Forensik

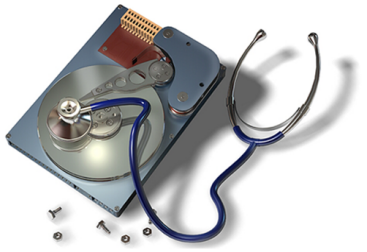
[8]



Gliederung

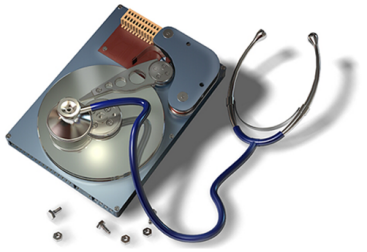
4 Part 2: IT-Forensik
- Was ist das?
- Vorgehen
- Schutzmechanismen
- Demo

- Fazit
- Medien-/Quellenverzeichnis



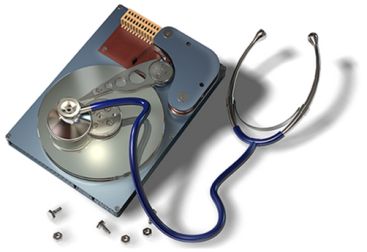
IT-Forensik

- Hat sich aus Spezialwissenschaft für Ermittlungsbehörden entwickelt
  - Ziel: Findung von gerichtsfesten Beweisen, um einen Täter einem Vorfall zuzuordnen
- Auch von Unternehmen eingesetzt
  - ➔ Um Angriffe nachzuvollziehen und aus Fehlern zu lernen
  - ➔ Gerichtsfeste Analyse nicht notwendig, aber sinnvoll



IT-Forensik

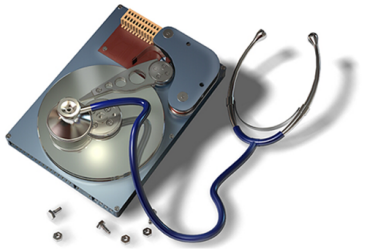
- Bedingungen für Gerichtsfestigkeit:
  - Durchführung von Experten
  - 4-Augen-Prinzip
  - Benutzung anerkannter Tools
  - Genaue Dokumentation aller Schritte
  - Sichere und nicht manipulierbare Verwahrung der Beweise



IT-Forensik

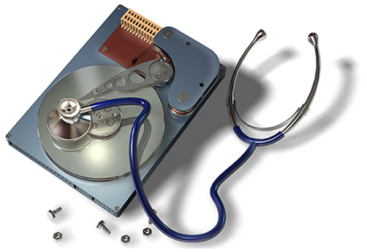
- Unterscheidung:
  - Post-Mortem-Analyse
    - Verwendet hauptsächlich Methoden der Datenrettung
  - Live Forensik
- Häufig im Konflikt zu Incident Response Management
  - Schnelles Beheben des Problems

    vs.
  - Gründliche Beweissicherung



IT-Forensik

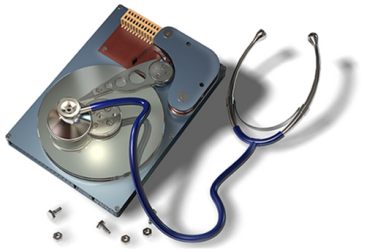
- Einsetzbar z.B. bei:
  - Datendiebstahl o. Manipulation durch Mitarbeiter
  - Unternehmensbetrug
  - Arbeitszeitbetrug
  - Besitz illegaler Daten
  - Illegale Downloads
  - ...



Gliederung

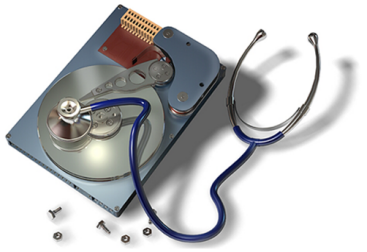
4 Part 2: IT-Forensik
- Was ist das?
- Vorgehen
- Schutzmechanismen
- Demo

- Fazit
- Medien-/Quellenverzeichnis



IT-Forensik - Vorgehen

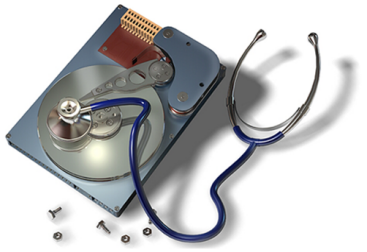
- SAP-Modell:
  - Secure
  - Analyse
  - Present
- Nicht nur Daten selbst, sondern auch Logdaten, Metadaten usw. sind wichtig
  - ➔ Verbindungsprotokolle erstellen
  - ➔ Zeitliche Rekonstruktion einer Straftat



Gliederung

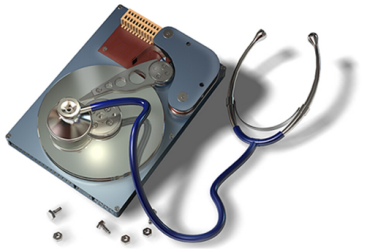
4 Part 2: IT-Forensik
- Was ist das?
- Vorgehen
- Schutzmechanismen
- Demo

- Fazit
- Medien-/Quellenverzeichnis



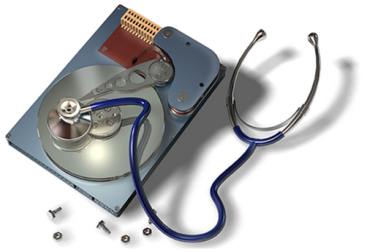
IT-Forensik - Schutz

- Gründe:
  - Kann auch von Angreifern verwendet werden
  - Man hat etwas zu verbergen
- Ziel:
  - Wiederherstellungsversuche so aufwendig gestalten, dass sie sich nicht mehr lohnen



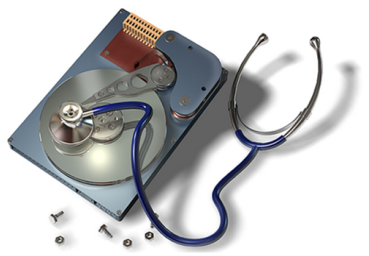
IT-Forensik - Schutz

- Methoden:
  - Verschlüsselung
  - "Sicheres" Löschen!
    - ➔ Überschreiben von Speichermedien mit zufälligen Daten
    - ➔ Damit kein Auslesen des nicht zugewiesenen Speichers möglich ist
    - ➔ Vergleichbar mit Schreddern von Papierdokumenten

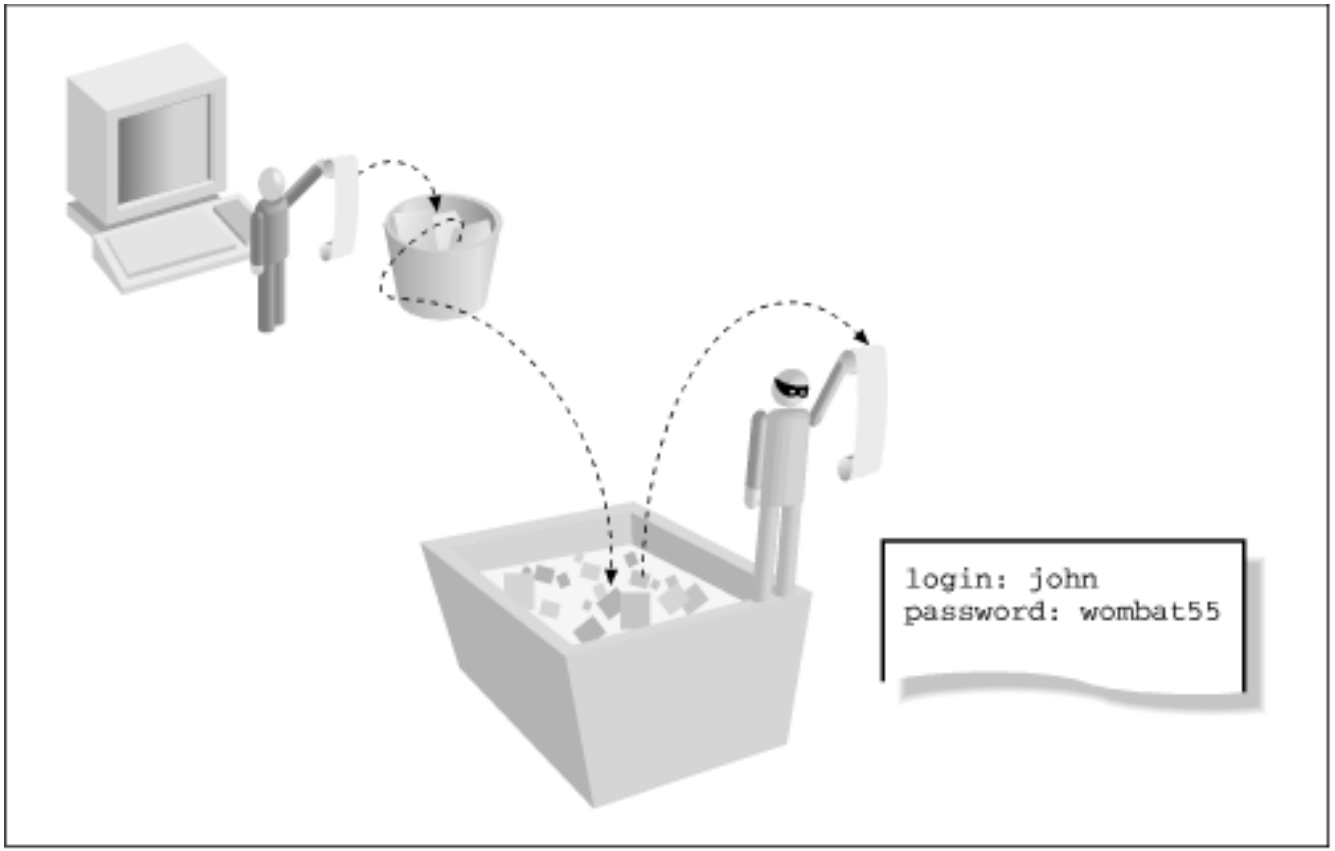


IT-Forensik - Schutz

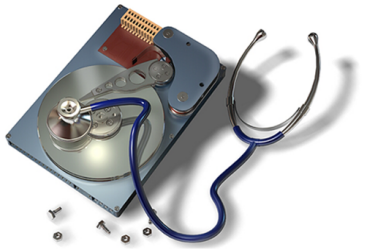
- Methoden:
  - Entmagnetisieren (Degausser)
    - Nur bei Magnetischen Datenträgern
    - Macht die meisten Datenträger unbrauchbar
  - Zerstörung der Festplatte
    - Tatsächliches Schreddern
    - Hammer
    - ...



IT-Forensik - Schutz

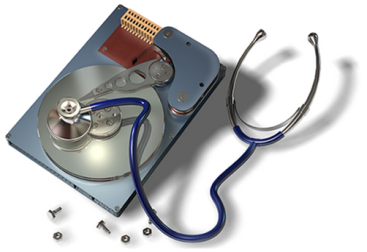


[9]



IT-Forensik - Schutz

- Auch hier gilt: Je mehr Methoden man verwendet, desto schwerer sind sie zu rekonstruieren!
- ABER: Auch wenn Daten erfolgreich unlesbar gemacht werden können - eine Datenzerstörung ist immer erkennbar!
  - ➔ Man kann erkennen, dass jemand etwas zu verbergen hat, weiß nur nicht was

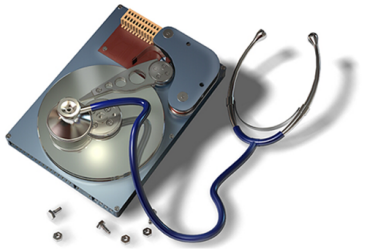


Gliederung

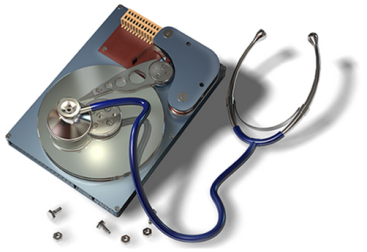
4 Part 2: IT-Forensik
- Was ist das?
- Vorgehen
- Schutzmechanismen
- Demo

- Fazit
- Medien-/Quellenverzeichnis

Datenwiederherstellung

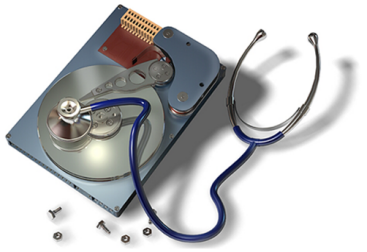


DEMO



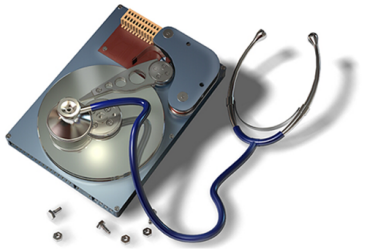
Gliederung

- Part 2: IT-Forensik
  - Was ist das?
  - Vorgehen
  - Schutzmechanismen
  - Demo
- Fazit
- Medien-/Quellenverzeichnis



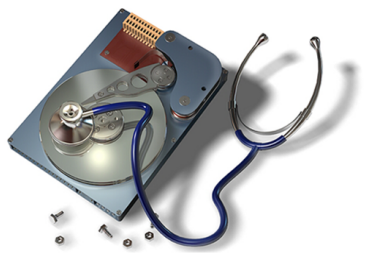
Fazit

- Datenwiederherstellung ist keine gute Alternative zu Datensicherung!
  - ➔ Sollte nur in Ausnahmefällen angewendet werden müssen
- Keine Sicherungsmethode kann Backups ersetzen!



Fazit

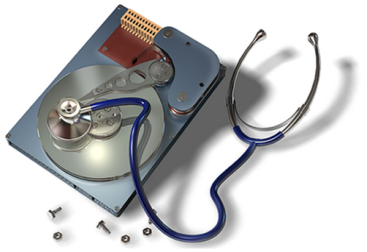
- Mit den richtigen Tools können auch Laien viele Daten retten!
- Jeder kann meine Daten wiederherstellen – auch Unbefugte!
  - ➔ Datenträger vor Entsorgung unlesbar machen



Fazit

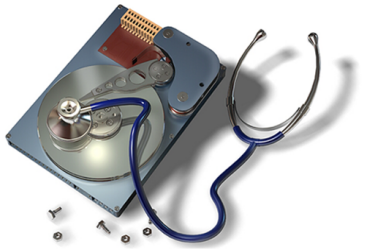
ALSO...

Datenwiederherstellung



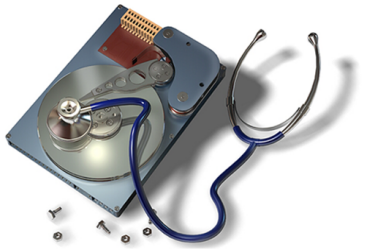
Fazit

- Wenn euch eure Daten wichtig sind:
  - Vetrauliche Daten verschlüsseln!
  - Unverzichtbare Daten regelmäßig separat sichern!
  - Im Ernstfall schnell handeln!
  - Im Notfall lieber Experten fragen!



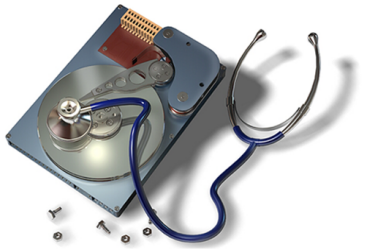
Fazit

- Wenn euch eure Daten wichtig sind:
  - Immer mit dem schlimmsten rechnen → Vorbereitet sein!
  - ➔ Nicht denken "Sowas passiert mir nicht" oder "wer will schon MEINE Daten haben!"



Gliederung

4. Part 2: IT-Forensik
   - Was ist das?
   - Vorgehen
   - Schutzmechanismen
   - Demo
- Fazit
- Medien-/Quellenverzeichnis



Medienverzeichnis

[1] Logo für Foliendesign: https://static1.squarespace.com/static/52224c6de4b0b90e69169ea2/t/522aa271e4b0c5431461a882/1378525813383/hardware.png

[2] Screenshot von https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

[3] https://assets.krollontrack.com/hv3/images/img_ursachen-datenverlust_krollontrack.jpg

[4] https://upload.wikimedia.org/wikipedia/commons/0/0c/ComputerMemoryHierarchy.svg

[5] Eigener Screenshot

[6] https://blog.teesupport.com/wp-content/uploads/2012/03/S.M.A.R.T.-HDD.jpg

[7] http://www.stellardatenrettung.de/wp-content/uploads/2015/08/FBP0127.jpg

[8] https://www.hwzdigital.ch/files/2016/03/digital-forensic-banner-1280x0-c-default.jpg

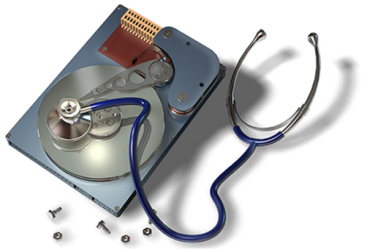
[9] https://hackerstribe.com/wp-content/uploads/2013/06/dumpster-diving.gif

Bild-Quellen für Demo:

[10] https://images.celebfamily.com/wp-content/uploads/2014/09/jennifer-katharine-gates.jpg

[11] https://upload.wikimedia.org/wikipedia/commons/thumb/e/ec/Melinda_Gates_-_World_Economic_Forum_Annual_Meeting_2011.jpg/1200px-Melinda_Gates_-_World_Economic_Forum_Annual_Meeting_2011.jpg

[12] http://starschanges.com/wp-content/uploads/2016/11/bill-gates-family-1-950x600.jpg

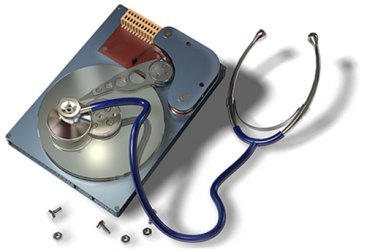


Quellenverzeichnis

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2
https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html
https://www.cubespotter.de/cubespotter/it-forensik-digitale-spurensuche/
http://www.admin-magazin.de/Das-Heft/2013/11/Forensische-Toolkits-zur-Rekonstruktion-von-Browser-Sessions
https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik_node.html
https://www.pcwelt.de/ratgeber/Was-genau-passiert-beim-Loeschen-von-Daten-Ratgeber-Datenrettung-182351.html
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Datensicherung/Datenverlust/datenverlust_node.html
http://www.pc-magazin.de/ratgeber/ssd-flash-geloeschte-daten-wiederherstellen-datenrettung-tools-download-tipps-2111154.html
https://www.brandmauer.de/blog/it-security/was-sind-die-wesentlichen-ursachen-fuer-datenverlust
https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reports-wrl12345usen-20170719.pdf
https://svs.informatik.uni-hamburg.de/teaching/gss-10einfsi.pdf
wikipedia.org
https://de.slideshare.net/TobiasScheible/vortrag-zum-thema-digitale-forensik
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-de-4/s1-response-plan.html
https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html
https://svs.informatik.uni-hamburg.de/teaching/gss-20resi.pdf
https://www.storagecraft.com/blog/5-reasons-raid-not-backup/
https://www.youtube.com/watch?v=bYHsClMdJUs
http://datasecurityinc.com/security/degausser.html
https://www.intersoft-consulting.de/it-forensik/it-forensik-praxisfaelle/
https://www.storagecraft.com/blog/5-reasons-raid-not-backup/
http://www.searchsecurity.de/definition/Security-Information-and-Event-Management-SIEM
https://public.dhe.ibm.com/common/ssi/ecm/wr/en/wrl12345usen/watson-customer-engagement-watson-marketing-wr-other-papers-and-reports-wrl12345usen-20170719.pdf
www.krollontrack.de

Alle Internetquellen wurden zuletzt aufgerufen am: 05.12.2017

Datenwiederherstellung



Vielen Dank für die Aufmerksamkeit!