Datenspeicherung und Backups als Beweismittel

Grundlagen und Herausforderungen

Archimedes: Virtueller 11. Techniker / Juristen Dialog
11. November 2020

Begriffe: Daten und Datei

- Daten
  - Symbole zur Darstellung von Informationen
  - IKT zur Speicherung und Verarbeitung: elektronische Daten
- Dateien
  - Menge von Daten die als zusammengehörig definiert und gespeichert sind
  - Daten sind -zumindest in Teilen- zusammengehörig interpretierbar
  - Festlegungen zur Interpretation: Dateityp, Codierung, Formate
    - eml, xls, xlsx, doc, docx, pdf, gif, jpg, dwg, mpeg mp4 …….
    - Z.B.: Für Texte, Bilder, Tabellen, Projektpläne …….
- Darstellung von Dateiinhalten
  - Benötigt ein Anzeigeprogramm (oft das Bearbeitungsprogramm oder Viewer)
  - Dateien können auch Input für Programme zur Verarbeitung beinhalten
  - Spezialisiert für den Inhaltstyp, oder bezogen auf das Erstellungsprogramm

Dateien: Informationen

- Untergliederung von Dateiinhalten entsprechend einer Kategorisierung
  Hier wesentlich:

- „Dateiinhalt“ („data“, …)
  Jene Information deren Interpretation (laut jeweiliger Konvention) den Dateiinhalt verwendbar (meist „sichtbar“) macht

- Metadaten (Header, Tags, ….)
  Zugehörige Information betreffend den Inhalt. Z.B.: Info über die Codierung und Art, Zeitpunkte (Erstellung, Zugriff, Änderung …), Geo- Information, Geräteinformation, ……..

Wesentliche technische Dateieigenschaften

- Technische Lesbarkeit
  - Möglichkeit die Daten (Datei) aus einem Speichermedium fehlerfrei auszulesen

- Konsistenz
  - Entsprechung der Daten nach definierten Konsistenzkriterien

- Interpretierbarkeit
  - Möglichkeit den Dateninhalt dem definierten Zweck gemäß darzustellen
  - Z.B.: Ein Bild anzuzeigen, einen Projektplan zu befüllen, …

Voraussetzungen dafür:
Lesbarkeit, Konsistenz (Defizite oft tw. „sanierbar“)
Programm zur Anzeige bzw. Bearbeitung – oft ist das auch das Erstellungsprogramm

Datenbank

- Als zusammengehörig definierte, strukturierte Sammlung von Daten
  Auch: Datenbasis
- Datenbankmanagementsystem (Software: DBMS) zur Verwaltung von Datenbanken
  Technisch individueller struktureller Aufbau der Datenspeicherung je Datenbankprodukt (z.B.: MS SQL, Oracle, Progress, proprietäre DBMS …)
- DB Inhalt: Interpretation definiert durch Bildungsregeln und Konsistenzkriterien
- Konsistente Datenbank: Ergibt sich aus der Überführung einer konsistenten DB durch Anwendung einer (zulässigen) Transformation
  Erlaubt eine Widerspruchfreie vollständige Interpretation der Inhalte

Beweismittel: Herstellung von Kopien

Technischer Vorgang: „Kopieren von – nach“

Kopieren von Dateien - einzeln oder programmgesteuert
- Wesentlich: Zeitpunkte der jeweiligen Speicherung der Kopie
- Problem: unverfälschte Übernahme der Metadaten (soweit vorhanden)

Kopieren von Dateisystemen (Folder) mit zusammengehörigen Dateien
- Problem: sequentielles Kopieren – Risiko: Verlust der Konsistenz
- Problem: unbemerkte „blockierte“ Dateien (zB weil geöffnet)

Kopieren von Datenbanken – je nach DB ist der Inhalt in einer Datei oder in Dateisystemen (mehrere zusammengehörige Dateien
- Kopieren des gesamten DBMS samt Daten oder DB Export („dump“)
- Problem: „geöffnete“ DBs, inkonsistente Kopien

Backup

Set von Dateien die zusammengehörig für einen bestimmten Zweck kopiert werden.

Eigenschaften: Große Datenvolumina, spezielle Datenträger und Software für das Backup

Wesentliche Parameter: Quelle / Ziel (Speicherorte)

zB.: lokale Datenträger, „removable“ Datenträger, Cloud Storage

Übliche Zwecke:

Vorsorge zur Wiederherstellung nach Defekten

Herstellung von Kopien zur Verbringung an andere Orte

Backup - Verwertbarkeit

Geplanter Zweck: Z.B.: Wiederherstellung nach einem Defekt, oder Wiederherstellung von Dateien um einen bestimmten Sachverhalt beweisen zu können)

Vollständigkeit und Konsistenz sowie die Rechte auf alle Dateien zugreifen zu können erforderlich um die Verwendbarkeit zu gewährleisten und Eigenschaften beweisen zu können.

Frage als Beispiel:

Ein Datenbestand wird mit einer DB vom Zeitpunkt x , Dateien vom Zeitpunkt y und mit Emails vom Zeitpunkt z wiederhergestellt.

Ist die ableitbare Info korrekt und vollständig und kann das, was beweisen werden soll schlüssig dargestellt werden?

Beweismittel: Herstellung von Kopien

Technischer Vorgang: Herstellung von „vollständigen“ Kopien

Problem: Datenvolumen, Lizenzrechte (Programme können später nicht gestartet werden –abgelaufene Lizenz)

Kopieren von kompletten physischen „Maschinen“: Herstellung eines „Image“

Kopieren von kompletten virtuellen Maschinen: VM Image oder Dump

Jeweils der „gesamte“ Inhalt gesichert: Erlaubt die Wiederherstellung des gesamten Systems – falls nicht weitere Systeme (Computer, Datenträger, oder Web Dienste …) benötigt werden.

Herstellung von „Snap Shots“ von Speichersystemen (die das leisten)

Konsistentes Abbilds zu einem Zeitpunkt möglich

Verwendung von Dokumentationssoftware

Gesamte Funktion der Verwaltung und Speicherung von Projektdaten

in einer spezialisierten Applikation (für alle Dokumententypen) abgedeckt:

Konsistente Verwaltung von baurelevanten Daten

Pläne / Bilder / Videos / Berichte / Projektpläne / Kalkulationen / Aufwands und Mengenerfassungen / Dokumente allgemein / Emails

Wesentliche Anforderungen: Auffindbarkeit, Geo und Plan Zuordnung von Dokumenten (Metadaten), spezialisierte – mobile- Erfassungs und Zuordnungsmöglichkeit, Logging, revisionssichere Speicherung

Proprietäre Funktionen und Speicherungen, spezifische Funktionen müssen geklärt werden.

Beweismittel: Herstellung von Kopien

Variante: Datenquelle ist in einem Cloud Dienst

Variante: gesamte Funktion der Verwaltung und Speicherung von Projektdaten (technisch, kfm. und organisatorisch) wird als SaaS Dienst genutzt:
Software und Speicherung in einem Cloud System

Variante: Software lokal installiert, Daten und/oder Kopien und Backups in einem Cloud Speicher

Möglichkeit einer Archivfunktion mir revisionssicherer Speicherung
Nutzbar nur solange der Dienst aktiv ist
SLAs und Garantien über Speicherdauer, Export auf Anforderung und Verfügbarkeit wichtig

Beweismittel: Kritische Eigenschaften

Metadaten zu Inhalten:
Zeitpunkt der Erstellung, letzte Änderung, letzte Anzeige bzw. Zugriff
Weitere Informationen die in Metadaten enthalten sein können (je nach Art und Definition) –siehe vorstehend.

Gewährleistung von Eigenschaften und Nachweise dazu:
Integrität (unverfälscht), Vollständigkeit, Authentizität (Metadaten sicher zuordenbar) –z.B: Ersteller, Kamera, Absender (für Email) …

Grundlegend: Alle Daten inkl. Metadaten können (meist leicht) **gefälscht** werden. Nachweise oft nicht oder nur mit forensischen Methoden möglich.

Kryptographische Methoden erforderlich: Signaturen, Hash Werte (typ Werte die einen Dateiinhalt kennzeichnen.

Beweismittel: Signaturen

Signaturen können die Unverfälschtheit von Dateien –samt Metadaten- beweisbar absichern.

Technisch:

Aus den zu signierenden Dateien wird eine eindeutige nur der jeweiligen Datei zuordenbare Zeichenkette abgeleitet (Hash Wert)

Signatur: Der verschlüsselte Hash Wert

Verschlüsselung mit dem geheimen Schlüssel des Signators

Mit dem öffentlichen Schlüssel kann die Signatur entschlüsselt werden: das ist der Hash Wert –der dann mit jenem der aus einer zu verifizierenden Datei verglichen werden kann.

Es gibt unterschiedliche technische und rechtliche Qualitäten von Signaturen

Dateien als Beweismittel

Technische Lesbarkeit von Datenträgern: Übersicht möglichen Werten

Speichermedium	max. Lebensdauer (und größte Bedrohung)	
• Blu-ray	50-100 Jahre	(Wärme, Licht, Feuchtigkeit und Kratzer)
• DVD	30 Jahre	(Wärme, Licht, Feuchtigkeit und Kratzer)
• CD	30 Jahre	(Wärme, Licht, Feuchtigkeit und Kratzer)
• Festplatte extern	10 Jahre	(Feuchtigkeit, Stöße, Magnetismus)
• Festplatte intern	5-10 Jahre	(Wärme im Betrieb)
• SSD	10 Jahre	(Begrenzte Schreibzyklen)
• USB-Sticks	30 Jahre	(Begrenzte Schreibzyklen)
• Cloud-Speicher	theoretisch unbegrenzt	(Zugriff durch Dritte, Pleite des Anbieters)

Quelle: Internet / pc-magazin

Dateien als Beweismittel

Kriterium: Zeitpunkt und Zweck der Speicherung

Ad hoc: Beweissicherung eines aktuellen Status

Definition der Ziele: Was soll „gesichert“ und wiederherstellbar sein?

Definition der konsistent zu sichernden Daten
Definition der zur Wiederherstellung nötigen Programme

Sicherstellung der Authentizität und Integrität bzw. Nachweise dazu
Signaturen
Herstellung und Verwahrung durch Urkundspersonen (ZT)
Sicherstellung der Verwertbarkeit: Test

Dateien als Beweismittel

Kriterium: Zeitpunkt und Zweck der Speicherung

Nutzung bestehender Datenspeicherungen (Backups): retrospektiv

Unmittelbare Auswertung einzelner –relevanter- Inhalte
Dazu: Herstellung von Kopien und Auszügen aus Backups

Offen: Sicherung der Metadaten zum Ursprung –sind diese enthalten?

Analyse der Eigenschaften zum Zeitpunkt der Übernahme
Forensische Analyse zu Zeitstempeln und Unversehrtheit

Speicherung von Daten: Vorgangsweise

- Definition dessen was nachvollziehbar dokumentiert –später „bewiesen“- werden soll
- Ermittlung welche Dateien dazu nötig sind und zusammen „gehören“ (Konsistenz)

  Bemerkung: Das können ganz unterschiedliche Dateien an ganz unterschiedlichen Speicherorten sein.

  Z.B.: Emails in einem Mailsystem (am Server oder einem Client oder in einem Web Dienst), Dateien mit Bildern auf sog. „File Shares“ unterschiedlicher Art, Projektdaten (Status Info, Bug Management Infos) in Datenbanken, Plandaten in spezialisierten Systemen inkl. Versionsverfolgung…..
- Sicherstellung dass gesicherte Daten auch verwendet (angezeigt ..) werden können: d.h.: Sicherung der Programme zu den Dateitypen, Sicherung der Zugriffsdaten (Rechte)

Datenkopien: Sicherungsmaßnahmen

Herstellung: In Anwesenheit von Zeugen (Urkundsperson) - Protokoll

Minimum: technische Lesbarkeit überprüfen,

Kopieren: Backup herstellen

Stichproben zur Verwertbarkeit (Methode abhängig vom Inhalt)

Zweckmäßig: inhaltliche Verwertbarkeit verifizieren

D.h.: gesamten zusammengehörigen Datenbestand und

Anzeige- bzw. Bearbeitungsprogramme und Systemumgebungen re-installieren – prüfen ob das, was zu sichern war dargestellt werden kann

Sichere Verwahrung: Mit Protokoll (auch als öffentl. Urkunde) bei Personen mit öffentl. Glauben versehen, verwahren.

Backup und DSGVO

Personenbezogene Daten sind auch in Backups zu schützen.

Voraussetzung: es sind strukturierte Datensammlungen (Datenbanken) die automatisiert, elektronisch verarbeitet werden können.

Das wird in der Regel nötig sein um dem späteren Zweck zu entsprechen.

Verwendung von Verschlüsselungen, die den Zugriff nur durch die ursprünglichen Verarbeiter (die laut DSGVO eine rechtlich zulässige Verarbeitung vornehmen können) erlaubt.

Frage: Wer muß später dann dazu mitwirken?

Aufnahme der Datensicherung (sofern dies nicht technisch begründete übliche Sicherungen am ausgewiesenen Ort sind) in das Verarbeitungsverzeichnis

Beweissicherung: Szenarien

- Dispositive, periodische Beweissicherung während einer Projektlaufzeit

  Planung und Verifikation der Verwendbarkeit der gesicherten Daten zum Zeitpunkt der Einrichtung.

  Problem: Späterer Zweck vorab meist nicht im Detail bekannt
  daher: große Datenmengen, Unsicherheit ob „alles“ rekonstruierbar ist

- Ad Hoc Beweissicherung –anlassbezogen

  Die Planung und Verifikation kann unmittelbar auf den Zweck abgestellt werden.

  Verbesserungen der Methoden bei negativer Verifikation sofort möglich.

- Beweissicherung für zurückliegende Zweitpunkte auf Basis von aktuellen Datenbeständen und Backups

  Problem: Unvollständige Daten, Konsistenz oft nicht herstellbar und Unverfälschtheit nicht gesichert – forensische Analysen nötig

Dateien als Beweismittel: Zusammenfassung

- Zur Definition und Herstellung von beweistauglichen Sicherungen ist eine anwendungsspezifische, auf den Verwendungszweck bedachte technische Planung, und Verifikation der Verwendbarkeit unerlässlich.
- Am Besten: Man hat Sicherungen die als Beweismittel tauglich sind.
- Noch besser: Man benötigt diese nicht!