Datensicherung Strategie und Tools

PC-Treff-BB
Peter Rudolph, Roland Egeler

Wozu Datensicherung?

- Wertvolle Daten
  - Elektronische Dokumente
  - Dinge deren Wiederherstellung viel Aufwand bedeutet
  - Erinnerungen, z.B. Digitale Fotos, Videos
- Mögliche Katastrophen
  - Totalausfall von Festplatte/SSD oder Speichermedien
  - Virenbefall
  - Eigene Dummheit (falsches gelöscht)
  - Verschlüsselungstrojaner
  - Einbruch / Diebstahl
  - Brand, Hochwasser, Blitz, ...

Anekdoten

- Firma A
  - Da kommt ein Gewitter
- Firma B
  - Bandlaufwerk dejustiert Lesekopf
- Firma C
  - Datenträger verwechselt
- Privatmann D
  - Magische Funkmaus
- ...

Konzepte

- Gespiegelte Festplatten (RAID)
- Datei-Synchronisation (z.B. Unison)
- PC-Backup (z.B. Duplicati)
  - Kann alle von einem PC erreichbaren Dateien sichern
- Server-Backup (z.B. Bacula)
  - Backup-Steuerung: steuert Backup (Zeitpunkt, Medienverwaltung, ...)
  - Daten-Server: empfängt zu sichernde Daten
  - Sicherungs-Server: Liefert zu sichernde Daten

Strategien

- Welche Daten sollen gesichert werden?
  - Am Besten alle...
  - Wenn das nicht geht (Speicherplatz), priorisieren.
- Prioritäten setzen:
  - Unersetzlich
  - Schwer ersetzbar
  - Ersetzbar

Prioritäten

- Unersetzlich
  - Kann nicht wieder erzeugt werden.
  - Bsp: Eigene Filme, Fotos oder Tonaufnahmen aus vergangenen Zeiten
- Schwer ersetzbar
  - Braucht viel Zeit- oder Arbeitsaufwand.
  - Bsp: Digitalisierte Schallplatten oder Bilder, Betriebssystemeinstellungen
- Ersetzbar
  - Kann ohne Probleme aus anderer Quelle geholt werden.
  - Bsp: Betriebssystem, Daten von Bekannten, gekaufte Musik, Videos, ...

Prinzipien der Datensicherung

- Ein schlechtes Backup ist besser als keines
- Was?
  - Sich Gedanken machen, welche Daten sicherungswürdig sind
- Wann?
  - So oft wie möglich, am Besten automatisch
  - Entscheidung: Wie lange aufbewahren?
- Wohin?
  - Mehrere unterschiedliche Datenziele
  - Mindestens eines außer Haus
- Was wenn man den Backup braucht?
  - An die Wiederherstellung denken
  - Unbedingt auch ausprobieren

Sicherungsarten

- Systembackup
  - Sichert den gesamten PC
  - Wichtig: Wiederherstellungs-Tool
- Datenbackup
  - Sichert nur wichtige Daten
  - Ggf. Betriebssystemeinstellungen (unter Linux /etc)
  - Aufwand für Neuinstallation des Betriebssystems bedenken
- Gelegentliche manuelle Spiegelung
  - Synchronisieren von Ordnern, z.B. PC mit NAS
- Permanente Spiegelung
  - Jede Speicherung geht auf mehr als ein Medium (Platte)

Ziele für Datensicherung

- Speichermedien
  - USB-Sticks, SD-Karten, externe Platten
- Optische Medien
  - DVD, Blu-Ray
- Lokale Netzwerkziele
  - NAS, Router, Server
- Internet
  - Cloud-Service, Mietserver
  - Rechner von Bekannten

Backupverfahren

- Full Backup
  - Alle Daten werden gesichert
  - Braucht am meisten Platz
- Differentiell
  - Alle geänderten Daten seit letztem Full Backup
  - Daten werden redundant gesichert (Platzbedarf).
- Inkrementell
  - Beinhaltet alle geänderten Daten seit letzter Sicherung
  - Benötigt zur Wiederherstellung
    - Das letzte Full Backup
    - Das letzte differentielle Backup
    - Alle inkrementellen seit dem letzten differentiellen
  - Braucht weniger Platz

Best Practice

- Bewährte Strategie
  - Alle 1-6 Monate Full Backup
  - Alle 1-2 Wochen differentiell
  - Täglich inkrementell
  - Vorteile
    - Braucht wenig Platz
    - Kann dadurch weit in die Vergangenheit
    - Ist tagesaktuell
    - Relativ wenig Aufwand bei der Wiederherstellung
- Strategie PI-Data
  - Nur Datensicherung, nur Server
  - Gespiegelte Platten (RAID 1)
  - Backup-Platte wöchentlicher Wechsel (3 Stk.)
  - Jede Woche beginnt mit Full Backup, danach täglich inkrementell
  - Monatlich Kopie einer Wochensicherung auf USB-Platte

Unterstützende Maßnahmen

- Ausfallsicherheit erhöhen
  - Durch Plattenspiegelung (RAID)
  - Langlebige Platten kaufen (Server- oder RAID-Platten)
  - Bei Flash-Speichern SLC (Single Level Cells)
  - Im Dateisystem Snapshots einschalten
- Auswirkungen von Katastrophen reduzieren
  - USV hilft gegen kaputte Dateisysteme durch Stromausfälle
  - Blitzschutz durch geeignete Steckdosen oder Blitzableiter
  - Besser keine Rechner im Keller (Hochwasser)

Spezialfall Verschlüsselungstrojaner

- Kommen oft als Anhang einer E-Mail
- Löschen Daten nicht, sondern verschlüsseln sie
  - Dateien bleiben vorhanden, Benutzer arglos
  - Verschlüsselte Dateien werden gesichert
  - Im Einzelfall Entschlüsselung möglich
- Versuchen, Lösegeld zu erpressen
- Können unauffällig im Hintergrund laufen
- Befallen nicht nur lokale, sondern auch Daten auf Netzwerklaufwerken
  - Können auch dort liegende Backups unbrauchbar machen

Spezialfall Verschlüsselungstrojaner

- Lösungen
  - Beim Öffnen von E-Mails unbekannter Herkunft aufpassen
  - Keine unbekannten Anhänge öffnen
  - Backups über Protokolle machen, die nicht permanent Verbindung brauchen: (s)ftp, ssh, scp...
  - Backup läuft nicht auf lokalem Rechner
  - Ein externes Programm holt sich die Daten vom lokalen Rechner ab
  - Backup liegt auf Speicherplatz, der nicht direkt ansprechbar ist

Programme

- Duplicati
- Unison
- Areca Backup
- Back in Time
- Deja Dup
- Kup
- LuckyBackup
- BackupPC
- Bacula
- ...

Quellen

- https://wiki.ubuntuusers.de/Datensicherung
- c't 13/2013, Seite 112
- c't 7/2016, Seite 128
- c't 11/2016, Seite 102
- c't 11/2016, Seite 108