

Datenschutz und Kryptographie

Modul DSKRY-40 im Studiengang Informatik

Referent: Dr. Hendrik Siegmund

IT-Sicherheit

- **IT-Sicherheit – Datensicherung**
 - Warum Datensicherung?
 - Definition und Abgrenzung zu Archivierung
 - Datensicherungsarten, Konzepte und Strategien
 - Sicherungsmedien

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Warum Datensicherung?
 - Hohe Wahrscheinlichkeit für Datenverlust:

Dell EMC-Studie „**Global Data Protection Index**“ zeigt, dass 76% der befragten Unternehmen 2018 eine ungeplante IT-Unterbrechung erlebt haben und 27% einen nicht behebbaren Datenverlust



<https://www.emc.com/about/news/press/2019/20190321-01.htm>

IT-Sicherheit

- **IT-Sicherheit – Datensicherung**
 - Warum Datensicherung?
 - Datenverlust ist teuer
 - Ohne Backup lange, oft erfolglose Suche nach alten Dateiversionen
 - Rettung von defekten Datenträgern möglich aber teuer, z.B. 1 HDD 1000,- €
 - Nach Dell EMC-Studie: Durchschnittliche Kosten für Datenverlust in befragten Unternehmen in Deutschland 2018 bei 1,1 Mio \$
 - Kein Backup = grob fahrlässig, Datenverlust = Gesetzesverstoß
 - Aufbewahrungspflichtige Daten nicht zu haben kann strafbar sein
 - Handelsgesetzbuch (HGB) und Steuerrecht (GoBD), ITSG...

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Warum Datensicherung?
 - Datenverlust kann existenzgefährdend sein
 - Unternehmen kann Kosten und Aufwand eines Datentotalverlusts evtl. nicht stemmen

IT-Sicherheit

- IT-Sicherheit – Datensicherung

- Definition und Abgrenzung zu Archivierung
- Begriff Datensicherung = Backup
- Glossar Grundschutzkompendium:

„Bei einer Datensicherung werden zum Schutz vor Datenverlust **Sicherungskopien** von vorhandenen Datenbeständen erstellt.

Datensicherung **umfasst** alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der **Systeme** einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten **Daten**, **Programme** und **Prozeduren**.“

IT-Sicherheit

- **IT-Sicherheit – Datensicherung**
 - Definition und Abgrenzung zu Archivierung
 - Die Datensicherung ist ein vom Produktivbestand kopierter, redundanter Datenbestand zur Wiederherstellung nach einem Ausfall der produktiven Daten und/oder Systeme
 - Stichwort Redundanz: Mehrere Versionen an mehreren Standorten verwalten, auch ältere Versionen
- Aber: **Lange aufbewahrtes Backup ≠ Archiv!**

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Definition und Abgrenzung zu Archivierung
 - Die Datensicherung ist eine **Sicherungskopie** produktiver Daten
 - Theoretisch zeitlich unbegrenzt verfügbar (medienabhängig)
 - Keine Maßnahmen gegen Löschen oder Ändern von Daten (medienabhängig)
 - Zur Wiederherstellung nur rudimentäre Suchfunktionen
 - Archiv: **Dateiablage** zur Erfüllung von **Aufbewahrungs-** oder **Löschpflichten**
 - Angabe von Ablaufdaten mit automatischer Löschung/Sperrung
 - Unbedingte Wahrung des Originalformats, kein nachträgliches Ändern, WORM
 - Garantierte Haltbarkeit und definierte Migrationsszenarien
 - Umfangreiche und präzise Suchfunktionen in komfortabler Oberfläche









IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **Begriffe 1**
 - **Datensicherungsarten** definieren **wie**, ein Backup **erstellt** wird:
 - Vollsicherung
 - Differenzielle Sicherung
 - Inkrementelle Sicherung
 - Offline-Backup (Cold Backup, manchmal als Kopiesicherung bezeichnet)
 - Online-Backup (Hot Backup, Application-Aware)
 - Image-Backup
 - Sonderfälle: Virtuelle Maschinen, Deduplizierung und Volumenschattenkopien

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsverfahren und Strategien – **Begriffe 2**
 - **Datensicherungsstrategie** oder **Datensicherungskonzept** definieren, **wie** in einem Unternehmen prinzipiell Datensicherungen vorgenommen werden:
 - Was gesichert wird
 - Wer die Sicherung durchführt
 - Wann die Sicherungen durchgeführt werden (Zeiten und Intervalle)
 - Wo Sicherungen gelagert werden
 - Welche Medien zum Einsatz kommen
 - Wann und wie Wiederherstellungstests vorgenommen werden
 - ...

IT-Sicherheit

Name	Änderungsdatum	Typ	Größe	Attribute
 AV-TEST_Sicherheitsreport_2017-2018	25.04.2019 11:29	Adobe Acrobat D...	1.059 KB	A
 BA-DatS-ITSec	09.05.2019 00:01	Microsoft PowerP...	21.866 KB	A
 bgbl115s1324_12495	30.04.2019 12:32	Adobe Acrobat D...	91 KB	A
 bgbl117s2097_75493	03.04.2019 14:55	Adobe Acrobat D...	317 KB	A
 ChiffrierungWW2	01.04.2019 14:37	Adobe Acrobat D...	7.710 KB	A
 DatenschutzBA	18.04.2019 12:06	Microsoft PowerP...	10.978 KB	A
 Datensicherungen	21.05.2019 20:29	Microsoft PowerP...	267 KB	A
 DSG-EKD	17.04.2019 16:34	Adobe Acrobat D...	234 KB	A

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten
 - **Vollsicherung**, auch Komplettsicherung oder Normale Sicherung
 - Alle Daten aus einem begrenzten, definierten Bereich wie z.B. Laufwerk, Partition oder Ordnerstruktur werden auf ein Sicherungsmedium kopiert und auf dem Laufwerk als „gesichert“ markiert
 - In Windows-Dateisystemen wie FAT und NTFS gibt es für diese Markierung das **Archivbit**. Es wird auf Dateiebene bei jedem Schreibvorgang gesetzt und durch ein Sicherungsprogramm u.a. bei einer Vollsicherung wieder gelöscht.

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten - Vollsicherung
 - Pro:
 - Einfach, mit Befehlszeilenkommandos oder Bordmitteln von Windows durchführbar
 - Kopiert bei jeder Sicherung den kompletten Datenbestand
 - Contra:
 - Hoher Speicherplatzbedarf
 - Hoher Zeitbedarf für Erstellung

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten
 - Differenzielle Sicherung
 - Nur nach einer Vollsicherung geänderte oder neue Daten werden auf ein Sicherungsmedium kopiert. Das Archivbit wird nicht geändert.
 - Jede differenzielle Sicherung enthält alle Änderungen seit der letzten Vollsicherung

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten - Differenzielle Sicherung
 - Pro:
 - Zeitersparnis bei der Sicherung
 - Reduzierter Speicherplatzbedarf gegenüber mehreren Vollsicherungen
 - Contra:
 - Zeitersparnis nimmt mit zunehmendem Abstand zur letzten Vollsicherung ab
 - Zur Wiederherstellung werden letzte Vollsicherung und letzte differenzielle Sicherung benötigt
 - Werden viele große Dateien wie z.B. VHDs in virt. PCs gesichert, ergibt sich kein Vorteil gegenüber Vollsicherungen mehr.


IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten
 - Inkrementelle Sicherung oder Zuwachssicherung
 - Nur nach einer Vollsicherung geänderte oder neue Daten werden auf ein Sicherungsmedium kopiert. Das Archivbit wird gelöscht.
 - In jeder Inkrementellen Sicherung sind nur die Änderungen gegenüber der letzten inkrementellen Sicherung enthalten (Ausnahme: erste Inkr. Sicherung)

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten – Inkrementelle Sicherung
 - Pro:
 - Kürzest mögliche Zeiten für die Erstellung der Sicherungen
 - Geringstmöglicher Speicherplatzbedarf
 - Contra:
 - Zur Wiederherstellung werden die letzte Vollsicherung und **alle** inkrementellen Sicherungen benötigt
 - Wiederherstellung dauert wegen Verkettung aller Sicherungen deutlich länger und ist fehleranfällig, schon ein Medienausfall macht alle folgenden Sicherungen und damit aktuellere Daten unbrauchbar

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **Begriffe 1**
 - **Datensicherungsarten** definieren **wie**, ein Backup **erstellt** wird:
 - **Vollsicherung**
 - **Differenzielle Sicherung**
 - **Inkrementelle Sicherung****Klassische Sicherungsarten treten in den Hintergrund**
 - Offline-Backup (Cold Backup, manchmal als Kopiesicherung bezeichnet)
 - Online-Backup (Hot Backup, Application-Aware)
 - Image-Backup
 - Sonderfälle: Virtuelle Maschinen, Deduplizierung und Volumenschattenkopien

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – Alternativen
 - Online-Backup (Hot Backup, Application-Aware Backup)
 - Offline-Backup (Cold Backup, manchmal als Kopiesicherung bezeichnet)
 - Image-Backup
 - Sonderfälle: Virtuelle Maschinen, Deduplizierung und Volumenschattenkopien

IT-Sicherheit

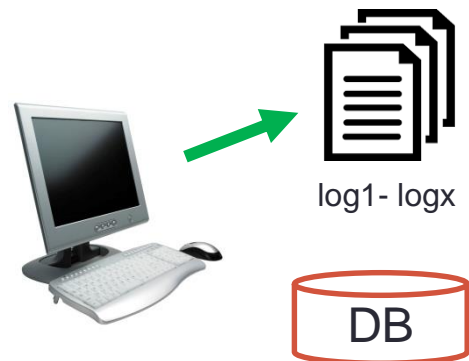
- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – weitere Arten
 - Online-Backup (Hot Backup, Application-Aware Backup)
 - Sicherung „im laufenden Betrieb“
 - Bei Datenbanken und Datenbank-basierten Applikationen
 - Microsoft SQL-Server und Oracle DB-Server...
 - Microsoft Exchange
 - Microsoft Active Directory

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – weitere Arten
 - Online-Backup (Hot Backup, Application-Aware Backup)
 - Datenbank alleine umfasst nicht den gesamten aktuellen Datenbestand
 - Zusätzlich werden Daten aus Transaktionsprotokolle benötigt
 - Datenbank ohne Transaktionsprotokolle ist „inkonsistent“
 - Datenbank wird bei der Sicherung in einen konsistenten Status überführt und dann gesichert
 - Datenbank- und Datensicherungssoftware interagieren miteinander, die Datensicherungssoftware kennt die Applikation, die sie sichert

IT-Sicherheit

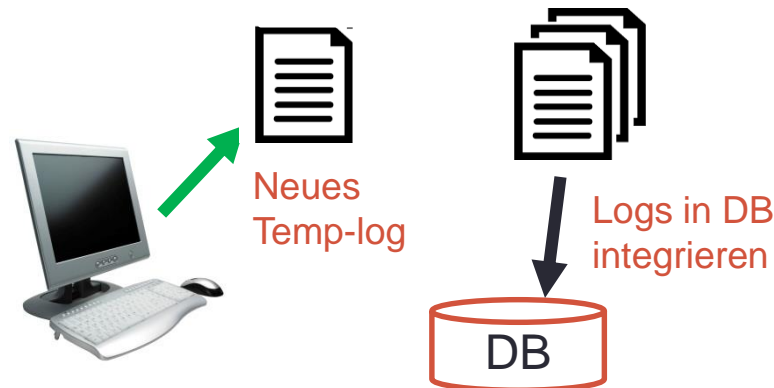
- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **weitere Arten**
 - Online-Backup (Hot Backup, Application-Aware Backup)



DB-Normalbetrieb

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **weitere Arten**
 - Online-Backup (Hot Backup, Application-Aware Backup)



DB-Sicherung Schritt 1

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **weitere Arten**
 - Online-Backup (Hot Backup, Application-Aware Backup)



DB-Sicherung Schritt 2: Datenbank kopieren

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **weitere Arten**
 - Online-Backup (Hot Backup, Application-Aware Backup)



DB-Sicherung Schritt 3: Alte Logs löschen, Temp-Log „normalisieren“

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – weitere Arten
 - **Offline-Backup** (Cold Backup)
 - Von manchen DB-Software Herstellern angebotenes Verfahren zur schnellen, konsistenten Sicherung der DB alleine.
 - Verfügbar für Microsoft Exchange als „Kopiesicherung“ und für Microsoft SQL und Oracle-Datenbanken
 - Datenbanken werden lediglich konsistent gemacht und dann kopiert, kein Löschen der Transaktionslogs.
 - Schnell, reduziert nicht den Speicherplatz auf Log-Laufwerken
 - Kann zum Exportieren der DB genutzt werden.

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – weitere Arten
 - Image-Backup
 - Sichert nicht nur Daten, sondern einen gesamten Datenträger, z.B. inkl Betriebssystem
 - Ergebnis ist ein Datenträgerabbild (Image), das wie eine Datei behandelt werden kann.
 - Images sind 1:1 auf neuen Datenträger übertragbar, z.B. auf ersetzte Festplatte
 - Images können im Dateisystem gemounted werden und sind dann wie ein Laufwerk durchsuchbar
 - Bekanntes Consumer-Produkt Acronis True Image

IT-Sicherheit



- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – weitere Arten
 - Image-Backup
 - Pro:
 - Ideal für Festplatten virtueller Server (Virtual Hard Disk, VHD), Image kann als VHD eines virtuellen Servers sofort starten
 - Wird in großen virtualisierten Serverumgebungen vorzugsweise eingesetzt, da klassische Datensicherungsarten hierfür nicht geeignet sind
 - Contra:
 - Großer Speicherplatzbedarf für viele vollständige Images
 - Images müssen durch Deduplizierung zusammengefasst werden

IT-Sicherheit

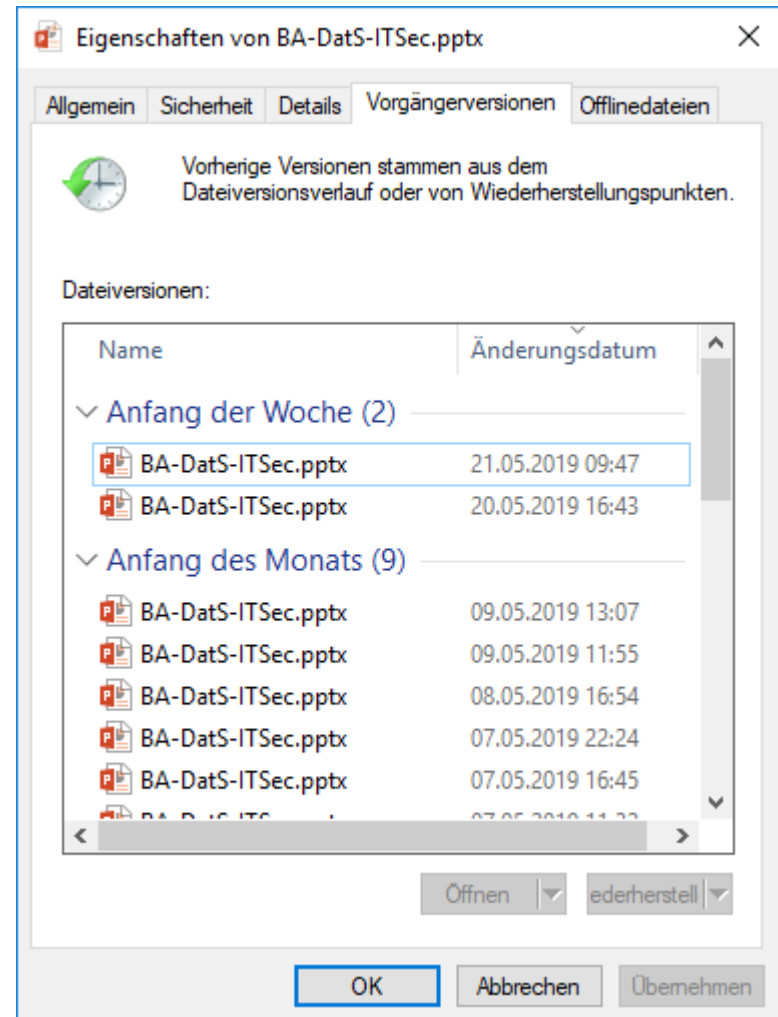
- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – Sonderfälle
 - Deduplizierung
 - In virtuellen Serverumgebungen existieren viele Images mit ähnlichen Inhalten, die VHDs der virtuellen Server
 - Ähnliche VHDs können von Backupsoftware zusammengefasst werden, um Speicherplatz zu sparen.
 - Hersteller versprechen Kompressionsraten bis 75%
 - Konsequenz: Kehr komplexe Sicherheitsbibliothek
 - Produktbeispiel Acronis Universal Backup

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **Sonderfälle**
 - **Volumenschattenkopie**
 - Auf Datenträgerebene (Block-Level) wird ein Protokoll aller Änderungen geführt: Das System macht „Snapshots“ (konsistente Momentaufnahmen) des Datenträgers und speichert die Snapshots in separatem Bereich
 - Unerwünschtes Löschen oder Ändern von Dateien kann mit dem Protokoll über eine Auswahl von Dateiversionen rückgängig gemacht werden
 - Der Nutzer (nicht die IT-Abteilung) wählt aus einer Liste der Dateiversionen die gewünschte Versionen aus und stellt sie wieder her.
 - Microsoft nutzt Volumenschattenkopien auch für Systemwiederherstellungen

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungsarten, Konzepte und Strategien – **Sonderfälle**
 - **Volumenschattenkopie**
 - Für gelöschte Dateien wird eine neue leere Datei gleichen Namens angelegt, der VSS fügt dann dieser neuen leeren Datei die Liste der Vorgängerversionen hinzu
 - Die Volumenschattenkopie ersetzt nicht die Datensicherung!



IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Datensicherungskonzepte und –strategien, **wesentliche Kriterien**
 - Zuerst festlegen, was gesichert wird und wer es tut, dann klären:
 - **Wann**: Zyklen der Sicherung und Mediennutzung
 - **Sicherungsmedien und Lagerungsort**: Disk to Disk to Tape, Cloud...

IT-Sicherheit

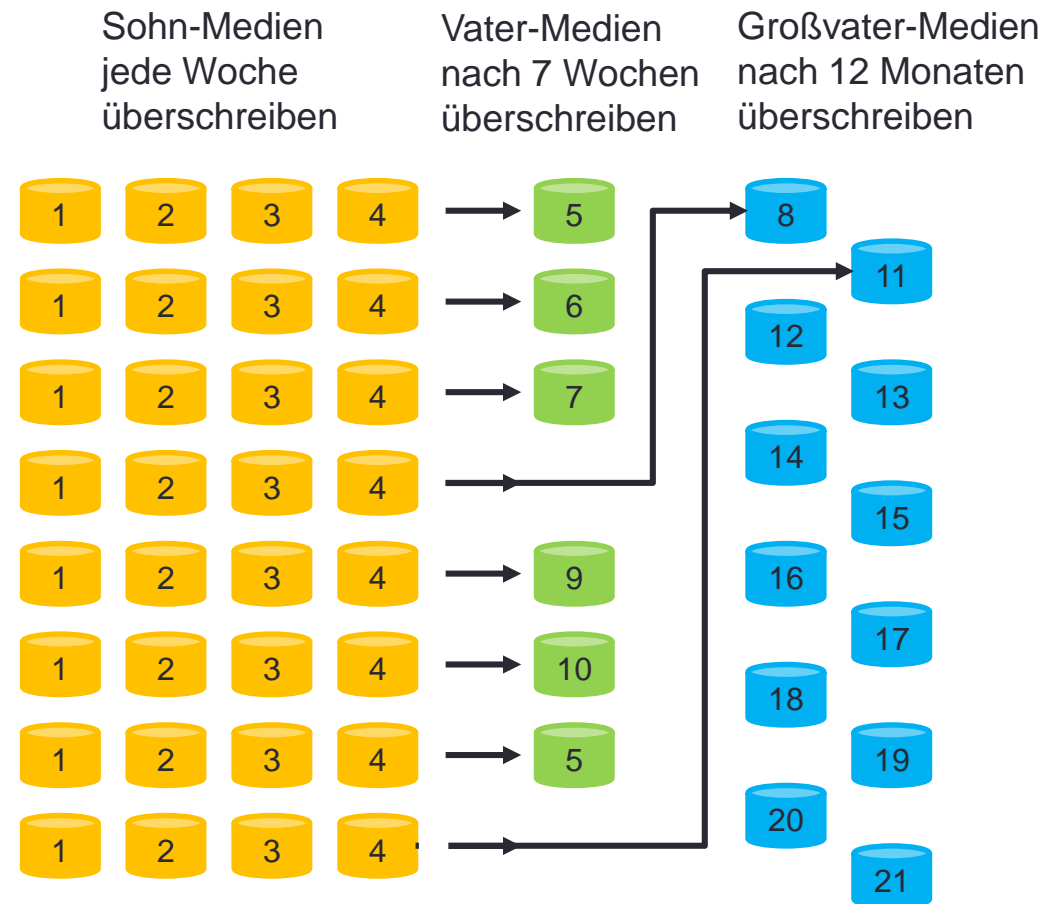
- IT-Sicherheit – Datensicherung
 - Datensicherungskonzepte und –strategien, wesentliche Kriterien
 - **Zyklen der Sicherung und Mediennutzung**
 - Herausforderung: Befriedigenden Kompromiss aus Vollständigkeit, Speicherplatzbedarf (Medienbedarf) und Aufbewahrungsdauer finden
 - Lebensdauer der Medien berücksichtigen
 - Übliche Sicherungsintervalle: Einmal je Arbeitstag, Mo-Fr
 - Datenbanken ggf. mehrmals täglich per „Snapshot“ sichern und alle Snapshots der tägl. Sicherung hinzufügen

IT-Sicherheit

- **IT-Sicherheit – Datensicherung**
 - Datensicherungskonzepte und –strategien, wesentliche Kriterien
 - Zyklen der Sicherung und Mediennutzung
 - Häufigstes Konzept: **Generationenprinzip**, auch „Großvater-Vater-Sohn“
- Rotationsprinzip, benötigt für ein Jahr 21 Medien, sofern der gesamte Datenbestand auf ein Medium passt
 - 4 Medien für tägliche Sicherung
 - 5 Medien für Wochensicherung
 - 12 Medien für Monatssicherung

IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Generationenprinzip – Funktionsweise (Konzept für Monat = 28 Tage)



IT-Sicherheit

- IT-Sicherheit – Datensicherung
 - Generationenprinzip, auch „Großvater-Vater-Sohn“
 - Pro:
 - Liefert wirtschaftliches Verhältnis zwischen maximaler Datensicherheit und vertretbarem Medienbedarf
 - Contra:
 - Komplex, bei unklarer Medienkennzeichnung fehleranfällig
 - Beansprucht Medien der einzelnen Generationen unterschiedlich stark, besonders Sohn-Medien müssen ggf. frühzeitig ersetzt werden
- Monatsmedien unbedingt an anderen Standort auslagern!

IT-Sicherheit

- **IT-Sicherheit – Datensicherung**
 - Datensicherungskonzepte und –strategien, wesentliche Kriterien
 - Zyklen der Sicherung und Mediennutzung
 - Alternative zum Generationenprinzip für geringeren Medienbedarf und dafür kürzere Vorhaltezeit: **FIFO-Prinzip**, z.B. wöchentlicher Medienwechsel mit fünf Medien
 - Start am Montag mit Vollsicherung, Di-Fr inkrementelle Sicherungen **hinzufügen** und am nächsten Montag Medienwechsel.
 - Ältestes Backup dann maximal 4 Wochen alt, **zwingend durch ausgelagerte zusätzliche Medien mit Bestand von 3, 6 und 12 Monaten ergänzen**

IT-Sicherheit

- IT-Sicherheit – Datensicherung
- Sicherungsmedien und Lagerungsorte
 - Klassisches Magnetband
 - Festplatten und Wechseldatenträger
 - CD, DVD
 - Mobile Datenträger
 - Cloud

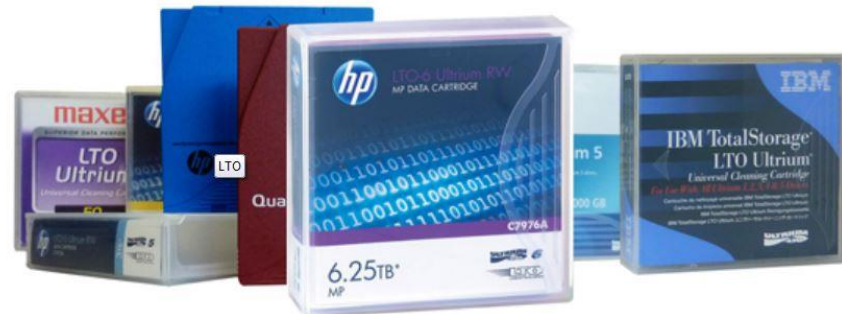


Bild: www.speicherguide.de

IT-Sicherheit

- IT-Sicherheit – Datensicherung
- Sicherungsmedien und Lagerungsorte
 - Klassisches Magnetband
 - Seit Jahrzehnten das Standard-Sicherungsmedium
 - Mehrere Standards, etwa DLT (Direct Linear Tape) und LTO (Linear Tape Open)
 - Bandkassetten, Bänder enthalten mehrere Spuren und werden an stehenden Magnetköpfen vorbeigezogen
 - Kapazitäten von 95 MB (DLT, 1984) bis 48.000 GB (LTO 10, 2017)
 - Sicherungen und Medienwechseln mittels Tape Loader oder Tape Library automatisierbar
 - Anwendbar auch für größere Datenmengen als Langzeitspeicher

IT-Sicherheit

- IT-Sicherheit – Datensicherung
- Sicherungsmedien und Lagerungsorte
 - Festplatten, Wechseldatenträger
 - Normale Festplatten in Wechselrahmen
 - Spezielle Wechselfestplatten, beispielsweise Dell RD 1000 Data Cartridge
 - Kapazitäten im Bereich wenige TB, abhängig vom Festplatte oder Modell
 - Keine Bandverschmutzung, längere Nutzungsdauer
 - Beschränkt auf kleinere Datenmengen, semiprofessionell, Einsatz im KMU



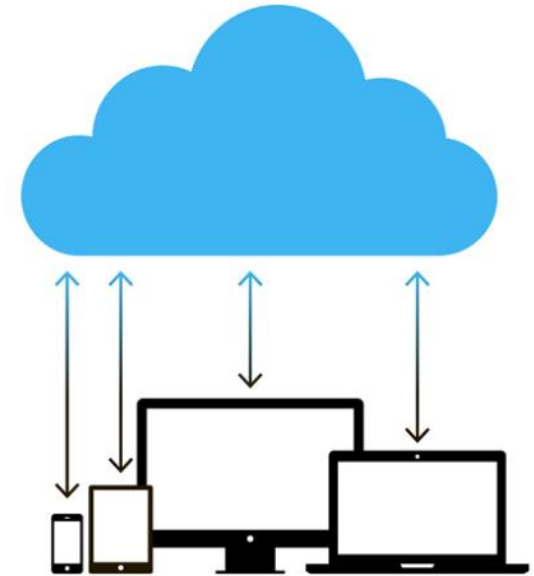
Wechselrahmen, Produktfoto Fa. Icy Box

IT-Sicherheit

- IT-Sicherheit – Datensicherung
- Sicherungsmedien und Lagerungsorte
 - CD, DVD, USB-Wechseldatenträger (inkl. USB-Festplatte)
 - Akzeptable Consumer-Lösung, nicht professionell
 - begrenzte Haltbarkeit,
 - klein, kommt leicht abhanden
 - Geringe Datenübertragungsraten und beschränkte Kapazität

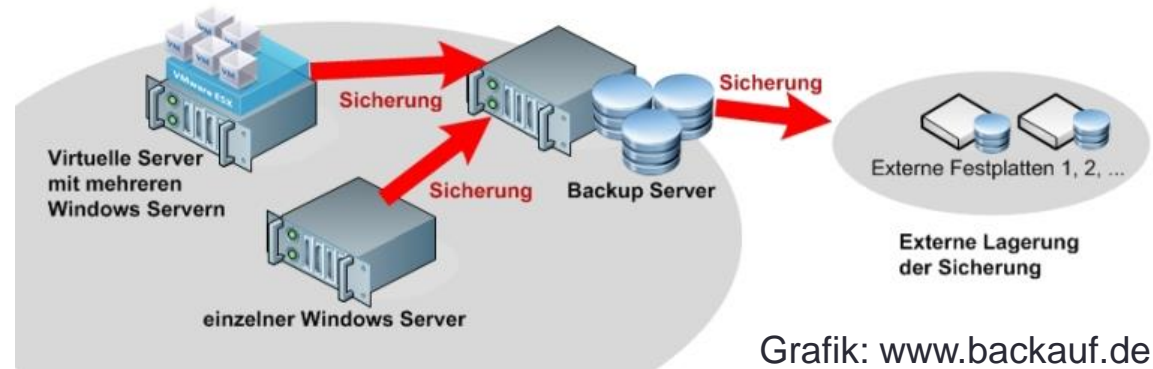
IT-Sicherheit

- IT-Sicherheit – Datensicherung
- Sicherungsmedien und Lagerungsorte
 - Online-Backup in die Cloud
 - Neues Geschäftsmodell von mehreren Anbietern, Strato, Acronis, Barracuda...
 - Datensicherungen werden teilweise automatisch in die Cloud synchronisiert
 - Frage des Datenschutzes bei nicht-EU-Serverstandorten, Verschlüsselung?
 - Sicherheitsanforderungen an Verfügbarkeit erfüllt?
 - Kostenbetrachtung, vor allem bei großen Datenmengen, z.B. 1 TB 15€ monatlich
 - Kann kostengünstige Lösung für KMU und Privatanwender sein
 - Ergänzend, aber nicht ausschließlich nutzen



Grafik: www.baysystems.ca/cloud-backup

IT-Sicherheit



- IT-Sicherheit – Datensicherung
- Sicherungsmedien und **Lagerungsorte**
 - Wo das Backup aufbewahren?
 - Mehrere Aufbewahrungsorte wählen, z.B. Geschäftsgebäude, aber anderer Brandabschnitt oder besser anderer Standort
 - Für KMU: Sicherungsmedien verschlüsselt mit nach Hause nehmen
 - Für große Unternehmen: Kombination aus mehreren Aufbewahrungsorten und Medien
 - Backup-Server mit lokaler Disk-Storage synchronisiert mit weiterem Server an anderem Standort
 - Backup-Server an Tape-Loader oder Library gekoppelt, Disk to Disk to Tape

IT-Sicherheit

- IT-Sicherheit – Datensicherung nach BSI-Grundschutz
 - Grundschutzbaustein CON 3 Datensicherungskonzept
 - Minimales Datensicherungskonzept erstellen
 - Datensicherungen müssen durchgeführt werden
 - Mitarbeiter zur Datensicherung verpflichten
 - Wiederherstellungstests sollten durchgeführt werden
 - Geeignete Aufbewahrungsorte finden
 - Bei erhöhten Sicherheitsanforderungen: Datensicherungen verschlüsseln
 - ...kann als Zusammenfassung dieses Kapitels gelten

IT-Sicherheit

Fragen zum Selbststudium

- Sie beantragen als Verantwortlicher für das Backup eine neue Backup-Software. Ihr Vorgesetzter fragt Sie, wozu die Datensicherung eigentlich erforderlich sei und ob man sie nicht wegfallen oder stark einschränken könne. Was antworten Sie und warum?
- Warum ersetzt das Aktivieren der Volumenschattenkopiedienste VSS auf einem Windows-Dateiserver keinesfalls eine regelmäßige Datensicherung?
- Warum sollte ein Microsoft Exchange Server mit einem Hot-Backup bzw. einer Backup-Software gesichert werden, die application aware ist?
- Was spricht dagegen, alle Unternehmensdaten einer Backup-Lösung mit Cloud-Speichern anzuvertrauen?