



September 2025

Datenschutz und -sicherheit

Für PC, Laptop, Server und Smartphone

Gerhard Meißner

Datenschutz und -sicherheit

Für PC, Laptop, Server und Smartphone

Inhaltsverzeichnis

I. Zielsetzung	2
II. Systeme im Einsatz	2
A. Desktop: AGANDO agua AMD Ryzen	2
B. Laptop: Lenovo ThinkPad L14	3
C. Server: QNAP TS-253A-4G 6 TB 2 Bay	4
D. Smartphone: Samsung Galaxy S24.....	5
III. Sicherung von Daten / Backup & Restore	5
A. Desktop: AGANDO agua AMD Ryzen	5
B. Laptop: Lenovo ThinkPad L14	7
C. Server: QNAP TS-253A-4G 6 TB 2 Bay	7
D. Smartphone: Samsung Galaxy S24.....	8
E. Desktop und Laptop: Outlook Backup	8
F. Evernote	10
IV. Cloudspeicher zur Sicherung und Austausch von Daten	11
B. Datensynchronisation mit Cloudspeicher	13
C. Desktop: Laufwerk - Synchronisation mit der Dropbox	14
D. Server: Laufwerk- Synchronisation mit OneDrive	15
E. Smartphone: Foto Synchronisation und -Backup	16
V. Datensynchronisation zwischen Desktop und Laptop	17
A. Outlook Synchronisation Desktop <—> Laptop	17

B.	Datensynchronisation Desktop ->> Laptop	17
C.	Die Datensynchronisation in der Praxis	18
VI.	Datenschutz durch Zugriffsschutz und Verschlüsselung	19
A.	Passwortschutz bei Systemstart / Login	19
B.	Verschlüsselung gespeicherter Daten	19
1.	Verschlüsselung externe Laufwerke	19
2.	Verschlüsselung wichtiger und sensibler Daten	19

I. Zielsetzung

Das Dokument beschreibt alle relevanten Aspekte, Prozesse und Programme für die Sicherheit und Gewährung der Vertraulichkeit der Daten auf meinen „IT-Systemen“ mit dem Fokus auf

- Backup & Recovery
- Schutz vertraulicher Daten vor unberechtigtem Zugriff
- Geräteübergreifende Synchronisation und Cloud Speicher

II. Systeme im Einsatz

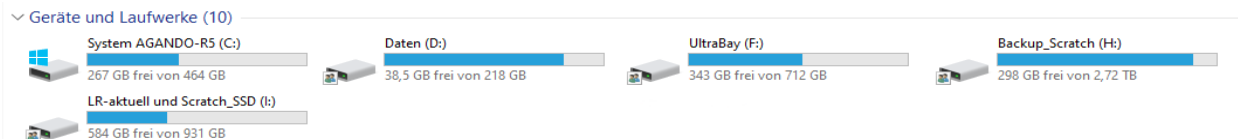
Ein Überblick der Gesamtinstallation (inkl. Multimedia-Devices) kann [hier](#) abgerufen werden.

A. Desktop: AGANDO agua AMD Ryzen

Die aktuelle Konfiguration des Desktops kann [hier](#) abgerufen werden.

Der Desktop ist der „Master“ aller meiner EDV-Aktivitäten und Daten. Er ist das „Standard-Arbeitsgerät“ mit allen relevanten Programmen und Daten (außer den auf den Server ausgelagerten Daten).

Die Speicherung der Daten erfolgt auf 4 internen Festplatten:



- **Partition C: auf einer SSD mit 500 GB**
Diese Partition enthält ausschließlich das Windows-Betriebssystem mit allen installierten Programmen. Benutzerdaten werden auf diesem Laufwerk nicht gespeichert, somit befinden sich in den Standard-Benutzerbibliotheken (Dokumente, Bilder, Musik) ausschließlich temporäre Daten. Ebenso liegen auf der Partition C: alle lokalen Datenbereiche für die Cloudspeicher.
- **Partition D: und F: auf einer konventionellen Festplatte mit 1 TB**
Die Partition D: enthält alle relevanten Benutzerdaten (keine Bilder).
Die Partition F: enthält im Wesentlichen den statischen Teil des Lightroom-Katalogs (Bilder und Videos) welcher aufgrund seines Alters keinen häufigen Änderungen mehr unterliegt.
- **Partition I: auf einer SSD mit 1 TB**
Die Partition I enthält im Wesentlichen den aktuellen Teil des Lightroom-Katalogs (Bilder und Videos) sowie laufende Multimedia-Projekte (abgeschlossene werden auf dem Server abgelegt).
- **Die Partition H: liegt auf einer konventionellen Festplatte mit 3 TB**
und wird im Wesentlichen für die Speicherung der automatischen Backups der übrigen Partitionen sowie als Arbeitsbereich für Programme verwendet.
Daten auf der Partition H: werden nicht gesichert!

B. Laptop: Lenovo ThinkPad L14

Die aktuelle Konfiguration des Laptops kann [hier](#) abgerufen werden.

Der Laptop ist der „kleine Bruder“ des Desktops für den mobilen Einsatz. Er enthält nicht alle Programme, welche auf dem Desktop installiert sind (einige machen wg. Performance und 14“-Display keinen Sinn).

Jedoch enthält der Laptop ein Spiegelbild der Partitionen D: F: und I: des Desktops und deren Daten, welche auf einem SSD Laufwerken mit 2 TB gespeichert werden.



In Bezug auf die temporären Arbeitsbereiche von Programmen gibt es zwangsläufig (keine Partition H: vorhanden) Abweichungen zum Desktop.

C. Server: QNAP TS-253A-4G 6 TB 2 Bay

Die aktuelle Konfiguration des Servers kann [hier](#) abgerufen werden.

Der Server mit dem Speicherplatz von 6 TB intern und 20 TB extern per USB 3.0 hat folgende Aufgaben:

- Netzwerkspeicher für die Archivierung von Daten, Fotos, Musik und Filme/Videos
- Streaming (TwonkyMedia) von Fotos, Musik und Filme/Videos ins lokale Netz
- VPN-Server für den sicheren externen Zugriff auf Systeme, Daten und Medien im lokalen Netz

Die beiden 3 TB-Datenplatten des Servers sind so konfiguriert, dass sie als ein zusammenhängender Datenpool „DataVol1“ genutzt werden.

Die Ablage der Daten geschieht auf „Freigabeordnern“, welche mit den Partitionen eines PC-Systems vergleichbar sind. Die folgenden „Freigabeordner“ sind konfiguriert:

Ordnername	Größe	Ordner	Dateien	Verst...	Volume
Download	8.2 GB	8	51	Nein	DataVol1
EvernoteBackupENEX	4.57 GB	14	132	Nein	DataVol1
MOBackup	81.81 GB	5	119	Nein	DataVol1
Meine Daten (NAS)	598.41 GB	2584	57820	Nein	DataVol1
Meine Fotos (NAS)	20.02 GB	441	30083	Nein	DataVol1
Meine Musik (NAS)	71.74 GB	2093	16626	Nein	DataVol1
Meine Safes (NAS)	12 KB	1	1	Nein	DataVol1
Meine Videos (NAS)	161.76 GB	12	357	Nein	DataVol1
Multimedia	2.9 MB	10	64	Nein	DataVol1
Public	28 KB	4	2	Nein	DataVol1
USB_Backup	2.03 TB	3283	350853	Nein	USB-Laufwerk Dev1Partition1
USB_Video_B	1.22 TB	13	1475	Nein	USB-Laufwerk Dev4Partition1
USB_Video_C	1.41 TB	11	1823	Nein	USB-Laufwerk Dev5Partition1
USB_Video_D	1.79 TB	9	1548	Nein	USB-Laufwerk Dev6Partition1
USB_Video_E	1.7 TB	11	506	Nein	USB-Laufwerk Dev2Partition5
USB_Video_F	3.27 TB	220	2718	Nein	USB-Laufwerk Dev3Partition1
Web	3.47 GB	139	11549	Nein	DataVol1
homes	172 KB	20	13	Nein	DataVol1

Zusätzlich sind am Server permanent 6 externe USB-Festplatten angeschlossen. USB_Backup ist das Speichermedium für die laufenden Datensicherungen der relevanten Serverdaten.

USB_Video_B - F enthalten die „Kino-Filme“ für das lokale Streaming. Die selbst erstellten Urlaubsfilme sind auf „Meine Videos (NAS)“ abgelegt.

D. Smartphone: Samsung Galaxy S24

Das Smartphone ist wie folgt ausgestattet:

- 256 GB interner Speicher
- Keine zusätzliche microSD-Speicherkarte, da die beiden Speicherslots mit je einer SIM-Karte belegt sind

Die sonstigen vorhandenen Smartphones und Tablettts werden in diese Betrachtung nicht mit einbezogen.

III. Sicherung von Daten / Backup & Restore

A. Desktop: AGANDO agua AMD Ryzen

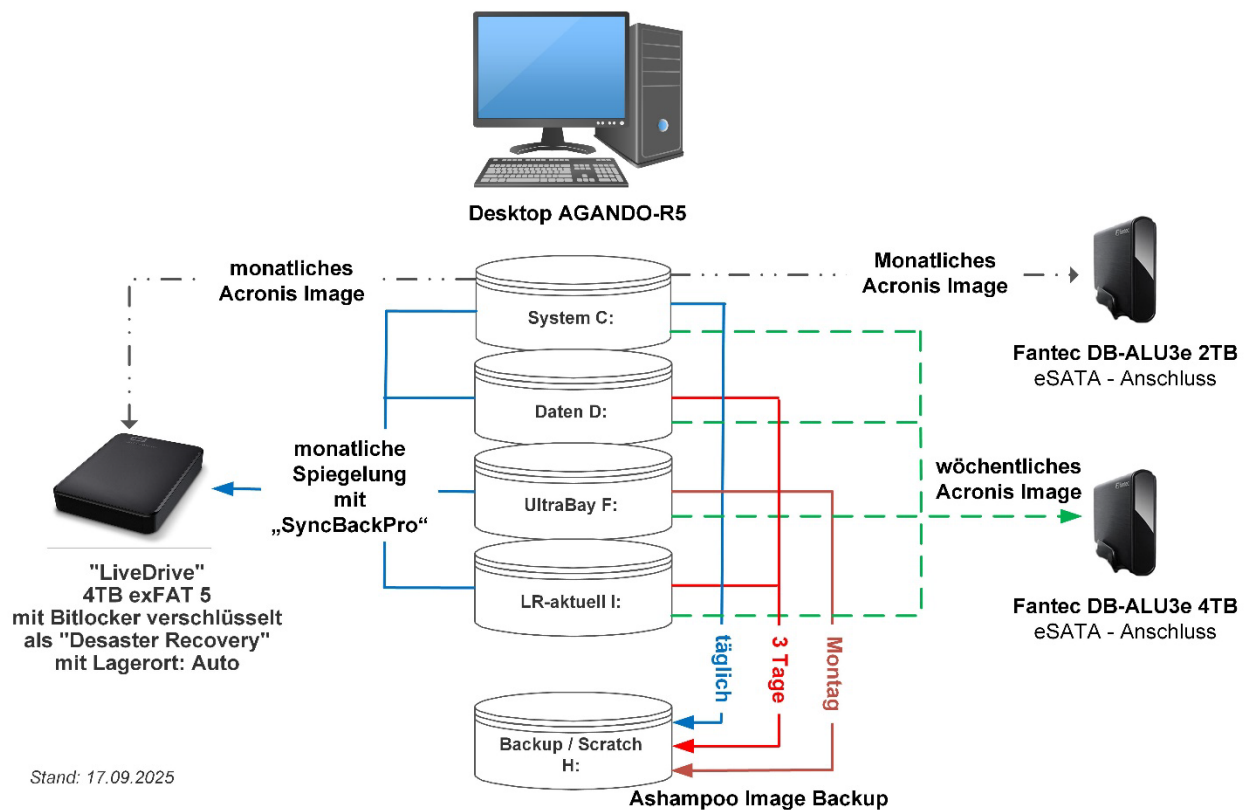
Für die Sicherung der Daten auf dem Desktop sowie Laptop werden die Programme [Acronis True Image](#) und [Ashampoo Backup](#) eingesetzt. Es werden ausschließlich Image-Sicherungen von Partitionen auf lokale oder externe Datenträger vorgenommen (die Programme lassen auch Sicherungen auf Verzeichnis- / Dateiebene zu, wird jedoch nicht verwendet).

Die aktuellen Programmversionen lassen auch die Sicherung in die Cloud zu. Nach einem ausgiebigen Test dieser Varianten wird dies jedoch nicht verwendet. Die wesentlichen Gründe hierfür sind für mich:

- Keine vollkommene, individuelle Steuerung und Transparenz der Backups
- Der Restore einer kompletten Partition oder gar eines gesamten Systems von der Cloud würde aufgrund des Datenvolumens zu lange dauern, sodass auf eine lokale Datensicherung nicht verzichtet werden kann.

Datensicherungskonzept für den Desktop

Alle Sicherungen – mit Ausnahme auf die externen Laufwerke – werden automatisch ausgeführt.



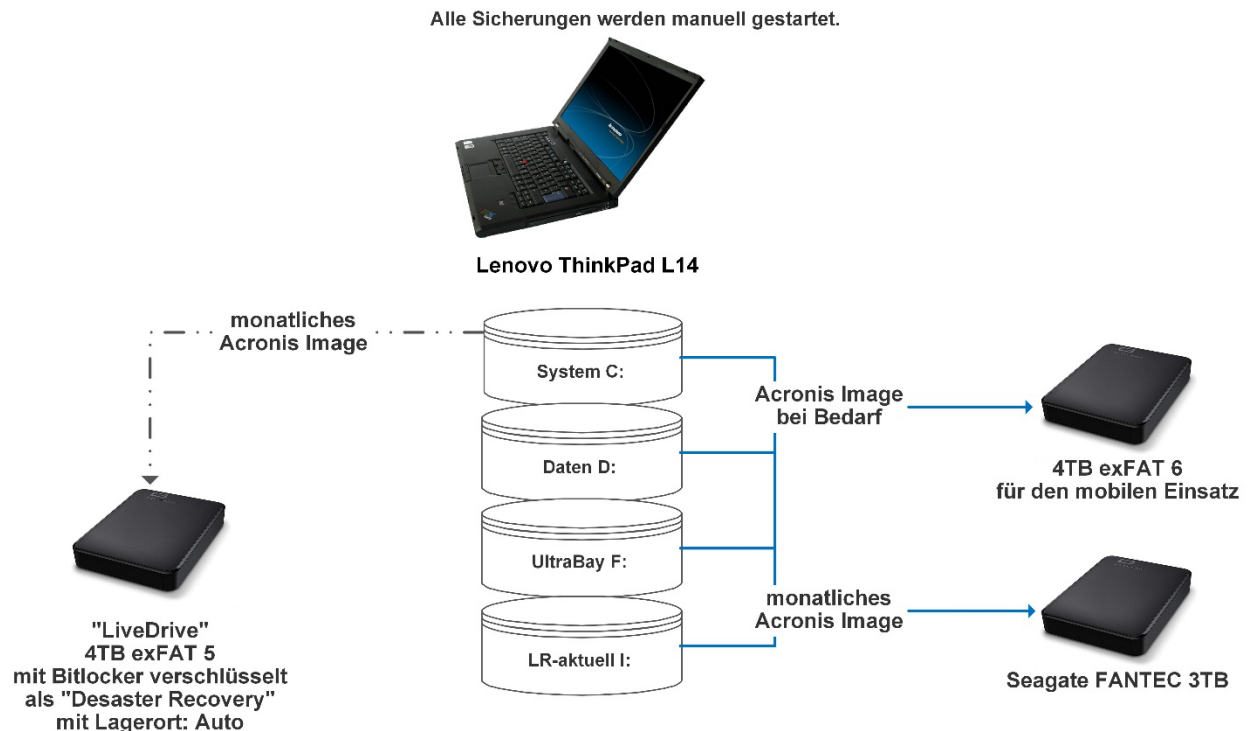
Da die externen eSATA-Laufwerke für die wöchentlichen und monatlichen Sicherungen jeweils nur dann angeschlossen werden und ansonsten offline sind, existiert auch dann noch ein zeitnaher Sicherungsbestand, wenn der lokale Datenbestand – und damit auch die automatischen Sicherungen auf das Laufwerk H: – durch einen technischen Defekt oder Virus zerstört werden.

Das externe Sicherungslaufwerk „LiveDrive“ wird als Disaster-Recovery im Auto gelagert, so dass bei einem Katastrophenfall – außer den Cloudspeichern – auch noch ein physischer Datenbestand zur Verfügung stehen sollte. *Diese Sicherung ist noch ein Relikt aus der Zeit ohne Cloudspeicher.*

B. Laptop: Lenovo ThinkPad L14

Für den Laptop erfolgen ausschließlich Image-Sicherungen mit [Acronis True Image](#). Die Backup Programme von Ashampoo und AOMEI laufen unter Windows 11 auf dem Laptop nicht fehlerfrei (Windows stürzt bei der Erstellung der Schattenkopie ab).

Datensicherungskonzept für den Laptop



Stand: 17.09.2025

C. Server: QNAP TS-253A-4G 6 TB 2 Bay

Die Sicherung / Synchronisation aller relevanten Verzeichnisse / Daten auf dem Server erfolgt täglich automatisch mit dem Programm [„HBS 3 Hybrid Backup Sync“](#) auf die am Server angeschlossenen USB-Platte *USB_Backup*:

- Homes
- Meine Daten (NAS)
- Meine Fotos (NAS)
- Meine Safes (NAS)
- Web
- EvernoteBackupENEX

Für die Kinofilme existiert zum überwiegenden Teil eine DVD oder Blu-ray. Für sonstige relevanten Filme wird manuell eine Kopie auf eine externe Platte gezogen.

D. Smartphone: Samsung Galaxy S24

Alle Daten auf dem Smartphone werden einmal im Monat mit dem Programm [„MyPhoneExplorer“](#) in das Verzeichnis „MPE Backup“ auf das externe Laufwerk „eSATA 2TB“ gesichert. Die Sicherung dient im Wesentlichen als Backup der lokal auf dem Smartphone gespeicherten Daten, welche nicht in einer Cloud gespeichert werden.

E. Desktop und Laptop: Outlook Backup

Outlook ist für mich eine zentrale und wichtige Anwendung, in welcher ich E-Mails, Termine*, Tasks und Kontakte* (*auch für Ursel) verwalte. Deshalb sind die Konfiguration und Daten von Outlook wichtig und bedürfen eines besonderen Schutzes.

Ab 01.09.2025 ist das cloudbasierte Microsoft Exchange mit lokalem Outlook 365 die zentrale Plattform für Emails, Kontakte, Kalender und Aufgaben für Desktop, Laptop und Smartphone, welche aufgrund seiner cloudbasierten Datenspeicherung prinzipiell keine zusätzlichen Sicherungsmaßnahmen benötigt.

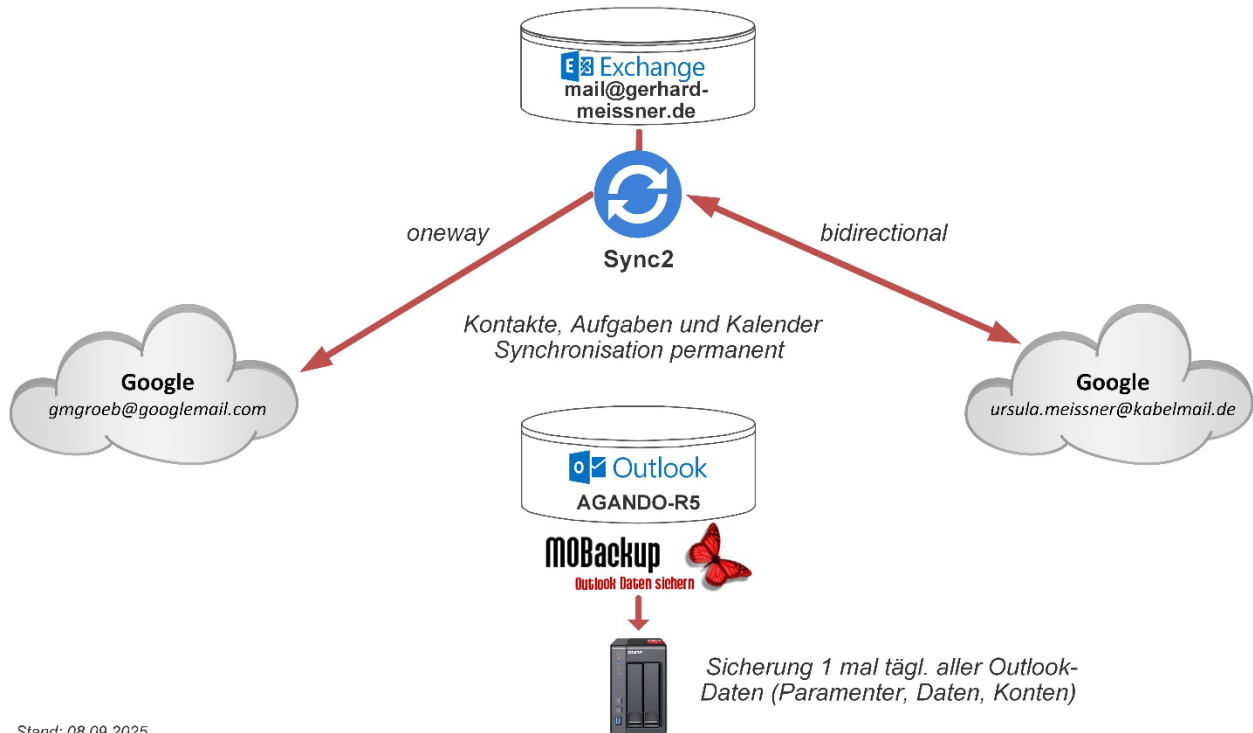
Um jedoch

1. Termine, Kontakte und Aufgaben für Ursel (in ihrem Google Konto) fürs Smartphone über Outlook mit verwalten zu können, wird weiterhin das Programm „Sync2“ eingesetzt.
2. Für meine Termine, Kontakte und Aufgaben ein zusätzliches Backup in meinem Google Konto vorzuhalten, kommt ebenfalls auf dem Desktop das Programm „Sync2“ zum Einsatz.

Die Outlook-Daten sind zwar alle auch in den Image-Sicherungen mit „AOMEI Backupper“ und/oder „Ashampoo Backup“ enthalten, doch sind diese bestenfalls vom Vortag. Die nachfolgend beschriebenen Maßnahmen erhöhen die Aktualität der Daten insbesondere für eine „nahtlosen“ Weiterführung der Arbeiten durch den Laptop bei einem Ausfall des Desktops.

- Auf dem Desktop erfolgt automatisch 1-mal täglich eine Komplettsicherung (Daten und Einstellungen) mit dem Programm [„MOBackup“](#) auf den eigenen Server.
- Ein [„MOBackup“](#) auf den Server wird auf dem Laptop regelmäßig manuell ausgeführt.

Outlook Backup & Sync



Stand: 08.09.2025

F. Evernote

Evernote ist für mich seit August 2022 wieder der „Standard“ zur Erfassung meiner Notizen (bin wg. Problemen mit *Nimbus Note* nach ca. 2 Jahren wieder zurück). Da alle Daten von *Evernote* mit der „Evernote – Cloud“ synchronisiert werden, wäre eigentlich kein zusätzliches Backup erforderlich.

Aufgrund der Erfahrungen mit *Nimbus Note* (Datenverluste) exportiere ich jedoch regelmäßig (jede Woche) meine Evernote-Ordner im ENEX-Format auf den QNAP-Server. Dort werden jeweils die letzten 3 Backups vorgehalten und im Rahmen der lokalen Sicherung (siehe C. Server: QNAP TS-253A-4G 6 TB 2 Bay) auf das externe USB-Laufwerk mitgesichert.

Diese Sicherung ermöglicht im Worstcase (z.B. Evernote stellt seinen Dienst ein) die Weiternutzung- / Verarbeitung der Daten mit Standardprogrammen wie Browser und/oder Textverarbeitung.

IV. Cloudspeicher zur Sicherung und Austausch von Daten

Der Einsatz der Cloudspeicher unterstützt folgende Zielsetzungen:

- Relevante / wichtige Daten sollen jederzeit, überall und geräteunabhängig (Desktop, Laptop, Smartphone, WEB) abgerufen werden können.
- Die Daten werden nur einmal bzw. an einem Gerät erfassen bzw. geändert und sind danach an allen Geräten aktuell verfügbar.
- Die am Markt befindlichen Cloud-Services / - Lösungen bieten im Wesentlichen vergleichbare Funktionen und unterscheiden sich nur geringfügig. Dass ich auf unterschiedliche Anbieter zurückgreife, hat u.a. folgende Gründe:
 - verwendete Funktionen waren früher noch nicht überall verfügbar
 - Unterschiede für Preise / Kosten für die verwendeten „Premiumfunktionen“ und Speicherplatz
 - Eingesetzte Software kann nur mit einem bestimmten Cloud-Service verwendet werden
 - Spezielle Ausrichtung für einen bestimmten Einsatzzweck
- Gemeinsame Verzeichnisse mit anderen Personen für den einfachen Austausch von Daten

Für meine Bedürfnisse setzte ich folgende Cloudspeicher bzw. cloudbasierte Services ein:

(1) **Dropbox**

Die [Dropbox](#) mit einem Speichervolumen von 2TB ist für mich die primäre Cloud-Anwendung mit den Aufgaben:

- Speicherung der wichtigsten Daten zur gemeinsamen Verwendung auf Desktop, Laptop und Smartphone.
Dabei werden sensible Daten mit der Software [Cryptomator](#) vor der Übertragung in die Cloud verschlüsselt und können wiederum nur über diese Software mit dem persönlichen Schlüssel auf dem jeweiligen System (Desktop, Laptop und Smartphone) entschlüsselt werden. Dadurch sind diese sensiblen Daten in der Cloud – auch über das Web-Interface der Dropbox – nicht zu lesen.
- Synchronisation / Sicherung aller Anwenderdaten des Desktops (*wie im weiteren Verlauf des Dokuments beschrieben*)

(2) **Microsoft OneDrive**

[OneDrive](#) wird mit dem eingesetzten „Office 365 Abo“ mit 1TB ausgeliefert und kommt zum Einsatz für:

- Speicherung von Anwenderdaten für geräteübergreifende Nutzung durch Microsoft Programme (wie z.B. OneNote, Sway oder andere)
- Austausch von Bildern und Videos mit anderen Personen
- Synchronisation / Sicherung aller Anwenderdaten des Servers (*wie im weiteren Verlauf des Dokuments beschrieben*)

(3) Google Drive

Der [Cloud-Service von Google](#) mit dem kostenlosen Speichervolumen von 17GB wird von mir für folgende Aufgaben verwendet:

- Speicherung von Anwenderdaten für geräteübergreifende Nutzung für spezielle Anwendungen, für welche Google Drive die – aus meiner Sicht – komfortabelste Benutzerschnittstelle bietet
- Standard-Sicherung von Apps und Daten auf dem Smartphone

(4) Samsung Cloud

Die von Samsung standardmäßig bereitgestellte Cloud mit 15GB wird ausschließlich für die Sicherung von Apps und Daten auf dem Smartphone verwendet.

(5) Adobe Creative Cloud

Die von Adobe im Rahmen des Foto-Abos bereitgestellte Cloud mit 20GB wird zum Austausch von Medien und PDFs zwischen Desktop, Laptop und Smartphone verwendet.

B. Datensynchronisation mit Cloudspeicher

Bei den Cloudservices wird ein - diesem zugeordneten - Verzeichnis auf der Festplatte automatisch mit dem online-Cloudspeicher synchronisiert. Somit stehen den Systemen (PC und Smartphone) und im WEB diese Daten für den Zugriff und die Verarbeitung zur Verfügung.

Welche Daten in welchem Cloudservice gespeichert werden, hängt ausschließlich von der jeweiligen individuellen Nutzung der Cloudservices ab.

Meine Verzeichnisse in der Cloud (Stand März 2020)

Dropbox

-  _eigene Daten
-  _Freigaben für Dritte
-  _Transfer
-  Acronis_AR5_Outlook
-  Adobe InDesign Vorlagen
-  Apps
-  Canon irista Upload Ordner
-  Canon Scan
-  Clever Printing Testform Print
-  Directory und USB-Stick portable
-  DropSync
-  DVD-Video-Archiv+ v8 Daten
-  FontArchiv aller Schriften
-  FontArchiv Neuzugänge für Webseite
-  FontArchiv private Schriften
-  Gemeinsamer Ordner Vogel - Meißner
-  Kamera-Uploads
-  Kamera-Uploads (1)
-  Meißner_gemeinsam
-  PathAway Projekte Ablage
-  Photos
-  Programm-Einstellungen-Sicherungen
-  Public
-  Safes in Dropbox
-  Screenshots
-  SmartDraws auf Dropbox
-  System-Setups für Dritte
-  ZipShare
-  .dropbox
-  desktop

Google Drive

-  000 Canon Scan
-  Anlagen
-  Blog Daten
-  Dynalist Attachments
-  Freigabe für Dritte
-  MindMapper Ablage
-  MindMapper Attachments
-  Temp (SSK Überweisungen per App)
-  Ursel - geteilt mit Gerd
-  desktop

OneDrive

-  Bilder
-  Blog Fotoalben
-  Dokumente
-  E-Mail-Anhänge
-  Freigegebene Favoriten
-  Musik
-  Öffentlich
-  OneDrive_encrypted
-  Transfer
-  Persönlicher Tresor

C. Desktop: Laufwerk - Synchronisation mit der Dropbox

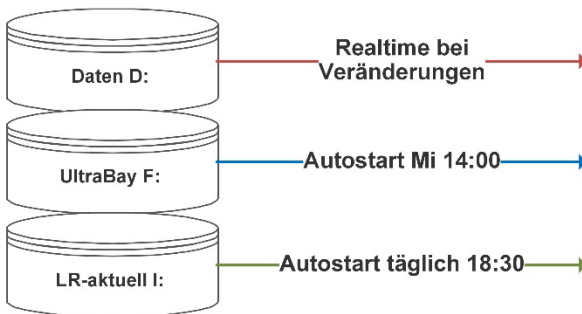
Synchronisation der Daten des Desktop mit dem Dropbox-Cloudspeicher

Die Synchronisation wird automatisch gem. der jeweiligen Konfiguration ausgeführt



Das Programm GoodSync synchronisiert die relevanten Daten auf dem Desktop (oneway) mit der Dropbox.

Die Zielverzeichnisse der Synchronisation sind aus der Standard-Synchronisation mit dem lokalen Dropbox-Ordner ausgeschlossen.



Stand: 26.04.2023

Durch die Synchronisierung der Daten in die Dropbox ergeben sich folgende Vorteile / Nutzen:

- Bei Bedarf ortsunabhängiger Zugriff auf die Daten per Smartphone und/oder WEB. Damit dieser Zugriff auch problemlos erfolgen kann, werden die Daten zur Speicherung auf der Dropbox nicht zusätzlich verschlüsselt.
- Der Laptop hat auch ohne vorherige AllSync-Synchronisation (siehe nachfolgende Beschreibung) die Möglichkeit auf aktuelle Daten des Desktops zuzugreifen.
- Verfügbarkeit der Daten auch nach „Katastrophenfall“.
- Die Dropbox speichert geänderte oder gelöschte Daten 30 Tage im „Versionsverlauf“. Die Daten können innerhalb dieses Zeitraums jederzeit wiederhergestellt werden. Damit erreicht man eine zusätzliche Sicherheit vor Verlust durch versehentliche Änderungen und/oder Löschungen.

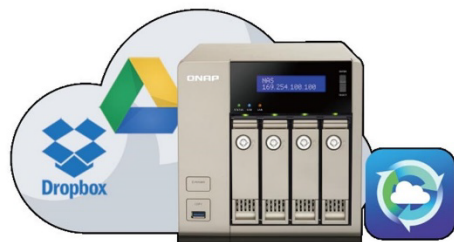
Die Synchronisation findet nur in eine Richtung: Desktop zur Dropbox statt!

D. Server: Laufwerk- Synchronisation mit OneDrive

Analog zu der Synchronisation der Desktop - Laufwerk - Synchronisation mit der Dropbox, erfolgt dies mit den relevanten Verzeichnissen auf dem Server.

Synchronisation der Daten des Servers mit dem OneDrive-Cloudspeicher

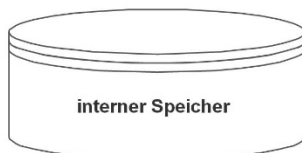
Die Synchronisation wird automatisch gem. der jeweiligen Konfiguration ausgeführt



Server: QNAP TS-253A-4G
App: HBS 3 Hybrid Backup Sync

Das Programm HBS 3 Hybrid Backup Sync synchronisiert die Daten auf dem NAS-Server (oneway) mit OneDrive.

Die Zielverzeichnisse der Synchronisation sind aus der Standard-Synchronisation mit dem auf Desktop und Laptop lokalen OneDrive-Verzeichnis ausgeschlossen und belegen dadurch dort keinen Speicherplatz.



- Folgende Verzeichnisse:
- homes + Multimedia + Public
 - Meine Daten (NAS)
 - Meine Fotos (NAS)
 - Meine Musik (NAS)
 - Meine Videos (NAS)
 - Web



Externe Laufwerke werden nicht gesichert!

Stand: 31.03.2021

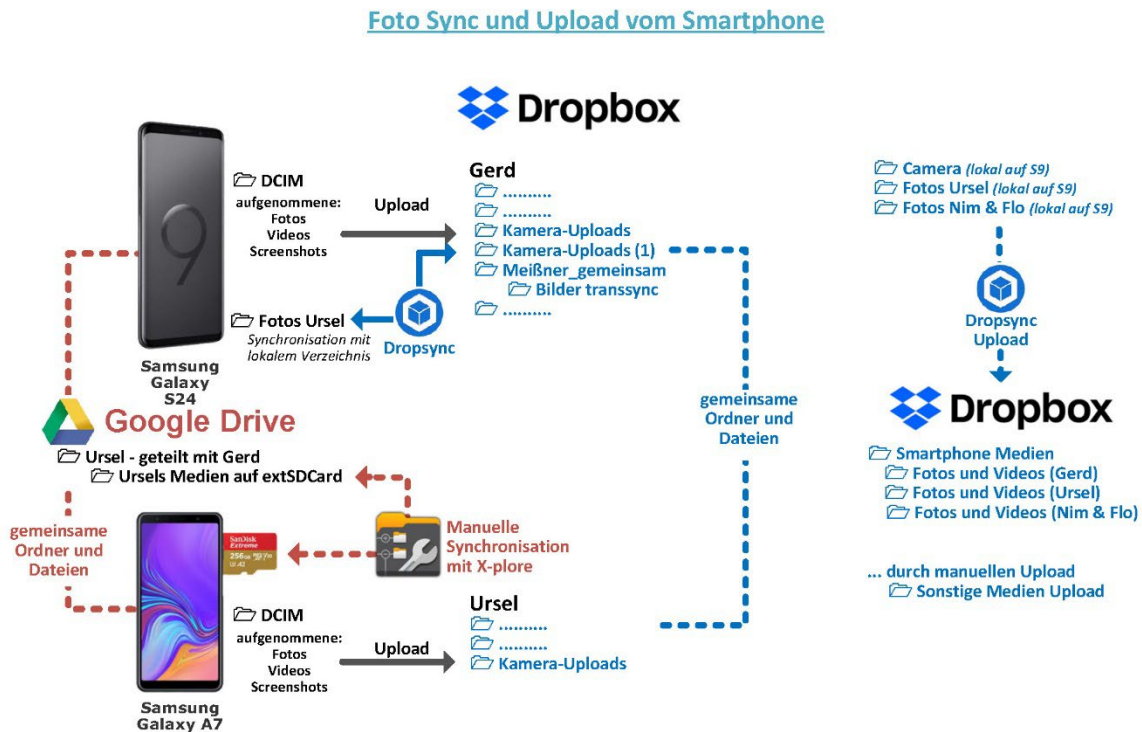
Die durch die Synchronisierung der Daten mit OneDrive erzielten Vorteile / Nutzen sind analog wie bei der Synchronisierung der Desktop-Daten mit der Dropbox (*siehe vorheriges Kapitel*).

OneDrive als Speicher für die Server-Daten wurde gewählt, da der Speicher im Rahmen des Office 365 – Abo zur Verfügung steht und da das Programm „[HBS 3 Hybrid Backup Sync](#)“ diesen Speicher gut und performant verwenden kann.

Die Synchronisation findet nur in eine Richtung: Server zu OneDrive statt!

E. Smartphone: Foto Synchronisation und -Backup

Unter Einsatz der Dropbox und Google Drive wurde folgender Prozess konfiguriert und implementiert:



Stand: 19.11.2024

Die wesentlichen Ziele dieser Konfiguration sind:

- Die auf den Smartphones aufgenommenen Fotos werden automatisch in die folgenden Dropbox-Verzeichnisse hochgeladen (nicht synchronisiert) und stehen somit am Desktop / Laptop und S24 ohne weiteres Zutun zur Verfügung
 - „Kamera-Uploads“ für Fotos von Gerd's S24
 - „Kamera-Uploads (1)“ für Fotos von Ursel's A7
- Ursel's „Medienarchiv“ auf der externen SDcard wird mit der App *X-plore* manuell mit Google Drive synchronisiert. Dadurch kann dieses Medienarchiv über alle Geräte mit Zugriff auf das Google Drive Verzeichnis aktualisiert werden.
- Alle aufgenommenen Fotos werden vom S24 automatisch in das Dropbox-Verzeichnis „\Smartphone Medien Upload\.....“ hochgeladen. Damit wird eine automatische Sicherung / Archivierung aller von den Smartphones aufgenommenen Fotos sichergestellt.

Für die Synchronisierung / den Upload auf den Smartphones wird die App „DropSync“ verwendet.

V. Datensynchronisation zwischen Desktop und Laptop

Um die nicht auf lokalen Cloudlaufwerken /-verzeichnissen befindlichen Daten auf dem Laptop mit denen des Desktops (Master) aktuell zu halten, sind folgende Programme / Verfahren implementiert:

A. Outlook Synchronisation Desktop <-> Laptop

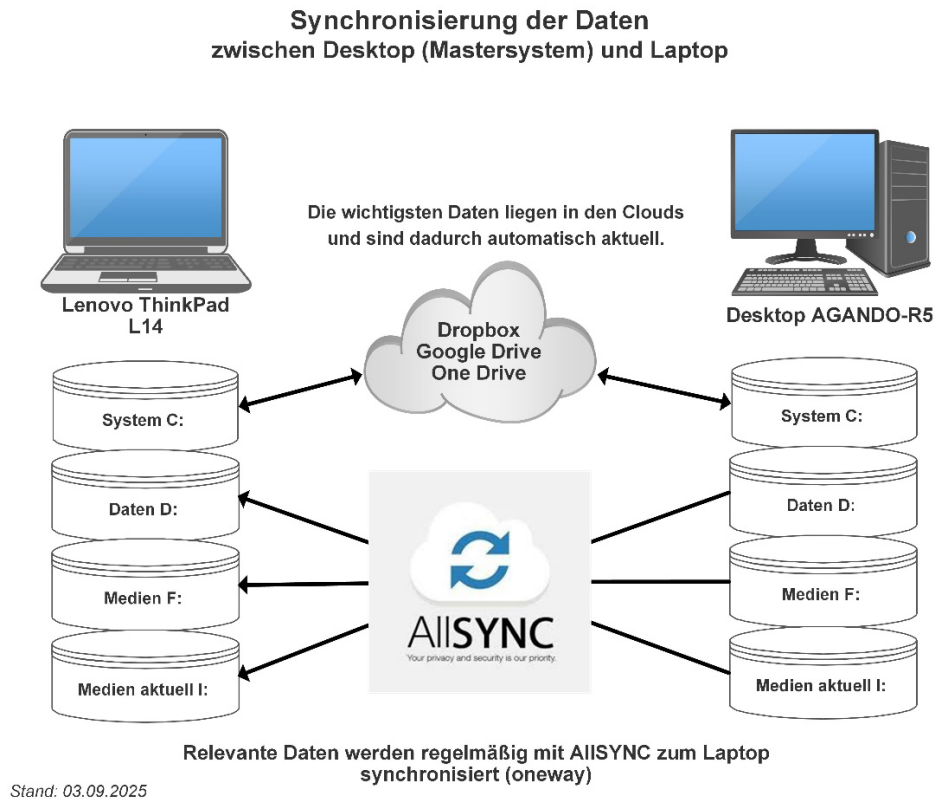
Die automatische Synchronisation der Inhalte von Outlook (E-Mail, Aufgaben, Kalender, Notizen und alle sonstigen Ordnerinhalte) erfolgt mit dem Programm „[SimpleSYN Business](#)“.

Das auf beiden Systemen installierte Programm verbindet die beiden Programme / Rechner automatisch,

- Über das lokale Netzwerk oder
- Das Internet (*nur Verbindung, keine Speicherung von Daten*)

sobald beide Rechner hochgefahren / online sind und synchronisiert bidirektional die Daten real-time, solange die Verbindung existiert.

B. Datensynchronisation Desktop ->> Laptop



Für diese Synchronisation wird das Programm „[AllSync](#)“ verwendet und wird bei Bedarf manuell gestartet. Es vergleicht die spezifizierten Laufwerke / Verzeichnisse und überträgt die Verän-

derungen auf dem Desktop auf den Laptop. Aus Sicherheitsaspekten ist es eine „oneway“-Synchronisation. Sofern Veränderungen von Daten auf dem Laptop auf den Desktop zurück übertragen werden müssen, ist muss dies über die „Datensynchronisation mit Cloudspeicher“ geschehen.

C. Die Datensynchronisation in der Praxis

Um den Laptop für den mobilen Einsatz vorzubereiten, werden beide Rechner im Heimnetz gestartet. Danach

- Erfolgt die Outlook Synchronisation automatisch
- Wird das Programm „AllSync“ manuell gestartet und der Datenbestand auf dem Laptop aktualisiert.

Nach Beendigung des mobilen Einsatzes, werden beide Rechner im Heimnetz gestartet. Danach

- Erfolgt die Outlook Synchronisation automatisch
- Müssen ggf. die auf einem Cloudspeicher befindlichen Änderungen bzw. neue Daten in die betreffenden Verzeichnisse (*sofern nicht Cloudspeicher*) manuell überführt werden.

Anmerkung:

Im Prinzip könnte mit dem Programm „GoodSync“ eine komplette bidirektionale Synchronisation der Daten zwischen Desktop und Laptop über die Dropbox implementiert werden (Ausnahme: Outlook), doch habe ich ausfolgenden Gründe davon Abstand genommen:

- *Die Programme „AllSync“ und „SyncBackPro“ waren bereits früher implementiert und im Einsatz*
- *Eine bidirektionale Synchronisation zwischen Laptop und Desktop erhöht die Gefahr, dass Daten des Desktops (ist das führende System = Master) unbeabsichtigt oder aus anderen Gründen verfälscht / gelöscht werden.*
- *Mit den implementierten Prozessen ist eine absolute Kontrolle des Datenflusses und damit die Sicherheit und Konsistenz der Daten gewährleistet.*

VI. Datenschutz durch Zugriffsschutz und Verschlüsselung

Ziel dieser Maßnahmen ist, sensible Daten auf den lokalen Speichern sowie in der Cloud vor unberechtigtem Zugriff zu schützen.

A. Passwortschutz bei Systemstart / Login

Um die unberechtigte Nutzung der Geräte einzuschränken sind folgende Maßnahmen implementiert:

- Desktop: Keine Prüfungen bei Systemstart
- Laptop: Passwort, PIN oder Fingerabdruck erforderlich
- Server: Passwortschutz bei Login und Zugriff auf Daten
- Smartphone: Passwort, PIN oder Fingerabdruck

B. Verschlüsselung gespeicherter Daten

Passwortschutz verhindert zwar die unbefugte Nutzung der Geräte, doch kann damit die Datensicherheit / Vertraulichkeit der Daten bei Hackerangriffen und Zugriff auf die physischen Speicher nicht gewährleistet werden. Hierfür sind folgende Maßnahmen implementiert:

1. Verschlüsselung externe Laufwerke

Externe Laufwerke für Sicherung / Archivierung von Daten im mobilen Einsatz sind mit dem Windows 10 – Tool „[Bitlocker](#)“ verschlüsselt. Dadurch

- Sind alle Daten auf den Laufwerken gegen den Zugriff durch Dritte geschützt. Für den Zugriff wird der Key zur Entschlüsselung benötigt.
- Um diesen Key am Desktop und Laptop nicht immer eingeben zu müssen, sind diese so konfiguriert, dass bei Verbindung der externen Laufwerke diese automatisch entschlüsselt werden.

2. Verschlüsselung wichtiger und sensibler Daten

Sämtlicher dieser Daten werden in „[Steganos® Safes](#)“ abgelegt. Die „Safes“ sind thematisch gruppiert (Dokumentenarchiv, Finanzen,) und werden physisch auf der Dropbox gespeichert (*dadurch: automatische Synchronisation Desktop – Laptop und zusätzliche Sicherheit durch Cloud mit Versionierung*).

Um auf die Daten zuzugreifen, muss ein Safe mit dem Programm „Steganos Safe“ mit dem individuell festgelegten Passwort geöffnet werden. Danach wird der Inhalt des Safes in einem virtuellen Laufwerk bereitgestellt.

Im geschlossenen Zustand liegen die Daten verschlüsselt in einer Datei, so dass

- ohne das Programm „Steganos Safe“ und dem Safe-spezifischen Passwort auf die Daten nicht zugegriffen werden kann

- dadurch – obwohl die Daten auch physisch in der Cloud / Dropbox gespeichert werden – auch dort die Sicherheit gewährleistet ist

Für das Smartphone gibt es keine App, um auf die Daten der in der Cloud liegenden Safes zuzugreifen. Da ich jedoch den Grundsatz vertrete, dass alle meine wichtigen Daten auch am Smartphone und per Web-Interface zur Verfügung stehen sollen, ist für das Dokumentenarchiv der nachfolgende Prozess implementiert:

- Die betreffenden Verzeichnisse werden regelmäßig mit dem Programm „[SyncBackPro](#)“ auf den Server gesichert.
- Dabei werden die Dateien automatisch per WinZip verschlüsselt.
- Durch die automatische Sicherung der Server-Daten in die Cloud OneDrive, stehen diese Daten dann auch auf dem Smartphone und per Web-Interface zur Verfügung, jedoch wird für die Entschlüsselung der Zip-Dateien der entsprechende Schlüssel benötigt.