Realisierungsbericht

|  |  |
| --- | --- |
| Status | Abgeschlossen |
| Projektname | Webbasierte Fotofreigabe für Kunden |
| Projektleiter | Vladan Vranjes |
| Auftraggeber | Claude Fankhauser |
| Autoren | Vladan Vranjes, Yanis Riedo, Luan Stauffer, David Ammann |
| Verteiler | Gesamte Gruppe |

**Änderungskontrolle, Prüfung, Genehmigung**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name oder Rolle |
| 1.0 | 07.05.25 | Erstellung der Vorlage & Erster Verbindungsaufbau zu Server | Alle Mitglieder |
| 1.1 | 14.05.2025 | Erarbeiten der Dokumentation – Zusammenfassung / Systemtests | Alle Mitglieder |
| 1.2 | 21.05.2025 | Abschluss von:   * Technische Detailspezifikation * Sytemtest | David, Yanis & Vladan |
| 1.3 | 28.05.2025 | Korrekturen von Layout Problemen | David & Vladan |
| 1.4 | 01.06.2025 | Abschluss von:   * Systemdokumentation * Weiterführung der Projektplanung | David & Vladan |
| 1.5 | 02.06.2025 | Abschluss von Tests | David, Vladan, Yanis & Luan |

**Definitionen und Abkürzungen**

|  |  |
| --- | --- |
| Begriff / Abkürzung | Bedeutung |
| Ggf. | Gegebenenfalls |
| Etc. | et cetera („und so weiter“) |
| EULA  CMS | End User License Agreement  Content-Management-System |
| GUI | Graphic User Interface, grafische Benutzeroberfläche |
| NAS | Network Attached Storage, Datenspeicher |
| SSL | Secure Sockets Layer, häufig als sichere Verschlüsselung für Websites verwendet |
| SFTP | Secure File Transfer Protocol, Dateiübertragung via SSH |
| VPN | Virtual Private Network, sichere Verbindung zwischen mind. 2 Maschinen |
| HTTPS | Hypertext Transfer Protocol Secure, Netzwerkprotokoll für Websites |
| SSE | Schnittstelle extern |
| SSI | Schnittstelle intern |
| Drag-and-Drop | Technologie, welche es erlaubt, Bilder durch Anwählen und «Fallenlassen» auf einen Ordner zu transferieren |
| SSH | Secure Shell, kryptografisches Netzwerkprotokoll |

**Inhaltsverzeichnis**

[1 Zusammenfassung 5](#_Toc199797321)

[2 Technische Detailspezifikation 5](#_Toc199797322)

[2.1 Systemdesign 5](#_Toc199797323)

[2.1.1 Struktur 5](#_Toc199797324)

[2.1.1.1 Subsystem 1: NAS 5](#_Toc199797325)

[2.1.1.2 Subsystem 2: Webserver 5](#_Toc199797326)

[2.2 Externe Schnittstellen 6](#_Toc199797327)

[2.3 Interne Schnittstellen 6](#_Toc199797328)

[2.4 Bildliche Darstellung der Architektur 7](#_Toc199797329)

[2.5 Sicherheit (ISDS) 7](#_Toc199797330)

[2.5.1 Schutzbedarfsanalyse 7](#_Toc199797331)

[2.5.2 Privacy by design 7](#_Toc199797332)

[2.5.3 Risikoanalyse 7](#_Toc199797333)

[2.5.4 Sicherheitsmassnahmen 8](#_Toc199797334)

[2.5.5 Zugriffskontrolle 8](#_Toc199797335)

[2.5.6 Verantwortlichkeiten 9](#_Toc199797336)

[2.5.7 Monitoring & Wartung 9](#_Toc199797337)

[2.5.8 Backup 9](#_Toc199797338)

[2.6 Anforderungszuordnung 10](#_Toc199797339)

[2.6.1 Funktionierender Filetransfer 10](#_Toc199797340)

[2.6.2 Usermanagement mit Benutzername und Passwort 10](#_Toc199797341)

[2.6.3 VPN-Verbindung zwischen NAS und Webserver 10](#_Toc199797342)

[2.6.4 Automatischer Upload der Fotos von NAS auf Server (mit Möglichkeit dies manuell auch zu erledigen) 10](#_Toc199797343)

[2.6.5 Website mit gültigem SSL welche öffentlich erreichbar ist 10](#_Toc199797344)

[3 Systemdokumentation 11](#_Toc199797345)

[3.1 Konfigurations-Dokumentation 11](#_Toc199797346)

[3.1.1 SSHD-Config File 11](#_Toc199797347)

[3.1.2 Docker Config 13](#_Toc199797348)

[3.1.3 Caddy 13](#_Toc199797349)

[3.1.4 Tailscale 14](#_Toc199797350)

[3.1.5 Ordnerstruktur 15](#_Toc199797351)

[3.1.6 DNS-Config 17](#_Toc199797352)

[3.1.7 Firewall Config 18](#_Toc199797353)

[3.2 Benutzerhandbuch 19](#_Toc199797354)

[3.2.1 Systemübersicht 19](#_Toc199797355)

[3.2.1.1 Ziele und Hauptfunktionen des Systems 19](#_Toc199797356)

[3.2.2 Anwenderfunktionalität 19](#_Toc199797357)

[3.2.2.1 Aufgabe 19](#_Toc199797358)

[3.2.2.2 Instruktion zu Anwendung und Betrieb 19](#_Toc199797359)

[3.2.2.3 Initialisierung 19](#_Toc199797360)

[3.2.2.4 Durchführung 19](#_Toc199797361)

[3.2.2.5 Terminierung 19](#_Toc199797362)

[3.2.2.6 Wiederanlauf («Restart») 19](#_Toc199797363)

[3.3 Supporthandbuch 20](#_Toc199797364)

[3.3.1 Massnahmen bei Benutzerproblemen 20](#_Toc199797365)

[3.3.2 Massnahmen bei technischen Problemen 21](#_Toc199797366)

[3.3.3 Anhang zum Supporthandbuch 21](#_Toc199797367)

[4 Systemtest 22](#_Toc199797368)

[4.1 Testspezifikation 22](#_Toc199797369)

[4.2 Testanforderungen 22](#_Toc199797370)

[4.2.1 Tests unter Normalbedingungen: 22](#_Toc199797371)

[4.2.2 Tests mit Grenzwerten: 22](#_Toc199797372)

[4.2.3 Tests unter Ausnahmebedingungen: 22](#_Toc199797373)

[4.2.4 Sicherheitstests: 22](#_Toc199797374)

[4.2.5 Rollentests: 22](#_Toc199797375)

[4.3 Testverfahren 23](#_Toc199797376)

[4.3.1 Vorbereitung 23](#_Toc199797377)

[4.3.2 Durchführung 23](#_Toc199797378)

[4.3.3 Auswertung 23](#_Toc199797379)

[4.3.4 Testkriterien 23](#_Toc199797380)

[4.3.4.1 Abdeckungsgrad 23](#_Toc199797381)

[4.3.4.2 Checkliste: 24](#_Toc199797382)

[4.3.5 Testfälle 24](#_Toc199797383)

[4.4 Testprozedur 25](#_Toc199797384)

[4.4.1 Vorbereitung 25](#_Toc199797385)

[4.4.2 Voraussetzungen: 25](#_Toc199797386)

[4.4.3 Konfiguration: 25](#_Toc199797387)

[4.4.4 Durchführungen 26](#_Toc199797388)

[4.4.5 Nachbearbeitung 27](#_Toc199797389)

[4.5 Testprotokoll 27](#_Toc199797390)

[4.5.1 Testobjekt 27](#_Toc199797391)

[4.5.2 Testresultate 28](#_Toc199797392)

[4.5.2.1 Webserver Test 28](#_Toc199797393)

[4.5.2.2 NAS & Tailscale 28](#_Toc199797394)

[4.5.2.3 Caddy 29](#_Toc199797395)

[4.5.2.4 SFTPgo 29](#_Toc199797396)

[4.5.2.5 Cronjobs 29](#_Toc199797397)

[4.5.2.6 NMAP-Portscan 29](#_Toc199797398)

[5 Weiterführung der Projektplanung 31](#_Toc199797399)

[5.1 Abgleich von Planung und tatsächlichem Verlauf der Phase Konzept 31](#_Toc199797400)

[*5.2* Aktualisierung der Risikosituation 31](#_Toc199797401)

[*5.3* Planung der nächsten Phase 31](#_Toc199797402)

**Tabellenverzeichnis**

[Tabelle 1: Subsystem NAS 5](#_Toc199795264)

[Tabelle 2: Subsystem Webserver 5](#_Toc199795265)

[Tabelle 3: Externe Schnittstellen 6](#_Toc199795266)

[Tabelle 4: Interne Schnittstellen 6](#_Toc199795267)

[Tabelle 5: Risikoanalyse 8](#_Toc199795268)

[Tabelle 6: Zugriffskontrolle 8](#_Toc199795269)

[Tabelle 7 : Anforderungszuordnung 10](#_Toc199795270)

[Tabelle 8: Kritikalität der Funktionseinheit 22](#_Toc199795271)

[Tabelle 9: Testverfahren -> Vorbereitung 23](#_Toc199795272)

[Tabelle 10: Testverfahren -> Durchführung 23](#_Toc199795273)

[Tabelle 11: Testverfahren -> Auswertung 23](#_Toc199795274)

[Tabelle 12: Testverfahren -> Testkriterien 23](#_Toc199795275)

[Tabelle 13: Testverfahren -> Checkliste 24](#_Toc199795276)

[Tabelle 14: Testfälle 24](#_Toc199795277)

[Tabelle 15: Vorbereitung 25](#_Toc199795278)

[Tabelle 16: Testobjekte 27](#_Toc199795279)

**Abbildungsverzeichnis**

[Abbildung 1: Architektur -> Aufbau des Systems 7](#_Toc199795365)

[Abbildung 2: Caddy 13](#_Toc199795366)

[Abbildung 3: Tailscale 14](#_Toc199795367)

[Abbildung 4: Ordnerstruktur 15](#_Toc199795368)

[Abbildung 5: Ordnerstruktur -> NAS 16](#_Toc199795369)

[Abbildung 6: DNS-Config 17](#_Toc199795370)

[Abbildung 7: Firewall-Config 18](#_Toc199795371)

[Abbildung 8: Testresultat -> Webserver 28](#_Toc199795372)

[Abbildung 9: Testresultat -> NAS & Tailscale 28](#_Toc199795373)

[Abbildung 10: Testresultat -> Caddy\_1 29](#_Toc199795374)

[Abbildung 11: Testresultat -> Caddy\_2 29](#_Toc199795375)

[Abbildung 12: Testresultat -> SFTPgo 29](#_Toc199795376)

[Abbildung 13: Testresultat -> Cronjobs\_1 Abbildung : Testresultat -> Cronjobs\_2 29](#_Toc199795377)

[Abbildung 14: Testresultat -> NMAP-Portscan 30](#_Toc199795378)

# Zusammenfassung

Dieses Dokument bezieht sich auf die Realisierung einer Webplattform zur Freigabe von Fotos, welche auf einem NAS-System hinterlegt sind. Ziel ist es, dass die in der Konzeptphase geplanten Anforderungen korrekt technischen umgesetzt werden.

Die Realisierungsphase umfasst die konkrete Implementierung der Systemarchitektur, die Konfiguration der Server und Dienste, die Umsetzung sicherheitsrelevanter Massnahmen sowie die Durchführung von Funktionstests. Zudem beinhaltet dieses Dokument die vollständige System-, Benutzer und Supportdokumentation.

Konzept, Planung und Projektgrundlagen wurden in dem Konzeptbericht dokumentiert und sind nicht Teil dieser Dokumentation.

# Technische Detailspezifikation

Unter der Detailspezifikation werden die Haupt- & Nebenbestandteile des Systems aufgezeichnet.

## Systemdesign

In diesem Abschnitt wird unser Design aufgezeigt und bildlich dargestellt.

### Struktur

In diesem Teil des Dokuments werden wir die Systemarchitektur genauer in Module und Schnittstellen aufteilen.

Gliederung der Lösung in Module

Nachfolgend werden unsere beiden Subsysteme in ihre Module aufgeteilt und erklärt.

#### Subsystem 1: NAS

Funktionen des Subsystems NAS:

|  |  |  |
| --- | --- | --- |
| Modul-Nummer | Modulname | Funktion |
| A1 | NAS-Datenspeicher | Lokaler Speicher für die Daten |
| A2 | Tailscale-Client | Stellt VPN-Verbindung zwischen NAS und Webserver her |
| A3 | Upload-Skript | Lädt Bilder auf den Webserver hoch |
| A4 | Zeitsteuerung | Triggert Skrips regelmässig (Cronjobs) |
| A5 | Logging & Monitoring | Protokolliert Uploads & Fehler |

Tabelle 1: Subsystem NAS

#### Subsystem 2: Webserver

Funktionen des Subsystems Webserver:

|  |  |  |
| --- | --- | --- |
| Modul-Nummer | Modulname | Funktion |
| B1 | Tailscale-Client | Stellt VPN-Verbindung zwischen NAS und Webserver her |
| B2 | SFTP-Server | Stellt Weboberfläche für die Website dar |
| B3 | Caddy | Produziert gültiges SSL |
| B4 | Reverse-Proxy | Leitet verschiedenste Dienste durch |

Tabelle 2: Subsystem Webserver

## Externe Schnittstellen

Nachfolgend werden alle externen Schnittstellen aufgeführt.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Schnittstelle | Bezeichnung | Verbindungspartner | Port | Richtung | Zweck |
| SSE-01 | VPN-Gateway | NAS | 1194 | Eingehend / Ausgehend | Aufbau einer Verbindung von externem Netz zu internem Netz |
| SSE-02 | SFTP-Server | Externe Clients | 22 / 443 | Eingehend | Zugriff von Extern auf den Webserver und Möglichkeit Bilder per SFTP herunterzuladen |
| SSE-03 | Admin-Zugriff | Autorisierte Admin-Clients | 22 | Eingehend | Möglichkeit per SSH auf Server zuzugreifen (benötigt dazugehörigen Schlüssel) |
| SSE-04 | Monitoring-Output | NAS | 514 | Ausgehend | Möglichkeit, Server zu loggen |
| SSE-05 | Reverse-Proxy Dashboard | Autorisierte Admin-Clients | 8443 | Eingehend | Zugriff auf ein Web-Interface für den Reverse-Proxy |
| SSE-06 | Reverse Proxy backend | NAS | 3000 | Ausgehend / Eingehend | Reverse-Proxy leitet verschiedene Dienste weiter |

Tabelle 3: Externe Schnittstellen

## Interne Schnittstellen

Nachfolgend werden alle internen Schnittstellen aufgeführt.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Schnittstelle | Bezeichnung | Verbindungs-partner | Port | Richtung | Zweck |
| SSI-01 | Tailscale-Netzwerk | Webserver | 1194 | Ausgehend / Eingehend | Aufbau einer Verbindung von internem Netz zu externem Netz |
| SSI-02 | Bild-Upload Script | Webserver | 22 | Ausgehend | Übertragung der Bilddateien |
| SSI-03 | Webinterface NAS | Autorisierte interne  Admin-Clients | 443 | Eingehend | Webinterface für eine vereinfachte Bedienung des NAS. Hier werden Bilder lokal auch über Drag-and-Drop hochgeladen |

Tabelle 4: Interne Schnittstellen

## Bildliche Darstellung der Architektur

Nachfolgend ist noch eine bildliche Darstellung der Systemarchitektur abgebildet

A cloud with lights and a black arrow

AI-generated content may be incorrect., Bild

Abbildung 1: Architektur -> Aufbau des Systems

## Sicherheit (ISDS)

Im folgenden Abschnitt werden die Konzeptpunkte für die ISDS geschildert und detailliert erklärt.

### Schutzbedarfsanalyse

Die Dateien, respektiv die Fotos und Videos, die auf dieser Infrastruktur behandelt werden, sind personenbezogen. Demnach sind die Vertraulichkeit und die Sicherheit derer sehr hoch gestuft.

Deren Integrität kann jedoch nichts angehabt werden, da nur der Admin Zugriff auf Änderungen der Webseite hat und nur dieser die Dateien hochladen kann.

Die Dateien der Kunden sollten jederzeit ab Freigabe zugänglich sein und laufen auf einem Cloud-Server.

### Privacy by design

Wie bereits im Dokument weiter oben erwähnt, ist das Projekt mit dem Prinzip «Privacy by Design» erstellt worden. Jeder Schnittstelle wird auf das Nötigste beschränkt, Verbindung zwischen internen Maschinen wird nur über VPN ermöglicht, und Zugriff auf das System von Extern wird so klein wie möglich gehalten.

Für jede Maschine sieht das nachher so aus:

* NAS
  + Liegt in einem privaten Netzwerk, welches zu jedem Zeitpunkt überwacht und auf höchste Sicherheit geprüft wird.
  + Verbindung auf Webserver funktioniert **nur** über VPN.
* Webserver
  + Firewall-Regelungen werden überprüft; nur nötigstes wird freigegeben,
  + SFTPgo regelt Userberechtigungen und sorgt dafür, dass nur mit gültigem Username und Passwort auf Bilder zugegriffen werden kann.
  + Zugriff auf den Webserver selbst ist **nur** über SSH mit gültigem Keypar möglich; zudem können Befehle via «sudo» nur mit zusätzlichem Passwort ausgeführt werden.
  + Via Caddy wird dafür gesorgt, dass die Website ein gültiges SSL hat und nur über HTTPS erreichbar ist.
  + Verbindung auf NAS funktioniert **nur** über VPN.

### Risikoanalyse

|  |  |  |  |
| --- | --- | --- | --- |
| Risiko | Auswirkung | Wahrscheinlichkeit | Massnahme |
| Unbefugter Zugriff auf Fotos / Videos | Hoch | Sehr klein | HTTPS-Verbindung & sicheres Zugriffsnetzwerk |
| Datenverlust durch Ausfall von Cloudservice | Hoch | Sehr klein | Lokaler Speicherbackup aus NAS |
| Passwortdiebstahl | Hoch | Klein | Starke Passwortrichtlinien |

Tabelle 5: Risikoanalyse

### Sicherheitsmassnahmen

Folgende Sicherheitsmassnahmen sind im Rahmen des Projekts & der Laufzeit des Webservers einzuhalten

**Netzwerksicherheit:**

* Firewall-Regeln im Heimrouter gezielt öffnen für NAS
* Nur nötige Ports freigeben (z. B. HTTPS 443)

**Webserver-Schutz:**

* Verwendung von HTTPS (SSL-Zertifikat)

**Login- & Zugangssicherheit:**

* Benutzerregistrierung mit E-Mail-Bestätigung
* Passwortregeln (Länge, Komplexität)
* Optional: Zwei-Faktor-Authentifizierung (z. B. TOTP via App)
* Keine Speicherung von Klartext-Passwörtern

**Datenschutz:**

* Datenschutzerklärung auf der Webseite
* Kunden geben aktiv Einwilligung zur Speicherung ihrer Fotos und Nutzerdaten

### Zugriffskontrolle

Mit der Folgenden Matrix wird gezeigt wer auf welche Daten / Prozesse Zugriff hat.

Der Systemadmin hat zusätzlich zu seinem Login eine 2FA, welche den Unbefugten Zugriff verhindert.

|  |  |  |  |
| --- | --- | --- | --- |
| Prozess / Datei | Wer ist befugt? | Zugriffsart | Sicherheitsmassnahme |
| User Erstellen & Passwort setzen | Kunden der Software | rwm | Starkes Passwort & Änderung alle 4 Monate |
| Hochladen & Löschen von Dateien | Systemadmin | rwm | Starkes Passwort Änderung alle 4 Monate  & 2FA |
| Video / Bilder herunterladen | Kunden der Software | r | Kundenlogin Passwort |
|  | Systemadmin | r |  |
| Löschen von Usern | Systemadmin | rwm | Starkes Passwort Änderung alle 4 Monate  & 2FA |
| Übertragung von Bildern & Videos von NAS auf Cloud | Automatisierter Prozess  (Manuell mit Admin möglich) | rw | Sichere Verbindung durch VPN-Tunnel |
| Zugriff auf eigene Fotos | Kunde der am Schiesstermin anwesend war | r | Fotos / Videos an Nutzer anhängen, damit fremde diese nicht ohne Befugnis ansehen können. |

Tabelle 6: Zugriffskontrolle

### Verantwortlichkeiten

Die nachfolgenden Verantwortlichkeiten sind gebunden an Personen:

**Projektleiter**: Umsetzung der Sicherheitsmassnahmen

**Benutzer**: Werden zur sicheren Passwortwahl und -verwendung aufgefordert. (AGB)

**Systemadmin**: Wartung, Patches, Monitoring & weiter Erhaltung der Sicherheitsmassnahmen

### Monitoring & Wartung

Damit die Sicherheit immer gewährt bleibt, werden folgende Massnahmen zur Überwachung geführt:

* Regelmäßige Protokollierung der Zugriffe auf den Server via Logs
* Automatische Warnung bei verdächtigen Login-Versuchen

### Backup

Das NAS speichert die Daten über die Synology-Software Hyper-Backup täglich auf eine zweite Festplatte, so dass jederzeit ein gültiges Backup vorhanden ist. User selbst können ihre Bilder nicht löschen, und selbst bei einem Festplattenausfall können wir so sichergehen, dass wir alles nochmals gespeichert haben.

## Anforderungszuordnung

Diese Tabelle bietet eine klare Übersicht von unseren Anforderungen an das Projekt, welche durch Tests anschliessend auf Funktionalität überprüft werden.

|  |  |  |
| --- | --- | --- |
| AFo.-Nr. | Anforderung (Stichwort) | Kritikalität |
| 1 | Funktionierender Filetransfer | Hoch |
| 2 | Usermanagement von Nutzern | Hoch |
| 3 | VPN (Server <-> NAS) | Hoch |
| 4 | Automatisierter Fotoupload | Mittel |
| 5 | Gültiger & öffentlicher Website SSL | Hoch |

Tabelle 7 7: Anforderungszuordnung

### Funktionierender Filetransfer

Für uns bedeutet ein funktionierender Filetransfer, dass ein User ohne speziell auftretende Probleme seine freigegebenen Bilder herunterladen kann und die Dateien dabei nicht korupt werden. Das System muss dafür alle benötigten Ports freigegeben haben, eine saubere SFTP-Ablage haben und keine Einschränkungen in der Firewall haben, welche den Prozess behindern könnten.

### Usermanagement mit Benutzername und Passwort

Unsere User können sich auf unserem Webinterface mit ihrem Benutzernamen und Passwort einloggen, damit sie Zugriff auf ihre Fotos haben können. Dafür muss SFTPgo sauber auf unserem Server installiert und eingerichtet sein. Zudem muss unsere Firewall auch die entsprechenden Ports freigeschalten haben.

### VPN-Verbindung zwischen NAS und Webserver

Wir müssen eine saubere VPN-Verbindung zwischen unserem NAS und Webserver haben, damit diese über einen sicheren Tunnel miteinander kommunizieren und Daten austauschen können. Dafür muss auf NAS und Webserver Tailscale installiert sein.

### Automatischer Upload der Fotos von NAS auf Server (mit Möglichkeit dies manuell auch zu erledigen)

Damit ein automatischer Upload funktioniert, müssen Scripts via Cronjobs auf unserem NAS & Webserver eingerichtet sein. Die Verbindung & die Möglichkeit Bilder manuell hochzuladen selbst wird durch den vorherigen Punkt bereits abgedeckt.

### Website mit gültigem SSL welche öffentlich erreichbar ist

Unsere Website soll bei Besuch via HTTPS erreichbar und ein gültiges Zertifikat aufweisen. Dieses erhalten wir via der Installation von Caddy auf dem Webserver.

# Systemdokumentation

In diesem Teil der Dokumentation wird beschrieben, wie wir unser System aufgebaut haben.

## Konfigurations-Dokumentation

In diesem Teil der Dokumentation wird erläutert, was die wichtigsten Konfigurationen sind und die jeweiligen Dateien werden hier angehängt.

### SSHD-Config File

Nachfolgend ist unsere SSHD-Konfigurationsdatei angehängt:



Zudem ist sie hier noch in Schriftform aufgeführt:

# $OpenBSD: sshd\_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See

# sshd\_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd\_config shipped with

# OpenSSH is to specify options with their default value where

# possible, but leave them commented. Uncommented options override the

# default value.

Include /etc/ssh/sshd\_config.d/\*.conf

#Port 22

#AddressFamily any

#ListenAddress 0.0.0.0

#ListenAddress ::

#HostKey /etc/ssh/ssh\_host\_rsa\_key

#HostKey /etc/ssh/ssh\_host\_ecdsa\_key

#HostKey /etc/ssh/ssh\_host\_ed25519\_key

# Ciphers and keying

#RekeyLimit default none

# Logging

#SyslogFacility AUTH

#LogLevel INFO

# Authentication:

#LoginGraceTime 2m

PermitRootLogin no

#StrictModes yes

#MaxAuthTries 6

#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized\_keys2 to be disregarded by default in future.

#AuthorizedKeysFile .ssh/authorized\_keys .ssh/authorized\_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none

#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh\_known\_hosts

#HostbasedAuthentication no

# Change to yes if you don't trust ~/.ssh/known\_hosts for

# HostbasedAuthentication

#IgnoreUserKnownHosts no

# Don't read the user's ~/.rhosts and ~/.shosts files

#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!

PasswordAuthentication no

#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with

# some PAM modules and threads)

ChallengeResponseAuthentication no

# Kerberos options

#KerberosAuthentication no

#KerberosOrLocalPasswd yes

#KerberosTicketCleanup yes

#KerberosGetAFSToken no

# GSSAPI options

#GSSAPIAuthentication no

#GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,

# and session processing. If this is enabled, PAM authentication will

# be allowed through the ChallengeResponseAuthentication and

# PasswordAuthentication. Depending on your PAM configuration,

# PAM authentication via ChallengeResponseAuthentication may bypass

# the setting of "PermitRootLogin without-password".

# If you just want the PAM account and session checks to run without

# PAM authentication, then enable this but set PasswordAuthentication

# and ChallengeResponseAuthentication to 'no'.

UsePAM yes

#AllowAgentForwarding yes

#AllowTcpForwarding yes

#GatewayPorts no

X11Forwarding yes

#X11DisplayOffset 10

#X11UseLocalhost yes

#PermitTTY yes

PrintMotd no

#PrintLastLog yes

#TCPKeepAlive yes

#PermitUserEnvironment no

#Compression delayed

#ClientAliveInterval 0

#ClientAliveCountMax 3

#UseDNS no

#PidFile /var/run/sshd.pid

#MaxStartups 10:30:100

#PermitTunnel no

#ChrootDirectory none

#VersionAddendum none

# no default banner path

Banner /etc/banner

# Allow client to pass locale environment variables

AcceptEnv LANG LC\_\*

# override default of no subsystems

Subsystem sftp /usr/lib/openssh/sftp-server

# Example of overriding settings on a per-user basis

#Match User anoncvs

# X11Forwarding no

# AllowTcpForwarding no

# PermitTTY no

# ForceCommand cvs server

### Docker Config

Unser Docker-Container wurde mit folgenden Einstellungen gestartet:

docker run -d \

--name SFTPgo \

-p 8080:8080 \

-p 2022:2022 \

-v sftpgo-data:/var/lib/sftpgo \

-v /srv/pictures:/srv/pictures:rw \

drakkan/sftpgo:latest

### Caddy

Nachfolgend ist die Konfiguration unserer Caddy-Datei:

A black screen with white text

AI-generated content may be incorrect.

Abbildung 2: 2 Caddy

### Tailscale

Nachfolgend ist ein Auszug aus dem Tailscale-Admincenter, wo unser Webserver unter dem Namen «porygon2» eingetragen ist:

A screenshot of a computer

AI-generated content may be incorrect.

Abbildung 33: Tailscale

### Ordnerstruktur

Nachfolgend ist die Ordnerstruktur auf unserem Webserver aufgeführt:

A green numbers on a black background

AI-generated content may be incorrect.

Abbildung 44: Ordnerstruktur

Dazu noch die Ordnerstruktur auf dem NAS:  
A screenshot of a computer

AI-generated content may be incorrect.

Abbildung 55: Ordnerstruktur -> NAS

### DNS-Config

Nachfolgend ist die Konfiguration unseres Hetzner DNS:

A screenshot of a record management

AI-generated content may be incorrect.

Abbildung 66: DNS-Config

Als Hinweis: Die Einträge für die Root-Adresse sind nicht für dieses Projekt relevant. Diese werden für die Zone aufgeführt, da ein separater Webserver darauf läuft.

### Firewall Config

Nachfolgend ist die Konfiguration unserer Hetzner Firewall:

A screenshot of a computer

AI-generated content may be incorrect.

Abbildung 77: Firewall-Config

## Benutzerhandbuch

In diesem Teil werden wir kurz erklären, wie das System aufgebaut ist.

### Systemübersicht

Nachfolgend ist eine kurze Systemübersicht.

#### Ziele und Hauptfunktionen des Systems

Bereitstellung einer sicheren Plattform für autorisierte Benutzer zum Austausch und Zugriff auf Fotos per SFTP und Web-GUI.

Integration in bestehende Infrastruktur für automatisierte oder manuelle Nutzung der bereitgestellten Dateien.

### Anwenderfunktionalität

#### Aufgabe

Austausch von Fotos durch Upload/Download via SFTP oder Web-GUI.

#### Instruktion zu Anwendung und Betrieb

SFTP: Verbindung über SFTP-Client → Login → Dateitransfer.

Web-GUI: Zugriff via HTTPS → Login → Dateiverwaltung im Browser.

#### Initialisierung

Benutzeranlage durch Admin.

Vergabe von Verzeichnis und Rechten.

Übergabe der Zugangsdaten an Benutzer.

#### Durchführung

Ausführungsoptionen: SFTP oder Web-GUI.

Benutzer-Eingabe: Login-Daten, Dateiaktionen.

Ausführung: Dateitransfer.

Erwartete Ausgabe: Erfolgreiche Dateiübertragung.

Beziehung zu anderen Funktionen: NAS-Zugriff via Tailscale.

#### Terminierung

Beenden der Verbindung im Client oder Browser.

#### Wiederanlauf («Restart»)

Neuverbindung jederzeit möglich.

Bei Systemneustart: Container + Dienste automatisch startbar.

## Supporthandbuch

Nachfolgend wird kurz erklärt, wie man bei verschiedenen Supportfällen vorgehen sollte.

### Massnahmen bei Benutzerproblemen

Nachfolgend sind beispielhaft Probleme aufgeführt:

**Passwort vergessen**

➜ Vorgehen:

Über die Admin-Oberfläche ein neues Passwort setzen (mit dem Hacken, dass der User dies beim nächsten Neustart ändern muss) und dem Benutzer mitteilen.

**Probleme beim Hochladen/Herunterladen von Dateien**

➜ Vorgehen:

Verzeichnisberechtigungen prüfen (Lesen/Schreiben)

Netzwerkverbindung des Benutzers prüfen

**Kein Zugriff trotz korrekter Anmeldedaten**

➜ Vorgehen:

Benutzerstatus prüfen (aktiv/deaktiviert)

Verzeichniszuweisung prüfen

### Massnahmen bei technischen Problemen

SFTPgo Container nicht erreichbar

➜ Vorgehen:

Container-Status prüfen:

docker ps -a | grep sftpgo

Container neu starten:

docker restart 3192d373d403

Netzwerkprobleme zwischen Webserver und NAS (Tailscale)

➜ Vorgehen:

Tailscale-Verbindung prüfen:

tailscale status

Prüfen ob NAS über Tailscale-IP erreichbar:

ping ohsubame

Falls keine Verbindung: Tailscale auf beiden Geräten neustarten:

sudo tailscale down && sudo tailscale up

Port von SFTPgo nicht erreichbar (z.B. Web GUI oder SFTP-Port)

➜ Vorgehen:

Docker Port Mapping prüfen:

docker inspect 3192d373d403 | grep HostPort

### Anhang zum Supporthandbuch

Falls einer der Dienste fehlschlägt, sind nachfolgend alle Dokumentationen hinterlegt.

SFTPgo Dokumentation: https://docs.sftpgo.com/2.6/

Tailscale Dokumentation: https://tailscale.com/kb/

Docker Dokumentation: https://docs.docker.com

Cron Dokumentation: https://man7.org/linux/man-pages/man5/crontab.5.html  
 https://man7.org/linux/man-pages/man1/crontab.1.html

Caddy Dokumentation: https://caddyserver.com/docs

# Systemtest

In diesem Abschnitt werden die Systemtests geschildert, ihre Anforderungen und weitere Netzwerkspezifische Aspekte.

## Testspezifikation

Die Testspezifikationen werden aufgeteilt unter der Kritikalität der Funktionseinheit.

In diesem Abschnitt werden Testauswirkungen und ihre Wichtigkeit geschildert.

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Funktionseinheit | Kritikalität | Beschreibung |
| FE01/ US1 | SHH-Zugang Webserver | Hoch | Zugang ist notwendig für die Einrichtung, Wartung und Sicherheit. |
| FE02 / US2 | Tailsacle-Verbindung NAS-Web | Hoch | Grundlage für sichere Datenübertragung zwischen NAS und Webserver. |
| FE03 / US3 | Caddy mit SSL | Hoch | SSL-Verschlüsselung für öffentliche und sichere Erreichbarkeit der Plattform. |
| FE04 / US4 | SFTPgo & Usermanagement | Hoch | Benutzer können Bilder nur über diese Schnittstelle runterladen. Berechtigung und Zugriffsrechte müssen richtig gesetzt sein. |
| FE05 / US5 | Traefik Reverse Proxy | Mittel | Wurde durch Caddy für seine Funktion ersetzt. |
| FE06 / US6 | Cronjobs für Bild-Upload | Mittel | Automatisierung ist sehr nützlich, manuelle Alternative wäre aber möglich. |
| FE07 / US7 NEU | Portsicherheit | Hoch | Überprüfung auf unnötig geöffnete Ports im Netzwerk und dessen Zugang. |

Tabelle 88: Kritikalität der Funktionseinheit

## Testanforderungen

Die Tests orientieren sich an den im Konzeptbericht dokumentierten User Storys (US1–US6) sowie an der Kritikalität der jeweiligen Funktionseinheiten Ziel ist es, die Stabilität, Sicherheit und Funktionalität der Webplattform umfassend zu überprüfen.

**Folgende allgemeine Anforderungen gelten für alle durchzuführenden Tests:**

### Tests unter Normalbedingungen:

* Standardabläufe wie Login via SSH (US1), Zugriff auf die Website (US3) oder Bild-Upload (US6) mit gültigen Benutzerdaten, stabiler Verbindung und erwartbaren Dateigrössen.

### Tests mit Grenzwerten:

* Upload von grossen Bilddateien, viele gleichzeitige Benutzerzugriffe oder maximale Anzahl an User-Accounts (US4, US6).

### Tests unter Ausnahmebedingungen:

* Unterbruch der Tailscale-Verbindung (US2)
* Ausfall des NAS während eines Uploads
* Ungültige oder abgelaufene SSH-Keys beim Login (US1)
* Zugriff mit falschen Rechten (User vs. Admin)

### Sicherheitstests:

* Zugriffsschutz durch Keypair-Login (US1), HTTPS-Verschlüsselung über Caddy (US3), und Zugriffskontrolle über SFTPgo (US4) werden gezielt getestet.

### Rollentests:

* Alle Kernfunktionen werden sowohl mit Admin- als auch mit Standardbenutzerrechten getestet, um sicherzustellen, dass Berechtigungen korrekt greifen.

Die Ergebnisse dieser Anforderungen fliessen direkt in die folgenden Kapitel zu Testfällen, Testdurchführung und Testauswertung ein.

## Testverfahren

Testdurchführungen werden immer anhand von diesen folgenden Schritten ausgeführt um auf ihre Integrität rückfolgend zugreifen zu können.

### Vorbereitung

Die Vorbereitung eines Tests umfasst:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Szenario  Nr. | Art | Vorbereitungsart | Bewirkung | Erhofftes Ergebnis |
| 1 | Verbindungsaufbau | Stabile Verbindung ins öffentliche Netz | Funktioneller Zugang auf Dateien & Administration | Fehlerfreie Verbindung ohne Error Code |
| 2 | Fileübertragung | Erstellen von Testdaten mit «randomfiles» | Kein Datenverlust, wenn die Testdaten verloren gehen. | Integrität der Daten bleibt vorhanden. |

Tabelle 99: Testverfahren -> Vorbereitung

### Durchführung

Die Testdurchführung basiert auf das Szenario gegeben im vorherigen Abschnitt und stimmt mit der Szenario NR. überein.

|  |  |  |  |
| --- | --- | --- | --- |
| Szenario  Nr. | Art | Durchführungsart | Erhofftes Ergebnis |
| 1 | Verbindungsaufbau | Verbindung über gegebene Protokolle | Erfolgreicher Verbindungsaufbau |
| 2 | Fileübertragung | Erstellen von Testdaten mit «randomfiles» | Integrität der Daten bleibt vorhanden. |

Tabelle 1010: Testverfahren -> Durchführung

### Auswertung

Die Auswertung der Test-Szenarien beruht auf der Art des Szenarios gegeben unter der Nummer unter der Vorbereitung & ebenfalls des Kriteriums welches ausschlaggebend ist ob der Test gelungen ist.

|  |  |  |
| --- | --- | --- |
| Szenario  Nr. | Art | Erhofftes Ergebnis |
| 1 | Verbindungsaufbau | Erfolgreiche Verbindung ohne Timeouts |
| 2 | Fileübertragung | Integrität der Daten bleibt vorhanden. |

Tabelle 1111: Testverfahren -> Auswertung

### Testkriterien

Die Testkriterien werden nummeriert abgegeben, damit diese in der Auswertung beiliegend ausgegeben werden können, um die Übersichtlichkeit stets zu behalten.

Auch wird festgelegt welcher Abdeckungsgrad genutzt wird & anhand von Checklisten geprüft ob diese Kriterien erfüllt sind.

#### Abdeckungsgrad

Es wird festgelegt, wie breit zu testen ist, um die Tauglichkeit des Testobjekts sicherzustellen

|  |  |  |
| --- | --- | --- |
| Abdeckung Nr. | Breitegrad | Abgrenzung |
| 1 | Hoch | Vollständige Übernahme der Kontrolle des Prozesses |
| 2 | Tief | Ab Benutzer wird nicht mehr überprüft |

Tabelle 1212: Testverfahren -> Testkriterien

#### Checkliste:

Hier wird auf die für den Test nötigen Checklisten hingewiesen.

|  |  |  |
| --- | --- | --- |
| Check Nr. | Deklarierung | Bsp. |
| 1 | Systemebene der inneren Betriebe des Prozesses werden auf Anfälligkeiten geprüft. | Interne Netzübertragung zwischen NAS & Webserver wird überwacht. |
| 2 | Protokoll- / Netzebene wird überprüft zwischen User und End Point. | Netzwerkprobleme beim Forwarding werden beispielsweise auf Firewall überprüft. |
| 3 | Allfällige User-Probleme werden aufmerksam aufgezeigt. | Enduser Funktionen werden getestet über das Webportal |

Tabelle 1313: Testverfahren -> Checkliste

### Testfälle

Folgende Testfälle werden mit ihren messbaren Zielen werden gestellt um anschliessend ihre Funktionstüchtigkeit zu testen

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test | ID | Szenario  Nr. | Ausgangslage | Check  Nr. | erwartetes Ergebnis | Bemerkungen, Prüfergebnis |
| 1 | FE01/ US1 | 1 | Admin möchte von Heimnetz über SSH-Verbindung zum Webadmin aufstellen mit seinen SSH-Keys | 2,3 | Keine Passwortabfrage | Erfolgreiche Verbindung über SSH ohne Timeout & PW-Abfrage |
| 2 | FE02 / US2 | 1 | Tailsacle-Verbindung NAS-Web wird für Automatisierung aufgebaut | 2 | VPN-Tunnel läuft verschlüsselt über Wireguard | Erfolgreich korret erstellte VPN-Verbindung |
| 3 | FE03 / US3 | 1 | SSL-Zertifikat wird erstellt. | 2 | Verschlüsselte Verbindung über HTTPS auf den Webservice ist möglich. | HTTPS Verbindung sicher aufgestellt. |
| 4 | FE04 / US4 | 2 | SFTPgo & Usermanagement sind bereit zum Einteilen der Berechtigungen | 3 | User & Gruppen haben jegliche nötige Zugriffe | User haben ihre Berechtigungen. |
| 6 | FE06 / US6 | 2 | Cronjobs für Bildupload sind erstellt für die automatische Ausführung der Übertragungs-Scripts | 3 | Tägliche 1:1  Synchronisation von NAS & Webserver | Fotos sind erreichbar und können von Usern heruntergeladen werden. |
| 7 | FE07 / US7 | 1 | Ungenutzte Ports sind geschlossen und werden mit Nmap vom öffentlichen Netz aus gescannt | 2 | Keine offenen Angriffsflächen | Durch erfolgreichen Nmap-Scan werden unnütz offene Ports ausgeschlossen. |

Tabelle 1414: Testfälle

## Testprozedur

In diesem Kapitel werden alle Testprozeduren aufgezeichnet und definiert.

### Vorbereitung

Die Vorbereitungen für die Tests benötigen je nach Testfall andere Ausgangslagen. Demnach haben wir für jede Situation eine Geschildert um diese möglichst genau und messbar zu machen.

|  |  |  |
| --- | --- | --- |
| Test | ID | Erforderlicher Ausgangszustand |
| 1 | FE01/ US1 | -SSH-Key auf dem Client wurde erstellt  -Der öffentliche Schlüssel ist auf dem Webserver im authorized keys-Verzeichnis |
| 2 | FE02 / US2 | -Tailscale ist auf dem NAS und dem Webserver installiert  -NAS und Webserver sind im gleichen Tailscale-Netz eingebunden |
| 3 | FE03 / US3 | -Caddy wurde korrekt installiert und konfiguriert  -Domain zeigt auf den Webserver |
| 4 | FE04 / US4 | -SFTPgo ist eingerichtet  -Benutzerkonten mit Berechtigungen wurden erstellt  -Ports wurden auf der Firewall geöffnet |
| 6 | FE06 / US6 | -Das Upload-Script wurde erstellt  -Cronjob für den periodischen Upload ist konfiguriert und aktiviert. |
| 7 | FE07 / US7 | -Nmap ist installiert auf einem externen Client  -Netzwerkzugang zum Webserver ist vorhanden |

Tabelle 1515: Vorbereitung

### Voraussetzungen:

Die Voraussetzungen für jeden Test beruhen darauf, dass der jeweilige Task ohne jeweilige zusätzliche eingriffe stattfinden kann und somit auch ohne Troubleshooting. Ansonsten wird der Test als «nicht bestanden» gelten.

### Konfiguration:

Zum Ausführen aller Tests ausser «FE07/US7» wird schlicht abgewartet, bis die Automation einschlägt. Denn diese sind aneinandergereiht, welches ein Logfile an den Webserver abgeben würde bei einem Fehler in der Funktionskette.

Zur Ausführung von Test FE07/US7 wird jedoch eine zusätzliche Open-Source Software benötigt, die die Ports auf offene Stellen scannen kann. In unserem Fall nutzen wir dafür NMAP.

### Durchführungen

**Durchführung Testfall 1 – SSH-Zugang Webserver (FE01 / US1)**

1. Terminal öffnen auf dem Client Gerät (Windows: Powershell / Linux: Terminal)

2. Prüfen, ob der SSH-Key vorhanden ist unter folgendem Pfad: C:\Users\Benutzername\.ssh\id\_rsa

3. Verbindung aufbauen mit zum Beispiel:   
 *ssh yanis@195.201.144.21 -i C:\Benutzer\<lokal User>\.ssh\id\_rsa*

4. Fingerprint mit “*Yes*” bestätigen

5. Schauen, ob: Keine Passworteingabe erscheint / Verbindung aufgebaut wird / kein Timeout entsteht

6. Nach dem Login sicherstellen, dass verschiedene Admin-Befehle ausgeführt werden können

**Durchführung Testfall 2 – Tailscale-Verbindung NAS-Webserver (FE02 / US2)**

1. Auf dem NAS und Webserver werden folgender Befehl ausgeführt: *Tailscale status* à Beide Geräte müssen online sein und im gleichen Tailscale-Netzwerk angezeigt werden

2. Jeweilige IP-Adressen von Tailscale vergleichen à müssen übereinstimmen

3. Einen Ping ausführen vom NAS zum Webserver: *ping <Tailscale-IP-Webserver>*  
 à Zu erwarten sind erfolgreich durchgekommene Antwortpakete, ohne Verlust

4. Einen Ping ausführen vom Webserver zum NAS: *ping <Tailscale-IP-NAS>*  
 à Zu erwarten sind erfolgreich durchgekommene Antwortpakete, ohne Verlust

5. Ein File über VPN transferieren: scp testbild.jpg *<User>@>tailscale-IP-Webserver>:/tmp/*

6. Check, ob die VPN während allen Tests stabil und ohne Timeouts oder Verbindungsausfällen bleibt

**Durchführung Testfall 3 – Caddy mit SSL (FE03 / US3)**

1. Auf dem Webserver wird folgender Befehl ausgeführt: *systemctl status caddy*  
 à Somit wird geprüft, ob der Dienst aktiv ist

2. Nun prüfen wir die Domain, indem wir diese im Browser aufrufen

3. Im Browser klicken wir auf das Schloss-Symbol und dann auf Zertifikat anzeigen  
 à Somit prüfen wir, ob ein gültiges «Let’s Encrypt Zertifikat» vorhanden ist

4. Wir stellen sicher, dass keine Zertifikatswarnung erscheint und das die Seite vollständig über HTTPS lädt

5. Die Seite soll ohne Redirect-Fehler aufrufbar sein und ohne Störungen laden

**Durchführung Testfall 4 – SFTPgo & Usermanagement (FE04 / US4)**

1. Das Webinterface von SFTPgo wird im Browser aufgerufen

2. Mit den Zugangsdaten können wir uns als Admin-Benutzer authentifizieren.

3. Im Admin-Panel kann ein Testuser erstellt werden, dieser bekommt Berechtigungen um auf ein definiertes   
 Verzeichnis zugreifen zu können.

**Durchführung Testfall 6 – Cronjobs zur Automatisierung der Synchronisation von NAS & Webserver**

1. Bilder werden aufs NAS geladen

2. Warten, bis die Automation einschreitet

3. Auf Webserver Nachsehen ob die Verzeichnisse synchron sind und alle Dateien 1:1 übertragen wurden.

**Durchführung Testfall 7 - Ports auf offene Stellen scannen**

1. «NMAP» Einrichten auf Standartkonfiguration

2. Im Feld «Target» fotos.david-ammann.ch eingeben & Scan Starten

3. Auf das Feld Hosts/Ports navigieren, dort stehen alle offenen Ports, welche über das öffentliche Netz erreichbar sind.

### Nachbearbeitung

Damit die Auswertung auf sauberer Basis stattfinden kann, müssen folgende Kriterien in jedem Test eingehalten werden.

1. Die automatisierten Teile der Umgebung müssen ohne Intervention ausgeführt werden, demnach müssen die Taks ohne menschliche Hilfe gestartet und beendet werden.
2. Manuelle Ausführungen wie die Verbindung per ssh müssen jedes Mal gelingen ohne Fehlermeldungen / Timeouts.

## Testprotokoll

In diesem Abschnitt werden die Testreihen durchgeführt, datiert & Ausgerwertet.

### Testobjekt

Nachfolgend sind die Testobjekte aufgeführt:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test | ID | Testobjekt | Tester | Ort | Datum | Zeit |
| 1 | FE01/ US1 | Webserver | David Ammann | Bern | 01.06.2025 | 17:00-17:45 |
| 2 | FE02 / US2 | NAS | David Ammann | Bern | 01.06.2025 | 16:00-16:45 |
| 3 | FE03 / US3 | Caddy Server v2.8.4 | David Ammann | Bern | 02.06.2025 | 16:00-16:45 |
| 4 | FE04 / US4 | SFTPgo v2.5.6 | Vladan Vranjes | Bern | 02.06.2025 | 17:00-17:45 |
| 6 | FE06 / US6 | Cronjob / Upload-Script | David Ammann | Bern | 02.06.2025 | 18:00-18:45 |
| 7 | FE07 / US7 | Portscan (Nmap v7.94) | Vladan Vranjes | Bern | 30.05.2025 | 15:00-15:45 |

Tabelle 1616: Testobjekte

### Testresultate

Nachfolgend sind unsere Testresultate aufgeführt.

Folgend kann man hier die Testresultate dokumentiert mit Bildausschnitten mitansehen:

#### Webserver Test

Webserver ist über das Internet erreichbar & mit Login kommt man rein:

Ein Bild, das Software, Multimedia-Software, Grafiksoftware, Computersymbol enthält.

KI-generierte Inhalte können fehlerhaft sein.

Abbildung 88: Testresultat -> Webserver

#### NAS & Tailscale

Webserver kann sich über Tailscale mit dem NAS erfolgreichper SSH verbinden:.

A screenshot of a computer

AI-generated content may be incorrect.

Abbildung 99: Testresultat -> NAS & Tailscale

A screen shot of a computer

AI-generated content may be incorrect.

#### Caddy

Gültige SSL wurde erkannt mit NMAP-Scan:



Abbildung 1010: Testresultat -> Caddy\_1



Abbildung 1111: Testresultat -> Caddy\_2

#### SFTPgo

Webportal Läuft und ist erreichbar mit gültiger SSL

Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

KI-generierte Inhalte können fehlerhaft sein.

Abbildung 1212: Testresultat -> SFTPgo

#### Cronjobs

Die Cronjob wurde erstellt damit es das Übertragungs-Script auslösen sollte

Diese haben im Test dies erfolgreich erledigt

Ein Bild, das Text, Screenshot, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

KI-generierte Inhalte können fehlerhaft sein.

Abbildung 1313: Testresultat -> Cronjobs\_1 Abbildung 14: Testresultat -> Cronjobs\_2

#### NMAP-Portscan

Unser Ziel war es so wenig Ports wie möglich offen zu lassen und somit nur diese Freizulassen welche für den Betrieb notwendig sind welche sind: 22, 80, 443, 2022

**Das Testergebnis aus dem NMAP-Scan ergibt dabei:**

Ein Bild, das Text, Screenshot, Software, Display enthält.

KI-generierte Inhalte können fehlerhaft sein.

Abbildung 1415: Testresultat -> NMAP-Portscan

# Weiterführung der Projektplanung

## Abgleich von Planung und tatsächlichem Verlauf der Phase Konzept

Grundlegend ist die Zeitplanung auf den Punkt eingeschätzt worden, jedoch mussten wir etwas mehr zeit beim Troubleshooting investieren damit die Automatische Übertragung von NAS à Webserver ohne jeglichen Eingriff erfolgen konnte.

Die Risiken wurden hervorragend gemeistert und die Sicherheit unseres Konstrukts wird mit Portschliessung von unnötigen offenen Stellen sowie auch 2FA komplett abgeriegelt, sodass die Daten ohne Erlaubnis nicht zugänglich sind.

Eine Abänderung der Planung wurde in einem Punkt jedoch hervorgenommen im Bereich vom Reverse-Proxy. Geplant war diese mit Traefik umzusetzen, aber da im Konzept Caddy bereits für das SSL verwendet wird und dieses auch den Reverse-Proxy übernehmen kann, haben wir dieses umgestellt.

Das wird aus dem Grund übernommen, da weniger Abhängigkeiten von Programmen weniger Errors verursachen können und auch mehr Übersicht verschaffen.

## Aktualisierung der Risikosituation

Die Risiken haben sich seit der Konzeptphase nicht verändert und jegliche genannten Risiken werden gleich wie zuvor behandelt.

## Planung der nächsten Phase

Für die Übernahme des Webservices werden weitere Betriebs- & Handhabungsanleitungen erstellt, damit nach der Übernahme die Entwickler keine weiteren Eingriffe übernehmen müssen.