Konzeptbericht

|  |  |
| --- | --- |
| **Status** | Absgeschlossen |
| **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 |
| 0.1 | 12.03.25 | Erstellung des Dokuments | Alle Mitglieder |
| 0.2 | 19.03.25 | Systemanforderungen | Alle Mitglieder |
| 0.2 | 26.03.25 | Ausbau ISDS & Testkonzept | Yanis, Luan, David |
| 0.3 | 23.04.25 | Verbesserungen | Alle Mitglieder |

**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**

[Konzeptbericht 1](#_Toc196344799)

[Zusammenfassung 4](#_Toc196344800)

[Systemanforderungen 5](#_Toc196344801)

[Anforderungen an die Funktionalität 5](#_Toc196344802)

[Funktionierender Filetransfer 5](#_Toc196344803)

[Usermanagement mit Benutzername und Passwort 5](#_Toc196344804)

[VPN-Verbindung zwischen NAS und Webserver 5](#_Toc196344805)

[Automatischer Upload der Fotos von NAS auf Server (mit Möglichkeit dies manuell auch zu erledigen) 5](#_Toc196344806)

[Website mit gültigem SSL welche öffentlich erreichbar ist 5](#_Toc196344807)

[Systemadministration 6](#_Toc196344808)

[Anforderungen an die Informationssicherheit und Datenschutz 6](#_Toc196344809)

[Systemarchitektur 7](#_Toc196344810)

[Gliederung der Lösung in Module 7](#_Toc196344811)

[Subsystem 1: NAS 7](#_Toc196344812)

[Subsystem 2: Webserver 7](#_Toc196344813)

[Schnittstellen 8](#_Toc196344814)

[Externe Schnittstellen 8](#_Toc196344815)

[Interne Schnittstellen 9](#_Toc196344816)

[Bildliche Darstellung der Architektur 9](#_Toc196344817)

[Konzeption für Informationssicherheit und Datenschutz (ISDS) 10](#_Toc196344818)

[Schutzbedarfsanalyse 10](#_Toc196344819)

[Privacy by design 10](#_Toc196344820)

[Risikoanalyse 10](#_Toc196344821)

[Sicherheitsmassnahmen 11](#_Toc196344822)

[Zugriffskontrolle 11](#_Toc196344823)

[Verantwortlichkeiten 12](#_Toc196344824)

[Monitoring & Wartung 12](#_Toc196344825)

[Backup 12](#_Toc196344826)

[Testkonzept 13](#_Toc196344827)

[Login über SSH 14](#_Toc196344828)

[Tailscale-Verbindung zwischen NAS und Webserver testen 14](#_Toc196344829)

[Caddy Installation 14](#_Toc196344830)

[SFTPgo Installation 15](#_Toc196344831)

[Traefik Installation 15](#_Toc196344832)

[Cronjobs für automatischen Bilderupload 15](#_Toc196344833)

[Projektplanung 17](#_Toc196344834)

[Risikoauswertung 18](#_Toc196344835)

**Abbildungsverzeichnis**

[Abbildung 1: Verbindungsweg 8](#_Toc196344252)

[Abbildung 2: Ausschnitt aus dem Projektplan 15](#_Toc196344253)

**Tabellenverzeichnis**

[Tabelle 1: Systemadministration -> Aufgaben 5](#_Toc196344473)

[Tabelle 2: Subsystem 1 - NAS 6](#_Toc196344474)

[Tabelle 3: Subsystem 2 - Webserver 6](#_Toc196344475)

[Tabelle 4: Externe Schnittstellen 7](#_Toc196344476)

[Tabelle 5: Interne Schnittstellen 8](#_Toc196344477)

[Tabelle 6: Risikoanalyse 9](#_Toc196344478)

[Tabelle 7: Zugriffskontrolle 10](#_Toc196344479)

[Tabelle 8: Testkonzept Usecases 12](#_Toc196344480)

[Tabelle 9: Erster Usecase 13](#_Toc196344481)

[Tabelle 10: Zweiter Usecase 13](#_Toc196344482)

[Tabelle 11: Dritter Usecase 14](#_Toc196344483)

[Tabelle 12: Vierter Usecase 14](#_Toc196344484)

[Tabelle 13: Fünfter Usecase 14](#_Toc196344485)

[Tabelle 14: Sechster Usecase 15](#_Toc196344486)

# 

# Zusammenfassung

Dieses Dokument bezieht sich auf die Konzeption und Umsetzung einer Webplattform zur Freigabe von Fotos, welche auf einem NAS-System hinterlegt sind. Das Ziel des Projektes ist es eine funktionsfähige und benutzerfreundliche Lösung zu entwickeln und umzusetzen, die einen Zugriff auf die gespeicherten Medien ermöglicht.

Folgend sind die wichtigsten Erkenntnisse pro Kapitel aufgeschrieben:

**Systemanforderungen**

* Funktionierender Filetransfer
* Usermanagement mit Benutzername und Passwort
* VPN-Verbindung zwischen NAS und Webserver
* Automatischer Upload der Fotos von NAS auf Server (mit Möglichkeit dies manuell auch zu erledigen)
* Website mit gültigem SSL welche öffentlich erreichbar ist

**Systemarchitektur**

Netzwerkplan zwischen NAS, Webserver, und Anbindung an World Wide Web mit Demonstration in Modulen und Schnittstellen.

**Konzeption für Informationssicherheit und Datenschutz**

Beschreibung, wie wir unser Projekt mit Datenschutz und Datensicherheit im Hinterkopf konzipiert haben, und dies planen umzusetzen.

**Qualitätssicherung**

Testfälle und Abnahmeprotokoll.

**Projektplanung**

Verweis auf das Dokument der Projektplanung.

# Systemanforderungen

Im folgenden Kapitel werden wir alles Systemanforderungen beschreiben und ausführlich beschreiben.

## Anforderungen an die Funktionalität

Kurz zusammengefasst sind unsere Anforderungen folgende:

* Funktionierender Filetransfer
* Usermanagement mit Benutzername und Passwort
* VPN-Verbindung zwischen NAS und Webserver
* Automatischer Upload der Fotos von NAS auf Server (mit Möglichkeit dies manuell auch zu erledigen)
* Website mit gültigem SSL welche öffentlich erreichbar ist

Anschliessend werden alle Ziele im Detail beschrieben, was dies genau für das System bedeutet und wie wir dies erreichen wollen.

### 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 die Installation von Caddy auf dem Webserver.

## Systemadministration

In folgendem Kapitel werden die wichtigsten Aufgaben des Systemadministrators beschrieben und wie diese durchgeführt werden können.

|  |  |
| --- | --- |
| *Aufgabe* | *Beschreibung der Ausführung* |
| *Neuen Benutzer erstellen* | 1. *Auf Webserver per SSH anmelden* 2. *Via SFTPgo User mit Username und Passwort erstellen* 3. *Verknüpfung auf korrespondierendem Ordner auf NAS erstellen* |
| *Manuell Fotos von NAS auf Webserver übertragen* | 1. *Auf NAS anmelden, Tailscale starten* 2. *Auf Webserver anmelden, Tailscale starten* 3. *Via Konsole auf entweder NAS oder Webserver Datenaustausch durchführen* |

Tabelle 1: Systemadministration -> Aufgaben

## Anforderungen an die Informationssicherheit und Datenschutz

Unser Projekt ist von Natur aus mit dem Prinzip «Privacy by Design» erstellt worden. Da wir mit Kundenfotos zu tun haben, welche in der Schweiz als besonders schützenswerte Daten deklariert sind, müssen wir dafür sorgen, dass jeder einzelne Datenaustausch so sicher wie möglich ist. Für dieses Projekt heisst das:

* Keine Möglichkeit, den Datentransfer zwischen NAS und Webserver abzufangen
* Keine Möglichkeit, ohne Benutzername und Passwort an die Fotos eines Kunden heranzukommen
* Kein möglicher Zugang (z.B. via SSH) auf Webserver / NAS ohne verschiedenste Voraussetzungen

Mit diesen Hauptpunkten sollte es möglich sein, dass die Daten der Kunden auf einem ansprechenden Niveau geschützt und gesichert sind.

# Systemarchitektur

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

|  |  |  |
| --- | --- | --- |
| 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 2: Subsystem 1 - NAS

### Subsystem 2: 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 3: Subsystem 2 - Webserver

## Schnittstellen

Im folgenden Kapitel werden alle unseren internen und externen Schnittstellen ausführlich beschrieben.

### 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 4: Externe Schnittstellen

### Interne Schnittstellen

Nachfolgend werden alle internen Schnittstellen aufgeführt.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Schnittstelle | Bezeichnung | Verbindungspartner | 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 5: 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.

Abbildung 1: Verbindungsweg

# Konzeption für Informationssicherheit und Datenschutz (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 6: 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 7: 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.

# Testkonzept

Folgend werden Userstorys definiert, die wir später beim Testen der Umgebung in der Realisierungsphase verwenden werden.

|  |  |  |
| --- | --- | --- |
| **Nr.** | **Abgedeckter Anwendungsfall oder User Stories** | **Beschreibung** |
| US1 | Login über SSH | Zugang des Webservers nur via gültigem Keypair einrichten. |
| US2 | Tailscale-Verbindung zwischen NAS und Webserver testen | Einrichten und Testen der Verbindung zwischen NAS und Webserver. |
| US3 | Caddy Installation | Erfolgreiche Caddy Installation; Website mit gültigem SSL erreichbar. |
| US4 | SFTPgo Installation | Erfolgreiche SFTPgo Installation; Erfolgreiches erstellen von Usern und dessen Zugriff auf ihre Fotos. |
| US5 | Traefik Installation | Erfolgreiche Installation von Traefik; Möglichkeit, gleichzeitig Website erreichbar zu halten und VPN-Verbindung zu erstellen |
| US6 | Cronjobs für automatischen Bilderupload | Verschiedenste Cronjobs auf NAS und Webserver eingerichtet, welche die Bilder 1x täglich von NAS auf Webserver synchronisieren. |

Tabelle 8: Testkonzept Usecases

## Login über SSH

|  |  |
| --- | --- |
| US1: User loggt sich mit gültigen SSH Key auf den Server ein. | |
| Kurzbeschreibung | Der Benutzer kann sich per gültigem SSH Key auf den Server erfolgreich anmelden. |
| Akteure | Benutzer |
| Vorbedingungen | -Der Benutzer verfügt über ein gültiges Login.  -Der Webserver ist erreichbar über sämtliche Browser. |
| Ablauf | 1. Der Benutzer findet per URL unser Webserver 2. Der Benutzer kann sich erfolgreich per SSH anmelden. |
| Erwartetes Resultat | Der Benutzer ist nun angemeldet und kann somit freigegebene Fotos einsehen und runterladen. |
| Resultat |  |

Tabelle 9: Erster Usecase

## Tailscale-Verbindung zwischen NAS und Webserver testen

|  |  |
| --- | --- |
| US2: Tailscale-Verbindung zwischen NAS und Webserver testen | |
| Kurzbeschreibung | Der Benutzer testet die fertig eingerichtete Tailscale-Verbindung, indem er vom Webserver auf das NAS zugreift. |
| Akteure | Benutzer oder Systemadministrator |
| Vorbedingungen | -Tailscale ist auf dem NAS und Webserver installiert  -Verbindung ist konfiguriert und aktiv |
| Ablauf | 1. Benutzer verbindet sich mit Tailscale  2. Er pingt das NAS über die Tailscale-IP  3. Greift auf eine Datei oder einen freigegebenen Ordner zu  4. Testet Lesezugriff |
| Erwartetes Resultat | Der Zugriff auf das NAS funktioniert und Dateien sind lesbar sowie übertragbar. |
| Resultat |  |

Tabelle 10: Zweiter Usecase

## Caddy Installation

|  |  |
| --- | --- |
| US3: User kann die Webseite über HTTPS erreichen, ein gültiges SSL-Zertifikat ist vorhanden. | |
| Kurzbeschreibung | Der Benutzer testet, ob die Webseite nach der Caddy-Installation über HTTPS erreichbar ist und ein gültiges SSL-Zertifikat verwendet. |
| Akteure | Benutzer |
| Vorbedingungen | -Caddy ist auf dem Webserver installiert  -Caddyfile ist korrekt konfiguriert  -DNS zeigt auf den Server  -Internetzugang ist vorhanden |
| Ablauf | 1. Benutzer öffnet die Webseite im Browser 2. Prüft, ob die Webseite über HTTPS läuft 3. Kontrolliert das SSL-Zertifikat (gültig und nicht selbstsigniert) 4. Testet allgemeine Funktionalität der Webseite |
| Erwartetes Resultat | Webseite ist über HTTPS erreichbar und verwendet ein gültiges SSL-Zertifikat. |
| Resultat |  |

Tabelle 11: Dritter Usecase

## SFTPgo Installation

|  |  |
| --- | --- |
| US4: Neue erstellte User haben Zugriff auf zugewiesene Fotos. | |
| Kurzbeschreibung | Neue User können erstellt werden und haben funktionierenden Zugriff auf ihre Fotos. |
| Akteure | Benutzer und Systemadministratoren |
| Vorbedingungen | -SFTPgo ist installiert und läuft  -Benutzerverwaltung ist möglich  -Speicherort für Fotos ist definiert und freigegeben |
| Ablauf | 1. Administrator erstellt einen neuen User in SFTPgo 2. Benutzer meldet sich mit seinen Zugangsdaten an 3. Administrator teilt dem Benutzer Zugriff auf ein Foto zu 4. Benutzer greift auf Testfoto zu |
| Erwartetes Resultat | Der Benutzer kann auf sich einloggen, Fotos herunterladen und hat nur Zugriff auf den freigegebenen Bereich. |
| Resultat |  |

Tabelle 12: Vierter Usecase

## Traefik Installation

|  |  |
| --- | --- |
| US5: HTTPS und VPN-Verbindung funktionieren parallel. | |
| Kurzbeschreibung | Nach der Installation von Traefik soll überprüft werden, ob die Webseite über HTTPS erreichbar ist und eine VPN-Verbindung parallel betrieben werden kann. |
| Akteure | Systemadministratoren und Benutzer |
| Vorbedingungen | -Traefik ist installiert und als Reverse Proxy konfiguriert  -DNS und SSL-Zertifikate sind eingerichtet  -Webseite und VPN-Dienste sind definiert und aktiv |
| Ablauf | 1. Administrator startet Traefik mit gültiger Konfiguration 2. Benutzer ruft die Webseite auf und prüft HTTPS-Zugriff 3. Zeitgleich wird eine VPN-Verbindung aufgebaut 4. Es wird getestet, ob beide Dienste ohne Konflikte laufen und funktionieren |
| Erwartetes Resultat | Webseite ist über HTTPS erreichbar und die VPN-Verbindung lässt sich gleichzeitig nutzen und aufbauen. |
| Resultat |  |

Tabelle 13: Fünfter Usecase

## Cronjobs für automatischen Bilderupload

|  |  |
| --- | --- |
| US6: Bilder werden täglich hochgeladen vom Nas auf den Webserver. | |
| Kurzbeschreibung | Es sollen Cronjobs eingerichtet werden, diese werden täglich automatisch Bilder vom NAS auf den Webserver synchronisieren. | |
| Akteure | Systemadministrator und Benutzer | |
| Vorbedingungen | -NAS und Webserver sind per Netzwerk verbunden  -SSH Zugriff oder entsprechender Sync-Dienst ist konfiguriert  -Schreibrechte auf dem Zielordner sind vorhanden | |
| Ablauf | 1. Cronjobs wird auf dem NAS eingerichtet 2. Optionaler Cronjob auf Webserver prüft Vollständigkeit 3. Testlauf durchführen und Logs prüfen | |
| Erwartetes Resultat | Die Bilder werden automatisch 1x täglich synchronisiert, somit ist kein manuelles Eingreifen erforderlich und sind direkt auf dem Webserver einsehbar. | |
| Resultat |  | |

Tabelle 14: Sechster Usecase

## Projektplanung

Nachfolgend ist unser Projektplan dargestellt. Link zum seperaten File wäre: [Zeitplan 300 306.xlsx](https://gibbch-my.sharepoint.com/:x:/r/personal/vvr140992_stud_gibb_ch/Documents/IET/Semester%206/Modul%20306/Zeitplan%20300%20306.xlsx?d=wa4b4e74e98b84a06a469a51250c48f0b&csf=1&web=1&e=JGexef)

A screenshot of a computer screen

AI-generated content may be incorrect.

Abbildung 2: Ausschnitt aus dem Projektplan

## Risikoauswertung

Es wurden zu den Risiken aus der Initialisierungsphase keine neuen Risiken hinzugefügt, jedoch wurden sie deutlicher erklärt was dagegen unternommen werden würde.

Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
Freihandzeichnungen
, Bild

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Der Projektleiter Vladan Vranjes

Bern, 23.04.2025