it.schule
stuttgart

# IT Schule Stuttgart Projekt Nr. 2

## Projekt Messe Auftritt


Durchführung:

**Holger Haack**
**Luis Scheurenbrand**
**Dennis Kreittner**

Lehrer:

**Hr. Serhan**


24.1.2024

# Abkürzungsverzeichnis

**PT** Packet Tracer

**IP** Internet Protokoll: Ein verbindungsloses Protokoll, dass die Adressierung von Computern und das Routing von Paketen ermöglicht.

**wr** Write memory: Ein wichtiger Befehl, bei der Konfiguration von Routern im Packet Tracer, genutzt damit Konfigurationen persistent sind.

**RADIUS** Remote Authentication Dial-In User Service: Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen in Netzwerke.

**AP** Access Point: Schnittstelle für kabellose Kommunikationsgeräte.

**LWAP** Light Weight Access Point: Schnittstelle für kabellose Kommunikationsgeräte.

**CIDR** Classless Inter-Domain Routing: Verfahren zur effizienten Nutzung von IP-Adress-Räumen unter Verwendung von Subnetzmasken.

**DHCP** Dynamic Host Configuration Protocol: Ein Verfahren um von einem Server aus Netzwerkkonfigurationen an Clients zuzuweisen.

**WPA2** Wi-Fi Protected Access 2: Sicherheitsstandard für Funknetze basierend auf AES.

**AES** Advanced Encryption Standard: Blockchiffre zur Verschlüsselung von Daten.

**ACL** Access Liste: Liste von zugelassenen und blockierten IP Adressen(-Bereichen).

**TCP** Transmission Control Protocol: Ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Layer 4 Netzwerk Protokoll.

**HTTPS** Hypertext Transfer Protocl Secure: Ein Kommunikationsprotokoll im World Wide Web, das eine Transportverschlüsselung darstellt.

**JSON** JavsScript Object Notation: Ein kompaktes Datenformat in einer einfach lesbaren Textform unabhängig von Programmiersprachen.

**SQL** Structured Query Language: Eine Abfragesprache um auf Daten in einer relationalen Datenbank zuzugreifen und diese zu verwalten.

**UI** User Interface: Englische Bezeichnung für Benutzeroberfläche.

**DTO** Data Transfer Object: Entwurfsmuster zur Bündelung von Daten, das dann zur Übertragung genutzt wird.

# Inhaltsverzeichnis

# 1 Einführung

Für den Messeauftritt Ihres Unternehmens am 24.1.2024 soll eine WLAN-Infrastruktur und eine Software zur Erfassung von Kundendaten bereitgestellt werden.

# 2 Anforderungsanalyse

Dieser Abschnitt befasst sich mit der Ausgangssituation die vor Ort vorliegt und den Anforderungen, die an die zu erstellenden Netzwerkkomponenten und Softwarelösungen gestellt werden.

## 2.1 Situationsbeschreibung

Die Firma XYZ plant den Besuch einer Messe. Auf der Messe sollen neben den üblichen Tätigkeiten nach Möglichkeit auch Daten potenzieller Neukunden erhoben und gespeichert werden. Zu diesem Zweck kann der Messestand Gutscheine ausstellen, mit denen vergünstigte Angebote auf der Messe wahrgenommen werden können. Voraussetzung ist die Registrierung im Portal der Firma XYZ.

### 2.1.1 Teilprojekt SAE: Datenerfassung Neukunden

Während des Messeauftritts sollen von Kunden im Self-Service Kundenkarten erstellt werden können, mit denen dann der Zugang zu weiteren Messeangeboten möglich wird. Dabei sollen Nachname, Vorname, Anschrift und ein Bild erfasst werden. Zusätzlich sollen ein oder mehrere Produktgruppen angegeben werden können, für die besonderes Interesse besteht. Bei Firmenvertretern soll zusätzlich ein Datensatz für die Firma angelegt werden. Die Speicherung der Daten soll langfristig in einer Datenbank erfolgen. Da die Zuverlässigkeit der Netzwerkverbindung während des Messeauftritts nicht immer sichergestellt werden kann, muss das Erfassungssystem auch offline funktionieren und in der Lage sein, die Daten auf Wunsch an die Firmenzentrale zu übermitteln. Die Übermittlung soll mit Hilfe einer REST-API an den Firmenserver erfolgen. Die gespeicherten Daten sollen von den MitarbeiterInnen auch abgerufen und durchsucht werden können. Da es sich um einen Self-Service handelt muss sichergestellt werden, dass nicht jede Person das System frei nutzen kann. Für die Erfassung des Fotos soll eine Webcam angebunden werden. Für die Erfassung der Daten sollen 4 firmeneigene Laptops zur Verfügung gestellt werden, die über WLAN an das Internet angebunden sind (siehe unten)
Folgende technische Rahmenbedingungen werden an die Softwarelösung gestellt:

- C# Applikation
- Rest API mit ASP.Net erstellen und konsumieren

- SQLite Datenbank
- Entity Framework Core
- Datenbankentwurf
- Prüfen: Design Pattern, Interface, Dependency Injection

### 2.1.2 Teilprojekt ITS: WLAN

Sie sollen für den Messeauftritt ein eigenes WLAN planen, da Sie nicht auf das dort verfügbare öffentliche WLAN zugreifen wollen. Zu diesem Zweck erhalten Sie vom Messeveranstalter einen internetfähigen Router mit der Auflage, nur Subnetze im Bereich 192.168.4.128/25 anzubieten. Das Netzwerk muss so aufgebaut sein, dass die im Teilprojekt SAE erfassten Daten bei Bedarf an die Firmenzentrale übermittelt werden können. Die insgesamt 16 firmeneigenen Endgeräte sollen über das WLAN angebunden werden. Die 4 für Kunden gedachten Laptops sollen sich in einem anderen Netz als die Geräte der Mitarbeiter befinden.
Folgende Anforderungen werden an die Netzwerkumsetzung gestellt:

- Subnetting
- Konfiguration WLAN
- Accesspoints
- Informieren: WLAN Controller, Radius, AAA-Server

# 3 Umsetzung Teilprojekt ITS

## 3.1 Netzwerkinfrastruktur Stand

### 3.1.1 Netzwerkaufbau

Zunächst wurde das Projekt mit dem Router 4331 und mit einem zusätzlichen Modul (NIM-ES2-4) gestartet, um den Router um 4 weitere Gigabit Ports erweitert, da jeweils ein AP einen Port belegt, der Radius Server einen Port belegt, und ein Port mit „dem Internet“ verbunden ist. Standardmäßig ist der Router allerdings nur mit zwei Gigabit Ports bestückt. Einen weiteren könnte man mit dem GLC-T Modul erweitern, dann wäre man aber nur bei 3 statt 4 Ports. Der Port, der „mit dem Internet“ verbunden ist, erhielt zusätzlich ein GLC-GE-100FX Modul, da man darüber über 2km Reichweite mit Glasfaser erreichen könnte, und das am ehesten der Realität entspricht. Dass mehr Ports benötigt werden, ist erst beim Aufbauen des Netzwerkes aufgefallen. Daher musste der Router einmal ausgeschaltet werden und mit den Modulen erweitert werden. Dabei hat sich der Befehl „wr“ bzw. „write memory“ als sehr wichtig herausgestellt, da andernfalls alle bisherigen Konfigurationen gelöscht werden, da sie flüchtig waren. Nachdem fast alle verkabelt war, außer der Radius Server, hat sich allerdings herausgestellt, dass das NIM-ES2-4 Modul nur auf Layer 2 arbeitet, also wie ein Switch. Es fehlte also ein Port für den Radius Server. Daher wurde der Router verworfen und es wurde ein PT-Empty mit 3x PT-ROUTER-NM-1CGE Modulen und einem PT-ROUTER-NM-1FGE Modul erweitert. Erstere werden verwendet, da die verwendeten AP nicht mit FastEthernet gearbeitet haben, und Letztere, um hohen Datentransfer zum Server zu gewährleisten. Vorteil: Der Router ist insgesamt günstiger als der ISR 4331, und er ist flexibel erweiterbar. Für diese Migration wurden die Konfigurations-Dateien der bisherigen Router exportiert, und in die neuen Router gemerged. Damit mussten die dhcp Konfigurationen nicht neu erstellt werden. Nachdem das Netzwerk soweit eingerichtet wurde, und es an die Konfiguration des RADIUS-Servers ging, hat sich herausgestellt, dass die im Vergleich zu den LWAPs günstigeren APs nicht direkt einen RADIUS-Server angeben können. Daher wurde ein PT-ROUTER-NM-1CGE und der RADIUS-Server als solcher entfernt, dass die Kosten abermals reduziert. Das fertige Projekt lässt sich Preis-Leistungstechnisch kaum weiter optimieren, da man trotz der geringen Gesamtkosten immer noch ein hohes Maß an sowohl Geschwindigkeit als auch Sicherheit erreicht. Näheres dazu unter dem Reiter WLAN, Zugang und Sicherheit. Im Folgenden die Tabelle für die Subnetze und die Netzwerkskizzen für das

Messe-Netzwerk und das Netzwerk in der Firmenzentrale:

| Netzwerk-Adresse | Subnetzmaske | Beschreibung |
|---|---|---|
| 192.168.4.128 | 255.255.255.224 | Dieses Netzwerk ist für die Firmengeräte auf der Messe gedacht. Es hat einen CIDR von /27, sodass alle 16 Geräte + Netzwerkadresse + Broadcastadresse in das Netz passen |
| 192.168.4.161 | 255.255.255.248 | Dieses Netzwerk ist für die Kunden-Geräte auf der Messe gedacht. Es hat einen CIDR von /29, sodass alle 4 Geräte + Netzwerkadresse + Broadcastadresse in das Netz passen |
| 142.250.183.0 | 255.255.255.0 | Dieses Netzwerk dient der Kommunikation zwischen dem Messe Router und dem Router der Firmenzentrale. Sie ist willkürlich gewählt, da sie normalerweise vom ISP vergeben wird, da das gleichzeitig auch die öffentliche IP-Adresse ist |
| 172.16.0.0 | 255.255.255.0 | Dieses Netzwerk soll das private Netzwerk innerhalb der Firmenzentrale darstellen. Da dieses nicht näher beschrieben wurde, wurde auch dieses willkürlich gewählt |

Tabelle 3.1: Netzwerke für das Subnetting

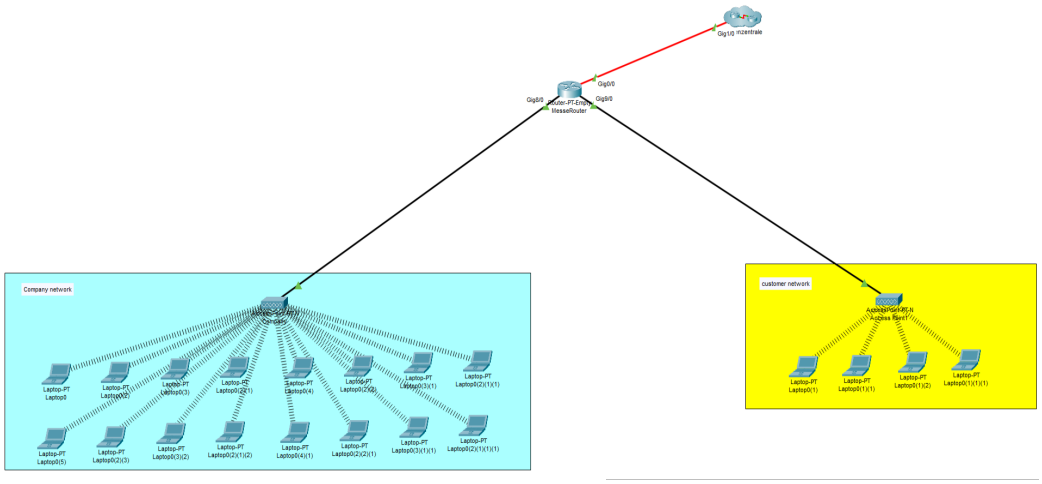


Abbildung 3.1: Netzwerkskizze Messe-Netzwerk

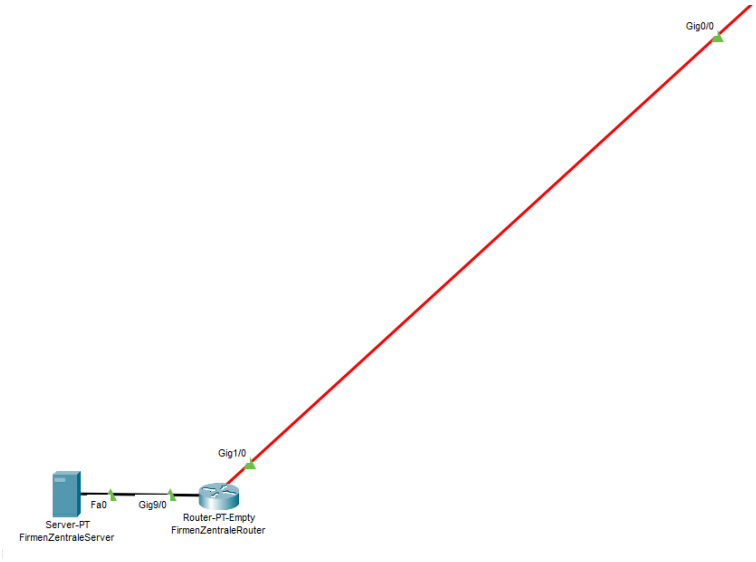


Abbildung 3.2: Netzwerkskizze Firmenzentrale-Netzwerk

### 3.1.2 Anbindung Messenetzwerk

#### Messe Router Interface Konfiguration

Das linke, untere Interface gig 8/0 befindet sich im company network, es ist also das größere Subnetz, da 16 Geräte benötigt werden. Die IP-Adresse lautet: 192.168.4.129 /27 (255.255.255.224). Die Subnetzmaske /28 konnte nicht verwendet werden, da neben den 16 Hosts auch eine Adresse für das Netzwerk und eine als Broadcastadresse verwendet wird. Das rechte, untere Interface gig 9/0 befindet sich im customers network für die Kunden-Geräte. Dessen IP-Adresse lautet: 192.168.4.161 /29 (255.255.255.248). Die nächstkleinere Subnetzmaske konnte aufgrund obiger Beschreibung ebenfalls nicht verwendet werden. Das obere Inter-

face gig 0/0, ist das Interface, das „ins Internet“ führt, und über das dann der Server in der Firmenzentrale erreicht werden soll. Seine IPv4 lautet: 142.250.183.14 /24 (generisch, da diese IP-Adresse normalerweise vom ISP bereitgestellt wird und es gemäß Aufgabenstellung keine weitere Einschränkung in Bezug auf diese Adresse gibt).

#### Firmenzentrale Router Interface Konfiguration

Der Port, der „aus dem Internet“ zugreifbar ist, ist Gig 1/0 zusammen mit einem PT-ROUTER-NM-1FGE Modul. Er hat die IPv4: 142.250.183.16 (generisch, da diese IP-Adresse normalerweise vom ISP bereitgestellt wird). Es wurde absichtlich eine Adresse innerhalb des gleichen Netzwerkes gewählt, da dies am ehesten der Simulation einer VPN-Verbindung entspricht. Aufgrund dieser Annahme, und da es sich nur um eine Simulation des Firmenservers handelt, wurde ansonsten keine weitere Konfiguration zum Beispiel in Form einer ACL angefertigt. Der Port, der mit dem Server der Firmenzentrale verbunden ist, hat den Port Gig 9/0 und das Modul PT-ROUTER-NM-1CGE. Er hat die IPv4: 172.16.0.10 /24 (generische, private IP-Adresse mit generischer Subnetzmaske).

### 3.1.3 Netzwerk Einrichtung und IP-Zuweisung

Die interface Adressen wurden den ip dhcp excluded adressen hinzugefügt, auch wenn das beim int gig 0/0 nicht notwendig gewesen wäre, da er nicht in die dhcp pools eingreift. Default Router sind entsprechend die ip adressen der Schnittstellen des Routers für die dhcp pools, also 192.168.4.129 für den company dhcp pool und 192.168.4.161 für den customers dhcp pool. Der dhcp pool company ist wie oben beschrieben für die Firmengeräte gedacht und hat das Netzwerk 192.168.4.128 255.255.255.224. Der dhcp pool customers ist für die Kunden-Geräte gedacht und hat das Netzwerk 192.168.4.160 255.255.255.248.

### 3.1.4 Routing

Theoretisch hätte man auch OSPF auf den Routern konfigurieren können, da dies eher dem Szenario entspricht, dass man erst „über das Internet“ geht und dann auf den Firmen-Server zugreift, wenn es aber darum geht, dass man sich über einen VPN-Tunnel mit dem Firmen-Server verbindet, und die Laptops ausschließlich mit dem Firmen-Server kommunizieren sollen und sonst nichts anderes können sollen, dann entsprechen statische Routen eher dem Anwendungsfall, weswegen wir uns dafür entschieden haben. Aufgrund der statischen Routen, müssen sowohl

für den Messe Router als auch für den Firmenzentrale Router Tabellen angefertigt werden.

| Ziel-Netzwerk | Ziel-Subnetzmaske | Next Hop | Quell-Port |
|---|---|---|---|
| 172.16.0.0 | 255.255.255.0 | 142.250.183.16 | Gig 0/0 |

Tabelle 3.2: Messe Router Routing Tabelle

| Ziel-Netzwerk | Ziel-Subnetzmaske | Next Hop | Quell-Port |
|---|---|---|---|
| 192.168.4.128 | 255.255.255.224 | 142.250.183.14 | Gig 1/0 |
| 192.168.4.160 | 255.255.255.248 | 142.250.183.14 | Gig 1/0 |

Tabelle 3.3: Firmenzentrale Router Routing Tabelle

## 3.2 WLAN

### 3.2.1 Zugang und Sicherheit

Der Zugriff auf das Netzwerk wurde mithilfe WPA2-PSK gesichert. Dieses Protokoll nutzt die AES-Verschlüsselung, die deutlich sicherer ist als TKIP, was noch von WPA verwendet wurde, und sich als Standard-Verschlüsselung etabliert hat. Da es sich nur um einen Messe-Aufenthalt handelt, muss man sich keine Gedanken über das zyklische tauschen des Schlüssels machen, was normalerweise der Fall wäre, um die Sicherheit zu erhöhen. Der Schlüssel wurde außerdem sehr lang gewählt, und wird in KeePass verschlüsselt gespeichert. Die Schlüssellänge wurde bewusst sehr lang gewählt, da es sowohl für die Firmengeräte als auch die Kundengeräte verwendet werden soll, was Administratoren die Arbeit erleichtert, da Sicherheit auch immer ein Abwägen zwischen Aufwand und Ertrag ist. Wie im Kapitel „Routing“ bereits erwähnt, wird davon ausgegangen, dass nur über eine VPN-Verbindung der Firmenzentrale Server erreicht werden kann, was ein großes Plus an Sicherheit für die Kommunikation zwischen dem Messer Router und dem Firmenzentrale Netzwerk bedeuten würde. Diese Sicherheit, und die gesicherte Verbindung zwischen den APs wurde durch die beiden ACLs erreicht, die auf dem Messe Router konfiguriert wurden:

#### ACL 1

##### Situationsbeschreibung

Nur Requests vom Server an die Netzwerke sollen erlaubt werden. Die Kommunikation zwischen den Netzwerken und die Paket-Weiterleitung der Pakete an

die Netzwerke von anderen IP-Adressen als der Server-Adresse sollen gestoppt werden. Für diesen Anwendungsfall reicht eine einfache ACL, da keine Protokolle spezifiziert werden müssen.

#### Befehle

- access-list 1 permit 142.250.183.16 255.255.255.0
- (int 8/0) ip access-group 1 out → Das Paket darf nur von diesem Netzwerk in das Netzwerk kommen.
- (int 9/0) ip access-group 1 out

### ACL 101

#### Situationsbeschreibung

Nur Anfragen an den Server aus den Netzwerken sollen erlaubt werden. Alle anderen Anfragen sollen fallen gelassen werden. Von den Anfragen, die zugelassen werden, sollen wiederum nur eine HTTPS Verbindung erlaubt werden, um zu gewährleisten, dass die Kommunikation verschlüsselt stattfindet. Dafür wird eine erweitere ACL benötigt, die TCP auf dem Standard-Port 443 erlaubt.

#### Befehle

- access-list 101 permit tcp 192.168.4.129 0.0.0.31 172.16.0.10 0.0.0.255 eq 443
- access-list 101 permit tcp 192.168.4.161 0.0.0.7 172.16.0.10 0.0.0.255 eq 443
- (int gig 0/0) ip access-group 101 out

#### Folgen

Aufgrund dieser restriktiven Einstellung war es zeitweise nicht möglich, die Notebooks über dhcp zu konfigurieren, da die dhcp discovery packages gedroppt wurden.

#### Lösung

Daher müssen die UDP-Ports, die für DHCP verwendet werden, ebenfalls erlaubt werden, und da die Notebooks zu dem Zeitpunkt noch keine IP haben, und das interface nicht kennen, wird any any verwendet:

- access-list 101 permit udp any any eq 67
- access-list 101 permit udp any any eq 68

### 3.2.2 Anbindung von Clients

Die Laptops haben standardmäßig ein Modul verbaut, welches nur einen Ethernet Port anbietet. Daher musste das integrierte Module der Laptops ausgebaut werden und durch ein WPC300N ersetzt werden, da dieses WLAN unterstützt. Um sich nun mit dem Netzwerk zu verbinden, muss man unter Desktop, PC Wireless, den nächsten AP auswählen und den Schlüssel eingeben. Ansonsten ist keine Verbindung mit dem Netzwerk möglich.

## 3.3 Inbetriebnahme

Bevor die Mitarbeiter auf die Messe fahren, sollten sie überprüfen, dass sie die 16 firmeninterne Laptops, die 2 APs, und den Router dabeihaben. Außerdem sollten sicherheitshalber LAN-Kabel mitgenommen werden, da wir nicht wissen, ob diese vor Ort verfügbar sind oder nicht. Da der Router und die firmeninternen Geräte vorkonfiguriert sind, müssen die Mitarbeiter die Komponenten nur noch an den Strom anschließen und starten. Vergewissern Sie sich, dass sie mit der Software vertraut sind und die Schulung verstanden haben. Bei Fragen zur Anwendung wenden Sie sich an die Mitarbeiter vor Ort. Es wird ein reibungsloser Ablauf erwartet, da es sonst rufschädigend sein könnte. Falls die Laptops den WLAN-Zugang nicht mehr gespeichert haben sollten, muss das WLAN mit der SSID company ausgewählt werden, und das folgende Passwort eingegeben werden:
JWB5EMkWFZeLtV1OVKaEqYhvxs3ICtw2
Die Kunden, von denen wir maximal 4 gleichzeitig bedienen können, nutzen das WLAN mit der SSID customers. Das Passwort hierfür ist jedoch das gleiche. Bitte stellen Sie sicher, dass sich die Kunden nach erfolgreicher Interaktion wieder von dem Netzwerk trennen, da sonst Plätze für neue Kunden blockiert werden würden.

# 4 Umsetzung Teilprojekt SAE

## 4.1 Datenbank

Dieser Abschnitt fokussiert sich auf die in der Softwarelösung verwendete Datenbank und deren Modellierung. Für die Software wurde eine SQLite Datenbank verwendet.
In der Software wurde das Entity Framework verwendet um Tabellen und Relationen anhand von zuvor definierten Klassen zu generieren. Dazu wurden 4 Klassen angelegt User, Company, Interest und Address, die dann zu Tabellen automatisch umgewandelt werden. Dabei wird aus Attributen wie z.B. der Name von User eine Spalte mit eben dieser Bezeichnung. Außerdem wird der Datentyp passend zum Attribut gewählt. Relationen werden ebenso erzeugt z.B. wenn ein User eine Adresse besitzt und damit ein Attribut vom Typ Address hat.

### 4.1.1 Datenbankmodell

Betrachten wir zunächst ein ER-Modell der Datenbank um einen Überblick zu erhalten.

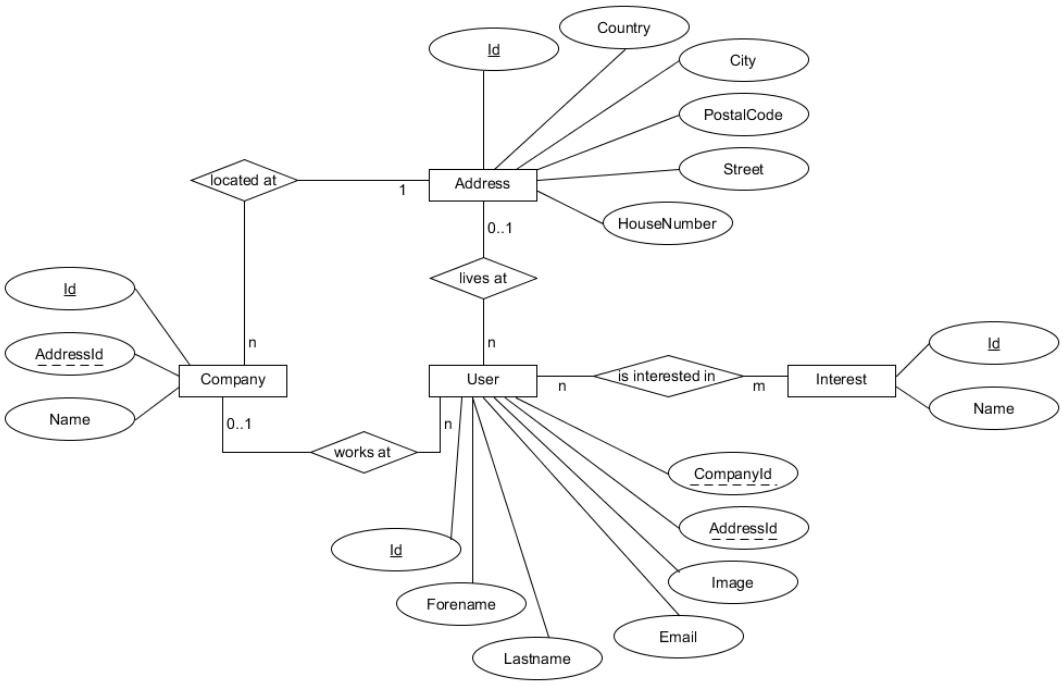


Abbildung 4.1: ER-Modell der Datenbank für die Softwarelösung

### 4.1.2 Entitäten

In diesem Abschnitt betrachten wir die Entitäten des ER-Modells und ihre Attribute genauer.

#### User

Die Entität User repräsentiert den Kunden, der seine Daten auf der Messe angegeben hat. Diese Person hat einen Vor- und Nachnamen, Email, Bild, Adresse und eventuell eine Firmenzugehörigkeit. Der Primärschlüssel ist Id, wohingegen AdressId und CompanyId Fremdschlüssel sind.

#### Company

Diese Entität repräsentiert eine Firma, der ein Kunde möglicherweise angehören kann. Sie hat eine Id als Primärschlüssel, einen Namen und eine Adresse mit AddressId als Fremdschlüssel.

#### Address

Die Entität Address hat eine primäre Id, Land, Stadt, Postleitzahl, Straße und Hausnummer.

#### Interest

Eine Interesse hat eine primäre Id und einen Namen.

### 4.1.3 Relationen

#### Company - Address

Eine Firma hat genau eine Adresse wohingegen an einem Standort auch mehrere Firmen angesiedelt sein können. Dies wird die gezeigte 1:n Relation widergespiegelt. Der Verweise von der Firma auf die Adresse wird mit Hilfe des Fremdschlüssels AddressId gelöst.

#### User - Address

Ein Kunde hat eine oder keine Adresse, wohingegen an einem Ort durchaus mehrere Leute wohnen können. Diese 1:n Relation wird durch den Fremdschlüssel AddressId modelliert.

### User - Company

Ein Kunde kann Mitarbeiter einer Firma sein, muss es aber nicht und eine Firma kann viele Mitarbeiter haben. Diese 1:n Relation wird durch den Fremdschlüssel CompanyId modelliert.

### User - Interest

Ein Kunde kann mehrere Interessen haben, aber eine Interesse wie z.B. Reisen kann von vielen Kunden favorisiert werden. Diese n:m Relation wird durch zwei Listen gelöst, wovon sich jeweils eine in der Entität User und Interest befindet.

## 4.2 Aufbau und Funktionsweise

Dieser Abschnitt befasst sich mit dem Aufbau, Architektur und Funktionsweise der Softwarelösung beschrieben mit Hilfe von grafischen Darstellungen mit verschiedenen Diagrammen.

### 4.2.1 Architektur

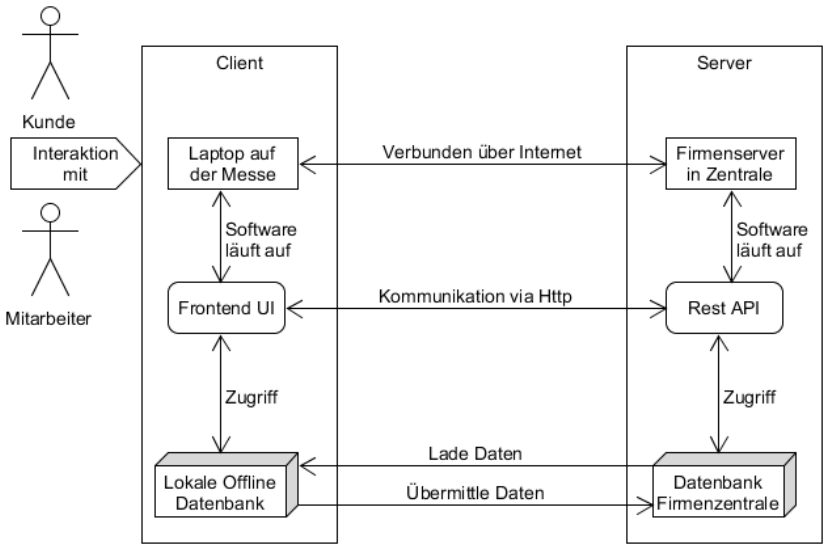


Abbildung 4.2: Grafische Darstellung der Architektur

Der Aufbau der Softwarelösung ist eine klassische Client-Server-Architektur. Abbildung 4.2 gibt einen Überblick über die beiden Komponenten und ihr Zusammenspiel.
Der Client befindet sich mit den Mitarbeitern am Messe Stand und ist dort auf den Laptops für die Kunden verfügbar. Dabei handelt es sich um die Frontend UI, die zur Eingabe von Kundendaten und zur Übermittlung an die Firmenserver mit grafische Komponenten dient. Sowohl Kunden als auch Mitarbeiter können den Client bedienen, wobei die Übermittlungsfunktion für Daten lediglich mit Angabe von zuvor registrierten Anmeldedaten benutzt werden kann. Im regulären Betrieb für Kunden befindet sich der Client in einer Art Offline Modus und speichert die Kundendaten in einer lokalen Datenbank ab. Erst nach aktiver Übermittlung an den Firmenserver durch einen Mitarbeiter, werden die Daten zur Firmenzentrale gesendet.
Die Backend Anwendung, eine Rest API, läuft auf den Firmenservern in der Zentrale. Diese wird über das Internet vom Client aus angesteuert, wenn neue

Daten durch Mitarbeiter übermittelt werden. Im Gegensatz zur lokalen Client Datenbank, die nur die Daten, des Geräts auf dem diese ausgeführt wird, enthält, sammeln sich in der Datenbank auf dem Firmenserver alle angegebenen Kundendaten an. Zusätzlich werden nach erfolgreicher Übermittlung die Daten vom Client entfernt, um Speicherplatz frei zu machen und Duplikate zu verhindern. Die Mitarbeiter und der Zentrale können im Backend via einer Swagger UI im Browser nach Angabe von validen Anmeldedaten die Kundendaten abfragen.
Zur Autorisierung von Mitarbeitern werden Json Web Tokens verwendet um die Daten zu bearbeiten und zu synchronisieren. Die Kommunikation mit der Zentrale geschieht mittels HTTPS, damit sichergestellt ist, dass die versendeten Daten verschlüsselst sind.

### 4.2.2 USE Case- und Klassen-Diagramme


Abbildung 4.3: Use Case Diagramm zur Softwarelösung

In Abbildung 4.3 ist ein Anwendungsfalldiagramm zur Softwarelösung zu sehen. Es gibt zwei Akteure den Kunden und den Mitarbeiter, die verteilt über Frontend UI und Backend Anwendung verschiedene Aktionen durchführen können. Dabei erbt der Mitarbeiter alle Funktionen des Kunden, da dieser auch ohne Angabe von Anmeldedaten alle Aktionen eines Kunden durchführen kann.

#### Aktionen eines Kunden

- Kamera auswählen: Mit eine Dropdown Liste kann in der Oberfläche eine Kamera unter all den angeschlossenen gewählt werden. Eine Kamera wird immer als Default ausgewählt sein.
- Kamera einschalten: Die ausgewählte Kamera wird eingeschalten und deren Übertragung angezeigt.

- Foto machen: Nachdem die Kamera eingeschaltet wurde, kann ein Foto von deren Übertragung gemacht werden.
- Persönliche Daten eingeben: Der Kunde kann verschiedene persönliche Daten, wie Name und Anschrift und diversen Textfeldern angeben.
- Daten lokal einreichen: Wenn alle notwendigen Daten angegeben wurden, können die Angaben eingereicht und damit lokal gespeichert werden.
- Interessen auswählen: Der Kunde kann zwischen verschiedenen vorgegebenen Interessen auswählen und diese per Klick selektieren.
- neue Firma anlegen: Wenn von den vorhandenen Firmen keine zusagt, kann eine neue Firma angelegt werden.
- Firma auswählen: Der Kunde kann aus verschiedenen angegebenen Firmen eine auswählen.

#### Aktionen eines Mitarbeiters

- Registrieren: Ein Mitarbeiter kann im Backend neue Anmeldedaten registrieren mit denen er sich später dann in Front- und Backend anmelden kann.
- Login Daten eingeben: Der Mitarbeiter kann sowohl im Front- als auch Backend die Anmeldedaten angeben um sich anzumelden.
- Daten übermitteln: Nach Angabe von Anmeldedaten kann ein Mitarbeiter die lokal gespeicherten Daten an die Firmenzentrale übermitteln.
- Alle Kundendaten abfragen: Ein Mitarbeiter kann nach Angabe von Anmeldedaten im Backend alle Kundendaten abfragen.
- Einzelne Kundendaten abfragen: Ein Mitarbeiter kann nach Angabe von Anmeldedaten im Backend einzelne Kundendaten spezifisch abfragen.
- Firmen abfragen: Ein Mitarbeiter kann nach Angabe von Anmeldedaten im Backend die Firmen abfragen.
- Interessen abfragen: Ein Mitarbeiter kann nach Angabe von Anmeldedaten im Backend die Interessen abfragen.

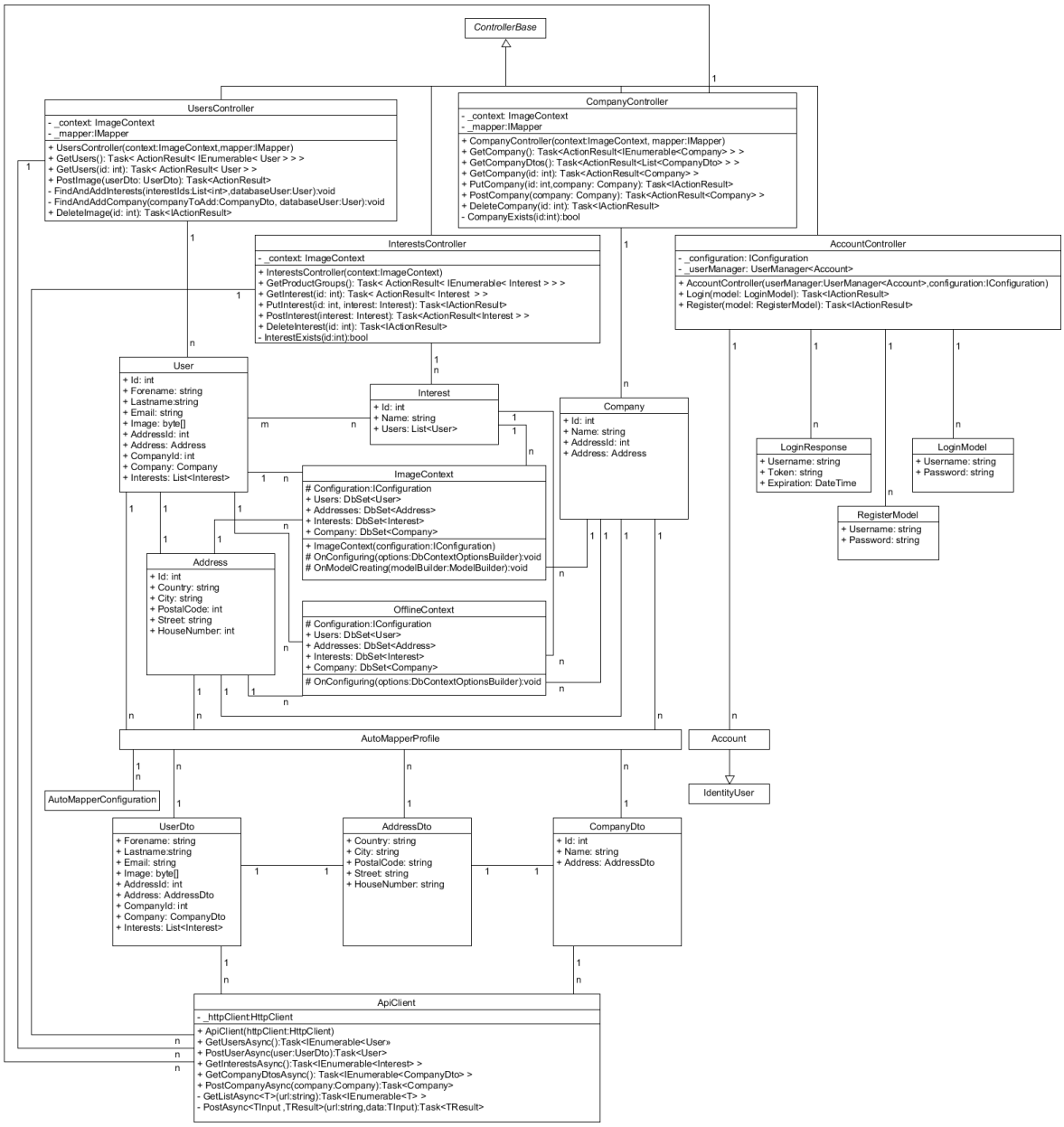


Abbildung 4.4: Klassen-Diagramm zur Softwarelösung

In Abbildung 4.4 ist ein Klassendiagramm zur Softwarelösung zu sehen. Im oberen Bereich des Diagramms befinden sich vier Controller Klassen. Diese beinhalten die Http Methoden, wie Get oder Post, die als Rest Api nach außen zum Aufrufen gerichtet sind. Dabei befasst sich UserController mit allen Aktionen rund um die Kundendaten, CompanyController mit den Firmen, zu denen ein Kunde gehören kann, InterestsController mit den Interessen, die Kunden haben können und AccountController mit den Mitarbeiteraccounts, die zum erfolgreichen Anmelden benötigt werden um spezifische Funktionen ausführen zu können.

Im Zentrum des Diagramms sind zum einen die Modellklassen der einzelnen Entitäten User, Interest, Company und Address, wie sie schon im Abschnitt zur Datenbankmodellierung aufgetreten sind. Außerdem befinden sich dort zwei Datenbank Kontext Klassen, ImageContext und OffloneContext. Der Erste Kontext ist die Datenbank auf Seite der Firmenzentrale. Der Zweite ist die lokale Datenbank auf den Clients, welche genutzt wird um die Kundendaten lokal zu speichern, damit kurzzeitige Internetausfälle bei Datenübertragungen umgangen werden. Mit Hilfe der Anmeldedaten eines Mitarbeiter können die lokalen Daten dann zur Firmenzentrale übertragen werden. Beide Datenbankkontext sind gleich aufgebaut, mit je einem DBSet zu allen vier Entitäten.
Im unteren Bereich des Diagramms haben wir zum einen den AutoMapper und die DTOs (Data Transfer Object) und zum anderen den ApiClient. Die ersten beiden werden genutzt um die Daten von den lokalen Datenbanken in DTOs umzuwandeln damit die Informationen dann in diesem Format an die Firmenzentrale geschickt wird. Im Firmenserver werden die DTOs dann wieder in die entsprechenden Entitäten umgemapped und in die dort ansässige Datenbank gespeichert. Der ApiClient wird auf Client Seite verwendet um alle Anfragen an die verschiedenen Teile der API (User, Company, Interest oder Account) zu bündeln und zu vereinfachen.

### 4.2.3 Prerequisites: Bibliotheken und Komponenten

Sowohl Frontend als auch Backend Anwendungen sind auf .NET 6.0 aufgebaut. Ebenso verwenden beide Anwendungen Automapper (12.0.1), Microsoft.EntityFrameworkCore.Design (6.0.25) und Microsoft.EntityFrameworkCore.Sqlite (6.0.25). Das Backend ist eine ASP.Net API und verwendet zusätzlich noch Microsoft.AspNetCore.Authentication.JwtBearer (6.0.25) und Microsoft.AspNetCore.Identity.EntityFrameworkCore (6.0.25). Das Frontend ist eine Windows Forms Anwendung und verwendet zusätzlich AForge (2.2.5)

### 4.2.4 Inbetriebnahme vor Ort

Nachdem die vier Laptops vor Ort mit dem Netzwerk verbunden wurden, muss die Frontend Software von den Mitarbeitern gestartet werden. Bei der Auswahl der Laptops muss zuvor darauf geachtet werden, dass diese eine Webcam besitzen, oder es werden zusätzliche Webcams mitgebracht, die jetzt vor Start der Anwendung an die Laptops angeschlossen werden müssen. Nachdem die Anwendung gestartet ist öffnet sich ein Fenster wie in Abbildung 4.5 zu sehen.

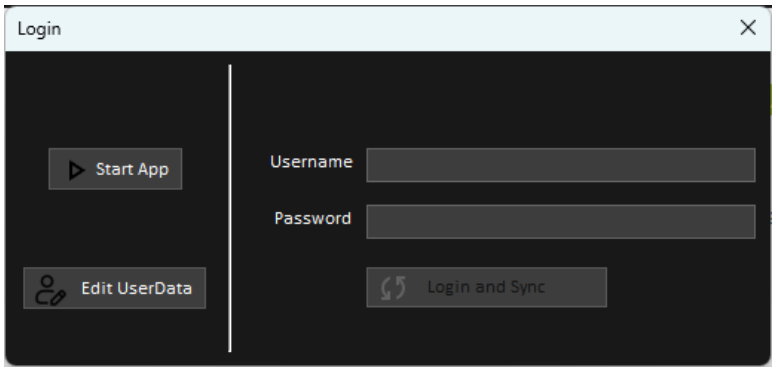


Abbildung 4.5: Login Bildschirm der Frontend Anwendung

Die Mitarbeiter sollten initial einmal ihre Anmeldedaten eingeben und den Button ”Login and Sync” drücken um die lokale Datenbank mit der aus der Firmenzentrale zu synchronisieren. Damit wird gewährleistet, dass Interessen oder Firmen, die bereits in der Datenbank der Firmenzentrale hinterlegt wurden, auch lokal für die Kunden zur Auswahl verfügbar sind. Anschließend nachdem die Synchronisation abgeschlossen ist öffnet sich automatisch das nächste Fenster (siehe Abbildung 4.6).
Ein Mitarbeiter sollte im oben links befindlichen Dropdown Menü, die Webcam auswählen, die gewünscht wird und auf den Button ”Start Cam” drücken um die Kamera zu starten. Jetzt ist die Anwendung einsatzbereit und kann von Kunden genutzt werden.

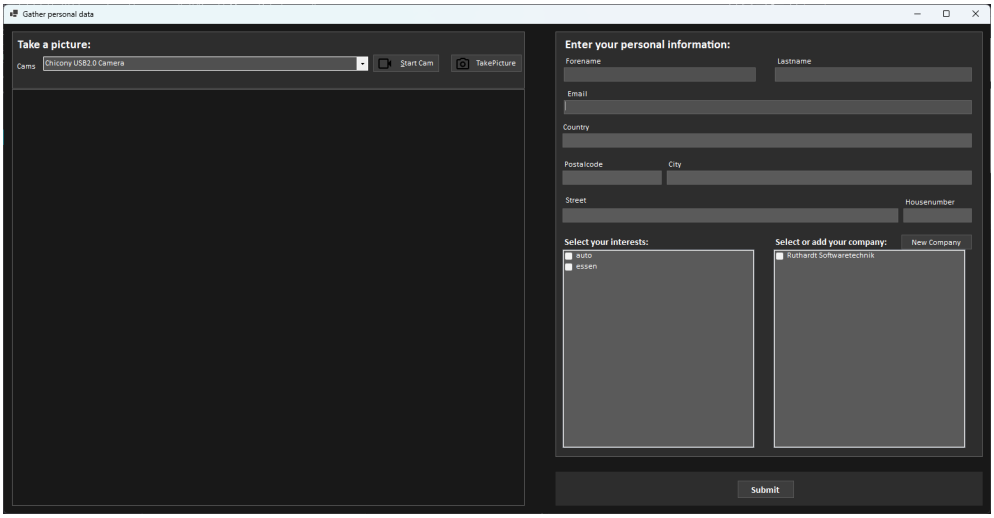


Abbildung 4.6: Hauptbildschirm der Frontend Anwendung

### 4.2.5 Technische Beschreibung der WebCam Anbindung

Um die Aufnahme der Webcam innerhalb der Frontend Anwendung anzuzeigen wird eine Picturebox verwendet, deren Image Attribute auf den Wert des aktuellen Frame der Webcam gesetzt wird. Für die Anbindung der Webcam wird das AFroge Paket verwendet. Zuerst wird wenn die Form des Hauptbildschirms geladen wird alle VideoInputDevices in eine Collection geladen und dem Dropdown Menü hinztugefügt, damit diese zur Auswahl für den Anwendet stehen (siehe Abbildung 4.7).

```
_filterInfoCollection = new FilterInfoCollection(FilterCategory.VideoInputDevice);
foreach (FilterInfo filterInfo in _filterInfoCollection) cboCamera.Items.Add(filterInfo.Name);
```

Abbildung 4.7: Collection von VideoInputDevices

Wenn nun der ”Start Cam” Button gedrückt wird, dann wird ein neues VideoCaptureDevice instanziiert anhand der aus dem Dropdown Menü ausgewählten Kamera. Anschließend wird dem NewFrame Event des neuen Objekts eine Methode zugewiesen, die den Frame eines neuen Frame Events eines Videodevices klont. Dieser wird schließlich im UI Thread dem Image der Picturebox zugewiesen (vgl. Abbildung 4.8).

```
    _videoCaptureDevice = new VideoCaptureDevice(_filterInfoCollection[cboCamera.SelectedIndex].MonikerString);
    _videoCaptureDevice.NewFrame += VideoCaptureDevice_NewFrame;
    _videoCaptureDevice.Start();
}

2 Verweise
private void VideoCaptureDevice_NewFrame(object sender, NewFrameEventArgs eventArgs)
{
    var frame = (Bitmap)eventArgs.Frame.Clone();
    Invoke(() => NewFrameOnUiThread(frame));
}

1 Verweis
private void NewFrameOnUiThread(Bitmap frame)
{
    pictureBox1.Image = frame;
}
```

Abbildung 4.8: Starten der Kamera und neuer Frame für Picturebox

### 4.2.6 Anleitung Bedienung durch den Kunden

Der Kunde tritt an den Laptop heran und sieht den Hauptbildschirm wie in Abbildung 4.6 zu sehen. Nun muss dieser auf der rechten Seite die persönlichen Daten angeben und kann Interessen auswählen oder eine Firma wo der Kunde Mitarbeiter ist. Dann kann der Kunde noch auf ”Take Picture” klicken um eine Foto der aktuellen Bilds der Webcam zu machen, damit auch sein Foto gespeichert werden kann. Wenn alle Daten zur Zufriedenheit angegeben wurden und das Fotos ebenso gefällt, kann der Kunde unten rechts auf ”Submit” klicken und damit seine Daten speichern.

### 4.2.7 Anleitung Datenabruf und Übermittlung

#### Übermittlung

Ein Mitarbeiter, der über Anmeldedaten verfügt, kann im Login Bildschirm (vgl. Abbildung 4.5) diese eintragen und dann auf ”Login and Sync” drücken. Damit werden die lokal gespeicherten Daten an die Firmenzentrale gesendet. Es ist zu beachten, dass die auf jedem lokalen Gerät auf der Messe durchgeführt werden muss. Außerdem ist wichtig, dass für diese Aktion eine Internetverbindung bestehen sollte, andernfalls können die Daten nicht erfolgreich an die Zentrale gesendet werden. Da das Versenden und lokal Speichern voneinander entkoppelt ist, sollten die Mitarbeiter darauf achten, die Synchronisation dann durchzuführen wenn sichergestellt werden kann, dass eine Verbindung vorliegt.

#### Datenabruf

Der Datenabruf von bereits an die Zentrale übertragenen Daten, kann dort von Mitarbeitern mit Hilfe der Swagger UI im Browser durchgeführt werden. Dazu muss der Mitarbeiter seine Anmeldedaten bereit halten. Zunächst wird die Login

von Account Teil der Api aufgeklappt und auf ”Try it out” geklickt (vgl. Abbildung 4.9). Dann wird in die Felder bei username und password wo string steht die Anmeldedaten eingetragen. Dann wird auf ”Execute’ gedrückt.

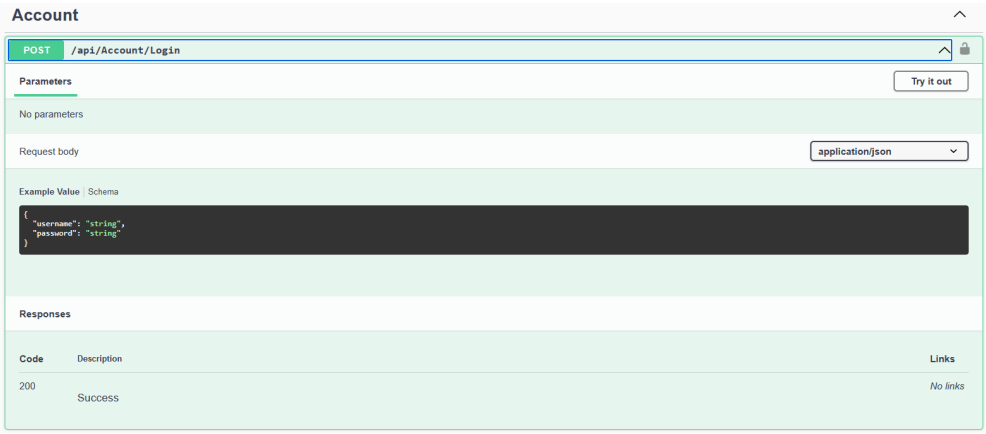


Abbildung 4.9: Login in Swagger UI für Token

Unten im Response body befindet sich dann ein Token, diese soll kopiert werden. Dann kann der Login wieder zugeklappt werden. Nun wird oben rechts auf ”Authorize” geklickt. In das Eingabefeld unter ”Value” wird zuerst das Wort ”Bearer” geschrieben und dann das zuvor kopierte Token eingefügt (vgl. Abbildung 4.10).

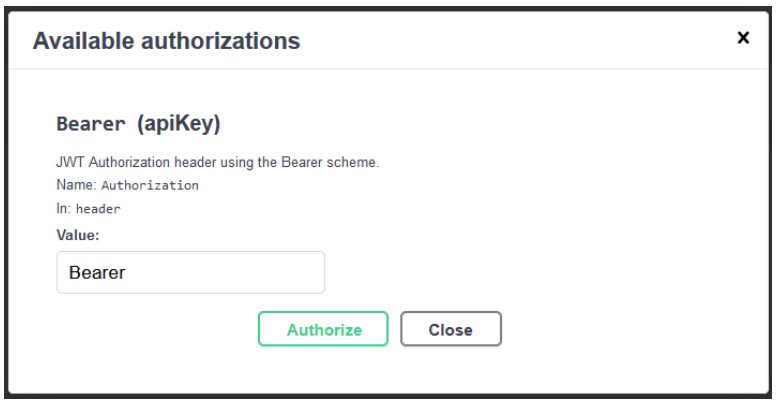


Abbildung 4.10: Login in Swagger UI mit Bearer Token

Nachdem der Mitarbeiter nun erfolgreich autorisiert wurde kann dieser alle möglichen Methoden der API nutzen. Um z.B. die in der Datenbank befindlichen Kundendaten abzufragen, gehen wir zum Abschnitt Users und klappen die erste Methode ”Get” auf. Klicke wieder auf ”Try it out” und dann auf ”Execute” (vgl. Abbildung 4.11). Nun ist im response body der Anfrage alle Kundendaten, mit den jeweiligen Attributen aufgelistet. Unten rechts ist noch die Möglichkeit diese Daten in die Zwischenablage zu kopieren oder gleich die gesamte JSON Ausgabe herunterzuladen.

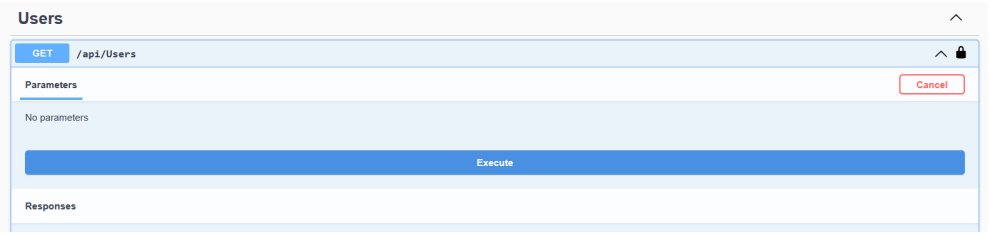


Abbildung 4.11: Abfragen Kundendaten

Alternativ kann von den Mitarbeitern im Backend die .db Datei, die sich im Ordner der Softwarelösung befindet mit dem Terminal oder einem Tool ihrer Wahl geöffnet und diverse Anfragen zum aktuellen Stand der Kundendaten gestellt werden.
Zusätzlich gibt es die Option nach einem Neustart der Anwendung den ”Edit User” Button zu drücken (vgl. Abbildung 4.5), das ein neues Fenster öffnet, wo alle lokal gespeicherten Daten angezeigt werden (Siehe Abbildung 4.12). Nachdem die Daten angepasst wurden muss der Vorgang durch Enter bestätigt werden, ansonsten werden die Änderungen verworfen. Mitarbeiter auf der Messe sollten beachten, dass kein Kunde die Daten alleine bearbeitet, sensitive Daten werden zwar nicht angezeigt, aber wir wollen vermeiden, dass falsche Daten mit der Firmenzentrale synchronisiert werden.

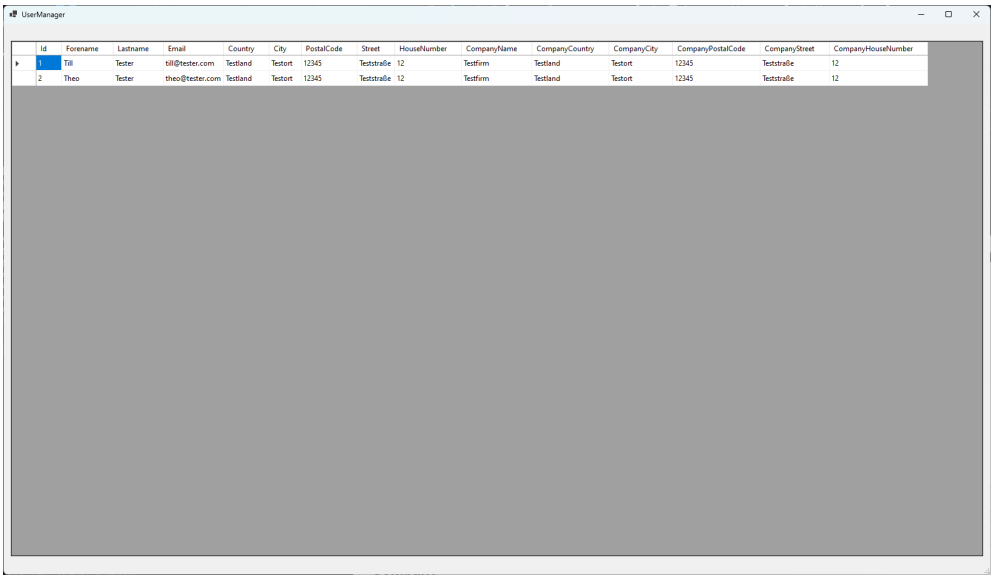


Abbildung 4.12: Kundendatenbearbeitung

### 4.2.8 Risiko-Einschätzung

#### Backend

Unser Firmenserver wird zunächst einmal durch eine Firewall und ACLs durch Netzwerkkomponenten geschützt. Darüber hinaus können nur autorisierte Nutzer, aufgrund der Nutzung von JWT, auf die Ressourcen zugreifen. Die Daten als solche liegen in plain Text vor. Das bedeutet, dass wenn jemand autorisierter Zugriff erhält, hat er sofort autorisierten Zugriff. Daher wird der Token regelmäßig rotiert. Stellen Sie sicher, dass die Administratoren regelmäßig, über die Messe hinweg, die Passwörter ändern.

#### Frontend

Zunächst einmal sollten die firmeninternen Geräte mit einem Passwort geschützt werden. Wenn kein Mitarbeiter vor Ort ist, um die Kundenaktivitäten zu überprüfen, müssen die Laptops gesperrt werden. Die Daten liegen auch hier in plain Text vor. Auslesen könnte man diese also. Da für die Synchronisierung allerdings Username und Passwort benötigt werden, ist der Server in der Hinsicht geschützt.

#### Kommunikation

Die Kommunikation zwischen backend und frontend erfolgt über https. Dies gewährleistet, dass die Daten während der gesamten Kommunikation verschlüsselt übertragen werden. Dies macht Man in the Middle attacks quasi nutzlos.

### 4.2.9 Testszenarien

Im Folgenden werden die Testszenarien aufgelistet, die an der Softwarelösung durchgeführt wurden.

| Testnummer | Testbeschreibung | Erwartetes Ergebnis | Bestanden |
|---|---|---|---|
| 1 | Mitarbeiter Registrierung im Backend | Erfolgreiche Registrierung und Erhalt Token | Ja |
| 2 | Start Anwendung Offline | Anwendung startet ohne Anmeldedaten | Ja |
| 3 | Synchronisierung und Anwendung Start mit Anmeldedaten | Daten werden synchronisiert dann öffnet sich Anwendung | Ja |
| 4 | Aktive Webcams und Auswahl | Liste aller verfügbaren Webcam angezeigt und auswählbar | Ja |
| 5 | Webcam starten | Webcam startet und wird angezeigt nach Button drücken | Ja |
| 6 | Lokal gespeicherte Daten bearbeiten | Über Ëdit User"können Daten vor dem absenden bearbeitet werden | Ja |
| 7 | Kundendaten anlegen | Es können Kundendaten angegeben, ein Bild aufgenommen und gespeichert werden | Ja |
| 8 | Interessen Auswahl | Es können Interessen aus einer Liste gewählt werden | Ja |
| 9 | Firmen Verwaltung und Auswahl | Firmen können angelegt und zum Kunden ausgewählt werden | Ja |
| 10 | Der Mitarbeiter versucht sich mit seinen Zugangsdaten anzumelden, während keine Verbindung zum Server besteht. | Es wird ein Fehler auftreten, der besagt, dass keine Verbindung mit dem Zielcomputer hergestellt werden konnte. Somit werden auch keine Daten gesendet. | ja |
| 11 | Bei bestehender Internetverbindung versucht der Mitarbeiter sich mit falschen Zugangsdaten anzumelden. | Es wird ein Fehler auftreten, der besagt, dass der Login Vorgang gefailed ist. | ja |

Tabelle 4.1: Tabelle der Testszenarien Teil 1

| | | | |
|---|---|---|---|
| 12 | Der Mitarbeiter startet die main app, gibt Vorname und Nachname ein. Schließt die Anwendung und loggt sich dann mit seinen Zugangsdaten ein. | Die Daten werden an den Server gesendet und es öffnet sich danach die main app. Überprüfbar ist dies mithilfe des GET endpoints des UserControllers. Die Werte für Address und Company sind null. | Ja, der neue Eintrag konnte gefunden werden und Address, sowie Company sind null. |
| 13 | Der Mitarbeiter startet die main app, gibt Vorname und Nachname ein. Außerdem gibt er einen validen Namen für eine Straße ein, wählt eine Interesse aus, und legt darüber hinaus eine neue Company an, die neben einem Namen auch als Country den Wert „Deutschland“ erhält. Dann schließt er die Anwendung und loggt sich dann mit seinen Zugangsdaten ein. | Die Daten werden alle samt an den Server gesendet und Address, Company und Interests sind nicht null. | Durch den GET endpoint konnte verifiziert werden, dass der User alle ausgewählten Attribute hat. |
| 14 | Der User gibt nur seinen Vornamen ein. | Es erscheint eine MessageBox, die angibt, dass man einen vollständigen Username, also sowohl Vor- als auch Nachnamen angeben soll. | Ja, diese MessageBox erscheint. |
| 15 | Der User gibt einen Vor- und Nachnamen ein. Alle anderen Felder bleiben leer. | Es wird der Nutzer angelegt, und es erscheint kein Fehler, da alle anderen Properties nullable sind. | Ja, der User wird erfolgreich angelegt (und kann beim Synchronisieren gesendet werden). |
| 16 | Der User gibt einen Vor- und Nachnamen ein, aber beide enthalten Nummern. | Es erscheint eine MessageBox, die ausgibt, dass ein valider Username angegeben werden soll. | Ja, diese MessageBox erscheint. |

Tabelle 4.2: Tabelle der Testszenarien Teil 2

| | | | |
|---|---|---|---|
| 17 | Der User gibt einen Doppelnamen mit Leerzeichen getrennt an, und einen validen Nachnamen. | Es wird der Nutzer angelegt, und es erscheint kein Fehler, da Doppelnamen erlaubt sind. | Der Nutzer wird erfolgreich angelegt. |
| 18 | Der User gibt einen validen Username an, und gibt darüber hinaus eine Zahlenfolge als Postleitzahl ein. | Es wird der Nutzer angelegt, und es erscheint kein Fehler, da die Postleitzahl als Integer geparsed werden kann. | Der Nutzer wird erfolgreich angelegt. |
| 19 | Der User gibt einen validen Username an, und darüber hinaus eine Postleitzahl, in der sich allerdings auch Buchstaben befinden. | Es erscheint eine MessageBox, die ausgibt, dass eine valide Postleitzahl angegeben werden soll. | Ja, diese MessageBox erscheint. |
| 20 | Der User gibt einen validen Username an, und darüber hinaus einen Straßennamen, der mit „-„ getrennt ist. | Es wird der Nutzer angelegt, und es erscheint kein Fehler, da solche Straßennamen erlaubt sein sollen. | Der Nutzer wird erfolgreich angelegt. |
| 21 | Der User gibt einen validen Username an, und darüber hinaus einen Straßennamen, der auch Zahlen enthält. | Es erscheint eine MessageBox, die ausgibt, dass eine valide Straße, also nur mit strings, angegeben werden soll. | Nein, der Nutzer wird dennoch angelegt. |
| 22 | Der User gibt einen validen Username an, und darüber hinaus eine Hausnummer, die allerdings mit einem Buchstaben vorangestellt ist. | Es erscheint eine MessageBox, die ausgibt, dass eine valide Hausnummer, also nur mit einer Zahl und einem Buchstaben am Ende, angegeben werden soll. | Ja, diese MessageBox erscheint. |
| 23 | Der User gibt einen validen Username an, und darüber hinaus eine Hausnummer, die zwar mit Zahlen beginnt, aber mit mehr als einem Buchstaben endet. | Es erscheint eine MessageBox, die ausgibt, dass eine valide Hausnummer, also nur mit einer Zahl und einem Buchstaben am Ende, angegeben werden soll. | Ja, diese MessageBox erscheint. |
| 24 | Der User gibt einen validen Username an, und darüber hinaus die Hausnummer 12a | Der User wird erfolgreich angelegt. | Der Nutzer wird erfolgreich angelegt. |

Tabelle 4.3: Tabelle der Testszenarien Teil 3