# ITK-Leitfaden

## 1. Zielgruppe und Kontext

Der Industrial MakerSpace (IMS) soll industriell ausgerichteten Innovations-Teams die bestmögliche Arbeitsumgebung bieten. **Zielgruppe dieses ITK-Leitfadens sind die Nutzer des IMS**. Das leistungsfähige **IMS-WLAN** verbunden mit dem breitbandigen **Internet-Anschluss** ist dabei ***Kern der digitalen Anbindung*** der Nutzer.

Das WLAN soll den Nutzern grenzenlose Mobilität innerhalb des IMS ermöglichen. Die Kompatibilität mit gängiger hardware soll gewährleistet werden um die Leitlinie „**BYOD** - ***bring your own device"*** umzusetzen.

## 2. Funktionale Anforderungen

- Breitbandiger Glasfaser-Hausanschluss mit einfach-redundanter Auslegung
- WLAN Access Points (dual band), die das gesamte Gebäude (Industriehalle, Büro-, Verkehrs- und Technikflächen) abdecken
- CAT7a Verkabelung im gesamten Gebäude als back-up und für Sonderanwendungen
- zentrale Firewall als "managed security service" bei einem professionellen Anbieter
- Internet-Service mit einer Geschwindigkeit von mind. 1Gbit/s (symmetrisch), ausreichender Kapazität pro Nutzer und Ausbaufähigkeit bis 10Gbit/s (symmetrisch)
- Switches und Router, die folgende Netz-Nutzung erlauben:
    - Ein offenes **Gäste-Netzwerk** für Gäste, Meeting-Teilnehmer und Konferenzen
    - Ein **zentrales, geschlossenes Netzwerk für alle Nutzer und Nutzer-Gruppen** mit geringerer Sicherheit (WPA2 Personal) für die einfache Anbindung von Druckern und WPA2-Enterprise inkompatible Geräte.
    - Möglichkeit jeweils **dezentrale geschlossene Netzwerke für einzelne Nutzer-Gruppen** mit state-of-the-art Sicherheit (WPA2 Enterprise) zu schaffen
    - Ein **zentrales geschlossenes Netzwerk** für die IMS-Administration (ITK-Admin, TGA-Admin, Mgt.-Admin)

## 3. Stand der Installation und Beauftragungen (Status Quo)

Zum heutigen Datum wurden u.a. installiert bzw. beauftragt:

- InterNet Service durch LEW TelNet GmbH, Product Business Connect LWL Premium 1G (1Gbit/s symmetrisch) seit 21.12.2017
- Managed Security Security Gateway, LEW TelNet GmbH, Produkt Next Generation Firewall seit 21.12.2017
- WLAN basierend auf Aruba AP 345 Access Points und Aruba 2930 M Switch seit 15.1.2018. Abschließende Messung erfolgte am 27.7.2018
- CAT 7/CAT7a – Verkabelung seitens Fa. Greulich Elektroanlagen GmbH im gesamten Gebäude mit Anschlussdosen in den offenen Kabelrinnen seit 31.7.2019
- LAN/RJ45-Access in den Besprechungszimmern, der Industriehalle und in den Druckerräumen (default-Zugang via: IMS-Pool) seit 1.1.2020

## 4. Optionen der Nutzer

### 4.1 Überblick

Die Nutzer haben verschiedenen Möglichkeiten die Netzwerk-Infrastruktur des IMS zu nutzen. Diese unterscheiden sich hinsichtlich der verwendeten Sub-Netzwerke, der Anforderungen an die Bandbreite und/oder an die Sicherheit (Verschlüsselung und Authentifizierungs-verfahren), sowie der ersten Einrichtung.

| | |
|---|---|
| Nutzer Netzwerke<br>**SSID: IMS-Nutzer**<br>Zugangsdaten: von IMS | **Eigenes abgesichertes Netzwerk pro Nutzergruppe im IMS**<br>- WPA2 Enterprise (AES)<br>- WLAN Standard IEEE 802.11n oder neuer IEEE 802.11ac<br>- State-of-the-Art Geräte kompatibel mit WPA2 Enterprise |

| | |
|---|---|
| Pool Netzwerk<br>**SSID: IMS-Pool**<br>Zugangsdaten: von IMS | **Gemeinsames abgesichertes Netzwerk aller Nutzer**<br>- WPA2 Personal (AES / Authentifizierung via PSK)<br>- WLAN Standard IEEE 802.11n oder neuer IEEE 802.11ac<br>- Pool oder Legacy-Geräte und/oder inkompatibel mit WPA2 Enterprise |

| | |
|---|---|
| Gäste Netzwerk<br>**SSID: IMS-Gast**<br>Zugangsdaten: von IMS | **Netzwerk für Besucher/Event-Teilnehmer**<br>- Zugang mittels globalem Browser Passwort<br>- Keine Verschlüsselung sowie Authentifizierung<br>- WLAN Standard 802.11n oder neuer |

**Abbildung 1: Übersicht der Netzwerke im IMS**

### 4.2 Default -Vorgehen (beste Leistung, höchste Sicherheit)

Einrichtung eines eigenen Netzwerks (technisch: dediziertes VLAN) mit eigenen Zugangsdaten (Benutzername und Passwort) innerhalb der ***SSID "IMS-Nutzer"***. Der verwendete Sicherheitsstandard des Funknetzwerks ist WPA2 Enterprise, d.h. die Kommunikation ist mittels des Verschlüsselungsverfahrens "Advanced Encryption Standards (AES)" abgesichert und die Authentifizierung der Benutzer erfolgt Zertifikatsbasiert und erfordert die Akzeptanz des entsprechenden Symantec- Zertifikates, um Nutzer-hardware/Endgeräte einzubinden.

### 4.3 Vorgehen für Legacy/Pool Geräte (reduzierte Leistung und Sicherheit)

Für gemeinsame Geräte, wie Drucker/Scanner, die inkompatibel zum WLAN Standard WPA2 Enterprise sind, wurde das Netzwerk mit der ***SSID "IMS-Pool"*** eingerichtet. Dieses Netzwerk nutzt den Sicherheitsstandard WPA2 Personal, d.h. die Kommunikation ist ebenso wie beim WPA2 Enterprise mittels des Verschlüsselungsverfahrens AES abgesichert, es nutzt aber im Gegensatz zur individuellen Authentifizierung sog. pre- shared keys (PSK). Bitte beachten Sie, dass zu diesem Netzwerk alle Nutzer des IMS sowie das Management des IMS Zugang haben, aber selbstverständlich keine Gäste.

Die Ethernet RJ45-Kabelanschlüsse in den ITK/Drucker-Räume sind mit diesem Netzwerk ***„IMS-Pool“*** verbunden.

### 4.4 Vorgehen für Gäste (geringste Leistung und Sicherheit)

Gäste und/oder Besucher nutzen das Netzwerk mit der ***SSID "IMS-Gast"***. Dieses Netzwerk bietet keine Verschlüsselung sowie Authentifizierung. Der Zugang zu diesem Netzwerk wird mittels Passwort-Eingabe im Browser durchgeführt. Das Passwort ist auf entsprechenden Schildern innerhalb des IMS zu finden und wird vom IMS-Management regelmäßig erneuert.

Alle nicht explizit anders ausgewiesenen Ethernet RJ45-Kabelanschlüsse sind mit diesem Netzwerk ***„IMS-GAST“*** verbunden.

### 4.5 Einrichtung einer eigenen Nutzer SSID

In begründeten Ausnahmefällen kann es für einzelne Nutzer sinnvoll sein eine eigene SSID einzurichten. Diese wären nach dem Standard WPA2-PSK-AES zu verschlüsseln, wobei die Leistung (Speed, Bandbreite) dann für das gesamte IMS-Netzwerk geringer ausfällt als unter 3.1. Daher kann diese Lösung nur auf begründete Ausnahmen beschränkt bleiben.

### 4.6 Einstellungen der Firewall

Eingesetzte Software und/oder Hardware kann es erforderlich machen diverse Ports bzw. Port-Ranges freizuschalten und/oder Weiterleitungen einzelner IP und/oder IP- Ranges festzulegen. Ihre Ansprechpartner (siehe 4.) helfen hierbei.

### 4.7 Anbindung an externe Firmennetze

Nutzer können vom IMS auf Ihr externes Netz (und umgekehrt) über eine sichere VPN- Anbindung zugreifen. Die entsprechenden Einstellungen nehmen **nach Freigabe durch**

**das IMS-Management**, die Ansprechpartner von IT-Dienstleister Quentia und ISP LEWTelNet vor.

### 4.8 Ablauf von Ersteinrichtung und laufender Unterstützung

Das **IMS-Management**, Thomas Dittler, steht als **erster Ansprechpartner** zur Verfügung um die in diesem Leitfaden definierten Vorgehensweisen zu realisieren. Die Anforderungen der Nutzer werden von diesen in geeigneter Weise dokumentiert, die Umsetzung vom IMS-Mangement freigegeben und an unsere Partner **Quentia** und **LEWTelNet** zur Einrichtung weitergeleitet. Die Kosten der einmaligen Ersteinrichtung trägt der IMS, alle weiteren Kosten auf Anfragen der Nutzer werden an diese direkt durch unsere ITK-Partner Quentia und LEW TelNet verrechnet.

Für **weitergehende Fragen** (z.B. Einrichtung VPN, zusätzliche SSIDs, Hilfestellung während der Nutzung, etc.) stehen den Nutzern unsere **ITK-Partner Quentia und LEW TelNet** zur Verfügung. Bitte nochmals um Beachtung, dass hierbei **Kosten** entstehen können, die **nicht** vom Industrial MakerSpace getragen werden. Es ist also im Interesse der Nutzer die ggfs. angefragten Leistungen genau zu spezifizieren und sich im Vorhinein nach den Kosten zu erkundigen.

Unsere ITK-Partner **Quentia** und **LEWTelNet** unterhalten ein **Service-Ticketing System**. Daher sollten immer zusätzlich zu persönlichen Ansprechpartner die E-Mail-Adressen support@quentia.de bzw. service@lewtelnet.de angesprochen werden. Zusätzlich als Kontrolle bitte immer it@industrial-makerspace.com in Kopie nehmen.

### 4.9 Zusammenfassung der Leistungsdaten des Netzwerkes

| Aktuelle Leistung | WLAN | LAN |
|---|---|---|
| Bandbreite | ~ 800 Mbit/s | ~ 1 GBit/s |
| Latenz | ~ 5 ms | ~ 5 ms |

**Abbildung 2: Übersicht über die Leistung der Netzwerke im IMS**

## 5. Kontaktdaten der Ansprechpartner

***IMS-Management (first level support):***
Thomas J. Dittler
Geschäftsführer
E-Mail: td@industrial-makerspace.com
Mobil: +49 (0) 175 2033804

Susann Schmidt-Engelmann
Community Manager
E-Mail: sse@industrial-makerspace.com
Mobil: +49 (0) 172 3835611

***IMS-eigene Systeme (Switches, Router, Server):***
Daniel Andres
Senior Consultant IT, Quentia GmbH
E-Mail: daniel.andres@quentia.de
Tel.: +49 (0) 821 2488 248

***Managed Security („Firewall“)/ Internet-Service:***
Fabian Wrba
Betriebsunterstützung, LEW TelNet GmbH
E-Mail: service@lewtelnet.de
Tel.: +49 (0) 821 328-4050

## 6. Rechte und Pflichten der Nutzer und Haftungsausschluss des IMS

Geräte (z.B. eigene WLAN-Router) und/oder Software (file-sharing Dienste), die den reibungslosen Einsatz der Infrastruktur des IMS behindern bzw. die Leistung anderer Nutzer einschränken, sind nicht erwünscht. Das IMS behält sich ggfs. vor die Nutzer zu bitten entsprechende Geräte vom Netz zu nehmen.

Der IMS haftet nicht für Schäden an den Geräten und Einrichtungen der Nutzer. BYOD (bring your own device) bedeutet u.a. auch, dass die Nutzer für Ihre mitgebrachten und im IMS genutzten Geräte im vollen Umfang eigenverantwortlich sind.

Der IMS haftet nicht für eine Verletzung von Rechten Dritter durch die Nutzer des IMS. Insbesondere gilt dies für eventuelle Verletzung von Software-Copyrights und anderen Software bezogenen Lizenzverletzungen auf Endgeräten der Nutzer, die sich in einem Netzwerk mit Internetanbindung des IMS befinden.

## 7. Geplanter weiterer Ausbau seitens des IMS

7.1. Herstellung der **einfachen Redundanz** durch

- „Internet via Satellite“-Anbindung in Ergänzung der terrestrischen Glasfaserleitung
- Installation von redundanten Back-Up-Systemen für Router und Firewall

7.2 Installation eines **USV-fähigen Batteriesystemes**, das den kompletten Nebenverteiler speist (TGA und Büro, 2 h min.)

7.3 **LAN/RJ45 – Access an allen Arbeitsplätzen** (IMS Pool und IMS Gast)

Ende

## Anlage:

Übersicht über die Architektur des IMS-Netzwerkes (Version 1.8)