**Systemdokumentation**

**Kundenname**

**Just Relax ICT**

Hauptstrasse 66

CH-4410 Liestal

Autor: Otto Normalverbraucher

Dokumentation vom: 01. Oktober 2017

Letzte Änderung: 27. Oktober 2019

Dateiname: Systemdokumentation\_V1-0.docx

Version: 1.0

Status: Final

# Change Management

|  |  |  |  |
| --- | --- | --- | --- |
| *Datum* | *Version* | *Autor* | *Bemerkung* |
| 01.05.2020 | 0.1 | ON | Erstellung Grundstruktur |
| 01.05.2020 | 0.2 | ON | Erfassung von LAN, DMZ, WAN |
| 03.05.2020 | 0.3 | ON | Verfassung fixe IPs, IP-Konzept |
| 05.05.2020 | 0.4 | ON | Hinterlegen von Kennwörtern |
| 20.05.2020 | 0.5 | ON | Berechtigungsmatrix |
| 21.05.2020 | 0.6 | ON | Installierte Software |
| 27.05.2020 | 1.0 | ON | Letzte Korrekturen, Übergabe an Kunde |
|  |  |  |  |

**Inhaltsverzeichnis**

Change Management 2

Netzwerk Kundenname 4

Netzwerkplan 4

Betriebene Netzwerk und deren Funktion 5

WAN – Swisscom 5

LAN – Produktives Netzwerk 5

DMZ – Demilitarisierte Zone 6

IP-Adresskonzept 6

Local Area Network (LAN) 6

Fixdefinierte IP-Adressen 7

Adressierung der Hosts 8

DHCP innerhalb LAN 8

Namenskonvention für Hosts 8

Domäne/Workgroup 8

Hardware-Übersicht 9

HPE ProLiant ML350 Gen4 9

Software-Übersicht 11

Zugriffskonzept 12

Backup 13

Nutz-/Konfigurationsdaten 13

Virtuelle Instanzen 13

Passwörter 14

# Netzwerk Kundenname

## Netzwerkplan

**NOCH NICHT VORHANDEN – SIEHE SEPERATES DOKUMENT**

## Betriebene Netzwerk und deren Funktion

Das Netzwerk von „unserem Kunden wird mittels einer Firewall geschützte. Die Sicherheits-Appliance verwaltet folgende Netzwerke (folglich genauer erläutert):

* WAN (Internet-Anschluss)
* LAN (Lokales Netzwerk)
* DMZ (DMZ, vorhanden jedoch nicht konfiguriert)

Die komplette Kommunikation zwischen den betriebenen Netzwerken wird mittels Firewall koordiniert und nur gemäss Konfiguration (Rule-Set) erlaubt.

Die Firewall selbst wurde nicht durch Just Relax ICT geliefert und konfiguriert.

### WAN – Swisscom

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | Internet-Anschluss |
| *Hersteller* | Unbekannt |
| *Verbindungstyp* | Ethernet |
| *Abo-Typ* | Unbekannt |
| *Netz* | Unbekannt |
| *Netzmaske* | Unbekannt |
| *Fixe IP-Adressen* | DHCP, keine fixe IP |
| *DNS-Server* | 8.8.8.8 |
| *Business Support* | nein |

### 

### LAN – Produktives Netzwerk

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | Produktives Netzwerk |
| *Hersteller* | Unbekannt |
| *IP-Adresse* | 172.16.16.0 / 24 |
| *DHCP aktiviert* | Unbekannt |
| *DHCP-Scope* | Unbekannt |

### 

### DMZ – Demilitarisierte Zone

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | Zone für externe Zugriffe, getrennt von LAN |
| *Hersteller* | Unbekannt |
| *IP-Adresse* | 10.110.120.0 / 29 |
| *DHCP aktiviert* | Unbekannt |
| *DHCP-Scope* | Unbekannt |

### 

## IP-Adresskonzept

### Local Area Network (LAN)

Das IP-Adress-Konzept beruht auf einer 24iger Subnetzmaske (255.255.255.0), welche die Adressierung von 28 möglichen Host bzw. Endgeräten im gleichen Netz ermöglicht (256 Stück; abzüglich der Netzwerkadresse und der Broadcast-Adresse; = 254 Hosts).

|  |  |  |
| --- | --- | --- |
| *IP-Range* | *Host-Typ* | *Anz. Möglicher Adressierung* |
| 172.16.16. 0 | Netzwerkadresse | - |
| 172.16.16. 1 – 9 | Security | 9 Stück |
| 172.16.16. 10 – 19 | Server | 10 Stück |
| 172.16.16. 20 – 29 | Wireless-Komponenten | 10 Stück |
| 172.16.16. 30 – 39 | Drucker | 10 Stück |
| 172.16.16. 40 – 99 | Reserve | 50 Stück |
| 172.16.16. 100 – 199 | DHCP-Scope | 100 Stück |
| 172.16.16. 200 – 209 | Kassen-Systeme | 10 Stück |
| 172.16.16. 254 | SecurePoint Firewall | 1 Stück |
| 172.16.16. 255 | Broadcastadresse | - |

**NOCH NICHT REALISIERT – DIENT NUR ALS VORLAGE!**

## Fixdefinierte IP-Adressen

|  |  |  |
| --- | --- | --- |
| *IP-Range* | *Hostname* | *Funktion* |
| 172.16.16.0 | - | Netzadresse |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| 172.16.16.255 | - | Broadcast |

**Per Juni 2021 nicht mehr gültig!**

|  |  |  |
| --- | --- | --- |
| *IP-Range* | *Hostname* | *Funktion* |
| 172.16.16.1 | NET-FW01 | **Firewall**  pfSense |
| 172.16.16.20 | NET-AP01 | **AccessPoint**  TP-LINK TL-WA901ND |
| 172.16.16.30 | NET-PR01 | **Stockwerk-Drucker 1. OG**  HP LaserJet 3050 |
| 172.16.16.31 | NET-PR02 | **Stockwerk-Drucker EG**  HP LaserJet 3050 |
| 172.16.16.40 | SRV-FS01 | **Datei-Server**  NAS4Free |
| 172.16.16.41 | SRV-PR01 | **Server für diverse Serverdienste**  Print, DNS, DHCP **(existiert noch nicht)** |

## Adressierung der Hosts

Die Zuteilung der IP-Adressen ist mittels Dynamic Host Configuration Protocol (kurz: DHCP) sichergestellte – bzw. Reservierungen auf dem DHCP-Server (siehe DHCP-Scope in der jeweiligen Netzwerk-Tabelle).

### DHCP innerhalb LAN

|  |  |
| --- | --- |
| *DHCP Scope* | 172.16.16.1 – 172.16.16.254  (nicht von **Just Relax ICT** konfiguriert – zu überarbeiten) |
| *Gateway* | 172.16.16.254 |

## Namenskonvention für Hosts

Für die Namensgebung (Hostnamen) innerhalb des Netzwerkes gelten folgende Konventionen, die es zu beachten gilt. Für die Namensgebung Computer/Notebook wird auf eine nichtstandortbezogene Lösung zurückgegriffen (keine Unterscheidungen der einzelnen Standorte).

In der folgenden Tabelle sind exemplarisch einige Hostnames dargestellt. Für eine genaue Übersicht der einzelnen Hostnames, konsultieren Sie bitte das aktuelle IP-Konzept.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Host-Typ* | *Präfix* | *Zusatz* | *Lauf-Nr.* | *Bsp. Hostname* |
| Firewall | NET | FW | 01 | NET-FW01 |
| File-Server | SRV | FS | 01 | SRV-FS01 |
| Netzwerk-Switch | NET | SW | 01 | NET-SW01 |
| PC | CLN | PC | 01 | CLN-PC01 |
| Notebook | CLN | NB | 01 | CLN-NB01 |
| Printer/Drucker | NET | PR | 01 | NET-PR01 |

## Domäne/Workgroup

Der Domänenname/Workgroup-Name (logische Netzwerkeinteilung) der Umgebung wurde wie folgt definiert: **m157.intra**

Hardware-Übersicht

## HPE ProLiant ML350 Gen6

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | HP ProLiant ML350 Gen6 |
| *Funktion* | **Typ-1 Hypervisor** (VMWare ESXi) |
| *Serien-Nummer* | CZ180431DF |
| *Standort* | Büro 1. OG |
| *ILO* | Administrator / ads3-rER |
| *IP-Adresse / Hostname* | 172.16.16.201 / SRV-HV01 |
| *Arbeitsspeicher* | 16 GB (2x 8GB) |
| *Harddisk* | **RAID 1 – System-Installation / Data Store VMs**  1x HPE 256 GB – SATA – 7200RPM S/Nr. MYE666202D Bay 1 1x HPE 256 GB – SATA – 7200RPM S/Nr. MYE666203D Bay 2 |
| *Netzwerk* | 2x OnBoard NICs |
| *Übersicht* | HP ProLiant ML350 G6 Tower Server | Configure-to-Order |

## TP-Link 24 Port Switch TL-SG1024DE

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | Netgear ProSafe JGS524E Gigabit Ethernet |
| *Funktion* | Switching |
| *Serien-Nummer* | unbekannt |
| *IP-Adresse / Hostname* | unbekannt |
| *Übersicht* | NETGEAR ProSafe JGS524E Gigabit Ethernet 24-Port Switch [1000 MBit/s, QoS, VLAN, lüfterlos] |

## TP-Link TL-WA901ND

|  |  |
| --- | --- |
| *Typ / Bezeichnung* | TP-Link: TL-WA901ND |
| *Hostname* | NET-AP01 |
| *IP-Adresse* | 172.16.16.20 |
| *MAC-Adresse* | 50-C7-BF-8D-EF-6E |
| *Garantie bis* | September 2017 *(Kauf seitens Kunde bei MediaMarkt - 2015)* |
| *Funktion* | WLAN-AccessPoint |
| *Zugangsdaten Administration* | User: admin Passwort: gibbiX12345 |
| *SSID* | Kunden-Netzwerk |
| *PreShared Key* | **Sonne1234** |
| *Übersicht* |  |

Software-Übersicht

|  |  |
| --- | --- |
| *Software* | **Fakturama** |
| *Version* | unbekannt |
| *Anbieter* | Ralf Heydenreich & Diverse |
| *Lizenzschlüssel* | OpenSource |
| *Installiert auf* | vmWP1 |

|  |  |
| --- | --- |
| *Software* | **Putty** |
| *Version* | unbekannt |
| *Anbieter* | Simon Tatham |
| *Lizenzschlüssel* | OpenSource |
| *Installiert auf* | vmWP1 |

|  |  |
| --- | --- |
| *Software* | **WinSCP** |
| *Version* | unbekannt |
| *Anbieter* | Martin Přikryl |
| *Lizenzschlüssel* | OpenSource |
| *Installiert auf* | vmWP1 |

|  |  |
| --- | --- |
| *Software* | **NAS4Free** |
| *Version* | 11.1.0.4 |
| *Anbieter* | unbekannt |
| *Lizenzschlüssel* | OpenSource |
| *Installiert auf* | SRV-FS01 |

|  |  |
| --- | --- |
| *Software* | pfSense |
| *Version* | 2.3.4 |
| *Anbieter* | pfSense Projekt |
| *Lizenzschlüssel* | OpenSource |
| *Installiert auf* | NET-FW01 |

Zugriffskonzept

Die hier hinterlegte Tabelle definiert, wer auf welche Netzwerkfreigabe Zugriffs- und Mutationsrechte hat:

Ein Bild, das Tisch enthält.

Automatisch generierte Beschreibung

**Zugriffskonzept noch nicht realisiert, da SRV-FS01 noch nicht mit FreeNAS aufgesetzt wurde und die Daten noch nicht migriert sind. Daher sind im Moment alle Freigaben für alle bereits erfassten Benutzer auf „rw“ gesetzt.**

**Da der Speicher jedoch bereits produktiv betrieben wird, muss bei der Datenmigration darauf geachtet werden, dass die Meta-Daten der Ordner/Dateien (Ower, Timestamp ERSTELLT, Timestamp GEÄNDERT etc.) korrekt übernommen werden.**

Backup

## Nutz-/Konfigurationsdaten

Die Sicherung der Daten wird mittels Copy-Job täglich sichergestellt. Die zu sichernden Daten werden auf die NAS (NAS-FS01) geschrieben (**noch nicht vorhanden**), welche über ein Speichervolumen von rund 3.85 TB verfügt sollte.

|  |  |
| --- | --- |
| *Tägliches Backup* | **1) Montag – Sonntag 19:00 bis 20:45 Uhr** (jeweils zur Viertelstunde)  **2) Montag – Samstag 21:00 Uhr** (auf GoogleDrive verschlüsselt) |
| *Typ* | Inkrementell bzw. Vollbackup (Änderungssicherung) |
| *Montag – Sonntag* | Bis zu 100 Versionen (je Kalendertag), je nach Datenvolumen |
| *Tool* | 1) via Robocopy-Skript von Server (DB-Server) auf NAS  2) via Hyper-Backup von NAS auf DropBox (verschlüsselt) |
| *Sicherungsziel* | \\172.16.16.10\Backup-Data  🡪 Kopie täglich zu GoogleDrive |
| *Info* | Sicherungsabschlüsse werden in jedem Fall auf ict@gtg-ict.ch gemeldet (Cloud-Sync). |
| *Backup User (NFS)* | backup |
| *Backup Password (NFS)* | -.Save2017.- |
| *Key für Verschlüsselung* | **.#Backup---2017#.** |

## Virtuelle Instanzen

Die Sicherung der virtuellen Maschinen wird mittels wöchentlicher Sicherung realisiert. Die zu sichernden Daten werden auf die NAS (NAS-FS01) geschrieben, welche über ein Speichervolumen (für VM-Backup) von rund 3.85 TB verfügt.

|  |  |
| --- | --- |
| *Wöchentliches Backup* | **Sonntag 05:00 Uhr** |
| *Typ* | Vollbackup |
| *Tool* | OnBoard-Mittel von Windows Server |
| *Sicherungsziel* | \\172.16.16.10\Backup-VMs |
| *Backup User (NFS)* | backup |
| *Backup Password (NFS)* | -.Save2017.- |

# Passwörter

|  |  |  |  |
| --- | --- | --- | --- |
| **Hostname** | **Zugriff via** | **Benutzername** | **Passwort** |
| NET-FW01 | https://172.16.16.199 sollte noch geändert werden | admin | gibbiX12345 |
| SRV-FS01 | http://10.110.120.4 | admin | gibbiX12345 |
| vmWP1 | direkt | vmadmin | gibbiX12345 |
| - | Proxy-User für BBZBL | m157.proxy | G1Bm33#!# |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Stand: **Oktober 2019**