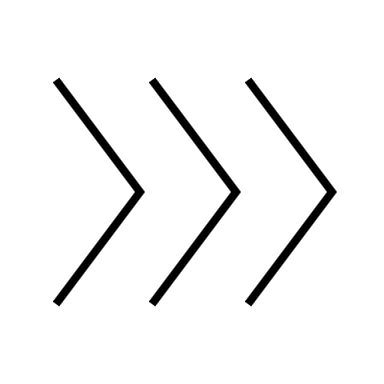
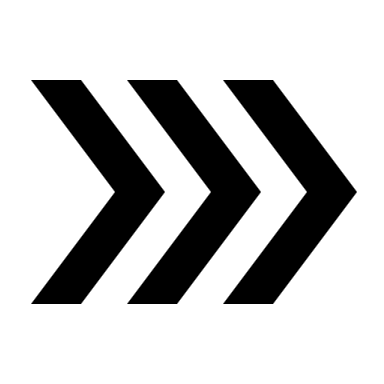
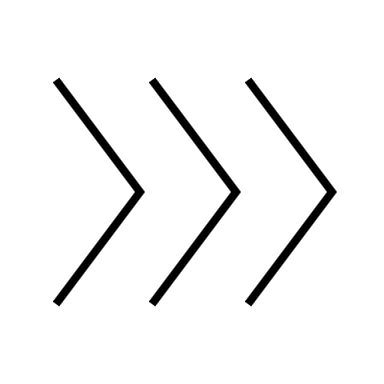
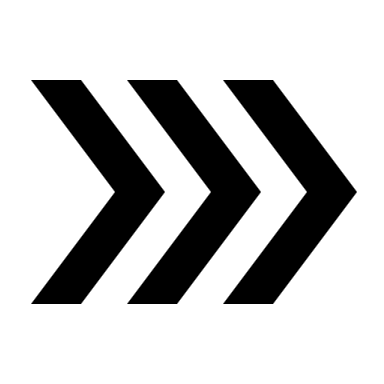
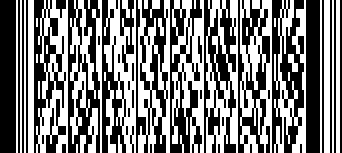
**CONFIDENTIAL INFORMATIONS**





**Authorised persons and**

**organizations**

**Security notice**

This document is subject to medical confidentiality and may not be disclosed without the consent of the owner.

Project ResilienceResilienceEventX AG is released exclusively to the following persons or organizations.

The certificate of authorization and the release are stored in the footer note.

**EventX AG**

**Migration**

Inhalt

[Management Summary 3](#_Toc148383180)

[IST Situation 3](#_Toc148383181)

[Soll Zustand 3](#_Toc148383182)

[Ausgangslage 4](#_Toc148383183)

[Aktueller Netzwerkplan 4](#_Toc148383184)

[Vorgehensplanung 5](#_Toc148383185)

[Konzepte 7](#_Toc148383186)

[Netzwerkkonzept 7](#_Toc148383187)

[IP-Adresskonzept 7](#_Toc148383188)

[WAN - Swisscom 8](#_Toc148383189)

[LAN 9](#_Toc148383190)

[DMZ 10](#_Toc148383191)

[Fixe Adressen 10](#_Toc148383192)

[Namenskonzept 13](#_Toc148383193)

[Firewallkonzept 13](#_Toc148383194)

[Backupkonzept 14](#_Toc148383195)

[Zugriffskonzept 16](#_Toc148383196)

[Gruppen- und Nutzerkonzept 16](#_Toc148383197)

[Passwortkonzept 16](#_Toc148383198)

[Offerte Neuanschaffung 17](#_Toc148383199)

[Server 17](#_Toc148383200)

# Management Summary

## IST Situation

Das Migrationsprojekt wurde von der Firma Just Relax ICT angefangen, jedoch nicht zu Ende geführt, da die Firma Konkurs angemeldet hat. Die Migration muss nun überprüft und überarbeitet werden.

Die Firma EventX AG organisiert Privat- und Firmenanlässe und hat einen guten Ruf als seriöses und zuverlässiges Unternehmen.

# Soll Zustand

Anhand der Systemdokumentation gehen folgende Aufgaben hervor:

* Netzwerkplan überarbeiten
* IP-Adresskonzept überarbeiten
  + Für bestimmte Geräte und Anwendungen wird ein separates Subnetz benötigt.
  + Fix definierte Adressen angeben und überarbeiten
* Software prüfen
* Zugriffskonzept überarbeiten
* Backupkonzept überarbeiten
* Passwörter überarbeiten
* Bestehende Hardware aufnehmen
* Neue Hardware evaluieren
* Neue Hardware beschaffen und in Betrieb nehmen
* Aktuelle Systeme aktualisieren
* Testszenarien ausarbeiten und durchführen.

# Ausgangslage

Die Systemdokumentation wurde nicht fertiggestellt und muss überprüft und überarbeitet werden. Die Konzepte müssen ebenfalls überprüft und allenfalls überarbeitet werden. Es müssen aber auch Konzepte von Grund auf neu erarbeitet werden. Die Migration wird zusätzlich erschwert, da der Prozess mittendrin abgebrochen wurde und die Systeme sowie Dokumentationen in einem Migrationszustand sind, welcher zuerst mit viel Aufwand verifiziert werden muss.

## Aktueller Netzwerkplan

Ein Bild, das Text, Diagramm, Plan, Karte enthält.

Automatisch generierte Beschreibung

# Vorgehensplanung

|  |  |  |
| --- | --- | --- |
| **IST-Situation** | **SOLL-Situation** | **Machbarkeit** |
| Netzwerkkonzept wurde nur teilweise konzeptioniert, wurde jedoch noch nicht umgesetzt. Netzwerkplan wurde noch nicht finalisiert. | Netzwerkkonzept fertigstellen und umsetzen.  Netzwerkplan muss fertiggestellt werden. | IP-Adressierung prüfen und konzeptionieren. Netzwerkplan muss überprüft und überarbeitet werden. |
| Firewallkonzept ist nicht ausgereift und muss überarbeitet werden | Firewallkonzept ist fertig und sicher konzeptioniert. | Firewall muss überprüft und neu konfiguriert werden. |
| Backupkonzept ist fertig, muss jedoch noch überprüft und eventuell überarbeitet werden. | Neues Backupkonzept ist ausgearbeitet und umgesetzt. | Backupkonzept muss überprüft werden. Anhand der vorhandenen Informationen werden die Systeme geprüft und es wird ein Backup erstellt. Anhand des neuen Konzepts werden dann die Systeme gesichert. |
| Hardware muss aufgenommen werden und überarbeitet werden. | Neue Hardware ist evaluiert und aufgesetzt. | Es muss neue Hardware evaluiert werden und dementsprechend aufgesetzt und eingerichtet werden. Es muss unbedingt ein HW Standard erarbeitet werden, um die Kompatibilität zu gewährleisten. |
| Zugriffe sind nicht richtig gesetzt und es wird ein neues Konzept benötigt. | Zugriffe sind nach Kundenwunsch konzeptioniert, eingerichtet und dokumentiert. | Das Zugriffskonzept muss überprüft und nach Kundenwunsch angepasst werden. |
| Namenskonzept ist noch nicht ausgereift und muss überarbeitet werden. | Namenskonzept ist fertiggestellt und die Geräte werden dementsprechend benannt. | Das Namenskonzept muss überprüft und neu gemacht werden. |



# Konzepte

## Netzwerkkonzept

### IP-Adresskonzept

LAN

Im LAN Bereich werden mehrere 24iger Subnetze verwendet, um die Geräte voneinander zu trennen und zu unterscheiden. Es wird somit ein Subnetz für Clients, Printer, Networkmanagement, Kassensysteme und Security geben.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Netz** | **Subnetz** | **Typ** | **Adressierung** | **Anz. Hosts** | **VLAN** |
| 172.16.16.0 | 24 | Clients | DHCP | 254 | 16 |
| 172.16.17.0 | 24 | Printer | Statisch | 254 | 17 |
| 172.16.18.0 | 24 | Server | Statisch | 254 | 18 |
| 172.16.241.0 | 24 | Management | Statisch | 254 | 241 |
| 172.16.240.0 | 24 | Security | Statisch | 254 | 240 |
| 172.16.30.0 | 24 | Kassen | Statisch | 254 | 30 |
| 10.110.210.0 | 24 | DMZ | Statisch | 254 | 210 |

|  |  |
| --- | --- |
| **Typ** | **Beschreibung** |
| Clients | In diesem Bereich befinden sich alle Clients. Mit Clients werden alle Geräte eines Benutzers gemeint, also Notebook, Workstation und allenfalls noch Smartphone. |
| Printer | In diesem Bereich befinden sich alle Drucker, welche mit dem Netzwerk verbunden sind. |
| Server | In diesem Bereich befinden sich alle internen Server, die keinen Zugang zum Internet haben und auch nur von Intern erreichbar sein müssen. |
| Management | In diesem Bereich sind alle Management Adressen erreichbar.  FW Management  Switch Management  Accesspoint Management  Server Management (ILO) |
| Security | In diesem Bereich werden alle Security relevanten Systeme ihren Platz finden. Dies können Kameras, Badge gesicherte Türen oder auch weitere Zutrittssysteme betreffen. |
| Kassen | In diesem Bereich werden die Kassensysteme ihren Platz finden, welche über das Netzwerk angesteuert werden. |
| DMZ | In diesem Bereich werden die Server untergebracht, welche einen Internetzugang haben werden. Diese sind dann auch von ausserhalb der Firma erreichbar und beheimaten unteranderem auch die Firmen Website. |

### WAN - Swisscom

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Internet-Anschluss |
| **Hersteller** | Swisscom |
| **Verbindungstyp** | Ethernet |
| **Abo Typ** | Unbekannt |
| **Netz** | Unbekannt |
| **Netzmaske** | Unbekannt |
| **Fixe-IP-Adressen** | Fixe IP |
| **DNS** | 8.8.8.8 |
| **Business Support** | Nein |

### LAN

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Clients |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.16.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Ja |
| **DHCP-Scope** | 172.16.16.20 – 172.16.16.200 |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.16.1 |
| **VLAN** | 16 |

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Printer |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.17.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.17.1 |
| **VLAN** | 17 |

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Server |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.18.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.18.1 |
| **VLAN** | 18 |

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Management |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.241.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.241.1 |
| **VLAN** | 241 |

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Security |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.240.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.240.1 |
| **VLAN** | 240 |

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | Kassen |
| **Hersteller** | Unknown |
| **IP-Adresse** | 172.16.30.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 172.16.30.1 |
| **VLAN** | 30 |

### DMZ

|  |  |
| --- | --- |
| **Typ / Bezeichnung** | DMZ |
| **Hersteller** | Unknown |
| **IP-Adresse** | 10.110.210.0/24 |
| **Netzmaske** | 255.255.255.0 |
| **DHCP** | Nein |
| **DHCP-Scope** | Unknown |
| **DNS** | 172.16.18.25 |
| **Default Gateway** | 10.110.210.1 |
| **VLAN** | 210 |

### Fixe Adressen

|  |  |  |
| --- | --- | --- |
| **IP (Range)** | **Hostname** | **Funktion** |
| 172.16.16.1 | CHEBSFW01 | Default-Gateway Client |
| 172.16.17.1 | CHEBSFW01 | Default-Gateway Printer |
| 172.16.18.1 | CHEBSFW01 | Default-Gateway Server |
| 172.16.241.1 | CHEBSFW01 | Default-Gateway Management |
| 172.16.240.1 | CHEBSFW01 | Default-Gateway Security |
| 172.16.30.1 | CHEBSFW01 | Default-Gateway Kassen |
| 10.110.210.1 | CHEBSFW01 | Default-Gateway DMZ |
|  |  |  |
| 172.16.16.2 | CHEBSFW02 | FW Failover |
| 172.16.17.2 | CHEBSFW02 | FW Failover |
| 172.16.18.2 | CHEBSFW02 | FW Failover |
| 172.16.241.2 | CHEBSFW02 | FW Failover |
| 172.16.240.2 | CHEBSFW02 | FW Failover |
| 172.16.30.2 | CHEBSFW02 | FW Failover |
| 10.110.210.2 | CHEBSFW02 | FW Failover |
|  |  |  |
| 172.16.241.3 | \* | FW Failover Com |
| 172.16.241.4 | CHEBSFW01 | MGMT |
| 172.16.241.5 | CHEBSFW02 | MGMT |
| 172.16.241.11 | CHEBSEGSW01 | MGMT |
| 172.16.241.12 | CHEBSEGSW02 | MGMT |
| 172.16.241.13 | CHEBSOG1SW01 | MGMT |
| 172.16.241.14 | CHEBSOG1SW02 | MGMT |
| 172.16.241.41 | CHEBSEGAP01 | MGMT |
| 172.16.241.42 | CHEBSEGAP02 | MGMT |
| 172.16.241.43 | CHEBSOG1AP01 | MGMT |
| 172.16.241.44 | CHEBSOG1AP02 | MGMT |
| 172.16.241.101 | CHEBSESXILO01 | MGMT |
| 172.16.241.102 | CHEBSESXILO02 | MGMT |
| 172.16.241.103 | CHEBSESXILO03 | MGMT |
| 172.16.241.104 | CHEBSESXILO04 | MGMT |
|  |  |  |
| 172.16.18.21 | CHEBSESX01 | ESXi Host |
| 172.16.18.22 | CHEBSESX02 | ESXi Host |
| 172.16.18.23 | CHEBSESX03 | ESXi Host |
| 172.16.18.24 | CHEBSESX04 | ESXi Host |
| 172.16.18.25 | VCHEBSDNS01 | DNS Server |
| 172.16.18.26 | VCHEBSDNS02 | DNS Server |
| 172.16.18.27 | VCHEBSDHCP01 | DHCP Server |
| 172.16.18.28 | VCHEBSDHCP02 | DHCP Server |
| 172.16.18.29 | VCHEBSPRN01 | Print Server |
| 172.16.18.30 | VCHEBSPRN02 | Print Server |
| 172.16.18.31 | VCHEBSSRV01 | Kassen Server |
| 172.16.18.32 | VCHEBSSRV02 | Kassen Server |
| 172.16.18.33 | VCHEBSSQL01 | SQL Datenbank Server |
| 172.16.18.34 | VCHEBSSQL02 | SQL Datenbank Server |
| 172.16.18.35 | CHEBSNAS01 | NAS |
| 172.16.18.36 | CHEBSNAS01 | NAS |
| 172.16.18.37 | CHEBSNASCAM01 | Kamera NAS |
| 172.16.18.38 | CHEBSNASCAM02 | Kamera Nas |
| 172.16.18.39 | CHEBSFS01 | Fileserver |
| 172.16.18.40 | CHEBSFS02 | Fileserver |
|  |  |  |
| 172.16.240.21 | CHEBSSEC01 | Zutrittssteuerung |
| 172.16.240.22 | CHEBSSEC01 | Zutrittssteuerung |
| 172.16.240.51 | CHEBSCAM01 | Kamera |
| 172.16.240.52 | CHEBSCAM02 | Kamera |
| 172.16.240.53 | CHEBSCAM03 | Kamera |
| 172.16.240.54 | CHEBSCAM04 | Kamera |
| 172.16.240.55 | CHEBSCAM05 | Kamera |
| 172.16.240.56 | CHEBSCAM06 | Kamera |
|  |  |  |
| 172.16.30.21 | CHEBSKZKS01 | Kasse |
| 172.16.30.22 | CHEBSKZKS02 | Kasse |
| 172.16.30.23 | CHEBSKZKS03 | Kasse |
| 172.16.30.24 | CHEBSKZKS04 | Kasse |
|  |  |  |
| 10.110.210.21 | VCHEBSFS01 | File Server DMZ |
| 10.110.210.22 | VCHEBSWEB01 | Webserver |
| 10.110.210.23 | VCHEBSWEB02 | Webserver |

## Namenskonzept

Die Hostnamen der mobilen Geräte werden simpel gehalten, damit diese nicht an einen Standort oder Ort gebunden sind und dann einfach nicht mehr da sind. Für die Stationären Geräte werden jedoch auch Standortbezogene Daten im Namen angegeben.

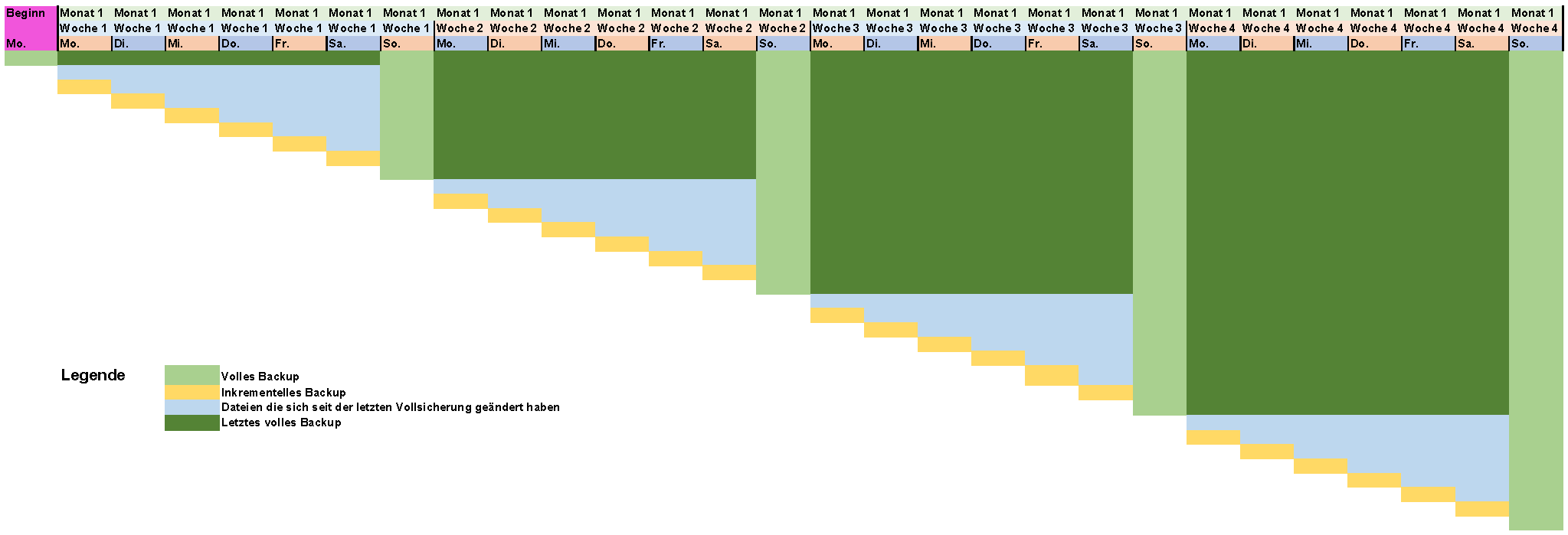
Für Server werden lediglich die Angaben zum Standort benötigt. Bei den Netzwerkgeräten und Kassensystemen wird eine zusätzliche Angabe benötigt. Für die Switches wird das Stockwerk benötigt und auch bei den Accesspoints wird das Stockwerk mit angegeben. Für die Firewall wird diese Information nicht benötigt, da diese immer im Rechenzentrum zu finden ist. Selbes gilt für die Server, denn diese sind ebenfalls nur im Rechenzentrum zu finden. Bei virtuellen Servern gilt zusätzlich, dass ein V vorangestellt wird. Bei physischen Servern wird lediglich auf das V verzichtet. Sollte es sich um einen Dienst handeln, der auf dem Server läuft, wird der Dienst als Kürzel angegeben anstelle des SRV.

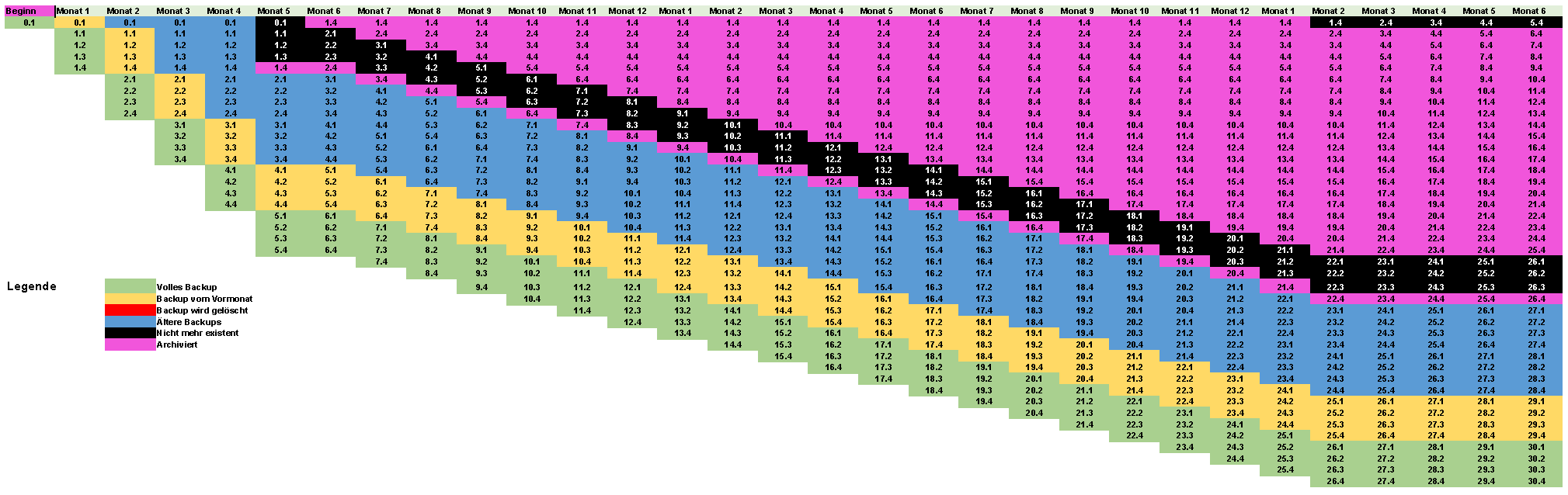
Die Kassensysteme haben den Kürzel KZ noch mit dabei, damit man weiss ob es sich um ein Kassensystem im Kundenzentrum handelt oder um eine in der Kantine. Sollte kein KZ im Namen vorhanden sein, dann handelt es sich um ein Kassensystem in der Kantine.

|  |  |  |  |
| --- | --- | --- | --- |
| Standort | Typ | Laufnummer | Hostname |
| \* | NB (Notebook) | 0001 | NB0001 |
| \* | WS (Workstation) | 0001 | WS0001 |
| \* | PRN (Printer) | 001 | PRN001 |
| (V) CHE BS  (Schweiz/Basel) | SRV (Server)  DNS (DNS Server)  ESX (ESXi Host) | 01 | CHEBSSRV01  VCHEBSDNS01  CHEBSESX01 |
| CHE ZH | NAS | 01 | CHEZHNAS01 |
| CHE BS EG  (Schweiz/Basel  Erdgeschoss) | SW (Switch) | 01 | CHEBSEGSW01 |
| CHE BS OG1 | AP (AccessPoint) | 001 | CHEBSOG1AP001 |
| CHE ZH | FW (Firewall) | 01 | CHEZHFW01 |
| CHE BS KZ  (Schweiz/Basel  Kundenzentrum) | KS (Kassensystem) | 01 | CHEBSKZKS01 |

## Firewallkonzept

## Backupkonzept





## Zugriffskonzept

## Gruppen- und Nutzerkonzept

## Passwortkonzept

# Offerte Neuanschaffung

## Server

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Artikel | Beschr. | Preis | Anz. | Total |
| HPE ML350 | HPE ProLiant ML350 G9 8SFF | 929.- | X2 | 1’858.- |
| Intel Xeon | Intel Xeon E5-2680v3 | 33.- | X2 | 66.- |
| 32GB DDR4 | 32GB DDR4 RDIMM 2400MHz | 39.- | X16 | 624.- |
| iLO4 Std. | iLO4 Standard Lizenz | Inkl. | X2 |  |
| HP 500W | Powersupply HP 500W | 21.- | X2 | 42.- |
| 4x 1GB RJ45 | 4x 1GB RJ45 PCI-e | 21.- | X2 | 42.- |
| SSD 480GB | SSD 48GB SATA 2.5 + Caddy | 79.- | X16 | 1’264.- |
| **TOTAL** |  |  |  | **3’869.-** |