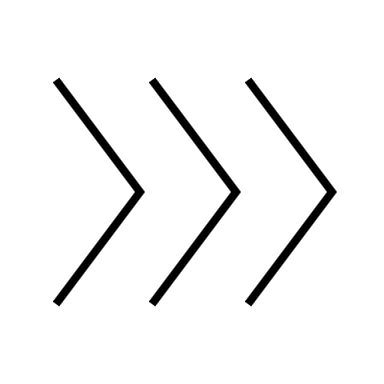
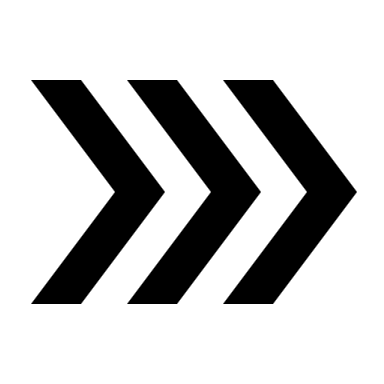
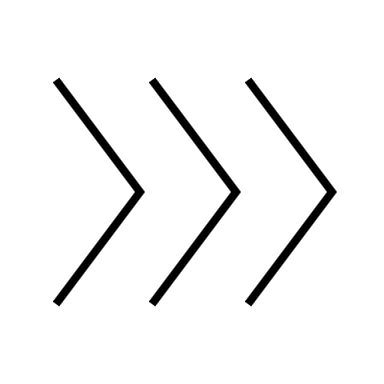
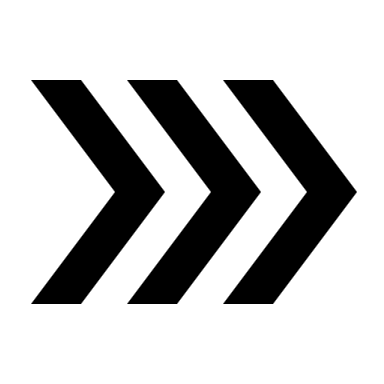
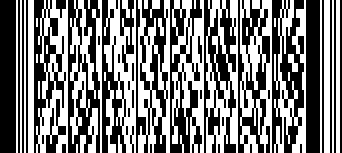
**CONFIDENTIAL INFORMATIONS**





**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](#_Toc149920081)

[IST Situation 3](#_Toc149920082)

[Soll Zustand 3](#_Toc149920083)

[Ausgangslage 4](#_Toc149920084)

[Aktueller Netzwerkplan 4](#_Toc149920085)

[Vorgehensplanung 5](#_Toc149920086)

[Konzepte 7](#_Toc149920087)

[Netzwerkkonzept 7](#_Toc149920088)

[IP-Adresskonzept 7](#_Toc149920089)

[WAN - Swisscom 8](#_Toc149920090)

[LAN 9](#_Toc149920091)

[DMZ 10](#_Toc149920092)

[Fixe Adressen 10](#_Toc149920093)

[Netzwerkplan 13](#_Toc149920094)

[Namenskonzept 14](#_Toc149920095)

[Firewallkonzept 15](#_Toc149920096)

[Backupkonzept 16](#_Toc149920097)

[Zugriffskonzept 18](#_Toc149920098)

[Gruppen- und Nutzerkonzept 19](#_Toc149920099)

[User 19](#_Toc149920100)

[Gruppen 20](#_Toc149920101)

[Passwortkonzept 21](#_Toc149920102)

[Testszenarien 22](#_Toc149920103)

[Offerte Neuanschaffung 23](#_Toc149920104)

[Server 23](#_Toc149920105)

[Netzwerkgeräte 23](#_Toc149920106)

[Lizenzen 23](#_Toc149920107)

[Arbeit 24](#_Toc149920108)

[Wichtige Hinweise 24](#_Toc149920109)

[Selbstständigkeitserklärung 25](#_Toc149920110)

# 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

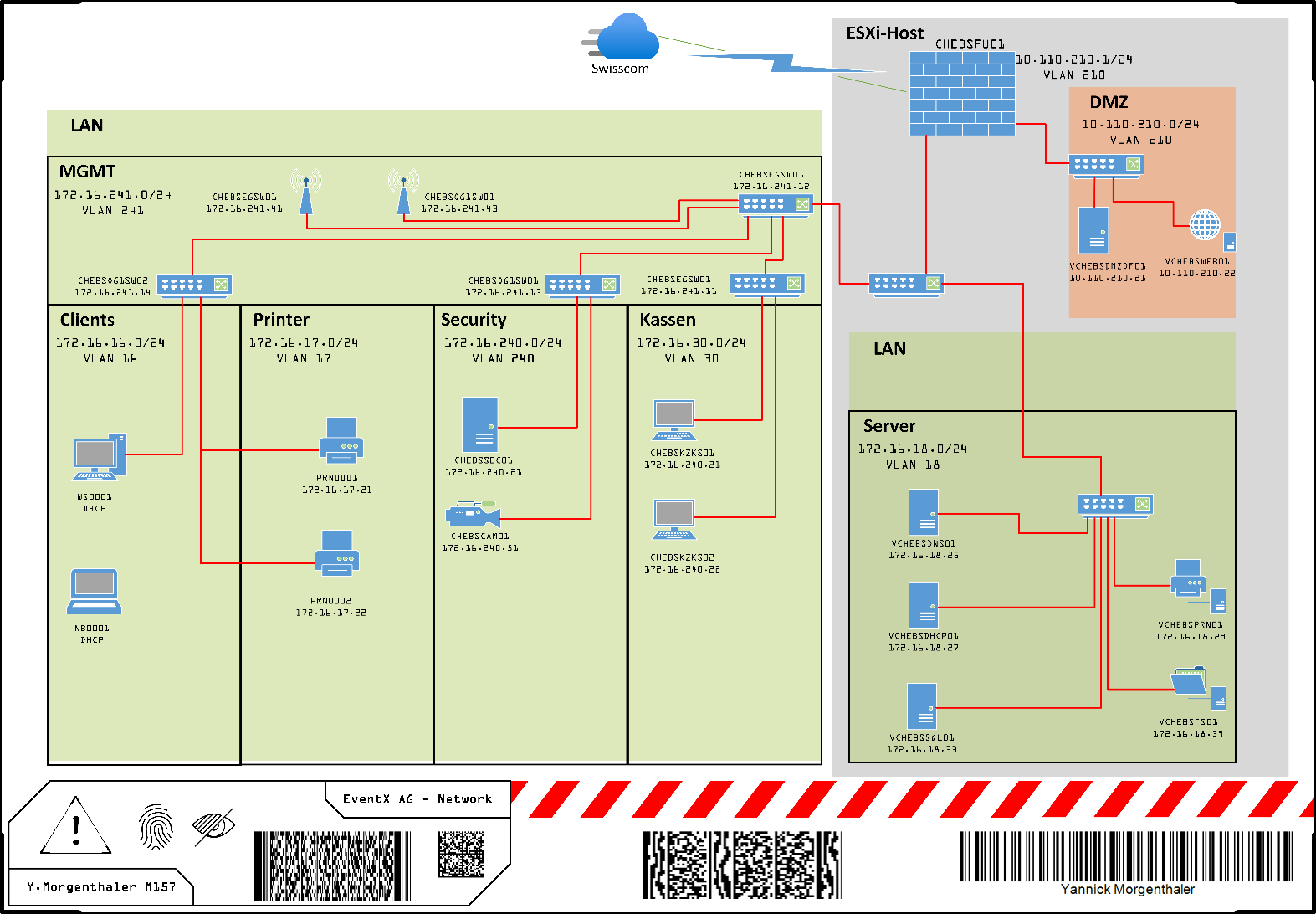
|  |  |  |
| --- | --- | --- |
| **IP (Range)** | **Hostname** | **Funktion** |
| 172.16.16.1 | CHEBSFW01 | Default-Gateway Client |
| 172.16.17.1 | CHEBSFW01 | Default-Gateway Printer |
| 172.16.18.1 | CHEBSFW01 | Default-Gateway Server |
| 172.16.241.1 | CHEBSFW01 | Default-Gateway Management |
| 172.16.240.1 | 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 | CHEBSSEC02 | 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 | VCHEBSDMZOF01 | OpenFire DMZ |
| 10.110.210.22 | VCHEBSWEB01 | Webserver |
| 10.110.210.23 | VCHEBSWEB02 | Webserver |

## Netzwerkplan

Dieser Netzwerkplan zeigt lediglich die schematische Darstellung der Netzwerksegmentierung und deren Aufbau.

ES SIND NICHT ALLE KOMPONENTEN AUFGEZEIGT!

Weitere Informationen können dem Netzwerkkonzept entnommen werden.



## 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

Durch die Segmentierung des Netzwerkes, benötigen wir komplett neue Firewall Regeln. Um eine maximale Sicherheit zu gewährleisten, werden die Netze unterteilt. Die bestehende Firewall wird in ihrem aktuellen Zustand vollständig durch eine neue ersetzt. Um dies so kostengünstig wie möglich zu halten, haben wir uns dazu entschieden diese zu virtualisieren und das System von pfSense zu verwenden. Zudem werden folgende Regeln neu gesetzt.

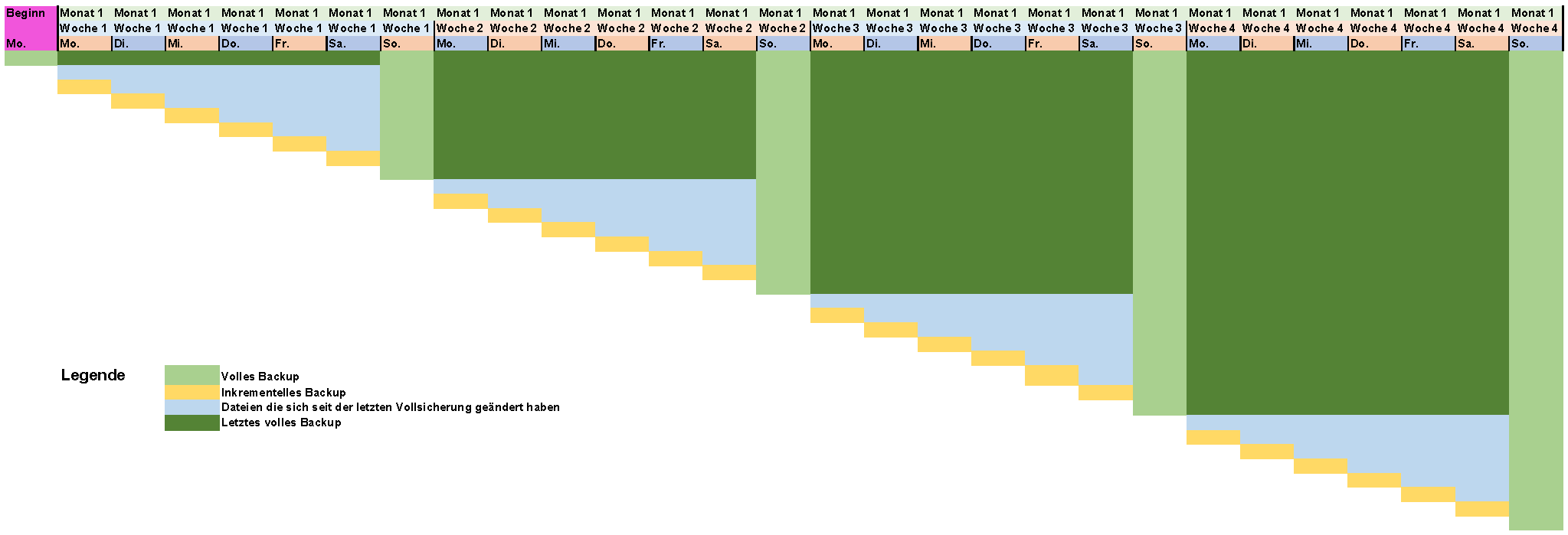
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Source** | **Destination** | **Protocol** | **Port** | **Permission** | **COM** |
| 172.16.16.0/24 | 172.16.241.0/24 | SSH | 22 | ALLOW |  |
| 172.16.16.0/24 | 172.16.17.0/24 | ANY | ANY | ALLOW |  |
| 172.16.16.0/24 | 172.16.240.0/24 | ANY | ANY | ALLOW |  |
| 172.16.16.0/24 | 172.16.18.0/24 | RDP | 3389 | ALLOW |  |
| 172.16.16.0/24 | 172.16.18.0/24 | SSH | 22 | ALLOW |  |
| 172.16.16.0/24 | 172.16.18.0/24 | ARPA | 42 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | STUN | 3478 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | STUN | 3479 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | CtS | 5222 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | CtS | 5223 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | FCD | 5229 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | HTTP Binding | 7070 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | HTTP Binding | 7443 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | FTP XMPP | 7777 | ALLOW |  |
| 172.16.16.0/24 | 10.110.210.21 | ADM Console | 9091 | ALLOW |  |
| \* | \* | ANY | ANY | DENY |  |

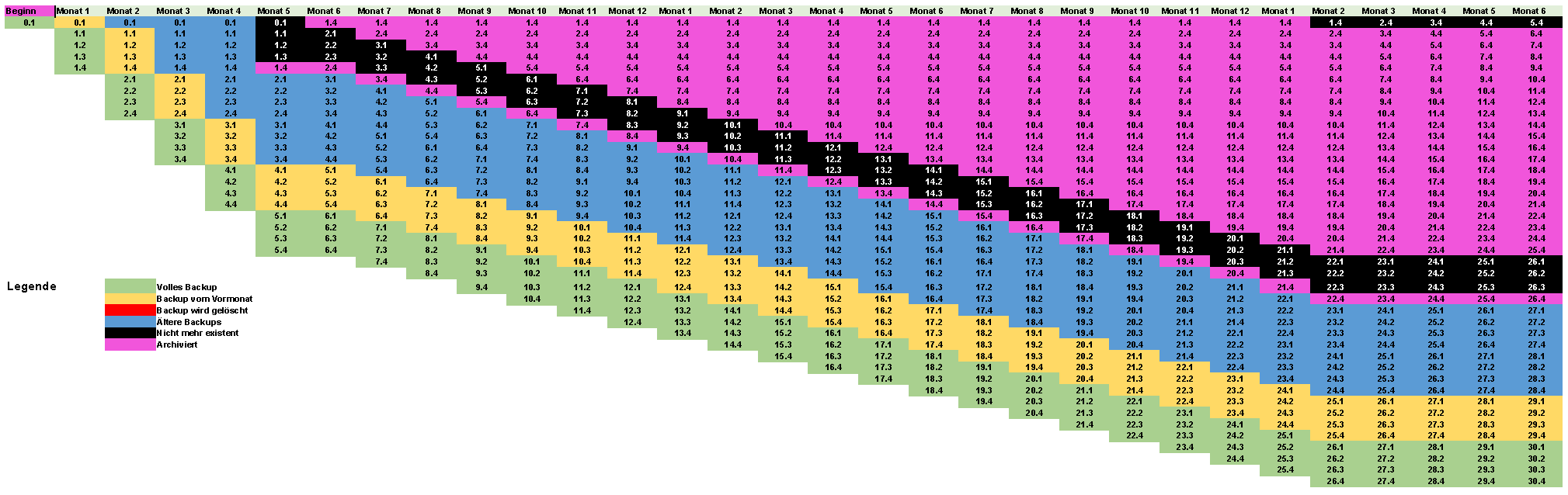
OpenFire Port description:

* 3478 - STUN Service (NAT connectivity)
* 3479 - STUN Service (NAT connectivity)
* 5222 - Client to Server (standard and encrypted)
* 5223 - Client to Server (legacy SSL support)
* 5229 - Flash Cross Domain (Flash client support)
* 7070 - HTTP Binding (unsecured HTTP connecitons)
* 7443 - HTTP Binding (secured HTTP connections)
* 7777 - File Transfer Proxy (XMPP file transfers)
* 9090 - Admin Console (unsecured)
* 9091 - Admin Console (secured)

ALLENFALLS WERDEN NOCH PORTS FÜR DIE AUTHENTIFIZIERUNG IM AD BENÖTIGT!!

## Backupkonzept





## Zugriffskonzept

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Username** | **Funktion** | **Gruppe** | **01 - Administration** | **02 - Gruppenlaufwerk** | **03 - Buchhaltung** | **04 - Personalwesen** | **05 - Geschäftsleitung** | **06 - Verkauf** | **07 - Einkauf** | **08 - IT** |
| Hufschmied | Jackie | 11003 | Buchhaltung | 03-BH | r/w | r/w | r/w | - | - | - | - | - |
| Morrison | Paula | 11004 | Buchhaltung / HR | 03-BH, 04-HR | r/w | r/w | r/w | r/w | - | - | - | - |
| Larson | Josefina | 11005 | Einkauf | 07-EK | - | r/w | - | - | - | - | r/w | - |
| Meier | Jimmie | 11006 | Einkauf | 07-EK | - | r/w | - | - | - | - | r/w | - |
| Oriet | Kathleen | 11007 | Einkauf | 07-EK | - | r/w | - | - | - | - | r/w | - |
| Collins | Faye | 11008 | Einkauf | 07-EK | - | r/w | - | - | - | - | r/w | - |
| Tschan | Jessie | 11009 | Einkauf | 07-EK | - | r/w | - | - | - | - | r/w | - |
| Rivera | Loretta | 11001 | Geschäftsleitung | 05-GL | r/w | r/w | r/w | r/w | r/w | r/w | r/w | r/w |
| Huber | Hubert | 11002 | Geschäftsleitung | 05-GL | r/w | r/w | r/w | r/w | r/w | r/w | r/w | r/w |
| Ingram | Sonya | 11010 | IT / Support | 08-IT | - | - | - | - | - | - | - | r/w |
| Ingram | Sonya | A11010 | ADM Account | 10-AMD-IT | r/w | r/w | r/w | r/w | r/w | r/w | r/w | r/w |
| Jefferson | Mathew | 11011 | IT / Support | 08-IT | - | - | - | - | - | - | - | r/w |
| Jefferson | Mathew | A11011 | ADM Account | 10-ADM-IT | r/w | r/w | r/w | r/w | r/w | r/w | r/w | r/w |
| Simon | Jody | 11012 | Personal / HR | 04-HR | r/w | r/w | - | r/w | - | - | - | - |
| West | Devin | 11013 | Personal / HR | 04-HR | r/w | r/w | - | r/w | - | - | - | - |
| Ramsey | Kara | 11014 | Sekretariat / Empfang | 01-ADM | r/w | r/w | - | - | - | - | - | - |
| Pena | Tom | 11015 | Sekretariat / Empfang | 01-ADM | r/w | r/w | - | - | - | - | - | - |
| Müller | Michele | 11016 | Sekretariat GL | 05-GL | r/w | r/w | r/w | r/w | r/w | r/w | r/w | r/w |
| Wilkins | Kenneth | 11017 | Verkauf | 06-VK | - | r/w | - | - | - | r/w | - | - |
| Reynolds | Edna | 11018 | Verkauf | 06-VK | - | r/w | - | - | - | r/w | - | - |
| Doppler | Rickey | 11019 | Verkauf | 06-VK | - | r/w | - | - | - | r/w | - | - |
| Peter | Mae | 11020 | Verkauf | 06-VK | - | r/w | - | - | - | r/w | - | - |

## Gruppen- und Nutzerkonzept

### User

Die Usernamen werden nicht wie bisher gewohnt aus den ersten 3 Buchstaben des Nachnamens und den ersten 3 Buchstaben des Vornamens gebildet, sondern es werden jetzt neu 5 stellige Laufnummern verwendet. Grund dafür ist, dass es einem Eindringling keinen Hinweis auf den Namen und der Zugehörigkeit des Users gibt.

|  |  |  |
| --- | --- | --- |
| **Name** | **Vorname** | **Username** |
| Hufschmied | Jackie | 11003 |
| Morrison | Paula | 11004 |
| Larson | Josefina | 11005 |
| Meier | Jimmie | 11006 |
| Oriet | Kathleen | 11007 |
| Collins | Faye | 11008 |
| Tschan | Jessie | 11009 |
| Rivera | Loretta | 11001 |
| Huber | Hubert | 11002 |
| Ingram | Sonya | 11010 |
| Ingram | Sonya | A11010 |
| Jefferson | Mathew | 11011 |
| Jefferson | Mathew | A11011 |
| Simon | Jody | 11012 |
| West | Devin | 11013 |
| Ramsey | Kara | 11014 |
| Pena | Tom | 11015 |
| Müller | Michele | 11016 |
| Wilkins | Kenneth | 11017 |
| Reynolds | Edna | 11018 |
| Doppler | Rickey | 11019 |
| Peter | Mae | 11020 |

Für die IT und deren Systeme werden dann noch spezielle User mit speziell erhöhten rechten benötigt. Grund dafür ist das erhöhte Sicherheitsrisiko, wenn die User auf den normalen Accounts erhöhte oder sogar Administrator Berechtigungen haben.

### Gruppen

Die Gruppen für die Benutzer werden der Ablagestruktur auf dem File Server angepasst. Grund dafür ist die einfachere Verwaltbarkeit und eine bessere Übersicht. Die IT erhält zusätzlich noch Accounts, welche einer Supportgruppe angegliedert sind. Mit diesen Accounts erhalten sie die Administrativen Rechte auf jegliche Systeme. Dies kann nicht auf den normalen User Accounts sein, da dies ein erhöhtes Sicherheitsrisiko mit sich bringt.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Vorname** | **Username** | **Funktion** | **Gruppe** |
| Hufschmied | Jackie | 11003 | Buchhaltung | 03-BH |
| Morrison | Paula | 11004 | Buchhaltung / HR | 03-BH, 04-HR |
| Larson | Josefina | 11005 | Einkauf | 07-EK |
| Meier | Jimmie | 11006 | Einkauf | 07-EK |
| Oriet | Kathleen | 11007 | Einkauf | 07-EK |
| Collins | Faye | 11008 | Einkauf | 07-EK |
| Tschan | Jessie | 11009 | Einkauf | 07-EK |
| Rivera | Loretta | 11001 | Geschäftsleitung | 05-GL |
| Huber | Hubert | 11002 | Geschäftsleitung | 05-GL |
| Ingram | Sonya | 11010 | IT / Support | 08-IT |
| Ingram | Sonya | A11010 | ADM Account | 10-ADM-IT |
| Jefferson | Mathew | 11011 | IT / Support | 08-IT |
| Jefferson | Mathew | A11011 | ADM Account | 10-ADM-IT |
| Simon | Jody | 11012 | Personal / HR | 04-HR |
| West | Devin | 11013 | Personal / HR | 04-HR |
| Ramsey | Kara | 11014 | Sekretariat / Empfang | 01-ADM |
| Pena | Tom | 11015 | Sekretariat / Empfang | 01-ADM |
| Müller | Michele | 11016 | Sekretariat GL | 05-GL |
| Wilkins | Kenneth | 11017 | Verkauf | 06-VK |
| Reynolds | Edna | 11018 | Verkauf | 06-VK |
| Doppler | Rickey | 11019 | Verkauf | 06-VK |
| Peter | Mae | 11020 | Verkauf | 06-VK |

## Passwortkonzept

Es gibt in Zukunft keine Standardpasswörter mehr. Grund dafür ist ein zu grosses Sicherheitsrisiko, das mit diesen Passwörtern einher geht. Es gibt jedoch Richtlinien, nach denen die Passwörter nun erstellt werden. Für die normalen Useraccounts werden folgende Kriterien benötigt:

* Mind. 8 Zeichen
* 1 Grossbuchstabe
* 1 Kleinbuchstabe
* 1 Zahl
* 1 Sonderzeichen

Für die Administrationsaccounts der IT sind folgende Kriterien nötig:

* Mind. 12 Zeichen
* 2 Grossbuchstaben
* 2 Kleinbuchstaben
* 2 Zahlen
* 2 Sonderzeichen

Grund für die erhöhte Komplexität der Passwörter sind die erhöhten Rechte, die mit diesen Accounts einher geht.

Systeme, die nicht an das AD oder an anderweitige Zentralauthentifizierungssysteme gebunden werden können, erhalten ein Standardpasswort. Dieses wird folgendermassen gebildet.

EventX AG -> (3v3nt#-46)

Dieses Passwort entspricht der Sicherheitsrichtlinie und kann durch eine Bruteforceattacke nur sehr schwer herausgefunden werden.

# Testszenarien

Um die Umgebung ordnungsgemäss abzusichern, werden noch Testszenarien benötigt.

Die Umgebung wird redundant aufgebaut, um einen Totalausfall eines Systems abfangen zu können.

Folgende Tests werden durchgeführt und geprüft:

* Abschaltung ESXi Host 1
  + Überprüfung der Übernahme des Host 2
  + Überprüfung der Übernahme der FireWall 2
  + Überprüfung der Übernahme der Windows Server
    - Überpfüfung DNS 2
    - Überprüfung AD 2
    - Überprüfung DHCP 2
    - Überprüfung FS 2
    - Überprüfung Print Server 2
    - Überprüfung DBS 2
    - Überprüfung WEB 2
    - Überprüfung OpenFire 2

Mit der Abschaltung des ESXi Host 1 können alle Tests durchgeführt werden. Somit wird kein weiterer Test benötigt um die Sicherheit des Systems zu garantieren.

# 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 10GB RJ45 | 4x 1GB RJ45 PCI-e | 370.- | X2 | 740.- |
| SSD 480GB | SSD 48GB SATA 2.5 + Caddy | 79.- | X16 | 1’264.- |
| **TOTAL** |  |  |  | **4’700.-** |

## Netzwerkgeräte

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Artikel | Beschr. | Preis | Anz. | Total |
| Netgear GS316EP | Netgear GS316EP Switch | 228.- | X4 | 912.- |
| Netgear WAX220 | Netgear WAX220 | 198.- | X2 | 396.- |
| **TOTAL** |  |  |  | **1’308.-** |

### Lizenzen

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Artikel | Beschr. | Preis | Anz. | Total |
| Win 11 | Windows 11 Pro | 144.- | X32 | 5'040.- |
| Win Serv 2022 | Windows Server 2022 | 875.- | X4 | 3'500.- |
| Veeam Essentials | Veeam Backup Essentials Yearly Subscripion | 363.- | X2 | 726.- |
| VMWare vSphere 8 | VMWare vSphere 8 Essentials Yearly Subscription (3 Hosts) | 522.- | X1 | 522.- |
| **TOTAL** |  |  |  | **9’788.-** |

### Arbeit

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Artikel | Beschr. | Preis | Anz. | Total |
| Arbeit | Stundensatz | 50.- | X440 | 22'000.- |
| Material | Alle vorangehenden Kosten | 15'796.- | X1 | 15'796.- |
| **TOTAL** |  |  |  | **37’796.-** |

# Wichtige Hinweise

DA ES SICH HIERBEI UM EIN SCHULPROJEKT HANDELT, WERDEN DIE TESTS NICHT DURCHGEFÜHRT, AUFGRUND MANGELNDER RESSOURCEN!

EBENSO WIRD AUF JEDES SYSTEM AUSSERHALB DES ESXi HOSTS VERZICHTET, DA DIE BENÖTIGTEN RESSOURCEN NICHT VORHANDEN SIND!

ES WIRD AUCH AUF DEN WEBSERVER VERZICHTET DA DIE NÖTIGE ZEIT NICHT VORHANDEN IST!

AUCH BEI DEN SERVERN WIRD DER FOKUS LEDIGLICH AUF DIE KERNSYSTEME GESETZT.

# Selbstständigkeitserklärung

Ich erkläre hiermit, dass es sich bei der von mir eingereichten schriftlichen Arbeit mit dem Titel

**EventX AG Migration**

um eine von mir selbst und ohne unerlaubte Beihilfe sowie in eigenen Worten verfasste Originalarbeit handelt.

Ich bestätige überdies, dass die Arbeit als Ganzes oder in Teilen noch nie zur Bewertung einer anderen schulischen Leistung an der BBZBL oder an einer anderen Ausbildungseinrichtung verwendet wurde.

Verwendung von Quellen und Sekundärliteratur

Ich erkläre weiterhin, dass ich sämtliche in der eingereichten Arbeit enthaltenen Bezüge auf Quellen und Sekundärliteratur als solche kenntlich gemacht habe. Insbesondere bestätige ich, dass ich ausnahmslos und nach bestem Wissen sowohl bei wörtlich übernommenen Aussagen (Zitaten) als auch bei in eigenen Worten wiedergegebenen Aussagen anderer Autorinnen oder Autoren (Paraphrasen) die Urheberschaft angegeben habe.

Sanktionen

Ich nehme zur Kenntnis, dass Arbeiten, welche die Grundsätze der Selbstständigkeitserklärung verletzen – insbesondere solche, die Zitate oder Paraphrasen ohne Herkunftsangaben enthalten –, als Plagiat betrachtet werden und entsprechende rechtliche und disziplinarische Konsequenzen nach sich ziehen können.

Ich bestätige mit meiner Unterschrift die Richtigkeit dieser Angaben.

**Autor**

|  |  |
| --- | --- |
| Name: | Morgenthaler |
| Vorname: | Yannick |
| Datum: | 03.11.2023 |
| Unterschrift | Y.Morgenthaler |