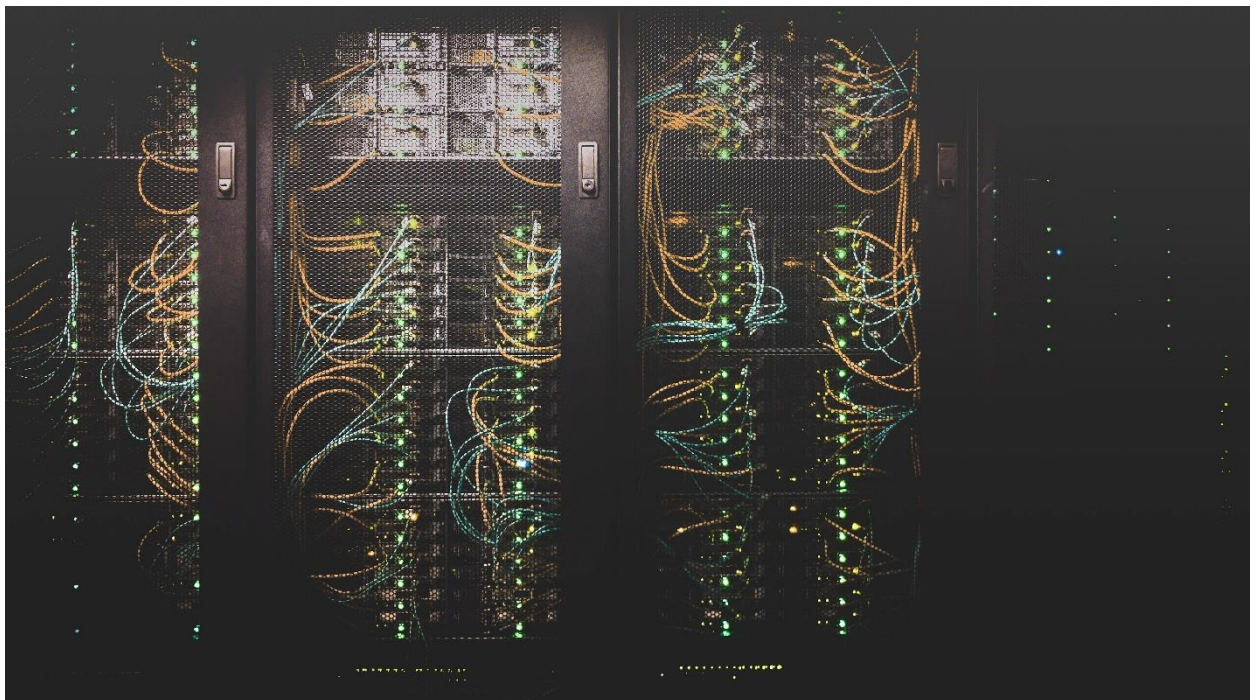


Autoren Medeea Barbu
Michalis Chatzimichalis
Luis Lüscher
Fachlehrperson Johan Widmer
Datum 16. November 2020
Version 1.0
Klassifikation Öffentlich
Seiten 116, inkl. Deckblatt

Dokumentation LB1

Modul 146

Internetanbindung für ein Unternehmen realisieren



Änderungsverzeichnis

Version	Status	Name	Datum	Beschreibung
0.1	Erledigt	Lüscher, Luis	16.11.2020	Dokument wurde erstellt
0.2	Erledigt	Lüscher, Luis Chatzimichalis, Michalis Barbu, Medeea	23.11.2020	Beschreibung Umfeld und Ablauf
0.3	Erledigt	Lüscher, Luis Chatzimichalis, Michalis Barbu, Medeea	23.11.2020	Beschreibung Projektmanagement
0.41	Erledigt	Barbu, Medeea Lüscher, Luis	16.11.2020	Beschreibung Realisierung VPN
0.42	Erledigt	Barbu, Medeea Lüscher, Luis	23.11.2020	Beschreibung Realisierung Übertragungsrate, Verfügbarkeit
0.43	Erledigt	Chatzimichalis, Michalis	23.11.2020	Beschreibung Realisierung WAN-Technologie
0.44	Erledigt	Lüscher, Luis	23.11.2020	Beschreibung Realisierung Internetservices
0.45	Erledigt	Lüscher, Luis	30.11.2020	Beschreibung Realisierung Sicherheit
0.46	Erledigt	Lüscher, Luis	30.11.2020	Beschreibung Realisierung Firewall
0.47	Erledigt	Chatzimichalis, Michalis Lüscher, Luis	30.11.2020	Beschreibung Realisierung Wartung/Überwachung
0.48	Erledigt	Barbu, Medeea Lüscher, Luis	30.11.2020	Beschreibung ICT System AG
	Erledigt	Barbu, Medeea Lüscher, Luis Chatzimichalis, Michalis	30.11.2020	Beschreibung IPERKA
0.5	Erledigt	Barbu, Medeea Chatzimichaiis, Michalis	07.12.2020	Beschreibung Scrum
0.55	Erledigt	Barbu, Medeea Lüscher, Luis	07.12.2020	Beschreibung SWOT
0.6	Erledigt	Chatzimichalis, Michalis	07.12.2020	Erstellen von Testfällen
0.65	Erledigt	Barbu, Medeea Chatzimichalis, Michalis	07.12.2020	Beschreibung Arbeitsumfeld
0.7	Erledigt	Chatzimichaiis, Michalis Lüscher, Luis	07.12.2020	Abnahmeprotokoll und Rechnung erstellt
0.8	Erledigt	Lüscher, Luis	07.12.2020	Reflexion erstellt
0.9	Erledigt	Barbu, Medeea	07.12.2020	Review Check 1 von 3
0.95	Erledigt	Chatzimichalis, Michalis	07.12.2020	Review Check 2 von 3
1.0	Erledigt	Lüscher, Luis	07.12.2020	Review Check 3 von 3

Lizenz

Creative Commons License



Abbildung 1: Abbildung CC BY-NC-SA

Dieses Werk ist unter einer Creative Commons Lizenz vom Typ Namensnennung – Nicht kommerziell – Weitergabe unter gleichen Bedingungen 3.0 Schweiz (CC BY-NC-SA 3.0 CH) zugänglich. Um eine Kopie dieser Lizenz einzusehen, konsultieren Sie <https://creativecommons.org/licenses/by-nc-sa/3.0/ch/> oder wenden Sie sich brieflich an Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Sie dürfen:

Teilen – das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten

Bearbeiten – das Material remixen, verändern und darauf aufbauen

Unter folgenden Bedingungen:

Namensnennung – Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstützt gerade Sie oder Ihre Nutzung besonders.

Nicht kommerziell – Sie dürfen das Material nicht für kommerzielle Zwecke nutzen.

Weitergabe unter gleichen Bedingungen – Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.

Keine weiteren Einschränkungen – Sie dürfen keine zusätzliche Klauseln oder technische Verfahren einsetzen, die anderen rechtlich untersagen, was die Lizenz erlaubt.

Inhaltsverzeichnis

1. Vorwort	10
1.1. Einleitung	10
1.2. Zielgruppe	10
1.3. Danksagung	10
1.4. Darstellung und Aufbau	10
1.4.1. Abbildung	10
1.4.2. Tabelle	10
1.5. Modulidentifikation	11
1.5.1. Handlungsnotwendige Kenntnisse	12
1.5.2. Leistungsbeurteilungsvorgaben	13
1.6. Fiktives Unternehmen	15
1.6.1. Internet Auftritt	15
1.6.1.1. Jira Ticket Documentation	16
2. Umfeld und Ablauf	17
2.1. Aufgabenstellung	17
2.1.1. Titel der Arbeit	17
2.1.2. Ausgangslage	17
2.1.3. Mittel und Methoden	17
2.1.4. Vorkenntnisse	17
2.1.5. Individuelle Beurteilungskriterien	18
2.1.5.1. Dokumentation	18
2.1.5.1.1. Grundsätzliche Beurteilungskriterien Dokumentation	18
2.1.5.1.1.1. L1 - Grundlagen	18
2.1.5.1.1.2. L2 - Architektur	18
2.1.5.1.1.3. L3 - Entscheidungsmatrix	19
2.1.5.1.1.4. L4 - Vergleichskriterien	19
2.1.5.1.1.5. L5 - Realisations-Varianten	19
2.1.5.1.1.6. L6 - Formale Vorgaben	19
2.1.5.1.2. Fachliche Beurteilungskriterien Dokumentation	20
2.1.5.1.2.1. L1 - Übertragungsrate, Verfügbarkeit	20
2.1.5.1.2.2. L2 - WAN-Technologie	21
2.1.5.1.2.3. L3 - Internetservices	21
2.1.5.1.2.4. L4 - Sicherheit	22
2.1.5.1.2.5. L5 - Wartung / Überwachung	23
2.1.5.1.2.6. L6 - Firewall	24
2.1.5.1.2.7. L7 - VPN	24
2.1.5.2. Präsentation	25
2.1.5.2.1. L1 - Art des Vortrages	25
2.1.5.2.2. L2 - Einsatz von Medien	25
2.1.5.2.3. L3 - Inhaltliche Dichte	25
2.1.5.2.4. L4 - Fachliche Tiefe	26
2.1.5.2.5. L5 - Ablauf	26
2.1.5.2.6. L6 - Zeitplanung	27
2.1.5.2.7. L7 - Inhaltliche Struktur	27
2.2. Projektantrag	28
2.3. Arbeitsumfeld	29
2.3.1. Arbeitsplatz	29

2.3.2. Hardware & Software.....	30
2.3.2.1. Hardware Luis Lüscher	30
2.3.2.2. Hardware Medeea Barbu.....	30
2.3.2.3. Hardware Michalis Chatzimichalis	30
2.3.2.4. Software	30
2.3.3. Dokumentablage	30
2.4. Namenskonvention.....	31
2.4.1. Gerätetypen	31
2.5. Zeitplanung.....	32
2.5.1. Termine.....	32
2.5.2. Arbeitstage.....	32
2.5.3. GANTT	33
2.5.3.1. Erklärung GANTT.....	34
2.5.4. Scrum Board	35
2.5.4.1. Jira Task Beispiel.....	36
2.6. Arbeitsjournal	37
2.6.1. Tag 1.....	37
2.6.2. Tag 2.....	37
2.6.3. Tag 3.....	38
2.6.4. Tag 4.....	39
3. Projektmanagement	40
3.1. IPERKA.....	40
3.1.1. Informieren.....	40
3.1.2. Planen	40
3.1.3. Entscheiden.....	41
3.1.4. Realisieren.....	41
3.1.5. Kontrollieren	41
3.1.6. Auswerten	41
3.2. Scrum	42
3.2.1. Rollen	42
3.2.1.1. Product Owner	42
3.2.1.2. Entwicklungsteam.....	42
3.2.1.3. Scrum Master	42
3.2.2. Stakeholder	42
3.2.2.1. Kunden	42
3.2.2.2. Anwender	42
3.2.2.3. Management.....	43
3.2.3. Scrum-Prozess.....	43
3.2.3.1. Product Backlog anlegen und pflegen	43
3.2.3.2. Im Sprint Planning das Sprint Backlog erstellen	43
3.2.3.3. Im Weekly Scrum den Arbeitsfortschritt besprechen.....	44
3.2.3.4. Im Sprint-Review die Sprint-Ergebnisse prüfen und abnehmen.....	44
3.2.3.5. Mit einer Sprint Retrospective die Zusammenarbeit besprechen.....	44
3.2.4. Kanban-Board	44
3.3. Projektaufbauorganisation.....	46
3.3.1. Berufsbeschreibung Projektleiter	47
3.3.2. Berufsbeschreibung System Engineer	47
3.4. Lastenheft	48
3.4.1. Offerte.....	48

3.5. Pflichtenheft.....	49
3.5.1. Auftragsbestätigung	49
3.5.2. Pflichtenheft Projektleiter	50
3.5.3. Pflichtenheft System Engineer.....	50
3.6. Aufgabenaufteilung.....	51
3.6.1. Aufgaben Luis Lüscher.....	51
3.6.2. Aufgaben Medeea Barbu.....	51
3.6.3. Aufgaben Michalis Chatzimichals	51
3.7. SWOT.....	52
3.7.1. Vorteile SWOT	52
3.7.2. Nachteil SWOT.....	52
3.7.3. SWOT Beschreibung	52
3.7.3.1. Strengths (Stärken)	52
3.7.3.2. Weaknesses (Schwächen)	52
3.7.3.3. Opportunities (Chancen).....	52
3.7.3.4. Threats (Bedrohungen).....	52
3.7.4. SWOT Strategien	52
3.7.4.1. SO-Strategie Strengths und Opportunities.....	53
3.7.4.2. WO-Strategie Weaknesses und Opportunities	53
3.7.4.3. ST-Strategie Strengths und Threats.....	53
3.7.4.4. WT-Strategien Weaknesses and Threats	53
3.7.5. SWOT-Analyse	54
3.8. Risikoanalyse.....	55
3.8.1. Erklärung.....	55
3.8.2. Vorgehensweise.....	55
3.8.3. Risikoanalysetabelle.....	56
3.8.4. Risikomatrix	56
4. Informieren	57
4.1. Auftrag klären	57
4.2. Formulierung des Auftrages.....	58
4.2.1. Aufgabenformulierung	58
4.2.2. Themenübersicht	59
5. Planen	62
5.1. Benötigte Infrastruktur.....	62
5.2. Testkonzept.....	62
6. Entscheiden	64
6.1. Ziele.....	64
6.1.1. Ziele Übertragungsrate & Verfügbarkeit.....	64
6.1.1.1. Beispiele	64
6.1.1.1.1. Beispiel 1 Übertragungsrate	64
6.1.1.1.2. Beispiel 2 Verfügbarkeit	64
6.1.1.1.3. Beispiel 3 Verfügbarkeit	64
6.1.2. Ziele WAN-Technologie.....	64
6.1.3. Ziele Internetservices.....	64
6.1.4. Ziele Sicherheit.....	64
6.1.5. Ziele Wartung & Überwachung	65
6.1.6. Ziele Firewall	65

6.1.7. Ziele VPN	65
7. Realisieren.....	66
7.1. Übertragungsrate & Verfügbarkeit	66
7.1.1. Übertragungsrate	66
7.1.2. Verfügbarkeit	66
7.1.3. Vergleich Provider.....	67
7.1.3.1. Begründung	69
7.2. WAN-Technologie	70
7.2.1. xDSL.....	70
7.2.1.1. Vorteile	70
7.2.1.2. Nachteile	70
7.2.2. Fibre (FTTH).....	70
7.2.2.1. Vorteile	70
7.2.2.2. Nachteile	70
7.2.3. Cable (Kupfer)	70
7.2.3.1. Vorteile	70
7.2.3.2. Nachteile	70
7.2.4. Radiolink.....	70
7.2.4.1. Vorteile	71
7.2.4.2. Nachteile	71
7.2.5. Satellit.....	71
7.2.5.1. Vorteile	71
7.2.5.2. Nachteile	71
7.2.6. Finaler Vergleich	71
7.2.7. Bewertungsmatrix	72
7.3. Internet Services	73
7.3.1. Erklärung.....	73
7.3.1.1. Eigener Server (House)	73
7.3.1.2. Dedizierter Server (Root-Server).....	74
7.3.1.3. Services beim Provider (Shared Hosting)	74
7.3.2. Fallbeispiele.....	75
7.3.2.1. Einfache Webpräsenz und Mail.....	75
7.3.2.2. Komplexe Datenbankanwendung mit PHP	75
7.3.3. Vergleichskriterien.....	75
7.3.4. Vergleich	76
7.3.4.1. Fall 1	76
7.3.4.2. Fall 2	77
7.3.5. Ergebnisse.....	77
7.3.5.1. Fall 1	77
7.3.5.2. Fall 2	77
7.4. Sicherheit	78
7.4.1. ISO Reihe 27000	78
7.4.2. Vertraulichkeit.....	80
7.4.3. Integrität	81
7.4.4. Authentizität und Authentisierung	81
7.4.4.1. Benutzername und Kennwort.....	81
7.4.4.2. Zertifikate	82
7.4.4.3. Biometrie.....	82
7.4.5. Zurechenbarkeit.....	82

7.4.6. Nicht – Abstreitbarkeit	83
7.4.7. Verlässlichkeit	83
7.4.8. Zugriffskontrolle	83
7.4.9. Sicherheitskonzept.....	84
7.4.9.1. Technische Massnahmen.....	84
7.4.9.2. Nicht technische Massnahmen	84
7.5. Wartung & Überwachung.....	85
7.5.1. Vergleich der Überwachungstools	85
7.5.1.1. Zabbix.....	85
7.5.1.2. PRTG.....	85
7.5.1.3. Nagios	85
7.5.1.4. SolarWinds Network Performance	85
7.5.1.5. LAN Guard	85
7.5.2. Bewertungsmatrix	86
7.5.3. Wartung	87
7.5.3.1. Change Management	87
7.5.3.1.1. Normale Change	87
7.5.3.1.2. SOP	87
7.5.3.1.3. Beschleunigte Change	87
7.5.3.1.4. Notfall Change.....	88
7.5.3.1.5. Der Change ohne Auswirkung	88
7.5.3.2. Rollen.....	88
7.5.3.2.1. Change Requestor.....	88
7.5.3.2.2. Change Coordinator.....	88
7.5.3.2.3. Change Implenebtor	88
7.5.3.2.4. Change Manager	88
7.6. Firewall.....	89
7.6.1. Verschiedene Firewall Arten	89
7.6.1.1. Packet Filter Firewalls.....	89
7.6.1.2. Circuit Level Gateways	89
7.6.1.3. Application Level Gateways.....	90
7.6.1.4. tateful Inspection Firewall.....	90
7.6.1.5. Next-Generation Firewalls	90
7.6.2. Firewall Lösungen	91
7.6.2.1. Günstige Hardware-Firewalls.....	91
7.6.2.2. PC-Lösung mit Linux	92
7.6.2.3. Firewall-Service des Providers	92
7.6.3. Vergleich	93
7.6.4. Entscheid.....	93
7.7. VPN.....	94
7.7.1. IPsec.....	94
7.7.1.1. SPD	95
7.7.1.2. SAD	95
7.7.1.3. IKE.....	95
7.7.2. SSL VPN oder IPsec VPN.....	96
7.7.2.1. SSL VPN	96
7.7.2.2. IPsec VPN.....	96
7.7.2.3. Fazit	97
7.7.3. VPN-Architekturen	98
7.7.3.1. Site-to-Site VPN	98

7.7.3.2. End-to-End VPN	98
7.7.3.3. End-to-Site VPN	98
7.7.4. VPN Lösungen.....	99
7.7.4.1. Hardwarelösung.....	99
7.7.4.2. VPN-Service des Providers	99
7.7.4.3. PC-Lösung	99
7.7.5. Vergleich	100
7.7.6. Entscheid.....	100
8. Kontrollieren	101
8.1. Testfälle.....	101
8.1.1. Übertragungsrate & Verfügbarkeit	101
8.1.1.1. Testfall 1	101
8.1.1.2. Testfall 2	101
8.1.1.3. Testfall 3	102
8.1.1.4. Testfall 4	102
8.1.2. WAN-Technologie	103
8.1.2.1. Testfall 5	103
8.1.2.2. Testfall 6	103
8.1.2.3. Testfall 7	104
8.1.3. Internetservices	104
8.1.3.1. Testfall 8	104
8.1.3.2. Testfall 9	105
8.1.4. Sicherheit	105
8.1.4.1. Testfall 10	105
8.1.4.2. Testfall 11	106
8.1.5. Wartung und Überwachung	106
8.1.5.1. Testfall 12	106
8.1.6. Firewall	107
8.1.6.1. Testfall 13	107
8.1.7. VPN.....	107
8.1.7.1. Testfall 14	107
9. Auswerten	108
9.1. Auswerten der Testfälle.....	108
9.2. Verbesserungsmöglichkeiten.....	108
9.3. Rechnung	109
9.4. Abnahmeprotokoll.....	110
10. Schlusswort	111
11. Glossar	112
12. Verzeichnisse.....	114
12.1. Quellenverzeichnis.....	114
12.2. Tabellenverzeichnis.....	115
12.3. Abbildungsverzeichnis	116

1. Vorwort

1.1. Einleitung

Im Rahmen der Leistungsbeurteilung 1 des Modul 146 werden die Schüler: Medeea Barbu, Michalis Chatzimichalis und Luis Lüscher, für ein schweizer Unternehmen eine Internetanbindung realisieren. Die erarbeiteten Resultate werden in diesem Dokument abgespeichert. Die Arbeiten werden innerhalb von vier Montagmorgen erarbeitet und dann anschliessend ein Thema ausgewählt und mittels PPP präsentiert.

1.2. Zielgruppe

Dieses Dokument richtet sich an fachlich kompetente Leser. Vorkenntnisse von IT-Security, Change Management, VPN, Firewall, Internet Services und WAN-Technologien.

1.3. Danksagung

Besten Dank an das gesamte Projektteam für eueren grossartigen Einsatz. Besten Dank an Herr Widmer für die guten und interessanten Ergänzungen im Unterricht sowie die Vorbereitung für das Modul.

1.4. Darstellung und Aufbau

Als Rechtschreibhilfe wurde die integrierte Überprüfungsfunktion von Word verwendet. Ausserdem wurde die Dokumentation von verschiedenen Personen auf die Rechtschreibung überprüft.

Es wird unter verschiedenen Textsorten unterschieden. Dafür wurde die Formatierung selbst definiert:

Text Zitierte Texte werden kursiv geschrieben.

Text Texte, welche besonders zu beachten sind, werden **fett** hervorgehoben.

URL Verlinkungen werden unterstrichen.

1.4.1. Abbildung



Abbildung 2: Beispiel für Abbildung

1.4.2. Tabelle

Tabelle 1: Beispiel für Tabelle

1.5. Modulidentifikation

Modulnummer 146

Titel Internetanbindung für ein Unternehmen realisieren

Kompetenz Entwickeln, Planen und Realisieren von Internetanschlüssen für Unternehmen unter der Berücksichtigung von Sicherheits-, Verfügbarkeits- und Leistungsaspekten.

Handlungsziele

- 1) Internetanschluss nach Kundenvorgaben (Sicherheit, Performance, Verfügbarkeit und Wartung) bestimmen.
- 2) Klassieren der eruierten Kundenvorgaben nach Prioritäten und Bedeutung für das Unternehmen und in einem Pflichtenheft für die Evaluation eines Serviceproviders festhalten.
- 3) Resultate der Evaluation unter Berücksichtigung des Pflichtenheftes und wirtschaftlichen Aspekten bewerten und darstellen.
- 4) Netzwerkplan und Netzwerkschema für die Internetanbindung erstellen oder anpassen.
- 5) Erforderliche Hardware- und Softwarekomponenten bestimmen und Beschaffungsantrag erstellen.
- 6) Inbetriebnahme der Internetanbindung realisieren und Abnahme durchführen.

1.5.1. Handlungsnotwendige Kenntnisse

- 1) Kennt die Anforderungen an eine Internetanbindung (Bandbreite, Verfügbarkeit, Sicherheit und Wartung).
- 2) Kennt die Sicherheits- und Überwachungsmassnahmen beim Betrieb eines Internetanschlusses.
- 3) Kennt die Zugangsmöglichkeiten zum Internet sowie deren Anbieter (Provider).
- 4) Kennt Methoden, um Kundenvorgaben zu klassieren.
- 5) Kennt Aufbau und Inhalt eines Pflichtenhefts.
- 6) Kennt den Ablauf eines Evaluationsprozesses.
- 7) Kennt die wichtigsten Kriterien für die Bewertung eines Angebotes.
- 8) Kennt Darstellungsarten für die Beurteilung von Offerten.
- 9) Kennt die Regeln für das Erstellen eines Namens- und Nummerierungskonzepts.
- 10) Kennt die Funktionsweise von Firewall, DMZ, Proxy und DNS.
- 11) Kennt gängige Darstellungsarten und Symbole für Netzwerkplan und Netzwerkschemata.
- 12) Kennt Aufbau und Inhalt eines Beschaffungsantrags aus der durchgeführten Evaluation.
- 13) Kennt das Vorgehen für die Planung und Inbetriebnahme des Internetzugangs.
- 14) Kennt das Vorgehen für die Übergabe des Systems in den operativen Betrieb.
- 15) Kennt Aufbau und Inhalt eines Abnahmeprotokolls.

1.5.2. Leistungsbeurteilungsvorgaben

Institution TBZ Technische Berufsschule Zürich

Übersicht Dreiteilige LBV; Erstes Element: Gruppenarbeit mit Präsentation / Zweites Element: Praktische Arbeit / Drittes Element: Schriftlicher Test

Der momentane Teil ist hellblau markiert, bereits absolvierte Teile sind hellgrün markiert.

Teil	1
Gewichtung	40%
Richtzeit (Empfehlung)	2
Element-Beschreibung	Erarbeiten einer Präsentation (ca. 10 Min. pro Gruppe) und einer Dokumentation nach zugewiesenem Thema. Der Auftrag enthält Leitfragen und formale Vorgaben die für alle Gruppen gleich sind, damit eine Leitlinie durch alle Präsentationen und Dokumentationen ersichtlich ist. Entscheidungen werden mit einer geeigneten Methode evaluiert und grafisch aufbereitet.
Hilfsmittel	frei
Bewertung	Punktebewertung mit Noten Präsentation nach einem vorgegebenen Raster durch Lehrperson bewerten (Gewicht 25%) Präsentation nach einem vorgegebenen Raster durch Lernende bewerten (Gewicht 25%) Dokumentation nach einem vorgegebenen Raster durch Lehrperson bewerten (Gewicht 50%)
Praxisbezug	Können Grundlagen aus abgegebenen Unterlagen herausfinden oder nachfragen Können in einem Team arbeiten Können Pflichtenhefte / Aufgaben klassieren Können Entscheidungen mit einer geeigneten Methode herbeiführen Können Informationen aufbereiten
Teil	2
Gewichtung	40%
Richtzeit (Empfehlung)	16
Element-Beschreibung	Praktische Umsetzung eines Auftrages in einem Team. Komplexe Internetanbindung mit Zonen und Firewall. Arbeit für Bewertung dokumentieren (Lernjournal oder andere Form).
Hilfsmittel	frei
Bewertung	Punktebewertung mit Noten 20% Netzwerkplanung und Netzwerkschema 50 % Internetanbindung realisieren 20 % Testszenarien 10% Abnahme
Praxisbezug	Können Kundenbedürfnisse herausfinden und festhalten Können die nötigen Unterlagen für das Netzwerk erstellen Können eine Internetanbindung realisieren Können geeignete Testszenarien erstellen und

	durchführen Können ein Abnahme durchführen
Teil	3
Gewichtung	20%
Richtzeit (Empfehlung)	1
Element-Beschreibung	Fragen über alle Handlungsziele
Hilfsmittel	schriftliche handgeschriebene Zusammenfassung
Bewertung	Punktebewertung mit Noten 40% Kundenvorgaben bestimmen, Klassifizieren, Evaluation 40% Netzwerkplanung und Netzwerkschema, Internetanbindung realisieren 20 % Testszenarien, Abnahme
Praxisbezug	frei

Tabelle 2: Leistungsbeurteilungsvorgaben

1.6. Fiktives Unternehmen

Als IT - Dienstleister haben wir für das Modul die fiktive Firma ICT System AG gegründet. Dies sollte auch den Auftrag um einiges professioneller und realistischer Wirken lassen.

Die ICT System AG wurde im Jahr 2020 von Luis Lüscher ins Leben gerufen und durch Michalis Chatzimichalis wurde der Internet Auftritt erstellt. Die ersten Dienstleistungen, die wir angeboten haben, war Web Hosting, danach ging es in den Bereich Web Entwicklung bis wir nun bei der Beratung angekommen sind. Wir haben uns auf die Beratung von Umstrukturierungen sowie Aktualisierungen von ganzen IT-Infrastrukturen spezialisiert und übernehmen ebenfalls den operativen Teil – wenn gewünscht.

1.6.1. Internet Auftritt

Um unserer Firma ebenfalls im Internet zu repräsentieren haben wir eine Website erstellt. Dies sollte dem Unternehmen den nötigen professionellen auftritt verschaffen. Unsere Website ist unter folgender URL erreichbar: <https://ictsystem.ch/>



Abbildung 3: ICT System GmbH

1.6.1.1. Jira Ticket Documentation

Zur besseren Übersicht des Prozess haben wir diesen hier ein wenig kleiner abgebildet, jedoch sind alle Task abgebildet. Der richtig dargestellte Prozess kann man [hier](#) herunterladen:

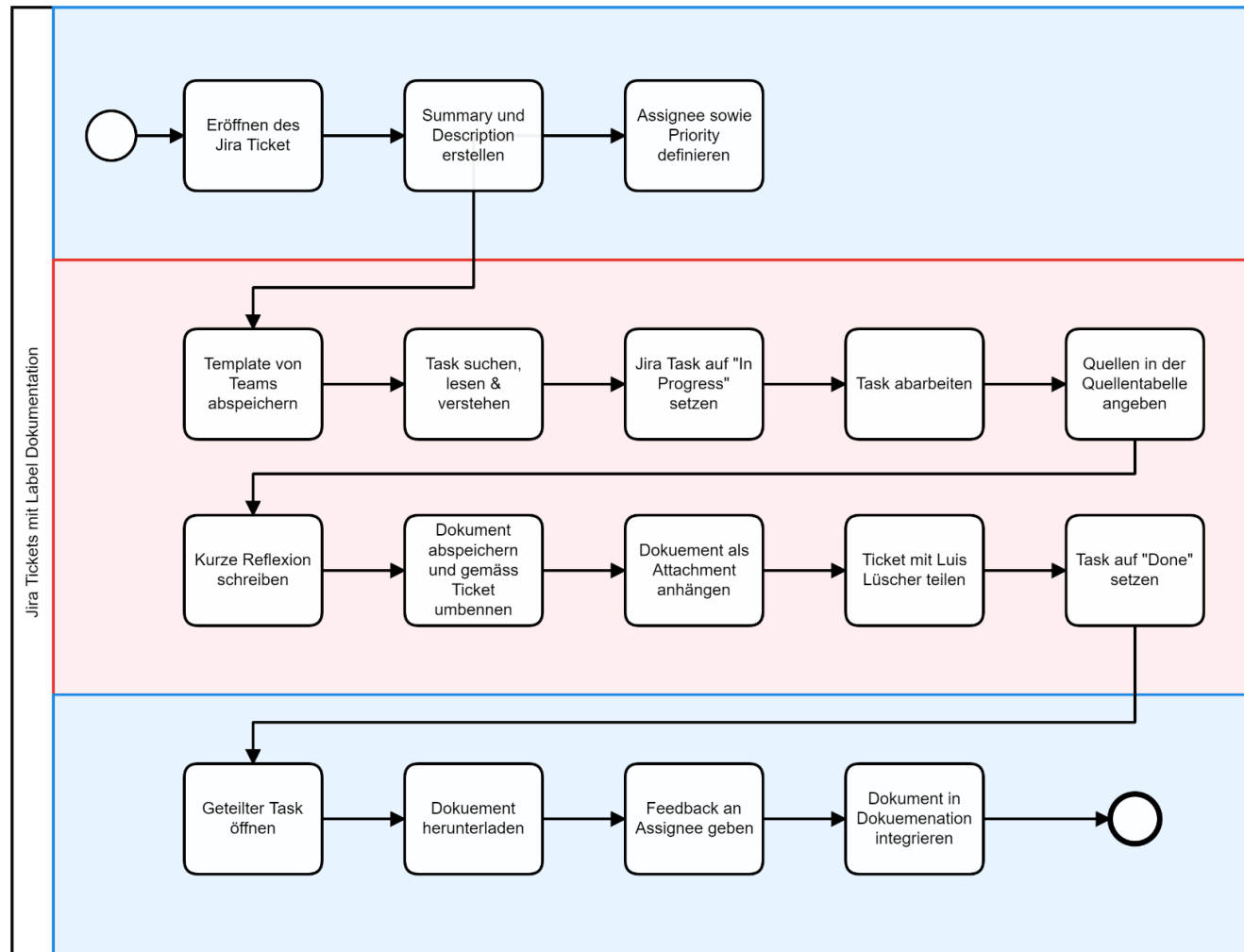


Abbildung 4: Bearbeitung eines Ticket im Jira

2. Umfeld und Ablauf

2.1. Aufgabenstellung

2.1.1. Titel der Arbeit

Originaltext gemäss MP146_LB1_v2.0.docx

LB1 - Grundlagen erarbeiten zu verschiedenen Aspekten einer Internetanbindung.

2.1.2. Ausgangslage

In einer Gruppenarbeit müssen verschiedene Kompetenzen und Themen bearbeitet werden. In unserem Fall sind in unserer Gruppe

- Barbu, Medeea
- Chatzimichalis, Michalis
- Lüscher, Luis

Die erarbeitenden Resultate müssen in einer Dokumentation abgelegt werden, zudem werden die Projektmitglieder einen Vortrag halten zu zwei von der Lehrperson ausgewählten Themen.

2.1.3. Mittel und Methoden

Für diese Arbeit wird IPERKA als Projektmethode verwendet. Diese vorgehen hat der Kandidat bereits mehrfach in der Schule angewendet. Die Inhalte werden via Recherchen und bereits vorhandenen Fachkenntnissen erarbeitet und so aufbereitet, dass diese gut anschaulich dokumentiert werden können.

2.1.4. Vorkenntnisse

Die Projektmitglieder verfügen über Fachkenntnisse im Bereich Projektmanagement und kennen einige der zu behandelnden Themen bereits aus dem Modul 145. Die zu erarbeitenden Themen sollte auf einer guten fachlichen Stufe erarbeitet werden.

2.1.5. Individuelle Beurteilungskriterien

Hier werden die Beurteilungskriterien für die Dokumentation sowie die Präsentation in Form von Leitfragen formuliert

2.1.5.1. Dokumentation

Die folgenden Leitfragen werden als Beurteilungskriterien für die Dokumentation verwendet. Die maximal Punktzahl pro Leitfrage, die vier Punkte beträgt, kann nur erreicht werden, wenn diese komplett und in sehr guter fachlicher Tiefe beantwortet wird.

2.1.5.1.1. Grundsätzliche Beurteilungskriterien Dokumentation

Dies sind die grundsätzlichen Beurteilungskriterien an die Dokumentation. Somit wird hier definiert, wie das Abgabedokument aussehen muss und welche Bedingungen das Projektteam erfüllen muss.

2.1.5.1.1.1. L1 - Grundlagen

Leitfrage 1	Die Grundlagen wurden erarbeitet:
	<ul style="list-style-type: none"> - Thema gut recherchiert - verständlich aufbereitet - gut strukturiert - mit unterschiedlichen Beispielen unterlegt
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	3 Anforderungen wurden erfüllt.
Gütestufe 0	Weniger als 3 Anforderungen wurden erfüllt.

Tabelle 3: Leitfrage Grundlagen Dokumentation

2.1.5.1.1.2. L2 - Architektur

Leitfrage 2	Architektur / Konzepte / Komponenten aufgezeigt und grafisch aufgearbeitet. Das Thema kann mit einer übersichtlichen Grafik bildlich erklärt werden.
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 4: Leitfrage Architektur Dokumentation

2.1.5.1.1.3. L3 – Entscheidungsmatrix

Leitfrage 3	Entscheidungsmatrix richtig angewendet. Gemäss Script einwandfrei angewendet.
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 5: Leitfrage Entscheidungsmatrix Dokumentation

2.1.5.1.1.4. L4 – Vergleichskriterien

Leitfrage 4	Vergleichskriterien gefunden (min. 5) Zum Thema passende Kriterien gefunden.
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 6: Leitfrage Vergleichskriterien Dokumentation

2.1.5.1.1.5. L5 – Realisations-Varianten

Leitfrage 5	Szenarien / Realisations-Varianten (min 3). Gute Szenarien gefunden, diese Szenarien mit Varianten versehen (min. 3).
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 7: Leitfrage Realisation-Variante Dokumentation

2.1.5.1.1.6. L6 – Formale Vorgaben

Leitfrage 6	Formale Vorgaben erfüllt Alle formalen Vorgaben erfüllt oder nur zu Teilen erfüllt. (PDF, Speicherort, Namensgebung)
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 8: Leitfrage Formale Vorgaben Dokumentation

2.1.5.1.2. Fachliche Beurteilungskriterien Dokumentation

Hier werden die fachlichen Beurteilungskriterien der Dokumentation festgelegt. Somit wird hier definiert, welche Inhaltlichen Punkte sowie in welcher Qualität diese erarbeitet werden müssen.

2.1.5.1.2.1. L1 - Übertragungsrate, Verfügbarkeit

Leitfrage 1	<p>Welche Übertragungsrate wäre für diese Anwendungen geeignet? Untersuchen Sie diese Frage unter der Annahme, dass die Server wie bisher beim Provider stehen und was sich an den Anforderungen verändern würde, wenn die Server bei der Firma intern betrieben würden.</p> <p>Welcher Verfügbarkeit müsste Ihre Anbindung ans Internet haben? Untersuchen Sie diese Frage unter der Annahme, dass ein Ausfall von 10 Stunden tolerierbar wäre und als zweiten Fall, dass ein Ausfall von 4 Stunden bereits untolerierbar wäre. Beachten Sie die Arbeitszeiten.</p> <p>Recherchieren Sie 5 Provider und bestimmen Sie einen geeigneten Provider für diese Firma. Ihre Entscheidung soll auf mindestens 5 Kriterien beruhen.</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 9: Leitfrage Übertragungsrate & Verfügbarkeit Dokumentation

2.1.5.1.2.2. L2 – WAN-Technologie

Leitfrage 2	<p>Vergleichen Sie verschiedene WAN-Technologien: xDSL Fibre (FTTH) Cable Radiolink Satellit</p> <p>Wie unterscheiden sich diese WAN-Technologien zueinander? Sie sollen mindestens 5 Unterscheidungsmerkmale finden und der Klasse eine sinnvolle Empfehlung abgeben, wann welche Technologie für unsere Situation vorteilhaft wäre.</p> <p>Welche Technologie bietet die sicherste Verbindung punkto Ausfallsicherheit? Welche Verbindung eignet sich auch für Backup-Leitungen?</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 10: Leitfrage WAN-Technologie Dokumentation

2.1.5.1.2.3. L3 – Internetservices

Leitfrage 3	<p>Vergleichen sie folgenden Möglichkeiten die Internetservices zu betreiben:</p> <p>eigene Server inhouse dedizierte Server (Root-Server) bei Provider Services beim Provider (Shared hosting)</p> <p>Nehmen Sie dafür für 2 Fälle einige Eckdaten an (z.B. Speicherplatz, Traffic, Dienste). Erstens eine einfache Webpräsenz zu Werbezwecken und Mail, zweitens eine komplexe Datenbankanwendung mit PHP für den Kundenzugriff.</p> <p>Welche Vergleichskriterien finden Sie, welche sind wie wichtig?</p>
--------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	Konstruieren Sie „typische Fälle“ und vergleichen Sie.
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 11: Leitfrage Internetservices Dokumentation

2.1.5.1.2.4. L4 – Sicherheit

Leitfrage 4	<p>Die Firma entscheidet sich, dass die Server alle inhouse stehen sollen.</p> <p>Welche Anforderungen an die Sicherheit gemäss ISO 27000 sind zu beachten? Bitte stellen Sie der Klasse ein sinnvolles Sicherheitskonzept für diesen Anwendungsfall vor.</p> <p>Beachten Sie, dass es technische und nicht technische Massnahmen geben kann.</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 12: Leitfrage Sicherheit Dokumentation

2.1.5.1.2.5. L5 - Wartung / Überwachung

Leitfrage 5	<p>Wie würden Sie die Überwachung des Internetzuganges dieser Firma sicherstellen?</p> <p>Beschreiben Sie konkret, mit welchen Tools Sie das machen würden. Es wird erwartet, dass Sie mindestens 5 geeignete Tools finden.</p> <p>Wie würden Sie die Wartung des Zuganges sicherstellen?</p> <p>Beschreiben Sie einen Wartungsprozess und machen Sie der Firma eine Empfehlung. Ihre Empfehlung muss auf Grund einer Evaluation mit Kriterien erfolgen.</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 13: Leitfrage Wartung & Überwachung Dokumentation

2.1.5.1.2.6. L6 – Firewall

Leitfrage 6	<p>Vergleichen Sie für einen Internetanschluss folgende Firewall-Lösungen:</p> <p>Günstige Hardware-Firewalls (Cisco-ASA, Zyxel Zywall oder ähnliche) PC-Lösung mit Linux Firewall-Service des Providers.</p> <p>Welche Vergleichskriterien finden Sie, welche sind für welche Einsatzfälle wie wichtig?</p> <p>Konstruieren Sie „typische Fälle“ und vergleichen Sie.</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 14: Leitfrage Firewall Dokumentation

2.1.5.1.2.7. L7 - VPN

Leitfrage 6	<p>Vergleichen Sie folgende VPN-Lösungen für ihren Internetanschluss:</p> <p>Hardwarelösung (Cisco-ASA oder Ähnliches) VPN-Service des Providers PC-Lösung mit Windows und Linux.</p> <p>Welche Vergleichskriterien finden Sie, welche sind für welche Einsatzfälle wie wichtig?</p> <p>Diskutieren Sie einige „typische Fälle“ und vergleichen Sie.</p>
Gütestufe 3	Alle Anforderungen wurden erfüllt (mit den Optionalen).
Gütestufe 2	Alle obligatorischen Anforderungen wurden erfüllt.
Gütestufe 1	Anforderungen wurden teilweise erfüllt.
Gütestufe 0	Anforderungen wurden nicht erfüllt.

Tabelle 15: Leitfrage VPN Dokumentation

2.1.5.2. Präsentation

Hier werden die Beurteilungskriterien der Präsentation festgelegt. Somit wird hier definiert, welche Inhaltlichen Punkte sowie in welcher Qualität diese erarbeitet werden müssen.

2.1.5.2.1. L1 – Art des Vortrages

Leitfrage 1	Folgende Gütestufen für die allgemeine Art des Vortrages:
Gütestufe 3	Frei und lebendig
Gütestufe 2	Mehrheitlich frei
Gütestufe 1	Ziemlich frei
Gütestufe 0	Monoton/abgelesen

Tabelle 16: Leitfrage Art des Vortrages Präsentation

2.1.5.2.2. L2 – Einsatz von Medien

Leitfrage 2	Es wurden mehrere Medien wie Texte, Bilder, Grafiken etc. eingesetzt:
Gütestufe 3	Gut lesbar, sehr schön
Gütestufe 2	Lesbar, Bilder & Grafiken wurden eingesetzt
Gütestufe 1	Lesbar, in Ordnung
Gütestufe 0	Schlecht lesbar / unübersichtlich

Tabelle 17: Leitfrage Einsatz von Medien Präsentation

2.1.5.2.3. L3 – Inhaltliche Dichte

Leitfrage 3	Der Vortrag war inhaltlich dicht geplant und durchgeführt.
Gütestufe 3	Vielfältig/dicht
Gütestufe 2	Inhalt dicht jedoch sehr trostlos
Gütestufe 1	In Ordnung
Gütestufe 0	Zu wenig Information

Tabelle 18: Leitfrage Inhaltliche Dichte Präsentation

2.1.5.2.4. L4 – Fachliche Tiefe

Leitfrage 4	Die Inhalte des Vortrages entsprechen einer des Publikum ansprechenden fachlichen Tiefe.
Gütestufe 3	Thema / Fachbegriffe / Auftrag fachlich sehr gut erklärt.
Gütestufe 2	Inhalte wurde teilweise erklärt, jedoch zu oberflächlich
Gütestufe 1	In Ordnung
Gütestufe 0	Zu wenig fachliche Tiefe

Tabelle 19: Leitfrag Fachliche Tiefe Präsentation

2.1.5.2.5. L5 – Ablauf

Leitfrage 5	Der Vortrag verlief reibungslos.
Gütestufe 3	Reibungslos
Gütestufe 2	Nur wenige Unterbrüche
Gütestufe 1	Viel Zeit beansprucht zum Nachdenken
Gütestufe 0	Oft Unterbrüche, weiss nicht weiter

Tabelle 20: Leitfrage Ablauf Präsentation

2.1.5.2.6. L6 – Zeitplanung

Leitfrage 6	Die vorgegebene Zeit wurde eingehalten.
Gütestufe 3	Zeit eingehalten (Plus / Minus 1 Min.)
Gütestufe 2	Plus / Minus mehr als eine Minute.
Gütestufe 1	Bis 3 Minuten Differenz
Gütestufe 0	Über 3 Minuten Differenz

Tabelle 21: Leitfrage Zeitplanung Präsentation

2.1.5.2.7. L7 - Inhaltliche Struktur

Leitfrage 7	Der Vortrag wurde logische strukturiert und hatte einen roten Faden.
Gütestufe 3	Logischer Aufbau, sehr gut strukturiert
Gütestufe 2	Struktur vorhanden, jedoch nicht durch den ganzen Vortrag erkennbar.
Gütestufe 1	Struktur teilweise erkennbar, manchmal etwas wirr
Gütestufe 0	Unlogisch, wirr, schwierig zu folgen

Tabelle 22: Leitfrage Inhaltliche Struktur Präsentation

2.2. Projektantrag


Projekttitel:	Grundlagen erarbeiten zu verschiedenen Aspekten einer Internetanbindung.	
Projektnummer:	00001	
Projektart:	Erarbeiten einer Grundlage zu verschiedenen Aspekten der Internetanbindung eines Kunden.	
Projektleiter/in:	Lüscher, Luis	
Projektmitglieder:	Barbu, Medeea Chatzimichalis, Michalis	
Projektauftraggeber/in:	Müller, Fritz (CEO Coffee GmbH)	
Projektkunde(n):	Coffee GmbH	
Projektdauer:	Geplanter Beginn: 22.11.2020 09:00 Uhr Geplantes Ende: 07.12.2020 11:50 Uhr	
Ausgangssituation / Problembeschreibung:	Ein Unternehmen hat einen veralteten Internetzugang mit einer Übertragungsrate von 50 Mbit/s im Download und 5 Mbit/s im Upload mit ADSL. Die Firma produziert Kaffeemaschinen in einer städtischen Gegend in der Schweiz. Das Marketing benutzt moderne Webapplikationen mit viel Multimediaanwendungen und ein Shop für Endkunden ist ebenfalls vorhanden. Alle Mitarbeitenden benutzen Mail und Browserapplikationen. Die Firma hat 120 Internetnutzer. Eine Firewall ist nicht vorhanden und die Server stehen alle beim Provider.	
Projektgesamtziel:	Dem Unternehmen kann anhand dieser Vorarbeit eine konkreter Vorschlag unterbreitet werden, wie die Internetanbindung verbessert werden kann.	
Projektressourcen:	Ressourcen:	Menge:
	Personal	3
	Notebooks	3
	Arbeitsplätze	3
Projektbudget	Das Projektbudget beläuft sich auf 150 000 CHF	
Sonstige relevante Informationen	Die erarbeiteten Aufgaben werden dokumentiert und zwei spezifische Themen vor der Klasse präsentiert.	
Unterschrift / Abnahme	Auftraggeber: Fritz, Müller _____	Auftragnehmer: Luis Lüscher 

Tabelle 23: Projektantrag

2.3. Arbeitsumfeld

In diesem Kapitel wird unser Arbeitsumfeld beschrieben. Wie sieht unser Arbeitsplatz aus und welche Hardware sowie Software wird für die Arbeit verwendet? Wo werden die Dokumente abgelegt?

2.3.1. Arbeitsplatz

Unser Arbeitsplatz sieht folgendermassen aus:

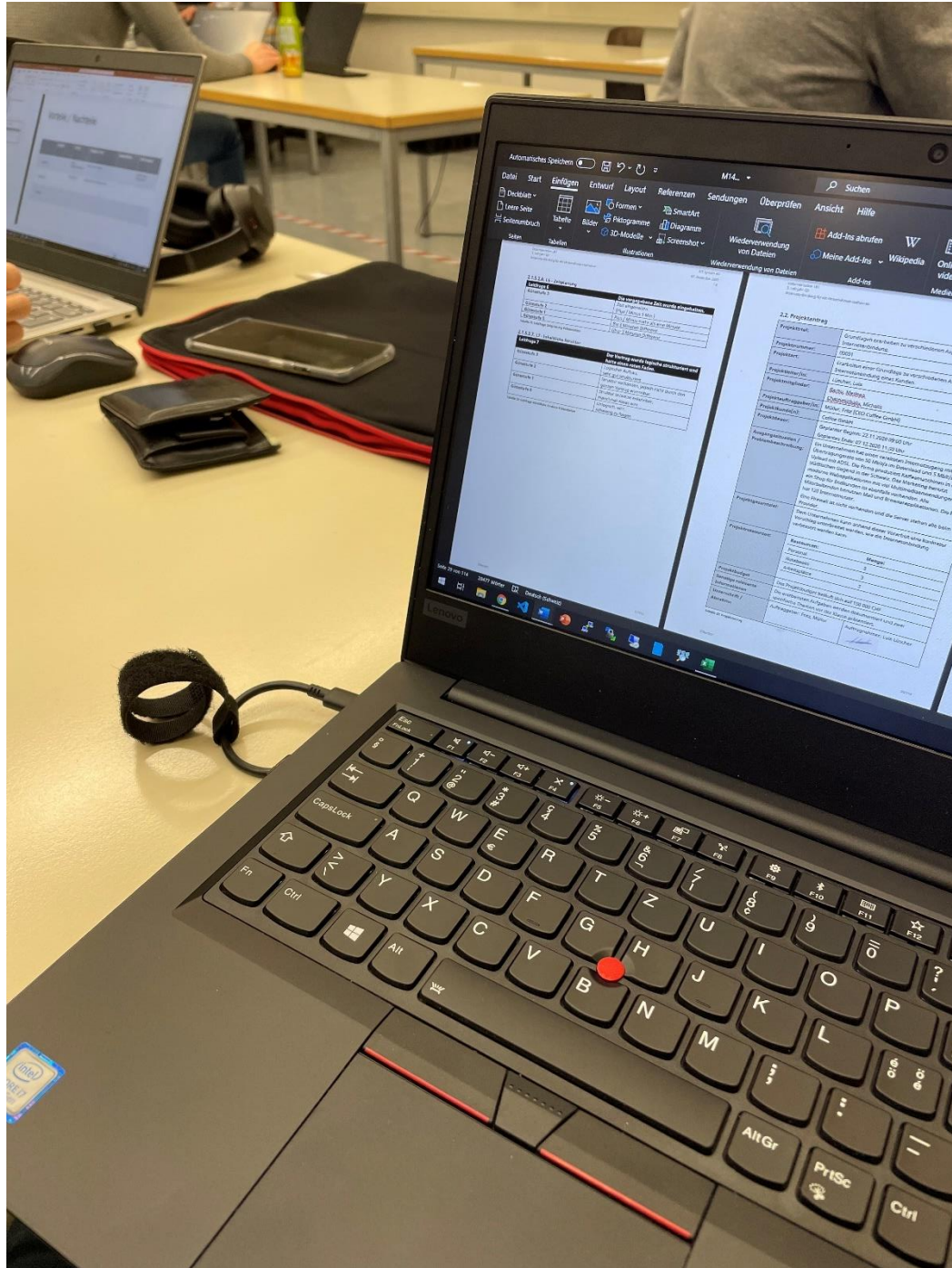


Abbildung 5: Arbeitsplatz am Platz 11 und 12 im Schulzimmer

2.3.2. Hardware & Software

2.3.2.1. Hardware Luis Lüscher

Lenovo ThinkPad E490

- **OS:** Windows 10 1909
- **CPU:** Core i7 8th Gen
- **RAM:** 8 GB
- **SSD:** 256 GB
- **GPU:** Intel UHD Graphics 620

2.3.2.2. Hardware Medeea Barbu

HP 250 G7

- **OS:** Windows 10 1909
- **CPU:** Core i7 7th Gen
- **RAM:** 16 GB
- **SSD:** 256 GB
- **GPU:** Intel UHD Graphics 620

2.3.2.3. Hardware Michalis Chatzimichalis

Acer Aspire 5

- **OS:** Windows 10 1909
- **CPU:** Core i7 8th Gen
- **RAM:** 8 GB
- **SSD:** 512 GB
- **GPU:** Intel UHD Graphics 620

2.3.2.4. Software

Im Rahmen des Projekt haben wir alle die selben Softwareprodukte verwendet:

- Google Chrome
- Mozilla Firefox
- Microsoft Word
- Microsoft Teams
- Microsoft Excel
- Adobe Acrobat Reader DC

2.3.3. Dokumentablage

Die Dokumentation wird auf dem SharePoint unseres Microsoft Teams Channel abgespeichert. Die Dokumentation wird durch Luis Lüscher geführt.

2.4. Namenskonvention

Nachfolgend werden die Namenskonventionen für alle Netzwerkgeräte beschrieben. Die Konvention ist so aufgebaut, dass man anhand des Hostnamens bereits viele Informationen erhält.

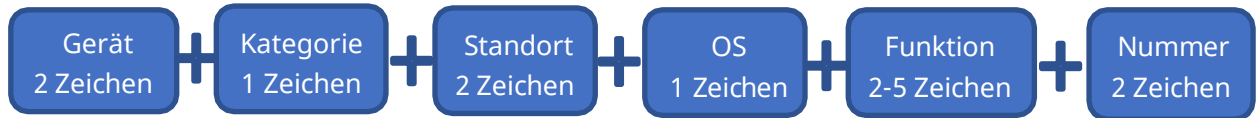


Abbildung 6: Aufbau Namenskonvention

Position	Beschreibung	Beispiel
Gerät	Eine bestimmte Abkürzung für den jeweiligen Gerätetyp.	sv =Server rt =Router
Kategorie	Wofür wird das System verwendet	p =Produktion, t =Testing, i =Integration, d =Development
Standort	Wo steht das Gerät	zh =Zürich, oe =Oberengstringen
OS	Das Betriebssystem des Servers	L =Linux, w =Windows
Funktion	Projektname, Servicename, Applikationsname	spk =Splunk ost =OS Ticket
Nummer	Aufzählung bei mehreren, gleichen Systemen.	01-99

Tabelle 24: Beschreibung Namenskonvention

2.4.1. Gerätetypen

Abkürzungen	Beschreibung
sv	Servers
ws	Workstations
pr	Printers
rt	Router
sw	Switch
fw	Firewall
ts	Terminal Servers
dc	Domain Controllers
wbs	Web Servers
msx	Mail Servers
sql	SQL Servers

Tabelle 25: Beschreibung verschiedener Gerätetypen

Beispiel: svtzhwtest01

2.5. Zeitplanung

2.5.1. Termine

Termin	Datum	Uhrzeit
Start LB1	22.11.2020	09:00
Ende LB1	07.12.2020	11:50
Präsentation	14.12.2020	Nicht bekannt

Tabelle 26: Termine

2.5.2. Arbeitstage

Tag	Datum	Pensum (in Lektionen)
1	Mo 22.11.2020	3
2	Mo 23.11.2020	3
3	Mo 30.11.2020	3
4	Mo 07.12.2020	3

Tabelle 27: Alle Arbeitstage der LB1

2.5.3. GANTT

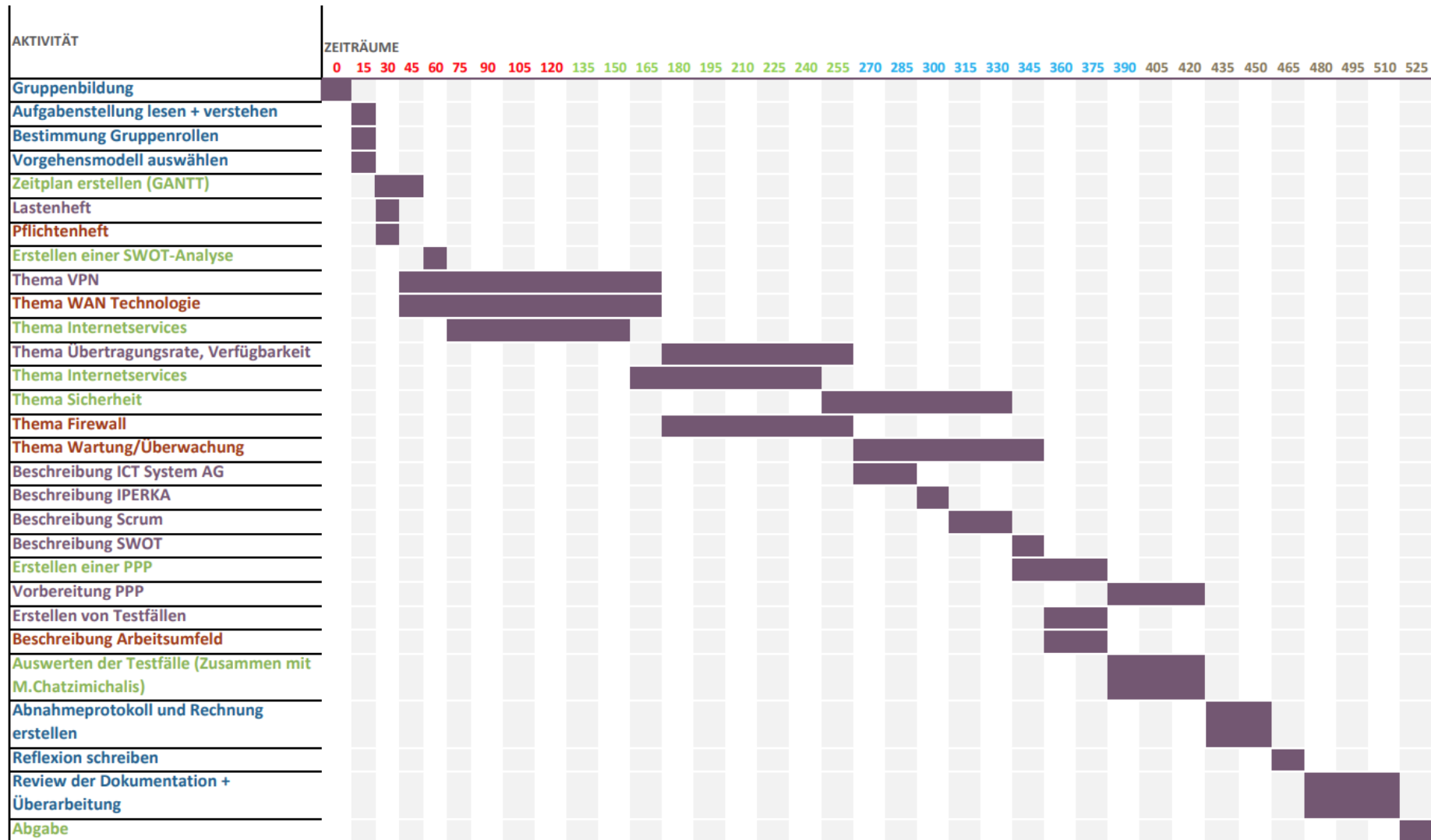


Abbildung 7: GANTT-Plan LB1

2.5.3.1. Erklärung GANTT

Der GANTT-Plan hat einen spezifischen Aufbau:

Links in der senkrechten Liste sieht man die verschiedenen Aktivitäten, die im Verlauf der 4 möglichen Tage erarbeitet werden sollten. Dabei werden unter verschiedenen Farben unterschieden:

- Aktivitäten in der alle Mitglieder mitarbeiten
- Aktivitäten die Luis Lüscher abarbeitet
- Aktivitäten die Michalis Chatzimichalis abarbeitet
- Aktivitäten die Medeea Barbu abarbeitet

Das GANTT kann auf der Website der ICT System AG heruntergeladen werden.

Unter folgenden Link steht es als XLSX Dokument zur Verfügung: https://ictsystem.ch/wp-content/uploads/2020/11/M146_LB1_Projektplan.xlsx

2.5.4. Scrum Board

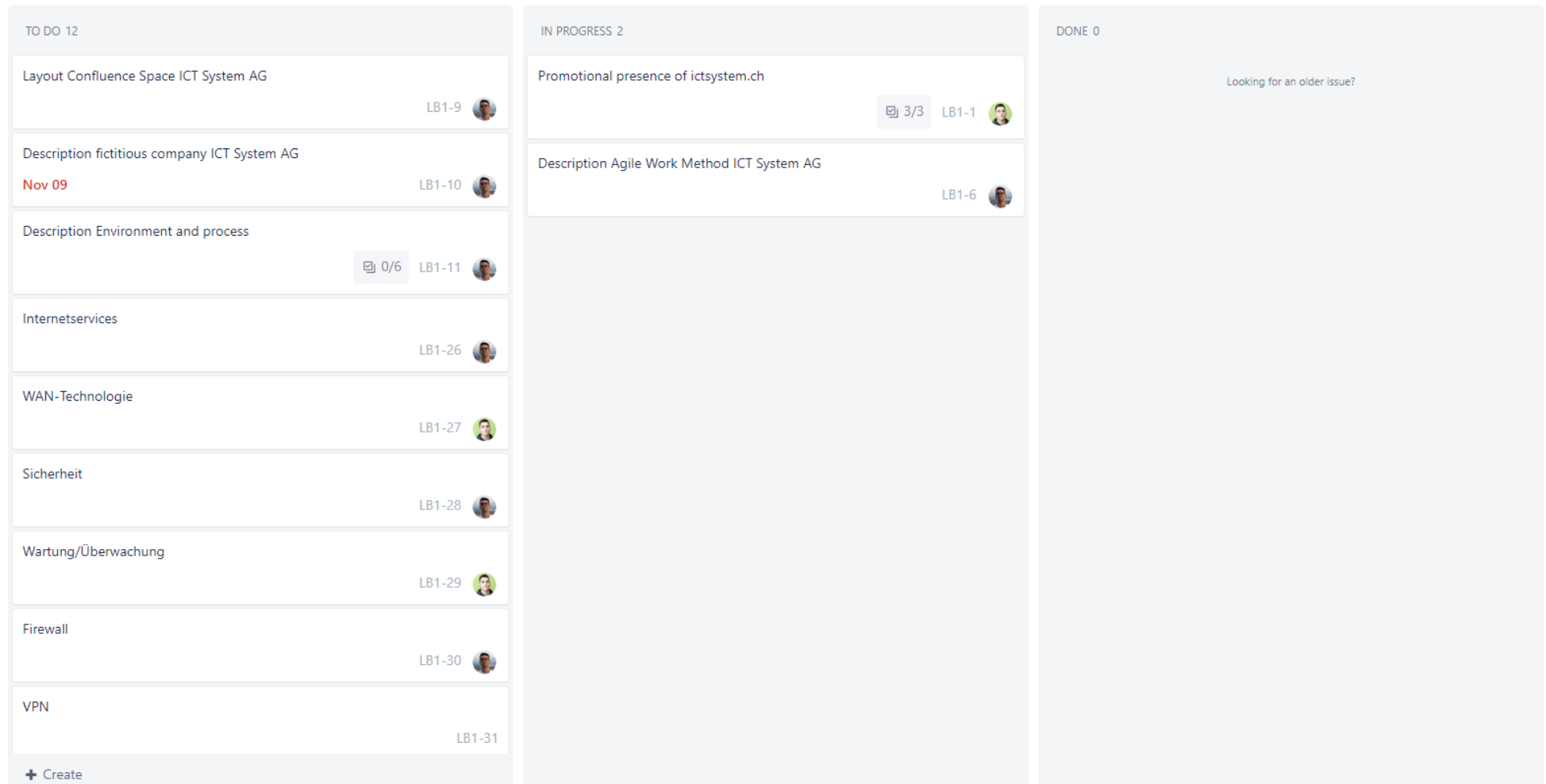


Abbildung 8: Jira Scrum Board

Dies ist eine Abbildung unseres Scrum Board welches wir via Jira realisiert haben. Alle Teammitglieder haben Zugriff auf das Board und sind dazu verpflichtet ihren aktuellen Stand hier abzubilden. Das Board dient in erster Linie für den Projektleiter, um zu überprüfen, ob das Projekt im Zeitplan ist und wo es Engpässe geben könnte. Andererseits ist so auch die Kommunikation um einiges einfacher, denn man kann Aufgabe (Task) und entsprechende Diskussion direkt im Jira führen (zB. beim Erarbeiten zuhause).

2.5.4.1. Jira Task Beispiel

The screenshot shows a Jira task interface. At the top, there's a header with 'LB1-30' and navigation icons. The task title 'Firewall' is prominently displayed. Below the title, there are buttons for 'Attach', 'Create subtask', 'Link issue', and a dropdown menu. The 'Description' section contains the following text: 'Vergleichen Sie für einen Internetanschluss folgende Firewall-Lösungen:', followed by a bulleted list: '• Günstige Hardware-Firewalls (Cisco-ASA, Zyxel Zywall oder ähnliche)', '• PC-Lösung mit Linux', and '• Firewall-Service des Providers.' Below this, it asks 'Welche Vergleichskriterien finden Sie, welche sind für welche Einsatzfälle wie wichtig?' and 'Konstruieren Sie „typische Fälle“ und vergleichen Sie.' It then states 'Folgende Ergebnisse sind zu erarbeiten (ansonsten Task nicht erledigt):' followed by another bulleted list: '• Die drei Firewall Lösungen wurden einzeln beschrieben s + Beispiel zB. PC-Lösung mit PC = pfSense etc.', '• Vor und Nachteile der einzelnen Lösungen wurden aufgezeigt', '• Zusammenfassung durch eine Übersichtliche Tabelle der Vor- und Nachteile', '• Alle Fragen wurden richtig und ausführlich beantwortet (Rot markiert)', and '• Kurzer Text in dem Beschrieben wird wie man sich entschieden hat. (Welche Technologie wird nun verwendet?)'. At the bottom, there's a comment section with a user profile picture and a text input field 'Add a comment...'. To the right, a sidebar shows metadata: 'Assignee' (Luis Ricardo Lüscher), 'Reporter' (Luis Ricardo Lüscher), 'Due date' (None), 'Labels' (Documentation), and 'Priority' (Medium). It also includes a 'Show 3 more fields' link and a 'Configure' gear icon. At the bottom of the sidebar, it shows 'Created November 6, 2020, 10:35 PM' and 'Updated 7 days ago'.

Abbildung 9: Beispiel eines Jira Task

Im Task ist in der Beschreibung ersichtlich um was es bei der Aufgabe geht und welche Kriterien erfüllt werden müssen. Zudem kann man mit der Kommentarfunktionen noch entsprechen Kommunizieren. Dies ist noch sehr praktisch, da wir ansonsten wiederum auf ein anderes Tool zurückgreifen müssen zB. WhatsApp, Microsoft Teams.

2.6. Arbeitsjournal

2.6.1. Tag 1

Tag 1	16.11.2020
Erledigte Arbeit	<ul style="list-style-type: none"> • Aufgabenstellung analysiert • Zeitplan erstellt
Zeitplan	Im Plan
Arbeitszeit	Soll: 135min Ist: 135min
Aufgetretene Probleme oder Unerwartetes	-
Lösungen	-
Beanspruchte Hilfestellung	-
Reflexion	<p>Nach einer Einleitung von Herr Widmer hat er unsere Gruppen gebildet und danach haben wir uns intern organisiert. So haben wir unsere Rollen definiert. Luis wird als Projektleiter die Organisation übernehmen und ist somit auch für die Dokumentation zuständig. Danach haben wir die Aufgabenstellung gelesen und verstanden. Zudem haben wir unser Vorgehensmodell gewählt. Wir haben uns für eine Mischung aus IPERKA und Scrum entschieden. So definieren wir unsere Projektvorgänge via IPERKA aber die einzelnen Aufgaben werden mit einer einfacheren Version von Scrum verwendet. Wir verwenden ein Scrum Board, halten wöchentlich zu Beginn der Arbeitszeit ein Meeting zum Abgleich des Arbeitsprozesses und haben klar terminierte Zeitpunkte für die Tasks (Eine Alternative zu den Sprints). Luis erarbeitete dann einen Zeitplan, Medeea erstellte ein Lastenheft und Michalis ein Pflichtenheft. Luis erstelle zudem eine SWOT-Analyse, Medeea begann das Thema VPN zu bearbeiten und Michalis das Thema WAN-Technologie. Wir sind perfekt mit dem Zeitplan. Der Abgabezeitpunkt kann sehr gut erreicht werden.</p>

Tabelle 28: Journal Tag 1

2.6.2. Tag 2

Tag 2	23.11.2020
Erledigte Arbeit	<ul style="list-style-type: none"> • Beschreibung VPN • Beschreibung WAN-Technologie • Projektplan
Zeitplan	Im Plan
Arbeitszeit	Soll: 135 Ist: 135
Aufgetretene Probleme oder Unerwartetes	-

Lösungen	-
Beanspruchte Hilfestellung	-
Reflexion	Zu Beginn der Lektion hat uns Herr Widmer etwas zum Thema FCAPS erklärt. Danach haben wir noch die Entscheidungsmatrix angeschaut, welche für die LB1 relevant ist. Danach arbeitete Luis am Projektplan, dort musste kurz was überarbeitet werden und danach begann er mit dem Thema Internetservices. Medeea arbeitete weiter am Thema VPN und Michalis am Thema WAN-Technologie. Die beiden Arbeiten wurden noch in der letzten Lektion beendet. Wir sind noch im Zeitplan und somit gut auf Kurs. Michalis und Medeea werden zuhause bereits an dem nächsten Task beginnen. Jira Scrum board ist up to date und somit funktioniert dies mit dem Board sehr gut.

Tabelle 29: Journal Tag 2

2.6.3. Tag 3

Tag 3	30.11.2020
Erledigte Arbeit	<ul style="list-style-type: none"> • Beschreibung Internetservices • Beschreibung Übertragungsrate, Verfügbarkeit • Beschreibung Sicherheit • Beschreibung Firewall • Beschreibung Wartung / Überwachung
Zeitplan	Im Plan
Arbeitszeit	Soll: 135 Ist: 135
Aufgetretene Probleme oder Unerwartetes	-
Lösungen	-
Beanspruchte Hilfestellung	-
Reflexion	Zu Beginn der Lektion hat uns Herr Widmer etwas zum Thema Firewall erklärt. Danach arbeitete Luis am Thema Internetservices, dort musste kurz was überarbeitet werden und danach begann er mit dem Thema Sicherheit. Medeea arbeitete am Thema Übertragungsrate, Verfügbarkeit und Michalis am Thema Firewall und nach dem Thema Wartung / Überwachung bearbeitet. Die Arbeiten wurden noch in der letzten Lektion beendet. Wir sind noch im Zeitplan und somit gut auf Kurs. Michalis und Medeea werden zuhause bereits an dem nächsten Task beginnen. Jira Scrum board ist up to date.

Tabelle 30: Journal Tag 3

2.6.4. Tag 4

Tag 4	07.12.2020
Erledigte Arbeit	<ul style="list-style-type: none"> • Vorbereitung PPP • Beschreibung Arbeitsumfeld • Auswerten der Testfälle • Abnahmeprotokoll und Rechnung erstellen • Reflexion schreiben • Review der Dokumentation + Überarbeitung • Abgabe
Zeitplan	Im Plan
Arbeitszeit	Soll: 135 Ist: 135
Aufgetretene Probleme oder Unerwartetes	-
Lösungen	-
Beanspruchte Hilfestellung	-
Reflexion	Zu Beginn der Lektion hat uns Herr Widmer etwas zum Thema Firewall und Zonenplan erklärt. Danach haben wir an unseren Vorträgen geübt und die LB1 erfolgreich abgeschlossen.

Tabelle 31: Arbeitsjournal Tag 4

3. Projektmanagement

3.1. IPERKA

Für dieses Projekt wird nach dem Vorgehensmodell IPERKA vorgegangen und die Planung ist entsprechend dem Modell aufgebaut. Dies spiegelt sich auch in der Dokumentation wider. IPERKA wurde bereits in einigen Schulprojekten eingesetzt und hat sich für solche Arbeiten bewährt.

Bei IPERKA beschreibt jeder Buchstabe des Namens einen Projektabschnitt:

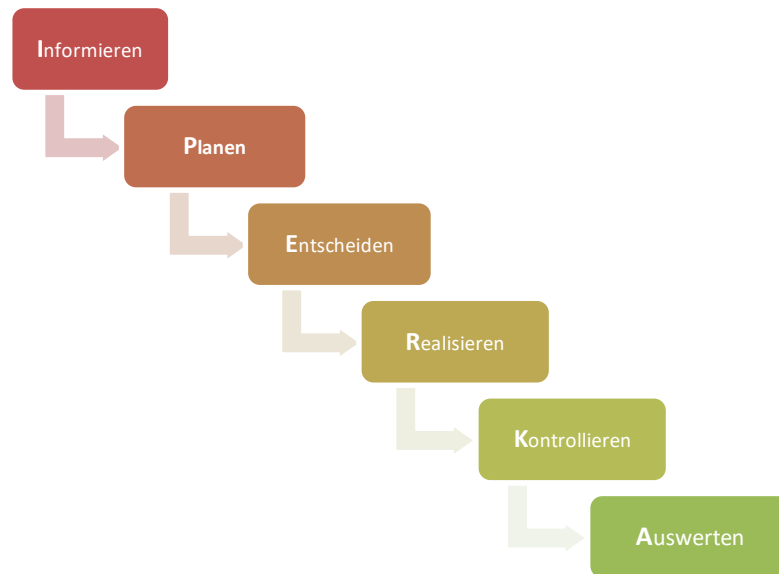


Abbildung 10: IPERKA

3.1.1. Informieren

Beim Informieren werden die Informationen abgeholt, die für die Durchführung des Projekts benötigt werden. Damit wird ein klares Bild des Auftrages geschaffen und erste Fragen werden bereits geklärt.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Wie lautet der genaue Auftrag?
- Was für Bedingungen muss ich erfüllen?
- Was ist das Ziel des Projekts?
- Habe ich die notwendigen Mittel, um das Projekt durchzuführen?

3.1.2. Planen

Beim Planen wird das ganze Projekt geplant. Sprich, hier wird ein genauer Zeitplan erstellt, in dem definiert ist, wer was wann macht. Ebenfalls werden die benötigten Ressourcen definiert. Hier soll klarwerden, wie das ganze Projekt durchgeführt wird.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Wie wird das Projekt realisiert?
- Was für Ressourcen werden benötigt?

- Was wird wann erledigt?

3.1.3. Entscheiden

Beim Entscheiden wird festgelegt, welche Tools und Produkte verwendet werden sollen, um das Projekt umzusetzen. Dafür werden passende Kriterien definiert und in Frage kommende Möglichkeiten verglichen.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Mit welcher Lösung setze ich das Projekt um?
- Ist diese Lösung sinnvoll?
- Hat die Entscheidung eine ausschlaggebende Begründung?

3.1.4. Realisieren

Beim Realisieren wird das Projekt effektiv umgesetzt. Das heisst, hier werden die geplanten Arbeiten zur Umsetzung des Projektes ausgeführt und der Auftrag nach Aufgabenstellung durchgeführt.

3.1.5. Kontrollieren

Beim Kontrollieren wird die gesamte Arbeit nochmals kontrolliert und es wird geprüft, ob das Gemachte den Anforderungen entspricht. Hier wird ein Testprotokoll erstellt und ausgefüllt und die Arbeit auf Fehler überprüft.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Entspricht mein Produkt den gestellten Anforderungen?
- Ist das Produkt vollständig getestet und fehlerlos?
- Sind alle Ziele erreicht worden?

3.1.6. Auswerten

Beim Auswerten wird auf das ganze Projekt nochmal zurückgeschaut. Es werden Erkenntnisse bezüglich der Projektarbeit festgehalten und ausgearbeitet, was in zukünftigen Projekten ähnlicher Art besser gemacht werden könnte.

Am Ende dieser Phase sind folgende Fragen beantwortet:

- Was lief gut?
- Was lief schlecht und was kann man besser machen?
- Ist man zufrieden mit dem Produkt?

3.2. Scrum

3.2.1. Rollen

Es gibt bei Scrum drei Rollen:

- Product Owner
- Scrum-Master
- Entwicklungsteam

3.2.1.1. Product Owner

Der Produkteigner vertritt die Anwender des Produkts oder die Stakeholder des Projekts. Das sind alle, die betroffen sind und ein Interesse am Erfolg des Projekts haben. Wenn eine neue Software oder IT-Lösung im Unternehmen eingeführt wird, sind das die Nutzer, denn sie wollen reibungslos mit ihren Programmen arbeiten. Bei Produkten sind es die Produktmanager, die als Stimme der Kunden auftreten. Der Produkteigner sollte wissen, was die Kunden haben wollen. Aber auch das Marketing, der Vertrieb und der Kundendienst können Anforderungen an das Projektteam stellen.

3.2.1.2. Entwicklungsteam

Ein Scrum-Team sollte zwischen fünf und zehn Mitarbeitern umfassen. Die Teammitglieder organisieren alle Aufgaben selbst. Es gibt im Team keine Hierarchie. Jeder hat dieselben Rechte und Pflichten, aber durchaus unterschiedliche Kompetenzen. Alle Fachbereiche, die zur Lösung beitragen, sollten vertreten sein. Wichtig ist, dass alle Teammitglieder aus eigenem Antrieb dabei sind. Sie sollten sich ihre Projekte selbst aussuchen können. Das setzt Vertrauen des Managements und Verantwortungsbewusstsein der Mitarbeiter voraus.

3.2.1.3. Scrum Master

Der Scrum-Master trägt die Verantwortung für den Scrum-Prozess. Der Scrum-Master ist Moderator und Unterstützer für das Projektteam. Er beseitigt Hindernisse und fördert die gute Zusammenarbeit im Team. Er beschafft die notwendigen Ressourcen und ist Ansprechpartner für Aussenstehende. Er hilft dem Team bei methodischen Problemen und stellt sicher, dass die Regeln des agilen Projektmanagements eingehalten werden.

3.2.2. Stakeholder

Stakeholder sind Rollen ausserhalb von Scrum. Die folgenden Rollen können helfen, die unterschiedlichen Stakeholder und deren Aufgaben zu differenzieren.

3.2.2.1. Kunden

Den Kunden wird das Produkt nach Fertigstellung zur Verfügung gestellt. Kunden können je nach Situation sowohl interne Fachabteilungen als auch externe Personen oder Gruppen sein. Es ist Aufgabe des Product Owners, seine Kunden durch Lieferung des Wunschproduktes zu begeistern. Deshalb sollten Product Owner und Kunden für die Dauer des Projektes im engen Austausch stehen. Vor Beginn der Entwicklung sollte der Product Owner ein möglichst genaues Verständnis von der Wunschvorstellung seiner Kunden gewinnen. Die Kunden sollten schon nach den ersten Sprints Gelegenheit haben, sich die neuen Funktionalitäten anzuschauen und hierzu Feedback zu geben.

3.2.2.2. Anwender

Anwender sind diejenigen Personen, die das Produkt benutzen. Ein Anwender kann, muss aber nicht zugleich Kunde sein. Die Rolle des Anwenders ist für das Scrum Team von besonderer Bedeutung, denn nur der Anwender kann das Produkt aus der Perspektive des Nutzers beurteilen.

Anwender und Kunden sollten beim Sprint Review und beim Product Backlog Refinement hinzugezogen werden, um das Produkt zu erproben und Feedback zu geben.

3.2.2.3. Management

Das Management trägt Verantwortung dafür, dass die Rahmenbedingungen stimmen. Dazu gehören die Bereitstellung von Räumen und Arbeitsmitteln, aber auch generell die Unterstützung für den eingeschlagenen Kurs. Das Management ist dafür verantwortlich, das Scrum-Team vor externen Arbeitsanforderungen zu schützen, adäquate personelle Besetzungen zu finden sowie den Scrum Master dabei zu unterstützen, Hindernisse auszuräumen.

3.2.3. Scrum-Prozess

Neben den Rollen ist es vor allem der Prozess, der kennzeichnend ist für Scrum. Am Anfang steht eine Produkt-Vision; eine Idee des Produkts, die der Auftraggeber des Projekts vorantreiben will und die auch den Anwendern einen Nutzen bringt. Eine solche grobe Vorstellung vom Produkt oder der Lösung, die im Scrum-Projekt erarbeitet werden soll, ist der Auftrag. Die Produkt-Vision wird in Story Cards überführt, die aus Sicht des Anwenders einzelne Elemente, Merkmale und Funktionen des Produkts beschreiben.

Mit dieser Grundlage startet ein agiles Projekt nach Scrum. Dann umfasst der Scrum-Prozess folgende Schritte:

3.2.3.1. Product Backlog anlegen und pflegen

Aus den Anforderungen des Produkteigners und den Story Cards wird ein sogenanntes Product Backlog zusammengestellt. Das ist eine Sammlung sämtlicher Funktionen und Merkmale, die das Produkt haben soll. Am Anfang ist diese Zusammenstellung noch grob, doch im Projektverlauf wird sie immer genauer.

Im Product Backlog werden Prioritäten vergeben. Eine hohe Priorität erhalten die Elemente und Funktionen, die am wichtigsten sind und eine hohe Zufriedenheit der Anwender sicherstellen. Andere Anforderungen sind nicht so wichtig, können aussortiert werden, werden mit anderen zusammengelegt, sind technisch nicht realisierbar oder werden verschoben. Sie werden dann bei der Überarbeitung oder bei der Erweiterung des Produkts behandelt.

3.2.3.2. Im Sprint Planning das Sprint Backlog erstellen

Agiles Projektmanagement mit Scrum ist ein iterativer Prozess, der sich aus mehreren Sprints zusammensetzt, bis das gewünschte Produkt fertiggestellt ist. Der Sprint ist der Kern eines Scrum-Projekts. Er ist eine fest vorgegebene Zeitdauer (Time Box) von maximal einem Monat. Im Sprint Planning werden die Aufgaben für den als nächstes anstehenden Sprint geplant und das Sprint-Ziel formuliert. Sie ergeben sich aus den Einträgen auf dem Product Backlog und den Prioritäten. Mit dem Sprint Planning wird geklärt:

- Was wird im nächsten Sprint entwickelt, erstellt oder durchgeführt?
- Wie werden die entsprechenden Aufgaben und Arbeiten erledigt?

Das Scrum-Team erstellt daraus ein Sprint Backlog. Das ist eine Auswahl der Product-Backlog Einträge für den nächsten Sprint ergänzt um den Umsetzungsplan. Ausserdem ist klar, woran sichtbar ist, ob die Aufgabe erledigt und das Teil-Produkt (Inkrement) des Sprints erstellt ist. Die sogenannte „Definition of Done“ wird formuliert.

Eine einzelne Aufgabe, die dann zu erledigen ist, wird Ticket genannt. Alle Tickets sind im sogenannten Sprint Backlog aufgeführt. Das ist der Massnahmenplan und der Arbeitsvorrat für das Entwickler-Team für den nächsten Sprint. Jedes Teammitglied übernimmt eigenverantwortlich

einzelne Tickets (Verpflichtungserklärung). Im Sprint arbeiten die Teammitglieder an ihren Aufgaben, den Tickets, bis diese fertig sind und das «Done» erreicht ist.

3.2.3.3. Im Weekly Scrum den Arbeitsfortschritt besprechen

Während des wöchentlichen, 15-minütigen Treffens, dem sogenannten Weekly Scrum, berichtet jeder der Reihe nach: Was er seit dem letzten Weekly Scrum gemacht hat, was er bis zum nächsten Weekly Scrum tun wird und was ihn bei seiner Arbeit behindert. Dabei haben alle das Sprint-Ziel im Blick und prüfen, ob es noch erreicht werden kann. Der Scrum-Master muss die Hindernisse aufgreifen und helfen, dass sie beseitigt werden.

3.2.3.4. Im Sprint-Review die Sprint-Ergebnisse prüfen und abnehmen

Jeder Sprint wird durch ein Sprint Review Meeting abgeschlossen. Das Team stellt die Ergebnisse und die Teil-Produkte dem Produkteigner vor. Er prüft, ob sie den Kriterien entsprechen, die mit der Definition of Done festgelegt wurden. Ist das der Fall, nimmt er die Sprint-Ergebnisse ab. Der Eintrag im Sprint Backlog ist damit abgehakt. Gleichzeitig werden die Einträge im Product Backlog aktualisiert oder angepasst.

Mit den Ergebnissen aus dem Sprint Review und mit dem überarbeiteten Product Backlog kann der nächste Sprint starten. Der Prozess beginnt wieder mit Schritt 2. Es folgen so viele Sprints, bis das Produkt entwickelt und das Projekt abgeschlossen ist.

3.2.3.5. Mit einer Sprint Retrospective die Zusammenarbeit besprechen

In gesonderten Treffen zwischen einem Sprint Review und dem nächsten Sprint Planning können die Teammitglieder besprechen, wie der Sprint in Bezug auf die Zusammenarbeit der beteiligten Personen, Abläufe, Kommunikation und Werkzeuge verlief. Sie halten fest, was für den nächsten Sprint verbessert werden sollte. Die Erkenntnisse sollten für zukünftige Scrum-Projekte genutzt werden; so wird ein Lernprozess unterstützt.

Alle Schritte im Scrum-Prozess sind in der folgenden Abbildung zusammengefasst.

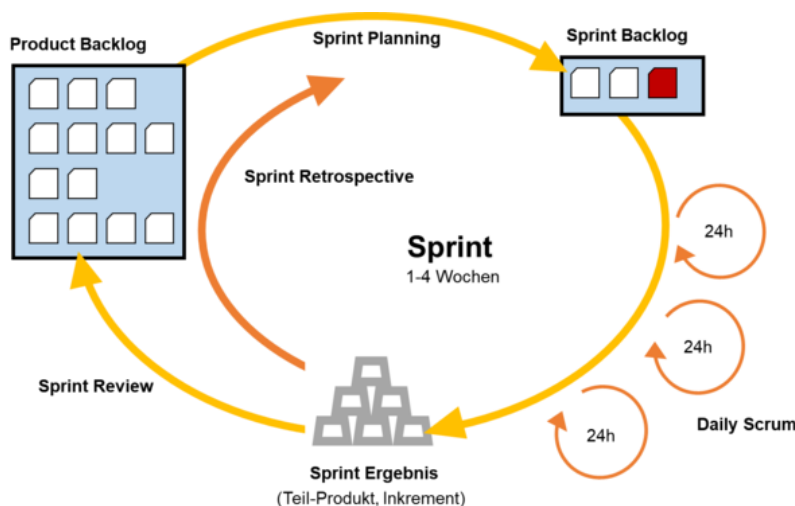


Abbildung 11: Scrum-Prozess von business-wissen.de

3.2.4. Kanban-Board

Damit alle Projektmitarbeiter eine Übersicht über den Projektstand und den Verlauf haben, werden bei Scrum alle Tickets eines Sprint Backlogs auf einer Tafel festgehalten (Task-Board). Dort wird sichtbar, was noch ansteht, was gerade in Bearbeitung ist und was schon fertig ist. Das Sprint

Backlog, der Aufgabenplan, hängt also für alle sichtbar an der Wand. Mit der Task-Board kann der Projektablauf transparent gesteuert werden. Sie wird dann Kanban-Board genannt.

Nach dem Kanban-Prinzip werden nur so viele Tickets für die Bearbeitung freigegeben, wie vom Projektteam bearbeitet werden können. Geht es an einer Stelle nicht voran, stauen sich dort die Tickets. Es wird schnell sichtbar, wo der Engpass liegt und was getan werden kann. Eilige Tickets können vorgezogen werden. So steuert das Team die Aufgabenverteilung und den Arbeitsfluss völlig selbstständig mit dem Kanban-Board als Wandtafel.

Kanban-Fluss – Wertschöpfung

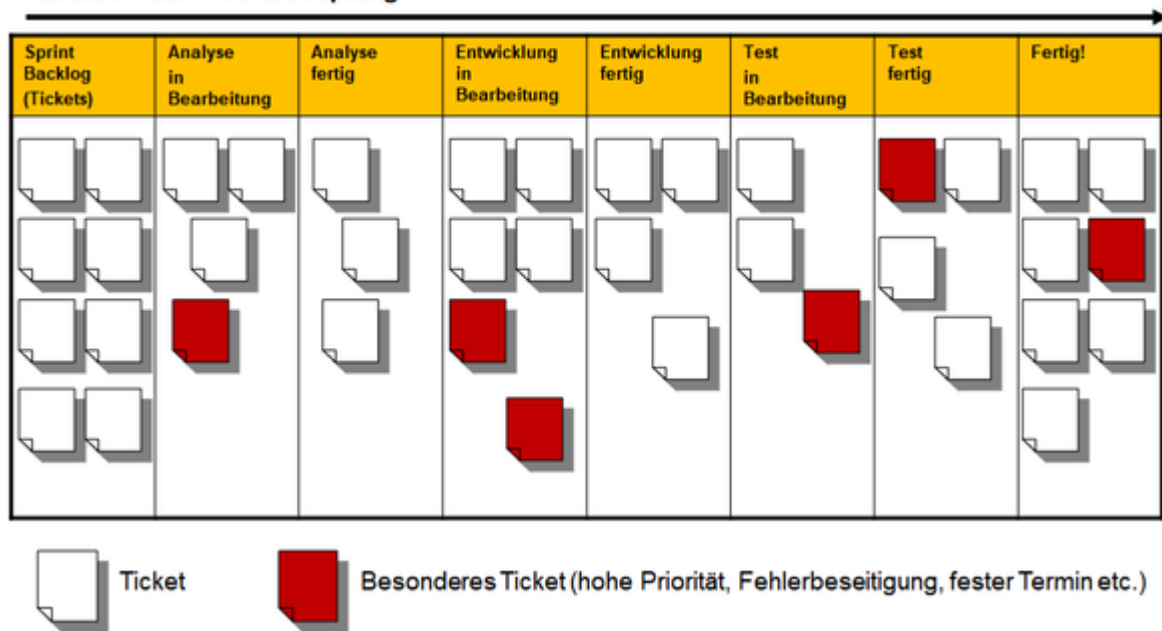


Abbildung 12: Kanban-Board von business-wissen.de

3.3. Projektaufbauorganisation

Das Projekt ist folgendermassen organisiert:

- **Johan Widmer** ist der Auftraggeber.
- **Luis Lüscher** ist der Projektleiter und leitet das gesamte Projekt. Die wichtigste Entscheidung muss er beim Abschnitt «Entscheiden» fällen. Dieser Schritt ist im IPERKA Model, sehr relevant für den Projektverlauf. Unterstützt wird er dabei von den beiden System Engineers. Zudem ist er für die Projektdokumentation verantwortlich.
- **Michalis Chatzimichalis** ist Teil des Projektteams und ist als System Engineer eingestellt. ist Teil des Projektteams und ist als System Engineer eingestellt. Sein Hauptaufgabentätigkeitsgebiet liegt in der Realisation sowie im Teil Kontrollieren. Zudem unterstützt er auch die Projektleitung bei verschiedenen Aufgaben.
- **Medeea Barbu** ist Teil des Projektteams und ist als System Engineer eingestellt. Ihr Hauptaufgabentätigkeitsgebiet liegt in der Realisation sowie im Teil Kontrollieren. Zudem unterstützt sie auch die Projektleitung bei verschiedenen Aufgaben.

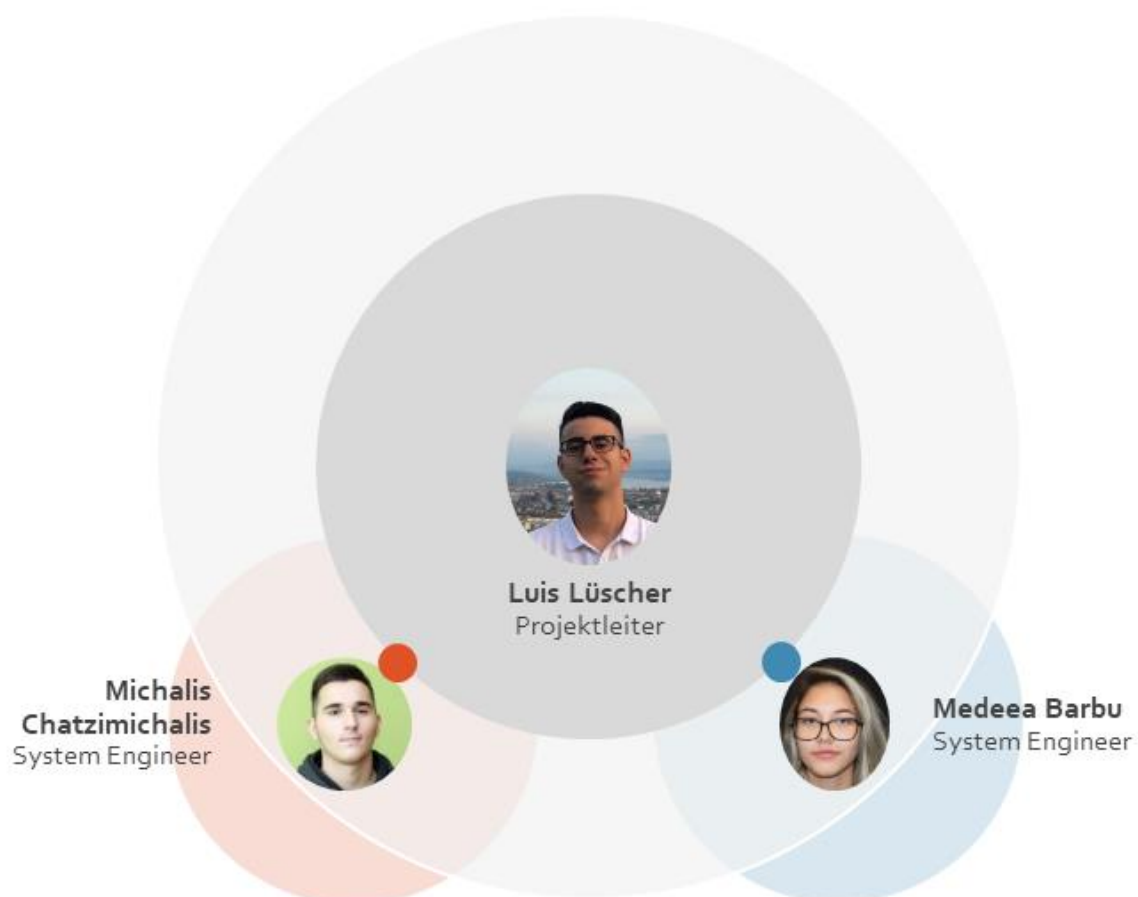


Abbildung 13: Projektorganigramm

3.3.1. Berufsbeschreibung Projektleiter

Beschreibung von [wikipedia.org](https://de.wikipedia.org)

Im Rahmen der Projektplanung bestehen die Hauptaufgaben des Projektleiters in der Ressourcen- und Budgetplanung sowie in der Festlegung der Ziele des Projekts.

- *Projektdefinition*
- *Projektorganisation*
- *Projektplanung*
- *Kommunikation*
- *Umfeldmanagement*
- *Projektcontrolling*
- *Projektdokumentation*
- *Mitarbeiterführung*

3.3.2. Berufsbeschreibung System Engineer

Der Systemtechniker beschäftigt sich mit der Funktionalität verschiedener Hardwarekomponenten. In diesem Bereich ist er vor allem für die systemorientierte Installation, Wartung und Planung zuständig.

- Wartung sowie Installation neuer Komponenten
- Verantwortung der gesamten IT-Infrastruktur
- Planen, realisieren und administrieren von ICT-Netzwerken
- Verfügbarkeit von Diensten sicherstellen
- Schulung von Anwendern
- Störungsmanagement
- Dokumentieren der Arbeit (Nachvollziehbarkeit)

3.4. Lastenheft

3.4.1. Offerte

ICT System AG

ICT System AG | Ausstellungsstr. 70 | 8005 Zürich
 Alan Brunner
 Altbergstrasse 19
 8953 Dietikon

Offert Nr. 2020-187
 Datum 29.11.2020
 Kundennummer 745682
 Ihr Ansprechpartner Luis Lüscher
 UID: 1234567

Offerte Nr. 2020-187

Sehr geehrte Damen und Herren

Vielen Dank für Ihre Anfrage. Wir erlauben uns, Ihnen die folgende Offerte zu unterbreiten.
 Dies beinhaltet nur die Analyse des momentanen Zustand sowie der Erarbeitung eines Vorschlag.

Pos.	Bezeichnung / Beschreibung	Menge	Preis/Stück	Positionspreis
1	Analyse IST-Zustand pro Stunde	2	120.00 CHF	240.00 CHF
2	Lösung Übertragungsrate, Verfügbarkeit pro Stund	3	120.00 CHF	360.00 CHF
3	Lösung WAN-Technologie pro Stunde	3	120.00 CHF	360.00 CHF
4	Lösung Internetservices pro Stunde	3	120.00 CHF	360.00 CHF
5	Lösung Sicherheit pro Stunde	3	120.00 CHF	360.00 CHF
6	Lösung Wartung & Überwachung pro Stunde	3	120.00 CHF	360.00 CHF
7	Lösung Firewall pro Stunde	3	120.00 CHF	360.00 CHF
8	Lösung VPN pro Stunde	3	120.00 CHF	360.00 CHF
9	Administrationskosten	1	180.00 CHF	180.00 CHF
	Zwischensumme			2'940.00 CHF
	Skonto	2%		58.80 CHF
	Mehrwertsteuer	7.7%		226.38 CHF
	Rechnungsbetrag	Inkl. MwSt.		3'107.58 CHF

Wir würden uns sehr freuen, diesen Auftrag für Sie ausführen zu dürfen!

Bei Rückfragen stehen wir jederzeit gerne zur Verfügung.

Gültigkeit der Offerte bis zum: 16.11.2020

Freundliche Grüsse

Luis Lüscher
 Projektleiter

ICT System AG
 Ausstellungsstr. 70
 8005 Zürich
 Schweiz

Credit Suisse AG
 IBAN CH 00 5905 6000 0541 9545
 BIC ABCDEF
 UID: 99999999

Tel.: +41 78 906 7005
 Web: ictsystem.ch

Abbildung 14: Offerte für die Coffee GmbH

Die Offerte kann [hier](#) heruntergeladen werden.

3.5. Pflichtenheft

3.5.1. Auftragsbestätigung

ICT System AG

Ausstellungsstrasse 70, 8005 Zürich

AUFTRAGSBESTÄTIGUNG

Empfänger:

Coffee GmbH
 Alan Brunner
 Altbergstrasse 19
 8953 Dietikon

Datum: 29.11.2020

Nummer: 2020-187

Kundennummer: 745682

Ausgestellt von: Michalis Chatzimichalis

Ansprechpartner: Luis Lüscher

Auftragsbestätigung

Sehr geehrter Herr Brunner

Gemäss Ihrer Bestellung vom 07.11.2020 stellen wir Ihnen folgende Auftragsbestätigung zu:

Bezeichnung	Anzahl	Einheit	Preis/Einheit	Mwst	MwSt-Betrag	Gesamt
Analyse IST-Zustand pro Stunde	2	h	120.00 CHF	7.7%	18.48 CHF	258.48 CHF
Lösung Übertragungsrate, Verfügbarkeit	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung WAN-Technologie	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung Internetservices	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung Sicherheit	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung Wartung & Überwachung	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung Firewall	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Lösung VPN	3	h	120.00 CHF	7.7%	27.72 CHF	387.72 CHF
Administrationskosten	1	Stk	180.00 CHF	7.7%	13.86 CHF	193.86 CHF

Zahlungskonditionen 20 Tage

Nettobetrag 2'940.00 CHF

Skonto 2% 58.80 CHF

MwSt. Betrag 226.38 CHF

Gesamtbetrag 3'107.58 CHF

Zögern Sie bitte nicht, uns bei Fragen zu kontaktieren. Sie erreichen uns jederzeit unter der Telefonnummer: +41 78 906 7005

Ihren Auftrag wird bis am 07.12.2020 ausgeführt.

Wir bedanken uns für Ihren Auftrag und Ihr Vertrauen.

ICT System AG

Ausstellungsstrasse 70

8005 Zürich

Schweiz

Kontaktinformation

Luis Lüscher | Junior Project Manager

Telefon +41 78 906 70 05

Email: l.luescher@ictsystem.ch

www.ictsystem.ch

Abbildung 15: Auftragsbestätigung für die Coffee GmbH

Die Auftragsbestätigung kann [hier](#) heruntergeladen werden.

3.5.2. Pflichtenheft Projektleiter

Stelle besetzt durch: Luis Lüscher

Folgende Pflichten innerhalb des Projekt:

- Teamorganisation
- Projektdokumentation
- Übersicht im Team
- Verlauf der Projektes bestimmen
- Zeitplan erstellen (Gantt)
- Bestimmung Gruppenrollen
- Aufgabenstellung lesen + verstehen
- Vorgehensmodell auswählen
- Zeitplan erstellen
- Ziele definieren
- Arbeitsjournal führen
- Unterstützung des Projektteam im «Daily Business»
- Review der Dokumentation
- Abgabe der Projektprodukte

3.5.3. Pflichtenheft System Engineer

Stellen besetzt durch: Michalis Chatzimichalis, Medeea Barbu

Folgende Pflichten innerhalb des Projekt:

- Abarbeiten der Aufgaben gemäss Aufgabenaufteilung
- Unterstützung der Projektleitung in verschiedenen Tätigkeiten
- Beschreibung Umfeld und Aufgabe
- Schreiben einer Reflexion
- Review der Dokumentation + Überarbeitung
- Aufgabenstellung lesen + verstehen
- Abnahmeprotokoll erstellen
- Rechnung erstellen
- Projektstatus an Projektleiter melden

3.6. Aufgabenaufteilung

Hier werden die effektiven Aufgaben der einzelnen Projektmitglieder aufgelistet. Diese stehen direkt oder indirekt im Zusammenhang mit dem im GANTT-Projektplan ersichtlichen Aktivitäten. Diese Aufgaben sind verbindlich und sind 1:1 so ins Jira übertragen worden.

Fett markierte Task sind von allen Beteiligten zusammen zu erarbeiten.

3.6.1. Aufgaben Luis Lüscher

- Pflegen der Dokumentation
- Beschreibung der Vorgehensmodelle
- Erstellen eines Zeitplan
- Erstellen einer Website
- Erstellen einer SWOT-Analyse
- Erstellen einer Risikoanalyse
- Beschreibung Thema Internetservices
- Beschreibung Sicherheit
- Erstellen einer PPP
- Auswerten der Testfälle (Mit M.Chatzimichalis)
- **Abnahmeprotokoll und Rechnung erstellen**
- **Reflexion schreiben**
- **Review der Dokumentation + Überarbeitung**

3.6.2. Aufgaben Medeea Barbu

- Erstellen eines Lastenheft
- Erstellen einer Offerte
- Beschreibung Thema VPN
- Beschreibung ICT System AG
- Beschreibung IPERKA
- Beschreibung Scrum
- Beschreibung SWOT
- Vorbereitungen PPP
- Erstellen von Testfällen
- **Abnahmeprotokoll und Rechnung erstellen**
- **Reflexion schreiben**
- **Review der Dokumentation + Überarbeitung**

3.6.3. Aufgaben Michalis Chatzimichalis

- Implementation von definierten Elementen auf der Website
- Erstellen eines Pflichtenheft
- Beschreibung Thema WAN Technologie
- Thema Firewall
- Thema Wartung/Überwachung
- Beschreibung Arbeitsumfeld
- Beschreibung Arbeitsumfeld
- Auswerten der Testfälle (Mit L.Lüscher)
- **Abnahmeprotokoll und Rechnung erstellen**
- **Reflexion schreiben**
- **Review der Dokumentation + Überarbeitung**

3.7. SWOT

Die SWOT-Analyse Strengths (Stärken), Weaknesses (Schwächen), Opportunities (Chancen), Threats (Gefahren) ist ein Werkzeug des strategischen Managements, wird aber auch für die Qualitätsentwicklung von Programmen und Projekten eingesetzt. Mit dieser einfachen und flexiblen Methode können sowohl Stärken und Schwächen innerhalb des Projektes als auch externe Chancen und Gefahren betrachtet werden. Aus dieser Kombination kann eine Strategie für die weitere Ausrichtung von Partizipationsprojekten abgeleitet werden.

3.7.1. Vorteile SWOT

- Schnelle Auseinandersetzung mit positiven und negativen Aspekten einer Situation.
- Projizierung dieser Situation in die Zukunft.

3.7.2. Nachteil SWOT

- Oberflächliche Ergebnisse bei fehlender Ernsthaftigkeit oder Infragestellen des Nutzens möglich.

3.7.3. SWOT Beschreibung

Um die einzelnen Bereiche zu untersuchen, bieten sich unter anderen folgende Fragen an:

3.7.3.1. Strengths (Stärken)

- Was zeichnet dein Unternehmen aus?
- Was sind/waren seine grössten Erfolge?
- Und im direkten Vergleich: Was kann das Unternehmen besser als seine Wettbewerber?

3.7.3.2. Weaknesses (Schwächen)

- Worin ist das Unternehmen nicht gut?
- Was fehlt im Unternehmen?
- Und wieder im direkten Vergleich: Was können die Wettbewerber besser?

3.7.3.3. Opportunities (Chancen)

- Welche positiven Trends zeichnen sich ab?
- Welche gesellschaftlichen, wirtschaftlichen, technologischen oder politischen Entwicklungen könnten dem Unternehmen zugutekommen?
- Welche sonstigen Rahmenbedingungen sind positiv (oder ändern sich in eine positive Richtung)?

3.7.3.4. Threats (Bedrohungen)

- Welche negativen Trends zeichnen sich ab?
- Welche gesellschaftlichen, wirtschaftlichen, technologischen oder politischen Entwicklungen könnten dem Unternehmen schaden?
- Welche sonstigen Rahmenbedingungen sind negativ (oder ändern sich in eine negative Richtung)?

3.7.4. SWOT Strategien

Mit der Analyse der vier Bereiche ist hat man nun zwar einen guten Überblick über die aktuelle Situation sowie anstehende Herausforderungen, aber wenn man jetzt aufhört, verpasst man einen wichtigen abschliessenden Analyseschritt.

Das eigentliche Ziel einer SWOT Analyse ist es nämlich nicht, diese Faktoren einfach zu sammeln, sondern – darauf aufbauend – strategische Massnahmen zu identifizieren. Dafür musst du nun die Wechselwirkungen der vier Bereiche analysieren. Aus den unterschiedlichen Kombinationen kann man wiederum vier Kategorien an strategischen Massnahmen ableiten:

3.7.4.1. SO-Strategie Strengths und Opportunities

- «Welche Stärken können wir nutzen, um von den Chancen zu profitieren?»
- Strategien, die hieraus abgeleitet werden, fallen in die Kategorie «Führungsposition ausbauen» und sind relativ einfach durchzuführen.

3.7.4.2. WO-Strategie Weaknesses und Opportunities

- «Welche Schwächen hindern uns daran, die Chancen zu nutzen?»
- Hieraus ergeben sich Strategien aus der Kategorie «Zum Wettbewerb aufholen».

3.7.4.3. ST-Strategie Strengths und Threats

- «Welche Stärken können wir nutzen, um Bedrohungen zu reduzieren?»
- Massnahmen aus diesem Bereich fallen in die Kategorie «Absichern».

3.7.4.4. WT-Strategien Weaknesses and Threats

- «Welche Schwächen hindern uns daran, die Bedrohungen zu reduzieren?»
- Massnahmen aus dieser Kombination fallen in die Kategorie «Vermeiden».

3.7.5. SWOT-Analyse

SWOT-Analyse		Projektanalyse	
		Stärken (Strengths)	Schwächen (Weaknesses)
<p>Im Rahmen von: Projektarbeit M146 «Internetanbindung für ein Unternehmen realisieren»</p> <p>Durchgeführt durch: Medeea Barbu, Michalis Chatzimichalis, Luis Lüscher</p> <p>Datum: 26. Oktober 2020</p>		<p>S1: Hohe Motivation der MA S2: Gute Sozialkompetenz S3: Erfahrungen in Bereich S4: Kurze Entscheidungswege S5: Hohes Selbstbewusstsein S6: Gute Dokumentation, da viel Erfahrung von Luis</p>	<p>W1: Dokumentation wird nur durch eine Person geführt W2: Abhängig von jedem Gruppenmitglied, da sehr straffer Zeitplan.</p>
Umweltanalyse	<p>Chancen (Opportunities)</p> <p>O1: Bessere Lösung als andere Teams erarbeiten O2: Umfangreiche Dokumentation O3: Zeitplan wird gelockert.</p>	<p>Aus welchen Stärken ergeben sich neue Chancen?</p> <p>SO1: Erarbeitung von tollen Produkten, da alle hohe Motivation haben. (Motivation MA) SO2: Umfangreiche Dokumentation, da hohe Motivation sowie erfahrene Projektmitglieder.</p>	<p>Schwächen eliminieren, um neue Chancen zu nutzen</p> <p>WO1: Arbeit gut aufteilen, sodass Last entsprechend verteilt ist. WO2: Kommunikation gut aufrechterhalten, sodass Engpässe ausgeschlossen werden können</p>
	<p>Risiken (Threats)</p> <p>T1: Umfang der Arbeit könnte zu gross sein. T2: Einfluss anderer Teams auf unser Projekt</p>	<p>Welche Stärken minimieren Risiken?</p> <p>ST1: Sozialkompetenz ist sehr gut, Kollaboration somit kein Problem. ST2: Kurze Entscheidungswege, dadurch schnelle Entscheidungen. (Weniger Diskussionen)</p>	<p>Strategien, damit Schwächen nicht zu Risiken werden?</p> <p>WT1: Dokumentation sollte vor der Abgabe durch alle Projektmitglieder angeschaut werden.</p>

Tabelle 32: SWOT-Analyse

Öffentlich

3.8. Risikoanalyse

3.8.1. Erklärung

Bei der Risikoanalyse handelt es sich um eine vorausschauende Diagnose, um mögliche Probleme zu erkennen, einzudämmen und zu minimieren.

Gründe für eine Risikoanalyse sind die Prävention für eventuell auftauchende Probleme, die vorausschauende Planung des Projektes und die Garantie eines reibungslosen Ablaufs.

3.8.2. Vorgehensweise

1. Ziele SMART beschreiben
 - a. M, R und T sind Vorgaben der Risikoanalyse
2. Risikobereich identifizieren
 - a. Suchen von möglichen Risiken, dabei alle Projektdimensionen beachten (Qualität, Ressourcen, Zeit). Dabei ist es wichtig, die Ursachen der Risiken zu benennen – nicht die Symptome (progressiv abstrahieren).
3. Symptome benenne
 - a. Symptome sind Erkennungsmerkmale für Risiken, die anzeigen, ob ein Problem bereits eingetreten ist oder eintreten droht.
4. Risiken bewerten und gewichten mittels Risikomatrix
 - a. Jedem Risiko die Kriterien «Wahrscheinlichkeit des Eintreffens» und Tragweite zuordnen.
5. Vorbeugende Massnahmen umsetzen mittels Risikoanalysetabelle
 - a. Verbindliche Umsetzung von Gegenmassnahmen, die entweder das Problem verhindern oder seine Auswirkung begrenzen.
6. Eventuellmassnahmen planen (Alternativplan, katastrophenplan) mittels Risikoanalysetabelle
 - a. Bei besonderen kritischen Problembereichen sollen bereits in der Planungsphase alternativen Vorgehensweisen vorgesehen werden.

3.8.3. Risikoanalysetabelle

Nr.	Risiko	Symptome	Wahrscheinlichkeit	Tragweite	Gegenmassnahmen
Nr. 1	Abgabetermin kann nicht eingehalten werden	- Termin werden gemäss - Zu viele Meinungen sind zu berücksichtigen	Mittel	Hoch	- Kunden auf kritische Termine hinweisen. - Zu Entscheidungen verpflichten - Meinungen nur berücksichtigen anhand Empfehlung Projektleiter (Sofort einleiten)
Nr. 2	Budget wird nicht eingehalten	- Kosten höher als Budget - Kunde hat Bedenken bei den Kosten	Mittel	Mittel	- Genügend kostengünstigere Alternativen vorbereiten - Erarbeitetes Resultat gut verkaufen, sodass Kunde keine Bedenken hat. (Sofort einleiten)
Nr. 3	Kunde kann nicht bezahlen	- Rechnungen werden nicht bezahlt	Niedrig	Hoch	- Finanzen vor Projekt abklären - Anzahlung verlangen
Nr. 4	Dokumentation geht verloren	- Dokumentation ist nicht mehr auffindbar - Dokumentation ist veraltet	Niedrig	Mittel	- Backup erstellen (Sofort einleiten) - Regelmässig in Teams Chat hochladen.
Nr. 5	Zu wenig Quellen für Informationen	- Es sind nicht genügend Informationen in einer Quelle	Niedrig	Niedrig	- Genügende Quellen vorbereiten - Quellen mit Kunde besprechen

Tabelle 33: Risikoanalysetabelle

3.8.4. Risikomatrix

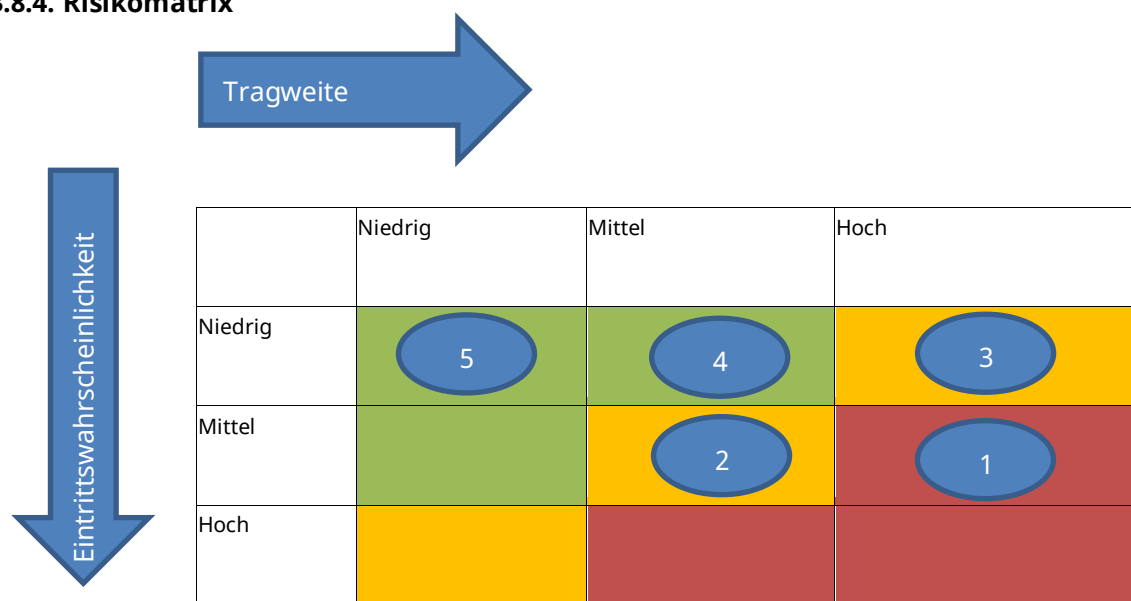


Tabelle 34: Risikomatrix

4. Informieren

In diesem Teil der Dokumentation wird der Auftrag analysiert und ein klares Bild des Auftrages geschaffen. Welche Bedingungen müssen erfüllt werden und sind die notwendigen Mittel vorhanden.

4.1. Auftrag klären

Folgende Aufgabenstellung wurde im Zusammenhang mit dem Projekt angegeben.

Originaltext gemäss MP146_LB1_v2.0.docx

Sie untersuchen in Gruppen die unten aufgeführten Themen im Zusammenhang mit der Internetanbindung eines Unternehmens. Dazu sollen Sie zu jedem Thema:

- *Zu jedem Thema die Leitfragen bearbeiten. Neue Fachwörter erklären und Zusammenhänge möglichst in einer grafischen Darstellung visualisieren.*
- *verschiedene Realisierungsmöglichkeiten (-Varianten) zeigen und erläutern.*

Zu zwei Themen sollen Sie in der Gruppe:

- *Vergleichskriterien bestimmen und damit die Realisierungsmöglichkeiten bewerten.*
- *typische Einsatzfälle definieren, und aus deren Sicht mit möglichen Vergleichskriterien gewichten.*

Sie werden die Erkenntnisse zu allen Themen in einer Dokumentation zusammenfassen und zusätzlich zwei Themen in einem Vortrag präsentieren.

Die Dokumentation soll im Sinne eines Leitfadens Ihre gesammelten Erkenntnisse, Empfehlungen und Varianten enthalten.

Zu zwei Themen soll auch eine Entscheidungstabelle erstellt werden und eine Entscheidungstabelle soll in der Präsentation vorgestellt werden. Für einen konkreten Einsatzfall sollen Sie zu einem Entscheid für eine bestimmte Variante kommen.

- *Vorgehen dokumentieren (IPERKA, etc.).*
- *Grundlagen zum Thema erarbeiten.*
- *verschiedene Realisierungsmöglichkeiten (-Varianten) zeigen und erläutern.*
- *Vergleichskriterien bestimmen (min. 5) und damit die Realisierungsmöglichkeiten bewerten.*
- *typische Einsatzfälle definieren und aus deren Sicht mit möglichen Vergleichskriterien gewichten.*

4.2. Formulierung des Auftrages

4.2.1. Aufgabenformulierung

Originaltext gemäss MP146_LB1_v2.0.docx

Ein Unternehmen hat einen veralteten Internetzugang mit einer Übertragungsrate von 50 Mbit/s im Download und 5 Mbit/s im Upload mit ADSL. Die Firma produziert Kaffeemaschinen in einer städtischen Gegend in der Schweiz. Das Marketing benutzt moderne Webapplikationen mit viel Multimediaanwendungen und ein Shop für Endkunden ist ebenfalls vorhanden. Alle Mitarbeitenden benutzen Mail und Browserapplikationen. Die Firma hat 120 Internetnutzer. Eine Firewall ist nicht vorhanden und die Server stehen alle beim Provider.

4.2.2. Themenübersicht

Originaltext gemäss MP146_LB1_v2.0.docx

Nr.	Themen
1.	<p>Übertragungsrate, Verfügbarkeit</p> <p><i>Welche Übertragungsrate wäre für diese Anwendungen geeignet? Untersuchen Sie diese Frage unter der Annahme, dass die Server wie bisher beim Provider stehen und was sich an den Anforderungen verändern würde, wenn die Server bei der Firma intern betrieben würden.</i></p> <p><i>Welcher Verfügbarkeit müsste Ihre Anbindung ans Internet haben? Untersuchen Sie diese Frage unter der Annahme, dass ein Ausfall von 10 Stunden tolerierbar wäre und als zweiten Fall, dass ein Ausfall von 4 Stunden bereits untolerierbar wäre. Beachten Sie die Arbeitszeiten.</i></p> <p><i>Recherchieren Sie 5 Provider und bestimmen Sie einen geeigneten Provider für diese Firma. Ihre Entscheidung soll auf mindestens 5 Kriterien beruhen.</i></p>
2.	<p>WAN-Technologie</p> <p><i>Vergleichen Sie verschiedene WAN-Technologien: xDSL Fibre (FTTH) Cable Radiolink Satellit</i></p> <p><i>Wie unterscheiden sich diese WAN-Technologien zueinander? Sie sollen mindestens 5 Unterscheidungsmerkmale finden und der Klasse eine sinnvolle Empfehlung abgeben, wann welche Technologie für unsere Situation vorteilhaft wäre.</i></p> <p><i>Welche Technologie bietet die sicherste Verbindung punkto Ausfallsicherheit? Welche Verbindung eignet sich auch für Backup-Leitungen?</i></p>

3. **Internetservices**

Vergleichen sie folgenden Möglichkeiten die Internetservices zu betreiben:

- *eigene Server „inhouse“*
- *dedizierte Server (Root-Server) bei Provider*
- *Services beim Provider (Shared hosting)*

*Nehmen Sie dafür für 2 Fälle einige Eckdaten an (z.B. Speicherplatz, Traffic, Dienste, ...).
Erstens eine einfache Webpräsenz zu Werbezwecken und Mail, zweitens eine komplexe
Datenbankanwendung mit PHP für den Kundenzugriff.*

Welche Vergleichskriterien finden Sie, welche sind wie wichtig?

Konstruieren Sie „typische Fälle“ und vergleichen Sie.

4. **Sicherheit**

Die Firma entscheidet sich, dass die Server alle inhouse stehen sollen.

*Welche Anforderungen an die Sicherheit gemäss ISO 27000 sind zu beachten?
Bitte stellen Sie der Klasse ein sinnvolles Sicherheitskonzept für diesen Anwendungsfall vor.*

Beachten Sie, dass es technische und nicht technische Massnahmen geben kann.

5. **Wartung / Überwachung**

*Wie würden Sie die Überwachung des Internetzuganges dieser Firma sicherstellen?
Beschreiben Sie konkret, mit welchen Tools Sie das machen würden. Es wird erwartet, dass Sie
mindestens 5 geeignete Tools finden.*

*Wie würden Sie die Wartung des Zuganges sicherstellen?
Beschreiben Sie einen Wartungsprozess und machen Sie der Firma eine Empfehlung. Ihre
Empfehlung muss auf Grund einer Evaluation mit Kriterien erfolgen.*

6. **Firewall**

Vergleichen Sie für einen Internetanschluss folgende Firewall-Lösungen:

- *Günstige Hardware-Firewalls (Cisco-ASA, Zyxel Zywall oder ähnliche)*
- *PC-Lösung mit Linux*
- *Firewall-Service des Providers.*

Welche Vergleichskriterien finden Sie, welche sind für welche Einsatzfälle wie wichtig?

Konstruieren Sie „typische Fälle“ und vergleichen Sie.

7. **VPN**

Vergleichen Sie folgende VPN-Lösungen für ihren Internetanschluss:

- *Hardwarelösung (Cisco-ASA oder Ähnliches)*
- *VPN-Service des Providers*
- *PC-Lösung mit Windows und Linux.*

Welche Vergleichskriterien finden Sie, welche sind für welche Einsatzfälle wie wichtig?

Diskutieren Sie einige „typische Fälle“ und vergleichen Sie.

Tabelle 35: Themenübersicht

5. Planen

In diesem Teil der Dokumentation wird das gesamte Projekt geplant. Hier wird ein Zeitplan erstellt und definiert wer was wann macht.

5.1. Benötigte Infrastruktur

- Atlassian Jira Scrum Board
- Atlassian Confluence
- Alle Beteiligten benötigen einen PC mit Office 365.
- MNS (Mundnasenschutz) aufgrund aktueller Covid-19 Situation.
- Tisch mit 3 Stühlen

5.2. Testkonzept

Das Testing ist unerlässlich bei einem Projekt. Für die Funktionstests wurde ein Testkonzept erstellt. Wie die Tests dokumentiert werden, ist in der Tabelle auf der nächsten Seite beschrieben.

Das Testing wird in verschiedene Testgebiete unterteilt, damit die Übersicht nicht verloren geht. Folgende Testgebiete sind definiert:

- Übertragungsrate & Verfügbarkeit
 - o Vergleichsmatrix mit fünf Providern wurde erstellt
 - o Änderung der Anforderungen für Beispiel 1 Übertragungsrate beschreiben
 - o Beispiel 2 Verfügbarkeit maximale Ausfallzeit von 10 Stunden beschreiben
 - o Beispiel 3 Verfügbarkeit maximale Ausfallzeit von 4 Stunden beschreiben
- WAN-Technologie
 - o Vergleich fünf WAN-Technologien
 - o Sicherste Verbindung im punkto Ausfallsicherheit
 - o Beste Leitung als Backup-Leitung
- Internetservices
 - o Drei verschiedene Services erarbeiten und dokumentieren.
 - o 2 Fälle ausarbeiten
 - Einfache Webpräsenz zu Werbezwecken und Mail
 - Komplexe Datenbankanwendung mit PHP für den Kundenzugriff
- Sicherheit
 - o Definierung von technischen sowie nicht technischen Massnahmen gemäss ISO 27000
 - o Sinnvolles Sicherheitskonzept
- Wartung & Überwachung
 - o Vergleich zwischen fünf Monitoring Tools erstellt
- Firewall
 - o Vergleich zwischen drei Firewall Lösungen
- VPN
 - o Vergleich zwischen drei VPN Lösungen

Testfall X	
Beschreibung	Hier wird der Testfall kurz beschrieben.
Testszenario	Hier werden die genauen Schritte des Tests aufgeschrieben. Es wird notiert, wie der Test durchgeführt wird und was mittels des Tests herausgefunden wird.
Involvierte Komponenten	Alle, vom Test betroffenen Komponenten werden hier aufgeschrieben. Beispielsweise Datenbanken, Server, Tools etc..
Erwartetes Resultat	Das Resultat aufgeschrieben, das erwartet wird, wenn der Test erfolgreich abläuft.
Tatsächliches Resultat	Nach der Durchführung des Tests wird hier das tatsächliche Resultat aufgeschrieben.
Ergebnis	Das Ergebnis wird hier farbcodiert notiert. <ul style="list-style-type: none"> • Erfolgreich: Das Ergebnis entspricht den Erwartungen. • Teilweise erfolgreich: Das Ergebnis entspricht nicht den Erwartungen, ist aber dennoch erfolgreich. • Fehlgeschlagen: Der Test ist fehlgeschlagen.
Fehler (falls nötig)	Falls der Test fehlgeschlagen ist, werden hier aufgetretene Fehler notiert.
Massnahmen	Hier werden die Massnahmen notiert, die unternommen werden, falls ein Test fehlschlägt.

Tabelle 36: Beispiel Testkonzept

6. Entscheiden

Die Phase «Entscheiden» beeinflusst den Verlauf des ganzen Projekts. In diesem Projekt wird unter drei verschiedenen Variationen entschieden. Wichtig ist, dass hier eine nachvollziehbare Entscheidung gefällt wird, die optimal für das Projekt ist.

6.1. Ziele

Da wir klare Ziele haben, werden wir als Entscheid die zu erreichenden Ziele definieren.

6.1.1. Ziele Übertragungsrate & Verfügbarkeit

Das Ziel ist es bei diesem Thema eine Vergleichsmatrix von fünf Providern zu erstellen. Die Entscheidung wollen wir dem Kunden überlassen, jedoch sollte die Matrix die entsprechende Entscheidungsgrundlage geben.

6.1.1.1. Beispiele

6.1.1.1.1. Beispiel 1 Übertragungsrate

Die Firma arbeitet mit einer Übertragungsrate von 50/5 Mbit. Dies bedeutet, dass die Coffee GmbH maximal 50 Megabit pro Sekunde Download zur Verfügung steht. Wie würden sich die Anforderungen ändern, würde der Server «inhouse» stehen.

6.1.1.1.2. Beispiel 2 Verfügbarkeit

Ein Unternehmen, kann einen Ausfall der Internet Anbindung maximal für 10 Stunden verkraften.

6.1.1.1.3. Beispiel 3 Verfügbarkeit

Ein Unternehmen, kann einen Ausfall der Internet Anbindung maximal für 4 Stunden verkraften.

6.1.2. Ziele WAN-Technologie

Das Ziel ist es über die fünf verschiedenen WAN-Technologien (DSL, Fibre, Cable, Radiolink & Satellit) zu informieren und diese zu vergleichen. Es sollen mindestens 5 Unterscheidungsmerkmale gefunden werden und wann welche Technologie vorteilhaft wäre.

Zudem sollte man sich Gedanken machen, welche die sicherste Verbindung ist im punkto Ausfallsicherheit und welche Leitungen sich als Backup-Leitung eignen würde.

6.1.3. Ziele Internetservices

Wir haben uns drei verschiedene Lösungen für den Internetservices erarbeitet:

- Eigene Server «inhouse»
- Dedizierter Server (Root-Server) bei Provider
- Services beim Provider (Shared Hosting)

Wir werden 2 Fälle ausarbeiten:

- Eine einfache Webpräsenz zu Werbezwecken und Mail.
- Eine komplexe Datenbankanwendung mit PHP für den Kundenzugriff

Die Vergleichskriterien werden in einer Tabelle ersichtlich sein.

6.1.4. Ziele Sicherheit

Die Coffee GmbH entscheidet sich dazu, dass die Server alle inhouse stehen sollten.

Ziel ist es nun technische und nicht technische Massnahmen gemäss ISO 27000 zu definieren. Zudem muss ein sinnvolles Sicherheitskonzept erstellt werden.

6.1.5. Ziele Wartung & Überwachung

Um Monitoring oder auch Überwachung und die entsprechende Wartung zu gewährleisten werden Monitoring-Tools verwendet.

Die Liste der Tools:

- PRTG
- LAN Guard
- Solar Winds Netowrk Performance
- Nagios
- Zabbix

6.1.6. Ziele Firewall

Es sollten folgende drei Firewall Lösungen verglichen werden.

- Günstige Hardware Firewall
- PC-Lösung mit Linux
- Firewall-Service beim Provider

Zudem sollte aufgeführt werden, welche Vergleichskriterien für welche Einsatzfälle wichtig sind.

6.1.7. Ziele VPN

Beim VPN geht es darum eine sichere Internetverbindung zu realisieren. Wir haben uns drei Lösungswege ausgedacht:

- Hardwarelösung
- VPN-Service des Provider
- PC-Lösung mit Linux

Mittels einer Entscheidungsmatrix können wir der Coffee GmbH die beste Lösung errechnen und entsprechen eine grossartige Lösung anbieten.

7. Realisieren

7.1. Übertragungsrate & Verfügbarkeit

Die Coffee GmbH hat einen zentralen städtischen Standort somit, kann man sicher gehen, dass die Wahrscheinlichkeit für Glasfaser hoch ist. Dies würden wir auch empfehlen, da diese Technologie sehr zukunftsorientiert ist und auch immer weiter ausgebaut wird. Die Internetverbindung ist für das Kerngeschäft zwar nicht essenziell, jedoch muss die Verbindung trotzdem stabil und die Übertragungsgeschwindigkeit genügend schnell sein.

7.1.1. Übertragungsrate

- Fallbeispiel 1: Server beim Provider
 - o Dies ist der aktuelle Stand der Coffee GmbH. Jedoch würden wir empfehlen eine symmetrische 200 Mbit/s FTTH Leitung sprich 200 Mbit/s Download und 200 Mbit/s Upload einzubauen, denn die momentane Übertragungsrate ist viel zu langsam.
- Fallbeispiel 2: Server steht inhouse
 - o Im Fall eines inhouse Betrieb, sollte auf jeden Fall eine Fibreleitung vorhanden sein, damit die ganzen Applikationen und der Webshop für Kunden sowie für die Mitarbeiter zur Verfügung stehen. Zusätzlich müsste eine Firewall installiert werden, um die Sicherheit der Daten und des System sicherstellen zu können. Wir würden der Coffee GmbH dringend eine symmetrische Fibre-Anbindung mit 250 Mbit/s empfehlen, durch den inhouse Betrieb gibt es einen erhöhten Traffic auf die Website der Coffee GmbH und somit sollte die Übertragungsrate entsprechend hoch sein.

7.1.2. Verfügbarkeit

- Fallbeispiel 1: (Ausfall 10h tolerierbar)
 - o Falls ein maximaler Ausfall von zehn Stunden tolerierbar wäre, müsste man eine Verfügbarkeit von 99.89% sicherstellen.
- Fallbeispiel 2: (Ausfall 4h tolerierbar)
 - o Falls ein maximaler Ausfall von vier Stunden tolerierbar wäre, müsste man eine Verfügbarkeit von 99.95% sicherstellen. Um dies zu realisieren müssen die Systeme mindestens einfach redundant geführt werden. Zusätzlich sollte ein TAM vorhanden sein und die Systeme müssen Hot-Swap fähig sein. Zudem kommen noch Backups die mit einer Zeitverschiebung auf den einzelnen Server des Clusters durchgeführt werden sollten.

7.1.3. Vergleich Provider

Auswahlkriterium	Gewichtung	Swisscom		Sunrise		UPC		iWay		GGA Maur	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	5	40	4	32	3	24	5	40	5	40
Stabilität	8	6	48	4	32	4	32	5	40	5	40
Qualität	8	6	48	4	32	5	40	4	32	5	40
Wirtschaftliche Kriterien	24										
Kosten / Nutzen	6	3	18	4	24	3	18	4	24	4	24
Wartungskosten	6	2	12	3	18	4	24	3	18	3	18
Betriebskosten	6	4	24	4	24	4	24	4	24	4	24
Lizenzgebühren	6	4	24	5	30	5	30	3	18	3	18
Strategische Kriterien	12										
Verhalten des Lieferanten am Markt	4	5	20	5	20	5	20	3	12	3	12
Stabilität des Lieferanten	4	5	20	5	20	4	16	3	12	4	16
Referenzen	4	5	20	4	16	5	20	4	16	4	16
Operative Kriterien	12										
Betriebbarkeit	4	5	20	4	16	4	16	4	16	5	20
Notwendiges Know-How	4	5	20	4	16	4	16	5	20	5	20
Support	4	5	20	3	12	3	12	5	20	5	20
Organisatorische Kriterien	6										
In Prozess einfügbar	3	5	15	4	12	4	12	5	15	5	15
Kommunikationsprozesse	3	5	15	4	12	4	12	5	15	5	15
Juristische Kriterien	6										
SLA	2	5	10	4	8	4	8	5	10	5	10
Verträge	2	5	10	4	8	4	8	5	10	5	10
Gesetze	2	6	12	6	12	6	12	6	12	6	12
Ökologische Kriterien	4										
Entsorgung	2	3	6	3	6	3	6	3	6	3	6
Wiederverwendbarkeit	2	3	6	3	6	3	6	3	6	3	6
Sicherheits Kriterien	12										
Verfügbarkeit	4	6	24	4	16	4	16	5	20	5	20
Vertraulichkeit	4	5	20	4	16	5	20	5	20	5	20
Integrität	4	4	16	4	16	5	20	5	20	5	20
Total			468		404		412		426		442
Rang			1		5		4		3		2

Abbildung 16: Bewertungsmatrix für fünf Provider

Provider	Angebot (Name)	Übertragungsrate	Preis	Technologie	Support	Security
Swisscom	Business L	10 / 10 Gbits	205 CHF / M	FTTH	7 × 24 h Service-Desk und Störungsentgegennahme Störungsbehebung bis am nächsten Arbeitstag Ausfallsicherung Bei Netzwerkausfall weiter telefonieren und surfen	Internet Security \ KMU für 10 Geräte (10 weitere Geräte für 4.90 CHF): - Schutz vor Viren, Hackern und Spyware - Schutz vor gefährlichen Internetseiten - Banking Protection - Schutz beim e-Banking
UPC	Business Internet 1000	1000 / 100 Mbits	49 CHF / M für 12 Monate danach 99 CHF / M	FTTH	Telefonsupport 24h täglich 365 Tage im Jahr	Für 3 CHF / M die Möglichkeit Business Secure Web zu verwenden
Sunrise	We Office M	500 / 500 Mbits	90 CHF / M	FTTH	Kostenloser technischer Telefon-Support unter (Mo – Sa 8.00 - 22.00 Uhr, So 9.00 - 22.00 Uhr)	Keine speziellen Angebote
iWay	Internet 1000/1000	1000 / 1000 Mbits	189.35 CHF / M	FTTH	Supportzeiten Mo - So: 7x24h Störungsbehebungszeit <8h Intervention Proaktiv (aktive Überwachung der Leitung)	Keine speziellen Angebote
GGA Maur	KMU Business-Internet 1000	1000 / 1000 Mbits	119 CHF / M	FTTH	Interventionszeit 4 Stunden nach Eingang der Störung Störungsbehebung Priorisiert, während Öffnungszeiten	Keine speziellen Angebote

Tabelle 37: Vergleich von fünf Provider

7.1.3.1. Begründung

Anhand der Daten, welche wir aus dem Internet beziehen konnten, haben wir eine Entscheidungsmatrix sowie eine Tabelle mit den wichtigsten Parametern erstellt. Am Ende haben wir aus den fünf Provider einen ausgewählt der unseren Empfehlungen an die Coffee GmbH am nächsten kommt.

Ranking:

- 1) Swisscom
- 2) GGA Maur
- 3) iWay
- 4) UPC
- 5) Sunrise

Besonderheiten

- Entsorgung
 - Bei der Entsorgung haben wir festgestellt, dass die meisten Provider ihre Geräte nur leihweise an ihre Kunden geben. So werden die Geräte nach Ablauf des Vertrages wieder an den Provider retourniert. So haben wir hier allen Provider die gleiche Punktzahl vergeben.
- Service-Desk von UPC
 - Luis konnte bereits Erfahrungen mit dem privaten Service-Desk von UPC sammeln, bereits dieser war seiner Meinung nach öfters sehr schlecht. Auch im Internet sind viele negativ Punkte zu UPC die schlechte Leistung des UPC Support Service. Für ein Unternehmen ist es sehr wichtig, wenn man Probleme mit dem Internet hat, dass man entsprechend professionell Beraten und unterstützt wird. Darum ist UPC bei unserer Bewertung auch so schlecht bewertet.
- Hohe Kosten Swisscom
 - Zwar sind die Kosten bei Swisscom sehr hoch, jedoch muss man auch dabei beachten, dass das Swisscom Angebot mit einer 10 Gbits Leitung mehr als nur genügt. Trotz der hohen Kosten sind wir vom Swisscom Angebot am meisten überzeugt und werden deshalb dieses Angebot der Coffee GmbH vorschlagen. Hauptgrund dafür ist, dass Swisscom nun auch eine interne Netzausfall Sicherheit hat (Internet Backup), sprich die Verbindung wird dann automatisch auf das mobile Datennetz von Swisscom umgeleitet. Klar hat man dann Performance Issues aber trotzdem kann das Unternehmen noch weiter arbeiten.

7.2. WAN-Technologie

7.2.1. xDSL

xDSL, welcher aller Typen DSL (Digital Subscriber Line) zusammenfasst, also ADSL, HDSL, SDSL, SHDSL, UDSL und letztlich VDSL.

7.2.1.1. Vorteile

ADSL bietet einem. Mit vDSL wird die Latenzzeit um einiges weniger als bei anderen Technologien. Als alternative Lösung sind xDSL-Typen gar nicht schlecht. Die Verbindung wird mit einem Twisted-Pair Kupferkabel, wie etwa das vom Telefon und deshalb ist langsamer als Glasfasertechnologie. Das Vorteil von DSL zur Glasfaser war jedoch die günstigere Ausbau und somit günstige Preise, was dazu führte, dass vor allem in den späten Jahren des 20. Jahrhunderts Menschen sich für DSL entschieden.

7.2.1.2. Nachteile

Wie ermittelt, ist die Geschwindigkeit der Verbindung einen Hindernis am Entscheid sowie die fast-wie-nicht verfügbare. Die Entfernung zwischen den Router fügt dazu, dass die Verfügbarkeit meist unterbrochen sein kann, im Gegensatz zu andere WAN-Arten.

7.2.2. Fibre (FTTH)

7.2.2.1. Vorteile

Die effektive Leistung, welche FTTH-Leitungen erbringen, sind für den Preis, den man bezahlt, dementsprechend erfüllen. Das grösste Vorteil von FTTH-Anbindungen sind die symmetrischen Geschwindigkeiten für das Down- und Upstream

7.2.2.2. Nachteile

Das grösste Nachteil an das Glasfaser Kabel ist, wenn es physisch beschädigt oder dreckig wird. Eine nachträgliche Verzögerung beträgt diese Verbindung, sodass einige Finanzinstituten auf Radiolink umgestellt sind.

7.2.3. Cable (Kupfer)

7.2.3.1. Vorteile

Die Kupferleitung verfügt über eine asymmetrische Leitung und weist somit. Wenn es in der Regel mit einem Modem ausgestattet wird, wird diese Methode schnelleres Internet als jegliche DSL-Leitungen liefern. Es weist noch Vorteile gegenüber Satelliten Internet, da dies stör anfälliger ist.

7.2.3.2. Nachteile

Alle die Cable haben hängen an einem Cluster. Das heisst, wenn der Nachbar eine 1 GB Datei herunterlädt habe ich weniger Bandbreite zur Verfügung da er etwas herunterlädt.

7.2.4. Radiolink

Eine Funkverbindung ist eine drahtlose Verbindung (auch drahtlose Punkt-zu-Punkt-Verbindung genannt) zwischen zwei Knoten oder Funkeinheiten in einem Datennetzwerk. Jede Funkeinheit besteht aus einem Transceiver (ein Gerät, das sowohl Kommunikation senden als auch empfangen kann) und einer hoch direktiven Antenne. Das bedeutet, dass die Antenne nur (>99%) in die Richtung sendet oder empfängt, in die sie gerichtet ist.

7.2.4.1. Vorteile

Funkverbindungen lassen sich schnell aufbauen, da keine physischen Kabel im Boden verlegt werden müssen. Dies macht sie in vielen Fällen zu einer kosteneffizienteren Lösung als Glasfaser.

7.2.4.2. Nachteile

Der primäre Nachteil ist, dass Funkverbindungen für eine optimale Leistung eine direkte so genannte Sichtverbindung erfordern. Im Vergleich zur Glasfaser ist die Verbindung weniger stabil, da schlechtes Wetter die Verbindung unterbrechen kann, insbesondere bei höheren Frequenzen.

7.2.5. Satellit

Eine Internetanschlusses des Typs Satellit ist lediglich eine drahtlose Verbindung, welche über 3 Satellitenschlüssel «verbunden» wird. Die erste Verbindung liegt bei einem Provider (UPC, Swisscom usw.), die zweite liegt im Weltall und die allerletzte beim Kunde zu Hause oder beim Arbeitsplatz. Der Satellitenschlüssel muss dann vom Kunde mit einem Modem/Routerbox des ISPs verbunden werden.

7.2.5.1. Vorteile

Die mehreren Vorteile von einer Satellitenverbindung sind folgende; Es gibt unterschiedliche, nützliche Dienste, welche gebührenlos sind. Das Empfangen von keiner Radiolink-Verbindung ist auch von Vorteil sowie die Abdeckung von Stationen mit ungenügendem Empfang. Bei mehrmaligen Ortswechsel wird diese Technologie bevorzugt, da die Satelliten.

7.2.5.2. Nachteile

Was man bei Flexibilität gewinnt, wird beim Punkt Geschwindigkeit exponentiell eingebüsst. Die Latenz liegt bei unglaublichen 500-700ms. Die Kosten eines Satellit-Internet einzusetzen ist im Gegensatz zu anderen Technologien um Einiges teurer. Natürliche Nachteile sowie schlechtes Wetter ist der Haupthindernis.

7.2.6. Finaler Vergleich

FTTH eignet sich für Firmen, welche Daten in Echtzeit nicht übertragen müssen (so etwa wie Börsenunternehmen, welche Radiolink benutzen würden) und über eine schnelle Internetverbindung verfügen wollen. Wenn man den Standort ständig ändert ist die Satelliten-Technologie zu empfehlen. Kabel Internet ist nützlich, falls man zu günstigen Preisen über mittelmässiges Internet verfügen will.

Bei abgelegenen und abgeschotteten Standorten, die keine grosse Datenmengen verschicken müssen, wäre Kupfer empfehlenswert, da die Übertragungsrate, wegen der minimalen Störungen am grössten wäre.

Als ausfallsicherste Technologie steht einem DSL, Kabel sowie Satellitenverbindung zur Auswahl. In einem weiteren Schritt ist die Kombination vom DSL und Kupferkabel möglich, sodass man die Ausfallsicherheit auf das Minimum begrenzen kann.

7.2.7. Bewertungsmatrix

Auswahlkriterium	Gewichtung	Kupfer		FTTH		Satellit	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	28	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	3	24	5	40	2	16
Stabilität	10	6	60	6	60	5	50
Qualität	10	5	50	6	60	5	50
Wirtschaftliche Kriterien	18						
Kosten / Nutzen	6	5	30	2	12	3	18
Wartungskosten	6	5	30	4	24	4	24
Betriebskosten	6	5	30	2	12	4	24
Lizenzgebühren	6	2	12	3	18	3	18
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	3	12	3	12	3	12
Stabilität des Lieferanten	4	5	20	5	20	5	20
Referenzen	4	3	12	4	16	4	16
Operative Kriterien	10						
Betriebbarkeit	4	6	24	6	24	6	24
Notwendiges Know-How	2	4	8	4	8	6	12
Support	4	4	16	6	24	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	5	15
Kommunikationsprozesse	3	5	15	4	12	4	12
Juristische Kriterien	6						
SLA	3	4	12	6	18	6	18
Verträge	2	3	6	4	8	5	10
Gesetze	1	3	3	3	3	3	3
Ökologische Kriterien	4						
Entsorgung	2	2	4	3	6	4	8
Wiederverwendbarkeit	2	2	4	2	4	3	6
Sicherheits Kriterien	16						
Verfügbarkeit	6	5	30	5	30	6	36
Vertraulichkeit	6	6	36	6	36	6	36
Integrität	4	5	20	5	20	4	16
Total	100		473		482		468
Rang			2		1		3

Abbildung 17: Bewertungsmatrix WAN-Technologien

7.3. Internet Services

Die Coffee GmbH hat sich noch auf keine Lösung für Ihren Internetservice einigen können. Darum werden wir einen Vergleich zwischen Inhouse, Root-Server und Shared-Server erstellen.

7.3.1. Erklärung

In diesem Teil werden die drei verschiedenen Lösungsansätze erklärt sowie deren Vor- und Nachteile gezeigt. Wir setzen dabei auf unsere Erfahrungen, die wir mit den unterschiedlichen Lösungen im Verlauf unserer Karriere sammeln konnten.

7.3.1.1. Eigener Server (House)

Der Begriff «Inhouse» stammt aus dem englischen und bezeichnet den Standort bzw. das Hosting eines Service im eigenen Unternehmen («in den eigenen vier Wänden»). Somit ist das Unternehmen selber für das Backup, Verfügbarkeit, Monitoring, Updates und Hardware zuständig.

Zu Beginn der Anschaffung einer On-Premise Lösung sind die Investitionskosten hoch, zumal Leistungsreserven beim Server miteinberechnet werden müssen. Zudem muss man die aufkommenden laufenden Ausgaben für Hardware (Ersatzteile), IT-Personal oder Wartung miteinberechnen. Die Kosten senken sich aber im Verlauf des System-Lebenszyklus.

Unternehmen die vor Ort hosten, können ihre Änderungen ohne weiteres unabhängig und selbstständig implementieren. Somit ist man mit einem Inhouse Server um einiges flexibler. Diese Flexibilität kann aber natürlich nur gut genutzt werden, wenn auch die Fachleute für ein solches Vorhaben vorhanden sind. Denn das Unternehmen ist für alle Updates und notwendige Systemerweiterungen selbst zuständig.

Ein wichtiger Aspekt ist hierbei ebenfalls die Sicherheit. Bei Inhouse Servern ist die Organisation selbst zuständig für die Sicherheit. Dies setzt voraus, dass Unternehmen Fachpersonal haben die sich in dem Bereichen BCM (Business Continuity Management) oder DRM (Disaster-Recovery-Management) auskennt und dies auch für ein Unternehmen realisieren sowie betreuen kann. Man muss sich bei Inhouse-Servern mehr Gedanken um Backups machen. Nicht nur dass man diese selbst machen muss sondern auch wie man diese aufbewahrt. Klar ein Backup, um ein Systemschaden zu verhindern, kann man eventuell neben dem Server aufbewahren in einem abschliessbaren Schrank. Wie sieht es aber bezüglich Wasserschäden? Oder «Loose of Building» allgemein aus? Was ist, wenn das Backup gestohlen wird? Gibt es ein Backup des Backups? Hier muss man sich sehr viele Fragen stellen, die man beim Outsourcing sich nicht stellen müsste.

Jedoch kann man durch einen Inhouse-Server sicherstellen das die Daten im Haus bleiben und immer unter eigener Kontrolle sind. Zudem ist man nicht auf eine funktionierende sowie genügend schnelle Internetverbindung angewiesen.

Vorteile:

- Volle Kontrolle über den Server
- Volle Verantwortlichkeit über Daten sowie deren Inhalte
- Günstiger Speicherplatz
- Einmalige Kosten bei der Beschaffung der Hardware
- Weniger Kommunikationsaufwand, da alles intern.

Nachteile:

- Volle Verantwortlichkeit über Daten sowie deren Inhalte

- Ein eigenes Backup Konzept muss erarbeitet werden.
- Mehr organisatorischer Aufwand

7.3.1.2. Dedizierter Server (Root-Server)

Bei einem Root Server oder auch dedizierter Server genannt handelt es sich um einen Server, der meistens nur für einen bestimmten Verwendungszweck vorgesehen ist. Somit kann die gesamte Leistung des Server für die vorgesehene Aufgabe verwendet werden. Der Server wird dann meistens bei einem Provider wie zum Beispiel Hosttech oder Infomaniak angemietet.

Handelt es sich um einen dedizierten Server, wird dieser mit seiner kompletten Hardware nur von einem Kunden verwendet. Bei einem dedizierten Server ist man somit nur für das OS und die Applikation zuständig.

Vorteile:

- Die Verantwortung der Hardware liegt beim Provider
- Ausfallsicherheit ist gegeben (die Redundanz bei Strom, Internet und Hardware ist bei den meisten Providern gegeben)
- Support
- Servereinstellungen können an die eigenen Bedürfnisse bestmöglich angepasst werden.
- Installation können selbst installiert werden
- Minutengenaue Abrechnung
- Speicherplatz in wenigen Minuten

Nachteile:

- Abhängig vom Provider
- Höhere monatliche Kosten als ein inhouse Server
- Der Server kann nur für bestimmte Zwecke verwendet werden.

7.3.1.3. Services beim Provider (Shared Hosting)

Beim Shared Hosting redet man eigentlich von dem klassischen Webhosting. Grundsätzlich beschreibt dieses Szenario einen physischen Server der in mehrere logische kleine Server aufgeteilt wird. Somit sind mehrere Websites auf einem Server. Dadurch kann man Geld sparen und sich die Kosten mit anderen Kunden «teilen». Einfach gesagt handelt es sich beim Shared Hosting um einen Server der gemeinsam genutzt wird und jeder erhält einen Prozentansatz von den vorhandenen Ressourcen.

Vorteile:

- Innerhalb einiger Minuten kann man sein Shared Hosting erhalten
- Die Kosten sind verhältnismässig tief
- Man bezahlt nur das was man gewählt bzw. benötigt.
- Updates werden vom Provider installiert
- Die Sicherheit der Plattform liegt in der Verantwortlichkeit des Providers
- Provider kann Support anbieten je nach SLA

Nachteile:

- Keine eigene IP-Adresse
- Bei Ausfällen ist man auf den Provider angewiesen
- Bei bestimmten Angeboten kann es mit limitierten Speicherplatz zu Problemen führen.
- Man kann keine eigene angepasste Software verwenden

7.3.2. Fallbeispiele

7.3.2.1. Einfache Webpräsenz und Mail

Ein Server mit installierten Webservice, welcher auch als Mailserver verwendet werden kann. Dadurch das dies nur Webanfragen oder allgemeiner Mailverkehr benötigt, braucht es nur wenig Traffic.

Bei der Auswahl der der entsprechenden Hosting-Variante, würden wir folgende Parameter empfehlen:

- Mind. 20 GB SSD Speicher
- Unlimitierter Traffic
- Unlimitierte Anzahl E-Mail
- SSL Verschlüsselung (Let's Encrypt Zertifikat)
- Serververfügbarkeit mind. 98.5 %
- Serverstandort in der Schweiz

7.3.2.2. Komplexe Datenbankanwendung mit PHP

Ein Server mit installierten Webservice, welcher auch als Mailserver verwendet werden kann. Dadurch das dies nur Webanfragen oder allgemeiner Mailverkehr benötigt, braucht es nur wenig Traffic.

- Mind. 50 GB SSD Speicher
- Unlimitierter Traffic
- Unlimitierte Anzahl E-Mail
- SSL Verschlüsselung (Let's Encrypt Zertifikat)
- Serververfügbarkeit mind. 99.5 %
- Serverstandort in der Schweiz
- Mind. 10 Datenbanken
- Mind. PHP 7.2

7.3.3. Vergleichskriterien

	Shared Hosting	Inhouse	Root Server
Kosten	Tief bis Mittel	Mittel	Mittel bis Hoch
Backup	Provider	Eigenverantwortung	Eigenverantwortung oder Provider
Updates	Provider	Eigenverantwortung	Eigenverantwortung
Monitoring	Provider	Eigenverantwortung	Provider
Standortabhängigkeit	Tief	Gross	Tief
Ausfallsicherheit	Tief	Hoch	Hoch
Skalierbarkeit	Gross	Mittel	Gross

Tabelle 38: Vergleichstabelle

7.3.4. Vergleich

7.3.4.1. Fall 1

Auswahlkriterium	Gewichtung	In House		Shared		Dedicated	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	5	40	5	40	5	40
Stabilität	8	6	48	6	48	6	48
Qualität	8	4	32	6	48	6	48
Wirtschaftliche Kriterien	24						
Kosten / Nutzen	6	4	24	5	30	5	30
Wartungskosten	6	5	30	4	24	3	18
Betriebskosten	6	2	12	4	24	3	18
Lizenzgebühren	6	2	12	3	18	3	18
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	4	16	3	12	2	8
Stabilität des Lieferanten	4	4	16	4	16	4	16
Referenzen	4	3	12	4	16	4	16
Operative Kriterien	12						
Betriebbarkeit	4	6	24	6	24	6	24
Notwendiges Know-How	4	5	20	5	20	4	16
Support	4	4	16	6	24	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	5	15
Kommunikationsprozesse	3	5	15	4	12	4	12
Juristische Kriterien	6						
SLA	2	4	8	6	12	6	12
Verträge	2	4	8	5	10	5	10
Gesetze	2	3	6	5	10	5	10
Ökologische Kriterien	4						
Entsorgung	2	3	6	6	12	4	8
Wiederverwendbarkeit	2	4	8	6	12	3	6
Sicherheits Kriterien	12						
Verfügbarkeit	4	6	24	6	24	6	24
Vertraulichkeit	4	6	24	6	24	6	24
Integrität	4	6	24	4	16	5	20
Total			440		491		465
Rang			3		1		2

Abbildung 18: Matrix für Fallbeispiel 1

7.3.4.2. Fall 2

Auswahlkriterium	Gewichtung	In House		Shared		Dedicated	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	5	40	5	40	5	40
Stabilität	8	6	48	6	48	6	48
Qualität	8	5	40	5	40	5	40
Wirtschaftliche Kriterien	24						
Kosten / Nutzen	6	5	30	5	30	5	30
Wartungskosten	6	5	30	3	18	3	18
Betriebskosten	6	2	12	3	18	3	18
Lizenzgebühren	6	2	12	3	18	3	18
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	4	16	2	8	2	8
Stabilität des Lieferanten	4	4	16	4	16	4	16
Referenzen	4	3	12	4	16	4	16
Operative Kriterien	12						
Betriebbarkeit	4	6	24	6	24	6	24
Notwendiges Know-How	4	5	20	3	12	4	16
Support	4	4	16	6	24	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	5	15
Kommunikationsprozesse	3	5	15	4	12	4	12
Juristische Kriterien	6						
SLA	2	4	8	6	12	6	12
Verträge	2	4	8	5	10	5	10
Gesetze	2	3	6	5	10	5	10
Ökologische Kriterien	4						
Entsorgung	2	2	4	3	6	4	8
Wiederverwendbarkeit	2	2	4	2	4	3	6
Sicherheits Kriterien	12						
Verfügbarkeit	4	6	24	6	24	6	24
Vertraulichkeit	4	6	24	6	24	6	24
Integrität	4	6	24	4	16	5	20
Total			448		445		457
Rang			2		3		1

Abbildung 19: Matrix für Fallbeispiel 2

7.3.5. Ergebnisse

7.3.5.1. Fall 1

1. Service beim Provider (Shared Hosting)
2. Dedizierter Server (Root-Server)
3. Eigener Server (House)

7.3.5.2. Fall 2

1. Dedizierter Server (Root-Server)
2. Eigener Server (House)
3. Service beim Provider (Shared Hosting)

7.4. Sicherheit

7.4.1. ISO Reihe 27000

ISO steht für «International Standard Organisation» und ist die Internationale Organisation für Normungen und erarbeitet internationale Normen in allen Bereichen mit Ausnahme der Elektrik, Elektronik und Telekommunikation, für die die Internationale Fernmeldeunion (ITU) zuständig ist. Gemeinsam bilden diese Organisationen die WSC (World Standards Cooperation).

Die ISO Reihe 27000 ist eine Reihe von Standards zur Informationssicherheit. Sie liefert Best-Practice-Empfehlungen für den Aufbau und Betrieb eines sogenannten «Information Security Management Systems» (ISMS) zum Schutz der gesamten IT-Organisation.

Bei der Sicherheit stehen die Fragen nach Vertraulichkeit, Integrität und Verfügbarkeit (CIA Prinzip genauere Erklärung auf der Website von Luis: <https://security.luis-luescher.com/documentations/cia/>) im Zentrum. Systeme und Rechenzentren können durch verschiedenste Attacken angegriffen werden wie zum Beispiel durch einen Distributed Denial of Service kurz DDoS genannt. Die ISO Reihe 27000 ist folgendermassen aufgebaut:



Abbildung 20: Offizielles Logo der ISO

- Das übergeordnete Rahmenwerk
 - o ISO 27000: Übersicht und Terminologie
 - Überblick über die gesamte ISO-27000-Normenreihe
Welche Normen gibt es, welche Funktionen erfüllen sie, und wie spielen sie zusammen?
 - Inhaltliche Einführung in das Thema «Information Security Management System» (ISMS)
Was ist ein ISMS, welche Vorteile bringt es mit sich, und was ist bei der Umsetzung zu beachten?
 - Glossar mit grundlegenden Begriffen und Definitionen, die in der ISO-27000-Normenreihe Anwendung finden
- ISMS-Anforderungen: Allgemein und Branchenspezifisch
 - o ISO 27001: ISMS-Anforderungen
 - Anforderungen an ein ISMS
 - Aufbau eines ISMS
 - Anforderungen an die Dokumentation
 - Verantwortung des Managements
 - Kontrollen des ISMS-Prozesses
 - Verbesserung des ISMS-Prozesses
 - Generische Sicherheitsmassnahmen («Controls»)
 - o ISO 27011: ISMS-Anforderungen an Telekommunikationsunternehmen
 - Allgemeine Richtlinien zur Informationssicherheit
 - Organisationsstrukturen
 - Verantwortlichkeiten für und Klassifizierung von Informationswerten
 - Sicherheitsmassnahmen für Mitarbeiter
 - Physische Schutzmassnahmen und öffentliche Versorgungsdienste
 - Netzwerk- und Betriebssicherheit
 - Zugriffskontrolle

- Systementwicklung und Wartung
 - Umgang mit Sicherheitsvorfällen
 - Notfallvorsorgeplanung
 - Einhaltung interner und rechtlicher Vorgaben
- ISO 27799: ISMS-Anforderungen an den Gesundheitssektor
 - Ziele für die IT-Sicherheit in Gesundheitseinrichtungen
 - Schutzbedürftige Informationen
 - Bedrohungen und Schwachstellen
 - Praktische Umsetzung entsprechend ISO 27001 und 27002
 - Spezifische Massnahmen als Ergänzung zu ISO 27002
- ISO 13569: ISMS-Anforderungen an Bankwesen
 - Unternehmensinterne Sicherheitsleitlinie
 - Informationssicherheitsprogramm
 - Organisation
 - Risikoanalyse und -bewertung
 - Auswahl und Umsetzung von allgemeinen und branchenspezifischen Sicherheitsmassnahmen
 - Betrieb, Wartung und Überwachung
 - Umgang mit Sicherheitsvorfällen
- ISO 62443: ISMS-Anforderungen an Industrieautomatisierungssysteme
 - Kommunikation im Gerätnetzwerk
 - Kommunikation im Automatisierungsnetzwerk
 - Anschluss von Wartungsgeräten (PCs) an das Automatisierungsnetzwerk
 - Kommunikation zwischen Produktionszellen
 - Kommunikation mit entfernten Einzelgeräten
 - Anbindung an das Büronetzwerk – Fernwartung – Kommunikation zwischen Leitständen
- Ergänzende Normen für die Umsetzung
 - ISO 27002: Code of Practice
 - Allgemeine Richtlinien zur Informationssicherheit
 - Organisationsstrukturen
 - Verantwortlichkeiten für und Klassifizierung von Informationswerten
 - Sicherheitsmassnahmen für Mitarbeiter
 - Physische Schutzmassnahmen und öffentliche Versorgungsdienste
 - Netzwerk- und Betriebssicherheit
 - Zugriffskontrolle
 - Systementwicklung und Wartung
 - Umgang mit Sicherheitsvorfällen
 - Notfallvorsorgeplanung
 - Einhaltung interner und rechtlicher Vorgaben
 - ISO 27003: Leitfaden zur Implementierung
 - Unterstützung durch das Management
 - Definition von Umfang, Grenzen sowie Leitlinien des ISMS
 - Analyse der Sicherheitsanforderungen

- Bewertung und Behandlung von Risiken
- ISMS-Design
- ISO 27004: Bewertung der ISMS-Effizienz
 - Ziele, Prozesse, Erfolgsfaktoren und Modell eines Messsystems
 - Verantwortlichkeiten des Managements
 - Entwicklung von Messsystemen
 - Betrieb von Messsystemen
 - Analyse und Reporting
 - Überprüfung und Verbesserung des Messsystems
- ISO 27005: Risiko-Management
 - Kriterien, Umfang und Organisation des Risiko-Managements
 - Risikobewertung
 - Risikobehandlung
 - Risikoakzeptanz
 - Risikokommunikation
 - Überwachung und Review

7.4.2. Vertraulichkeit

Bei der Vertraulichkeit (eng. confidentiality) geht es um den Schutz von Daten eines Unternehmen. Innerhalb von vielen Unternehmen werden so Daten klassifiziert, dass diese mit «Public», «Internal», «Confidential» und «Secret» vermerkt werden.

- **Public:** Sind alle Daten, die für die Öffentlichkeit gedacht sind, so sind Daten auf der Firmenwebsite oder Werbekampagnen als «Public» zu klassifizieren.
- **Internal:** Dies sind Daten die für Mitarbeiter des eigenen Unternehmen gedacht sind. So sind Daten im Intranet des Unternehmen oder auch Dokumentationen sowie Anleitungen als «Internal» zu klassifizieren.
- **Confidential:** Dokumente und Daten, die nicht für Kunden oder die Allgemeinheit bestimmt sind wie zum Beispiel Offerten sollten als «Confidential» eingestuft werden.
- **Secret:** Daten die als «Secret» eingestuft werden, sind geschäftskritische Angaben wie zum Beispiel für einen Konditor sein Geheimrezept oder auch die Bilanzen von Unternehmen.

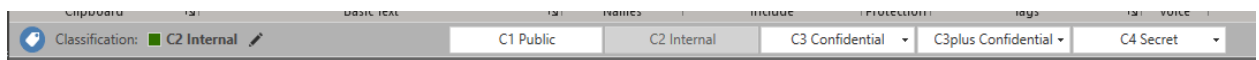


Abbildung 21: Beispiel einer Klassifizierung in Microsoft Outlook

7.4.3. Integrität

Die Integrität bezeichnet die Sicherstellung der Korrektheit somit deren Unversehrtheit von Daten und der korrekten Funktionsweise von Systemen. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Einfach gesagt darf es auf keine Weise und niemand möglich sein, zufällig oder unberechtigt Daten zu verändern. Deswegen sollte man sich die Frage stellen ob es zum Beispiel Sinn macht eine Datenbank in einen Netzwerkbereich gehört, der von aussen zugegriffen werden kann. Im Zusammenhang mit den Internetanbindungen von Firmen muss man sich folgende Frage stellen:

- Welche DB wird verwendet und welche Mitarbeitenden arbeiten damit?
- Arbeiten auch externe Personen mit den Daten?
- Welche erfolgt der Zugriff der externen Personen?

7.4.4. Authentizität und Authentisierung

Eine einfache Möglichkeit zur Identifizierung besteht über die Vergabe von Benutzernamen. Für die anschliessende Authentifizierung können verschiedene Elemente aus den folgenden Gruppen verwendet werden:

- Passwort oder PIN (Something u know)
- Smartcard oder rein anderes Authentifizierungsgerät (Something u have)
- Biometrische Erkennung wie Fingerabdrücke, Retinamuster oder Ähnliches (something u are)
- Geolokationserkennung mittels Geolokation der IP oder einer RFID-Card (Something u are)
- Verhaltenserkennung, mittels Analyse des Tippverhaltens bei der Eingabe (Something u do)

7.4.4.1. Benutzername und Kennwort

Diese Form der Authentifizierung ist sehr einfach realisierbar. Das Passwort wird verschlüsselt und in einer User-DB gespeichert. Die Anmeldung am System findet dann je nach Authentifizierungsprotokoll verschlüsselt oder unverschlüsselt. Eine grosse Gefahr besteht darin, dass das Passwort mit kryptografischen oder Social Engineering Techniken geknackt wird. Deshalb ist es wichtig, qualitative gute Passwörter zu verwenden und diese geheim zu halten. Folgende Regeln sollte dabei beachtet werden:

- Ein Passwort muss mindestens acht Zeichen lang sein.
- Es muss Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten.
- Es darf nicht mehr als drei aufeinanderfolgende gleiche Zeichen vom vorherigen Kennwort an irgendeiner Position beinhalten.
- Es darf nicht mehr als zwei aufeinanderfolgende identische Zeichen beinhalten.
- Es darf nicht User-ID (Benutzername) oder Variationen davon beinhalten.
- Es darf nicht leicht ableitbar oder zu erraten sein (zB. Autokennzeichen).

7.4.4.2. Zertifikate

Eine Zertifizierungsstelle stellt dabei Zertifikate aus, die vom Client-PC oder Benutzer akzeptiert werden. Sobald sich ein Benutzer an der Zertifizierungsstelle anmeldet und das Zertifikat als gültig erklärt worden ist, bekommt er den Zugriff auf alle verbundenen Ressourcen. Ein wesentlicher Vorteil liegt bei den Möglichkeiten der Zertifizierungsstelle, ungültige Zertifikate des Benutzers sehr schnell im ganzen Verbund einzuschränken oder zu verhindern.

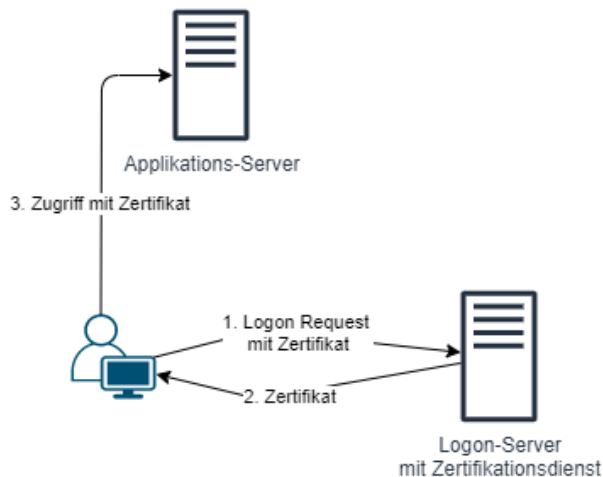


Abbildung 22: Funktionsumfang von Zertifikaten

7.4.4.3. Biometrie

Als biometrisches System bezeichnet man eine Erkennung körperliche Merkmale, die die Identität eines Benutzer verifiziert. Dabei stehen folgende Möglichkeiten zur Verfügung:

- **Gesichtserkennung:** Dabei werden Gesichtsmerkmale erkannt. Diese Erkennung wird heute in vielen Bahnhöfen, Flughäfen und öffentlichen Gebäuden eingesetzt.
- **Iris-Scan:** dieser Mechanismus identifiziert den farbigen Teil der Iris des Auges. Das Muster der Iris ist eindeutig und bei jedem Mensch individuell.
- **Retina-Scan:** Mit der Retinaerfassung wird ein Muster der Blutgefäße im Augenhintergrund verwendet. Das Verfahren arbeitet berührungslos und benutzt ein optisches System zur Erfassung der biometrischen Merkmale.
- **Fingerprint:** Die Fingerprint-erkennung ist heute sehr verbreitet. Viele Notebooks sind mit entsprechenden Lesern ausgestattet. Die Qualität dieser Authentifizierung hat im Laufe der letzten Jahre zugenommen, jedoch ist es relativ einfach, ältere Leser zu umgehen. Aktuelle Leser verwenden bis zu 300 verschiedene Messpunkte, um Fingerprints aufzunehmen.
- **Venen-Scan:** In Bereichen mit hohen Sicherheitsanforderungen werden Venen-Scanner eingesetzt. Hierbei muss die Hand eines Benutzers auf einen Leser gelegt werden. Dabei wird das Venenmuster erkannt. Die Erkennungsgenauigkeit ist bei diesem System sehr hoch.

7.4.5. Zurechenbarkeit

Briefe, Mails und anderer Daten sollten immer einem Owner zugeordnet werden können. So stellt sich zum Beispiel die Frage, ob Mails signiert werden müssen. Wichtig ist, dass die Zurechenbarkeit von Konfigurationsfiles der Firewall, Switches, Accesspoints und Router gewährleistet sein muss. Das heißt, es ist unklar, wer das Konfigurationsfile verfasst hat, so stellt dies ein Sicherheitsrisiko dar. So kann man für geteilte Netzwerkordner einen Owner definieren. Dieser ist dann dafür

zuständig, dass Anfragen für den Zugriff auf diesen Netzwerkordner, abgelehnt oder angenommen werden. Das selbe gilt auch für Shared Mailboxen. Wichtig ist auch, dass man einen Deputy definiert, damit die Anfragen auch bei Abwesenheit des Owner bearbeitet werden kann.

7.4.6. Nicht – Abstreitbarkeit

Dies ist eine Sicherheitsanforderung an Web-Shops. Aus Sicht der Internetanbindung kann man sich fragen ob ein Web Shop im Einsatz ist oder ob Bestellungen via Mail oder via das WEB erfolgen. Das soll man dann dokumentieren. Für den Kunden wäre ein Web Shop das einfachste und angenehmste sowie die modernste Lösung, jedoch erfordert dies erhöhte Sicherheit sowie entsprechende Ressourcen.

7.4.7. Verlässlichkeit

Die Verlässlichkeit ist sehr wichtig mit der Wartung der Internetzugänge. Man sollte sich daher folgende Fragen stellen:

- Wie ist die Wartung organisiert?
- Sind die Systeme zuverlässig gewartet?
- Werden Backups gemacht?
- Werden Patches regelmässig eingespielt?
- Ist PKI (Public Key Infrastructre) im Einsatz?
- Werden die Vulnerabilitätsdatenbanken regelmässig konsultiert?
- Werden die Firewalls intern oder extern gemanaged?
- Ist der BSI Grundschutz implementiert?

7.4.8. Zugriffskontrolle

Diese spielt in der Sicherheit eine grosse Rolle. Um den Internetzugriff gewährleisten zu können, sollte man definieren, wer, welchen Dienst verwenden darf. Unter Diensten versteht man eine Anwendung des Internets im technischen Sinne. Das Internet selbst stellt lediglich die Infrastruktur zur Übertragung der Daten zur Verfügung. Zudem sollte man jeden Dienst und Ort sowie die entsprechende Zugriffsart gut dokumentieren.

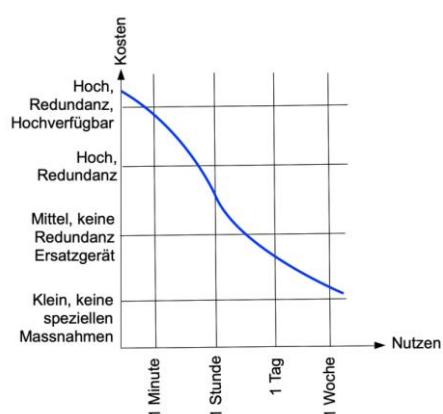


Abbildung 23: Verhältnis Kosten und Nutzen nach der Verfügbarkeit

7.4.9. Sicherheitskonzept

7.4.9.1. Technische Massnahmen

- Die Berechtigungen so verteilen, dass nur die nötigen Personen Zugriff auf die Dokumente haben.
- Den Zugriff überwachen, damit Veränderungen nachvollzogen werden können (Logging)
- Alle Infrastruktur relevanten Geräte haben ein sicheres Admin Passwort. Auf Servern und Notebooks ist zudem ein sicheres BIOS Passwort gesetzt.
- Server müssen durch eine USV Stromzufuhr betrieben werden.
- Webserver oder andere dienste in der DMZ sollten intern nur via Jump Server erreichbar sein.
- Wenn externe Mitarbeiter auf die Systeme Zugriff haben, sollte dies nur über einen sicheren Kanal passieren, wie VPN.
- Backups müssen täglich vom System gemacht werden.

7.4.9.2. Nicht technische Massnahmen

- Die Mitarbeiter schulen, damit sie sich bewusst sind, welche Auswirkungen eine Vernachlässigung mitnehmen kann (Schulung).
- Eine Sicherheits-Policy aufsetzen, welche verschiedene Massnahmen niederschreibt, die zu einem späteren Zeitpunkt zugegriffen werden, kann (Policy).
- Abgeschlossener Bereich für den Serverraum.
- Offene Switches in einem Schrank abschliessen.
- Bei jeder Berechtigung muss ein Owner definiert werden und entsprechend dokumentiert werden.
- Vendor Escalation für wichtige Dienste sowie Systeme müssen genau dokumentiert werden.

7.5. Wartung & Überwachung

7.5.1. Vergleich der Überwachungstools

Für den Vergleich der verschiedenen zur Verfügung stehenden Produkte haben wir folgende fünf ausgewählt und mit einer Bewertungsmatrix die besten drei ausgewertet.

7.5.1.1. Zabbix

Der Zabbix Server ist zuständig für das Sammeln und Auswerten der Monitoring-Daten. Gesammelte Daten werden in einer einheitlichen Datenbank gespeichert. Das Abfragen der Geräte erfolgt via SNMP, ssh oder ICMP (ping) oder mit dem Zabbix Agent direkt auf den Hosts. Im Falle einer Überschreitung der erfassten Werte kann der Zabbix Server Benachrichtigungen verschicken oder direkt selbst Massnahmen durchführen

7.5.1.2. PRTG

24/7 365 Tage im Jahr und haargenau überwachen bietet PRTG an und mit Ihren hochflexiblen Benachrichtigungssystem werden System-Administratoren zeitnah reagieren ohne dass grosse Probleme für die Firma entstehen. PRTG verfügt über einige spannende Features wie anpassbare GUIs, Maps und Dashboards, detaillierte Berichte, verteiltes Monitoring.

7.5.1.3. Nagios

Zur Überwachung interner Eigenschaften von Rechnern müssen Plug-ins meist direkt auf den Hosts ausgeführt werden. Eine andere Möglichkeit ist die Installation weiterer Programme (Add-Ons) auf den Hosts, die nur lokal vorkonfigurierte Systemabfragen ausführen können. Die Kommunikation zwischen diesen Programmen und dem Nagios-Server (Abfrage und Ergebnisübermittlung) erfolgt dann über eigene definierbare Netzwerk-Ports.

7.5.1.4. SolarWinds Network Performance

SolarWinds Network Performance Monitor ist eine leistungsstarke und erschwingliche Software für die Netzwerküberwachung, mit der man Netzwerkleistungsprobleme und Ausfälle schnell erkennen, diagnostizieren und beheben kann.

7.5.1.5. LAN Guard

Um zeitnah Sicherheitslücken im System zu erkennen, bevor sie von Angreifern verwundbar gemacht werden, wird GFI LanGuard eingesetzt. Netzwerk scannen, um zu sehen, von wo Bedrohungen hereinkommen ist u.a. eine der wichtigsten Funktionen, welche System Administratoren eingerichtet sollen. Das Ganze nennt sich Patch Management

7.5.2. Bewertungsmatrix

Aus den fünf Produkten haben wir die besten 3 ausgewählt, um einen Bewertungsmatrix zu erstellen. Die verteilten Punkte zur jede Kategorie sieht man im folgender Matrix ein und bemerkt, dass alle 3 Produkte als best-in-class sind und dafür der Mitarbeiter/Expert/Firma eine breite Auswahl an gute Produkte hat und somit sich beliebig entscheiden kann.

Auswahlkriterium	Gewichtung	Zabbix		Nagios		PRTG	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	22	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	2	3	6	3	6	3	6
Stabilität	10	5	50	5	50	6	60
Qualität	10	5	50	5	50	6	60
Wirtschaftliche Kriterien	24						
Kosten / Nutzen	8	6	48	5	40	5	40
Wartungskosten	4	3	12	4	16	5	20
Betriebskosten	6	4	24	3	18	2	12
Lizenzgebühren	6	6	36	3	18	2	12
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	6	5	30	5	30	4	24
Stabilität des Lieferanten	4	4	16	4	16	4	16
Referenzen	2	3	6	5	10	5	10
Operative Kriterien	14						
Betriebbarkeit	6	6	36	6	36	6	36
Notwendiges Know-How	4	6	24	6	24	5	20
Support	4	4	16	5	20	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	5	15
Kommunikationsprozesse	3	5	15	5	15	4	12
Juristische Kriterien	8						
SLA	4	4	16	6	5	6	24
Verträge	3	4	12	5	15	5	15
Gesetze	1	5	5	5	5	5	5
Ökologische Kriterien	2						
Entsorgung	1	4	4	4	4	4	4
Wiederverwendbarkeit	1	4	4	4	4	4	4
Sicherheits Kriterien	12						
Verfügbarkeit	6	4	24	6	36	6	36
Vertraulichkeit	3	5	15	5	15	5	15
Integrität	3	5	15	5	15	6	18
Total	100		479		463		488
Rang			2		3		1

Tabelle 39: Bewertungsmatrix für Überwachungstools

7.5.3. Wartung

Gemäss das vom FCAPS empfohlene System (genannt Fault Management) sowie das von ITIL vorgesehen Event Management wird die Wartung der eingesetzte Geräte definiert. Die Firma soll, wenn möglichst über einen internen Ticketsystem verfügen, welcher auch ein Teil vom ITSM (IT-Service Management) ist.

Beim Eintreten einer Wartung muss gemäss Fault Management ein sogenannter Change eingeführt werden. Die Kriterien, welcher das Change bestimmen und haben muss, sind folgende.

Kriterien	Beschreibung
Einhaltung des SLAs, also ein Start- und Enddatum	Explizit beschrieben werden, in welchem Zeitraum eine Wartung vorgenommen wird.
Das besagte Gerät (Configuration Item)	Das Gerät mit allen Netzwerkangaben soll deklariert werden (Hostname, MAC, IP).
Die Kollisionserkennung (Collision Detection)	Muss nachgeschaut werden, ob in der gleichen Zeitperiode auf demselben Gerät eine andere Wartung vorgenommen wird.
Ein Katalog mit allen Produkte (Product Catalog)	Darin wird erläutert, welche Programme/Applikationen und Dienste betroffen werden

Tabelle 40: Beschreibung Change Management

7.5.3.1. Change Management

Eine Change ist eine Änderung oder Erweiterung einer vorhandenen Spezifikation, eines Produktes oder einer Dienstleistung. Dies kann ein Erneuerung oder entfernen von Hardware, Patch Upgrades oder auch die Implementierung einer neuen Applikation. Ein SLA oder OLA ist dabei Pflicht.

7.5.3.1.1. Normale Change

Diese Art trifft am häufigsten auf. Dieser Change kann in voraus geplant werden und muss vom Change Manager sowie auch von der Approving Gruppe bewilligt werden.

7.5.3.1.2. SOP

Der Standard-Change benötigt einen genehmigten SOP (Standard Operating Procedure), dieser Change bezieht sich auf Standard Änderungen, meistens Teile des Tagesgeschäfts. Diese Change's kommen meistens automatisch und müssen nur noch durch den Change Manager automatisch überprüft sowie bewilligt werden. Da der Change kein hohes Risiko hat, kann der auch während der produktive Zeit durchgeführt werden.

7.5.3.1.3. Beschleunigte Change

Ist ein Hybrid aus dem «Normalen» und dem «Notfall-Change». Diese Art wird verwendet wenn eine bekannte Fehlerkorrektur durchgeführt werden muss oder um einen potenziellen Verlust oder Verschlechterung der Dienstleistung zu vermeiden. Diese Art von Change muss getestet werden.

7.5.3.1.4. Notfall Change

Auch Emergency Change genannt, stellt die höchste Gefahrenstufe dar. Diese Change's müssen so rasch wie möglich gemacht werden. Dieser Change entsteht aus einem Incident.

7.5.3.1.5. Der Change ohne Auswirkung

Diese Art von Change hängt mit keinem hohen Risiko im Zusammenhang. Dabei ist die IT-Infrastruktur der SIX nicht direkt betroffen, sondern die einer unserer Kunden. Dieser Change hat eher eine formelle Bedeutung, damit Systeme bzw. die Operator wissen, dass bei u Kunden gerade ein Change ist und nicht irgendwie zB. die System ungeplant heruntergefahren werden.

7.5.3.2. Rollen

7.5.3.2.1. Change Requestor

Der Change Requestor erfasst den Change. Er muss nicht dringend der Change Coordinator sein.

7.5.3.2.2. Change Coordinator

Der Change Coordinator übernimmt eine wichtige Rolle im Change Prozess. Am Change Requestor und Change Implementor kann gleichzeitig diese Rolle zugewiesen werden.

Der Change Coordinator ist für folgende Dinge zuständig:

- Sicherstellung des Informationsflusses zwischen allen an dem Change beteiligten Parteien
- Auswahl eines geeigneten Datums für die Umsetzung des Change
- Sicherstellung der umfangreichen Tests (der Koordinator muss lediglich den Nachweis der Prüfung erbringen, er tut es nicht).
- Bewertung des Risikos bzw. Bekanntgabe des Risikos im Change (Risk Level).
- Der Koordinator ist die Schnittstelle zum Change Management.
- Er stellt sicher, dass wichtige Änderungen mit dem Change Management mit der richtigen Erklärung besprochen werden (erfolgreich, nicht erfolgreich, erfolgreich mit Problemen)

7.5.3.2.3. Change Implementor

Der Change Implementor kann gleichzeitig der Change Coordinator sein, er kann auch vom Change Coordinator nominiert werden. In diesem Fall liegt es in der Verantwortung der Change Coordinators, eine Aufgabe innerhalb der Change zu etablieren und sie dem nominierten Change Implementor zuzuordnen.

7.5.3.2.4. Change Manager

Die Aufgabe des Change Manager besteht darin, dass er die Changes überwacht und überprüft. Er muss die Risiken so gut wie möglich einschätzen können.

7.6. Firewall

Als die ersten Internet-System-Administratoren erkannten, dass ihre Netzwerke häufig angegriffen wurden, war die Firewall unvermeidlich. Ziel war ein Prozess, der den Netzwerkverkehr auf klare Anzeichen eines Angriffs hin untersucht. Wie genau das funktionieren würde, war zunächst aber weniger klar. Der Begriff Firewall für das Filtern von unerwünschtem Netzwerkverkehr fiel erstmals um das Jahr 1987 herum. Er wird Steven M. Bellovin von AT&T zugeschrieben. Der Name war eine Metapher, die Firewalls mit Trennwänden vergleicht, die verhindern, dass ein Feuer von einem Teil einer physischen Struktur zum anderen wandert. Im Fall des Netzwerks ging es darum, eine Art Filter zwischen dem scheinbar sicheren internen Netzwerk und jeglichem Verkehr einzufügen, der über die Verbindung dieses Netzwerks mit dem Internet ein- oder ausgeht.

Mittlerweile hat sich der Begriff Firewall bereits so im IT-Sprachgebrauch etabliert, dass keine zufällige Unterhaltung über Netzwerksicherheit stattfinden kann, ohne ihn zumindest zu erwähnen. Im Laufe der Zeit haben sich verschiedene Arten von Firewalls herauskristallisiert. Unabhängig von ihrem Typ ist es die Aufgabe von Firewalls, etwas zu tun, das eigentlich unmöglich ist. Sie werden in ein Netzwerk eingefügt und untersuchen den gesamten ein- und ausgehenden Netzwerkverkehr. Dabei haben sie die Aufgabe zu sagen, welche Informationen gutartig und welche Daten Teil einer Attacke sind.

Ein Computerprogramm, das grundsätzlich eine Reihe von Computerbefehlen betrachten und deren Absicht feststellen kann, widerspricht einer grundlegenden These der Informatik, die besagt: Es gibt kein Computerprogramm, das das Ergebnis eines anderen Computerprogramms perfekt vorhersagen kann, ohne es auszuführen und dessen Aktionen zu sehen. Demnach ist es auch nicht möglich, den Netzwerkverkehr allgemein zu betrachten und seine Absicht zu erkennen. Es ist jedoch möglich, nach bekannten Mustern in Netzwerkpaketen zu suchen, die bereits bekannte Angriffe anzeigen und genau das war und ist die Aufgabe von speziellen Paketfilter-Netzwerk-Firewalls. Grundsätzlich wird jede Art von Firewall in einem Netzwerk mit einem ständig aktualisierten Satz von Firewall-Regeln eingesetzt, die verschiedene Kriterien definieren, nach denen ein bestimmtes Paket oder mehrere Pakete in einer Transaktion sicher an den vorgesehenen Empfänger weitergeleitet werden kann.

Hier sind fünf Arten von Firewalls, die bei der Entwicklung der Kategorie Firewall eine wichtige Rolle gespielt haben und spielen.

7.6.1. Verschiedene Firewall Arten

7.6.1.1. Packet Filter Firewalls

Dieser erste und ursprüngliche Firewall-Typ arbeitet an Knotenpunkten und Geräten wie Routern und Switches. Diese Firewall leitet jedoch keine Pakete weiter, sondern vergleicht jedes empfangene Paket mit einer Reihe von festgelegten Kriterien wie etwa erlaubten IP-Adressen, Pakettyp oder Portnummer. Pakete, die als problematisch erkannt werden, leitet die Firewall in der Regel nicht weiter, das heisst sie gelangen nicht ins interne Netzwerk.

7.6.1.2. Circuit Level Gateways

Verbindungs-Gateways identifizieren bösartiger Inhalte relativ schnell. Sie überwachen die TCP-Daten im gesamten Netzwerk und stellen fest, ob die gestartete Sitzung legitim ist und das entfernte System als vertrauenswürdig angesehen wird. Damit lassen sich auf einer Firewall beliebige IP-Adressen und Ports sperren oder freischalten. Circuit Level Gateways sind allerdings nicht in der Lage, die Paketinhalte selbst zu kontrollieren.

7.6.1.3. Application Level Gateways

Stateful Inspection Firewalls untersuchen nicht nur jedes Paket, sondern behalten auch den Überblick, ob dieses Paket Teil einer autorisierten TCP-Sitzung ist oder nicht. Dies bietet im Vergleich zur Paketfilterung und zu Verbindungs-Gateways höhere Sicherheit, belastet aber auch die Netzwerkleistung stärker.

Diese Art der Firewall überwacht jede Internet-Session von Anfang bis Ende und erzwingt Regeln auf Basis von Protokoll, Port sowie Quell- und Zieladresse. Die Firewall kann schnell verifizieren, dass neue eingehende Pakete den Kriterien für autorisierten Verkehr entsprechen. Pakete, die nicht Teil einer autorisierten Sitzung sind, werden abgewiesen. Eine weitere Variante der Stateful Inspection ist die Multilayer Inspection Firewall, die den Ablauf von Transaktionen über mehrere Schichten des OSI-Modells (Open Systems Interconnection) betrachtet.

7.6.1.4. Stateful Inspection Firewall

Diese Firewalls, manchmal auch als Proxy-Firewall bezeichnet, kombinieren einige der Eigenschaften von Paketfilter-Firewalls mit denen von Verbindungs-Gateways. Sie filtern Pakete nicht nur für den Service, für den sie laut dem angegebenen Ziel-Port bestimmt sind, sondern auch nach bestimmten anderen Merkmalen, wie etwa dem HTTP Request String. Sie kontrollieren zudem die Ausführung von Dateien oder die Bearbeitung von Daten spezieller Anwendungen. Gateways, die auf der Anwendungsschicht filtern, bieten zwar hohe Datensicherheit, können aber die Netzwerk-Performance erheblich beeinträchtigen.

7.6.1.5. Next-Generation Firewalls

Eine typische Next-Generation Firewall (NGFW) kombiniert Paketinspektion mit Stateful Inspection und integriert Deep Packet Inspection (DPI). Das heisst, sie untersucht nicht nur das verwendete Protokoll und den eingesetzten Port, sondern nimmt auch den Inhalt des Datenstroms unter die Lupe, erkennt ungewöhnliches Verhalten oder filtert infizierte Dateien aus. In der Regel erkennen NGFWs auch die Aktivitäten der im Netz tätigen Nutzer und entscheiden auf Basis von Richtlinien, was diese dürfen und was nicht.

Was mit Deep Packet Inspection gemeint ist, hängt sehr stark vom jeweiligen Anbieter ab. Der Kern der Sache ist, dass die Paketinspektion bei traditionellen Firewalls ausschliesslich den Header des Pakets betrachtet, während die Deep Packet Inspection die tatsächlichen Daten untersucht, die das Paket enthält. So kann eine solche Firewall den Fortschritt einer Web-Browsing-Sitzung verfolgen und feststellen, dass ein Paket nicht legitim ist und damit blockiert wird, wenn es mit anderen Paketen zu einer HTTP-Server-Antwort zusammengestellt wird.

Gleichgültig, für welche Art von Firewall sich Unternehmen entscheiden: Eine falsch konfigurierte Firewall kann in gewisser Weise schlimmer sein als eine fehlende Firewall, weil sie den gefährlichen Eindruck von Sicherheit vermittelt, während sie wenig oder gar keine bietet.

7.6.2. Firewall Lösungen

7.6.2.1. Günstige Hardware-Firewalls

Als günstige Hardware Firewall haben wir uns für Cisco entschieden. Cisco ist ein Unternehmen aus den USA und wurde in San Francisco gegründet.

Wir haben uns auf das Modell «Cisco ASA 5506-X» entschieden welches momentan auf Digitec für 289 CHF erhältlich ist. Die Firewall hat 8 Gigabit Ports, die man verschiedenen Zonen zuordnen kann. Diese Cisco Firewall ist ideal für KMUs. Seitens Cisco bietet dieses Firewall eine Application Control, eine Antivirus Funktionalität, einen Content Filter, einen Spam-Filter und eine VPN Funktionalität. Das OS ist von Cisco entwickelt und explizit auf die Hardware ausgelegt, was ein Vorteil gegenüber einer Lösung mit Linux ist.

Einige Kennzahlen zur Cisco ASA 5506-X Firewall:

- Durchsatzraten:
 - o SPI: 300 Mbit/s
 - o VPN: 100 Mbit/s
 - o Antiviren: 250 Mbit/s
 - o IDP: 125 Mbit/s
- Max. IPsec VPN Tunnels: 50
- Max. Sessions: 200000
- RAM: 4 GB

- Vorteile des Cisco ASA 5506-X
 - o Ermöglicht dynamisches Routing und Site-to-Site-VPN.
 - o Bietet integrierte IPS-, VPN- und Unified Communications Funktionen

7.6.2.2. PC-Lösung mit Linux

OPNsense ist eine Firewall- und Routing-Plattform auf der Basis von HardenedBSD. Die Appliance ist für den Betrieb auf physischer Hardware oder als virtuelle Maschine (VM) geeignet. OPNsense bietet unter anderem Funktionen wie Forward-Caching-Proxy, Traffic Shaping, Intrusion Detection und eine einfache OpenVPN-Client-Einrichtung. Die Stateful-Firewall unterstützt IPv4 und IPv6 und bietet Live-Einblick in den Datenverkehr.

Der grosse Vorteil an OPNsense ist, dass es Open Source ist und es sich so zu 100% auf die eigenen Bedürfnisse anpassen lässt.

Die Kernfunktionen von OPNsense:

- Traffic Shaper
- Zwei-Faktor-Authentifizierung im gesamten System
- Forward Caching Proxy (transparent) mit Blacklist-Unterstützung
- Virtuelles Privates Netzwerk (Site to Site & Road Warrior, IPsec, OpenVPN & alte PPTP-Unterstützung)
- Hochverfügbarkeit & Hardware-Failover (mit Konfigurationssynchronisation & synchronisierten Zustandstabellen)
- Erkennung und Verhinderung von Eindringlingen
- Eingebaute Berichts- und Überwachungswerkzeuge einschliesslich RRD-Grafiken
- Überwachung des Netzwerkflusses
- Unterstützung für Plugins
- DNS-Server & DNS-Weiterleitung
- DHCP-Server und -Relay
- Dynamisches DNS
- Verschlüsselte Konfigurationssicherung auf Google Drive
- Stateful-Inspektions-Firewall
- 802.1Q VLAN-Unterstützung

7.6.2.3. Firewall-Service des Providers

Die Swisscom ist eine der führenden MSS Anbieter in der Schweiz. Mit ihrem MSS-i Managed Firewall Service bietet die Swisscom ihren Kunden eine Firewall an, die nicht beim Kunden physisch steht, sondern bei der Swisscom. Bei dieser Lösung liegt der klare Vorteil, dass man kein weiteres Gerät an seinem Standort stehen hat. Dies kann aber auch ein Nachteil sein, da Anpassungen nicht direkt vor Ort vorgenommen werden können. Der Kunde muss sich zudem nicht um die Evaluierung der Hardware kümmern, einzige Voraussetzung für diesen Service ist, dass man bereits ein Swisscom Netz hat, sonst kann der Service nicht in das Unternehmen integriert werden.

Infos zur Firewall bei Swisscom

- Stateful-Inspection-Firewall
- DMZ
- Bereitstellungsmodelle: lokal, in Swisscom Clouds, in öffentlichen Clouds (Azure, AWS)
- Site-to-Site-VPN (IPSec)
- Client-to-Site-, Client-to-Portal-VPN
- Professionelle Firewall-Lösung zum Schutz des Internen Netzwerks vor Angriffen aus dem Internet
- Firewall-Management im hochsicheren, vollständig redundanten Swisscom Security Operation Center
- Zugriff via Webportal auf Firewall-Status, Logdaten, Statistiken und Reports

- Systemüberwachung und Helpdesk 24x7
- Release- und Patch-Management
- Change-Management je nach SLA
- Health- und Incident-Management je nach SLA

7.6.3. Vergleich

Auswahlkriterium	Gewichtung	Hardware Firewall		PC-Lösung		Firewall Service	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	5	40	5	40	4	32
Stabilität	8	6	48	5	40	6	48
Qualität	8	6	48	5	40	6	48
Wirtschaftliche Kriterien	24						
Kosten / Nutzen	6	5	30	6	36	4	24
Wartungskosten	6	6	36	5	30	6	36
Betriebskosten	6	5	30	6	36	5	30
Lizenzgebühren	6	4	24	6	36	5	30
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	6	24	5	20	5	20
Stabilität des Lieferanten	4	5	20	5	20	5	20
Referenzen	4	5	20	4	16	6	24
Operative Kriterien	12						
Betriebbarkeit	4	5	20	5	20	6	24
Notwendiges Know-How	4	4	16	5	20	6	24
Support	4	4	16	4	16	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	4	12
Kommunikationsprozesse	3	5	15	5	15	4	12
Juristische Kriterien	6						
SLA	2	5	10	4	8	6	12
Verträge	2	5	10	4	8	6	12
Gesetze	2	5	10	5	10	6	12
Ökologische Kriterien	4						
Entsorgung	2	3	6	3	6	6	12
Wiederverwendbarkeit	2	3	6	5	10	5	10
Sicherheits Kriterien	12						
Verfügbarkeit	4	6	24	6	24	6	24
Vertraulichkeit	4	6	24	6	24	5	20
Integrität	4	6	24	6	24	5	20
Total			516		514		530
Rang			2		3		1

Abbildung 24: Matrix für Firewall

7.6.4. Entscheid

Wir werden der Coffee GmbH einen Firewall Service der Swisscom empfehlen. Durch die Empfehlung des Internetanbieters, welcher ebenfalls auf Swisscom gefallen ist, trifft sich das sehr gut. Die Coffee GmbH hat nicht das ausgebildete Fachpersonal, um eine Firewall inhouse zu betreiben, dadurch ist es besser auf FWaaS zu setzen. Das MSS-i Managed Firewall von der Swisscom ist sehr gut. Für den Preis von 60 CHF ist der Service zwar noch recht teuer, aber der Kunde muss sich gar nicht mehr um eine Firewall kümmern, die Swisscom übernimmt alles.

7.7. VPN

7.7.1. IPsec

IPsec ist ein IETF-Standard. Arbeitet auf ISO Layer 3 Vermittlungsschicht und dessen wichtiger Anwendungsbereich ist die Realisierung von VPNs über Internetverbindungen. Ist ähnlich wie WireGuard wobei WireGuard eine höhere Verarbeitungs-geschwindigkeit besitzt.

IPsec sorgt für das CIA Prinzip (<https://security.luis-luescher.com/documentations/cia/>) der übertragenen Daten sowie sicheren Schlüsselaustausch.

- Vertraulichkeit => Verschlüsselung
- Integrität => Hash Funktion (Festgelegte Länge, Kollisionsresistent (unterschiedliche Eingabewerte = ein anderer Hashwert), Einwegfunktion (Inhalte in einen Hash umgerechnet werden aber nicht umgekehrt.)
- Authentizität => Identitätsüberprüfung (Die beiden VPN Peers wissen das es sich beim gegenüber um den Richtigen handelt.)

Grundsätzlich ist IPSec eine Sammlung von Algorithmen und Funktionen.

Die beiden VPN Peers müssen im Voraus untereinander abmachen, wie sie kommunizieren wollen. Somit müssen alle Parameter für eine VPN-Verbindung ausgehandelt werden eine sogenannte **Security Association**.

Folgende Parameter:

- Identifikation (entweder per PSK oder Zertifikat)
- Festlegung des zu verwendenden Schlüsselalgorithmus für die IPsec-Verbindung
- von welchem (IP-)Netz die IPsec-Verbindung erfolgt
- zu welchem (IP-)Netz die Verbindung bestehen soll
- Zeiträume, in denen eine erneute Authentisierung erforderlich ist
- Zeitraum, nach dem der IPsec-Schlüssel erneuert werden muss

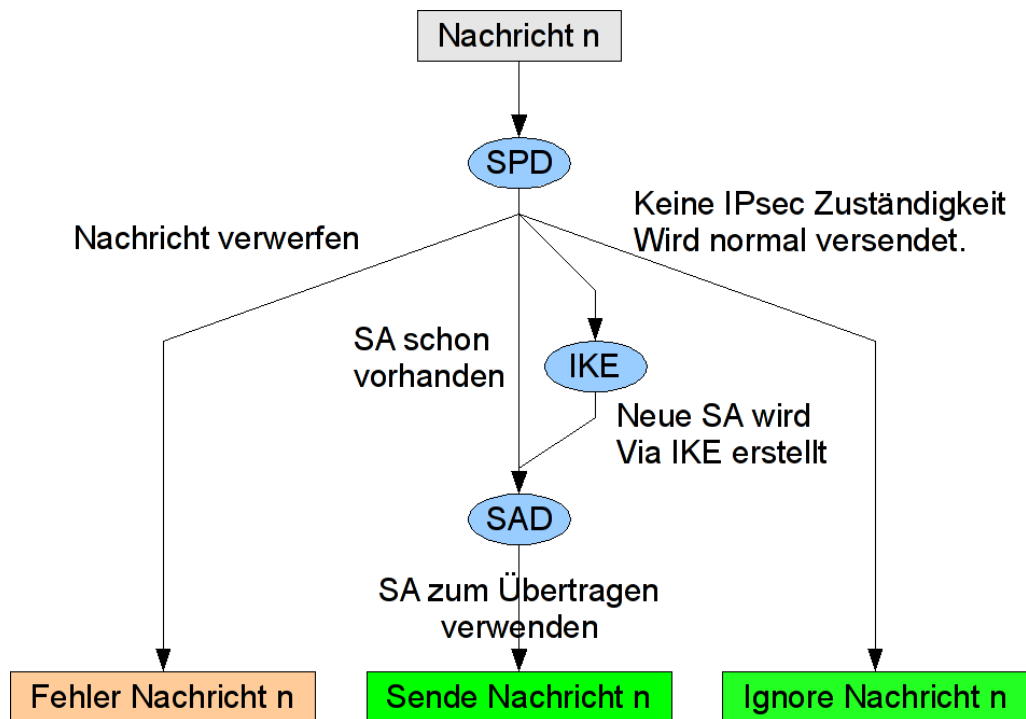


Abbildung 25: Einfache Erklärung von IPsec von [Wikipedia](#)

7.7.1.1. SPD

SPD steht für Security Policy Database.

Hier wird definiert wie die Verbindung zwischen den Kommunikationsendpunkten, die durch ihre IP-Adressen identifiziert sind, gesichert werden sollen.

7.7.1.2. SAD

SAD steht für Security Association Database

Hier werden die Security Associations abgespeichert, sprich wie die nötigen Parameter zwischen Host 1 und Host 2 sind, um einen Tunnel aufzubauen. Somit wird für jede Verbindung innerhalb der Datenbank ein eigener Eintrag erstellt.

7.7.1.3. IKE

IKE steht für Internet Key Exchange

Dient zur automatischen Schlüsselverwaltung für IPsec. Bevor man eine verschlüsselte Verbindung mittels IPsec aufsetzt müssen sich beide Seiten gegenseitig authentisieren und sich auf die verwendeten Schlüssel-algorithmen einigen. Dafür ist IKE gedacht. IKE ist somit für den sicheren Austausch von schlüsseln über ein unsicheres rechnernetz zuständig.

7.7.2. SSL VPN oder IPsec VPN

7.7.2.1. SSL VPN

Diese Virtual Private Networks haben noch mehr Vorteile:

- Sie benötigen in den meisten Fällen keine Extra-Software, um Daten sicher über das Netz auszutauschen.
- Weil die SSL-VPN-Technik über den Browser läuft, ist die Verfügbarkeit ausgezeichnet und die Nutzung vergleichsweise einfach. Beispielsweise lässt sich im Homeoffice ohne Probleme auf digitale Informationen im Büro zugreifen.
- Administratoren können genau festlegen, welcher Nutzer welche Applikationen nutzen darf. Das heisst, User haben keinen Zugriff auf das gesamte System, beispielsweise auf alle Serverdaten, sondern immer nur auf ausgewählte Hapen.

Doch wie immer gibt es auch Nachteile:

- Brisante Daten sind unter Umständen im Cache des Browsers gespeichert und dort anfällig für Malware.
- Webapplikationen können ausgespäht werden. Das heisst, findige Hacker lesen mit, wenn Sie Zugangspasswörter eingeben.
- Insgesamt sind SSL-VPNs nur so sicher, wie der Laptop, das Smartphone oder der Computer, auf dem sie laufen.

7.7.2.2. IPsec VPN

Die Vorteile im Überblick:

- Mit einer eigenständigen Client-Software wird ein sicherer Tunnel durch das Internet gebahnt.
Das ist kostengünstiger als eine reale Standleitung, die ebenfalls kontinuierlichen Kontakt hält.
- Es wird das gesamte Netzwerk auf einen Schlag für autorisierte Nutzer zugänglich gemacht – User müssen nicht für jede Kleinigkeit von Admins freigeschaltet werden.

Auch IPSec-VPNs haben Nachteile:

- Damit die Verbindung zwischen zwei Computern über das Internet funktioniert, müssen die beiden vorher Schlüssel austauschen. Damit wird die Tür zum sicheren VPN-Tunnel aufgeschlossen. Bekommen Hacker die Codes auf den Laptops oder Smartphones der Beteiligten in die Hände, so kann die Übertragung ausgespäht oder manipuliert werden.
- Die Client-Software, also das Extra-Programm, muss richtig konfiguriert werden. Sie brauchen einen fähigen Administrator.
- Auch IPSec-VPNs sind nur so sicher, wie der Laptop, das Smartphone oder der Computer, auf dem sie laufen – Sie erinnern sich, gleiches gilt für SSL-VPNs.

7.7.2.3. Fazit

Das führt zu unserem Kurzfazit. SSL-VPN und IPsec-VPN bieten in etwa die gleiche Sicherheit:

- SSL-VPN eignet sich vor allem, um Nutzern einen unkomplizierten Zugriff zu gewähren. Wenn beispielsweise Zugang zu speziellen Daten gebraucht wird, ist diese Option ideal.
- IPsec-VPN ist für lang andauernde Verbindungen übers Netz geeignet. Beispielsweise wenn ein Unternehmen mehrere Filialen hat, die regelmässig Daten austauschen.
- Wichtig ist, dass man grundsätzlich einen VPN nutzt.
- Als Faustregel gilt jedoch: Je mehr Anwender und je sensibler die Daten, desto eher ist ein IPsec-VPN sinnvoll.

7.7.3. VPN-Architekturen

7.7.3.1. Site-to-Site VPN



Abbildung 26: Site to Site VPN

Site-to-Site-VPN und LAN-to-LAN-VPN, oder auch Branch-Office-VPN genannt, sind VPN-Szenarien, um mehrere lokale Netzwerke von Aussenstellen oder Niederlassungen (Filialen) zu einem virtuellen Netzwerk über ein öffentliches Netz zusammenzuschalten. Bei VPNs über das Internet entstehen einmalige Kosten für die Einrichtung und laufende Kosten nur die, die für den Internet Service Provider zu bezahlen sind. Virtuelle private Netze (VPN) werden immer öfter über das Internet aufgebaut. Das Internet wird so zur Konkurrenz zu den klassischen WAN-Diensten der Netzbetreiber. VPNs lassen sich über das Internet billiger und flexibler betreiben.

7.7.3.2. End-to-End VPN



Abbildung 27: End to End VPN

End-to-End-VPN beschreibt ein VPN-Szenario, bei dem ein Client auf einen anderen Client in einem entfernten Netzwerk zugreift. Hierbei deckt der VPN-Tunnel die gesamte Verbindung zwischen zwei Hosts ab. Auf beiden Seiten muss eine entsprechende VPN-Software installiert und konfiguriert sein. In der Regel ist der Verbindungsaufbau nur durch die Unterstützung einer zwischengeschalteten Station möglich. Das bedeutet, eine direkter Verbindungsaufbau von Host zu Host ist nicht möglich. Stattdessen bauen beide Seiten eine Verbindung zu einem Gateway auf, dass die beiden Verbindungen dann zusammenschalten.

Typische Anwendung eines End-to-End-VPN ist Remote-Desktop über öffentliche Netze. Während RDP und VNC sich wegen der fehlenden Verschlüsselung nur für den Einsatz in lokalen Netzwerken eignet, gibt es für Remote-Desktop-VPNs meist nur proprietäre und kommerzielle Lösungen. Zum Beispiel Teamviewer und GotoMyPC.

7.7.3.3. End-to-Site VPN



Abbildung 28: End to Site VPN

End-to-Site-VPN beschreibt ein VPN-Szenario, bei dem Heimarbeitsplätze oder mobile Benutzer (Aussendienst) in ein Unternehmensnetzwerk eingebunden werden. Der externe Mitarbeiter soll so arbeiten, wie wenn er sich im Netzwerk des Unternehmens befindet. Man bezeichnet dieses VPN-Szenario auch als Remote Access.

Die VPN-Technik stellt eine logische Verbindung, den VPN-Tunnel, zum entfernten lokalen Netzwerk über ein öffentliches Netzwerk her. Hierbei muss ein VPN-Client auf dem Computer des externen Mitarbeiters installiert sein.

Im Vordergrund steht ein möglichst geringer, technischer und finanzieller Aufwand für einen sicheren Zugriff auf das entfernte Netzwerk.

7.7.4. VPN Lösungen

7.7.4.1. Hardwarelösung

Da viele Firewalls auch VPN unterstützen und es kaum Hardware gibt, welche nur für VPNs hergestellt wird, nehmen wir hier wieder den ASA 5506-X von Cisco. Dieser ermöglicht 50 VPN Nutzer was für die Coffee GmbH genügt.

7.7.4.2. VPN-Service des Providers

NordVPN ist ein sehr bekannter VPN Service welcher Anonymität im Internet gewährleistet. Die Verbindung wird dann immer über einen der insgesamt 5458 VPN Server in 59 Ländern weltweit geleitet. Die Verbindung ist zwischen dem Server und dem eigenen Computer immer verschlüsselt. Man kann sich ein 2 Jahres Abo für 3.15 CHF im Monat kaufen so würde der Service für zwei Jahre insgesamt 75.6 CHF kosten.

7.7.4.3. PC-Lösung

WireGuard ist eine noch sehr junge Technologie, um sichere und leistungsfähige virtuelle private Netze (VPNs) mit geringem Aufwand zu realisieren. Es handelt sich um ein Open-Source-Protokoll und eine Open-Source-Software, die eine Alternative zu etablierten VPN-Lösungen wie OpenVPN oder IPsec bieten soll.

Folgende Ziele wurden beim Design der VPN-Alternative verfolgt:

- einfache Nutzbarkeit
- hohe Performance
- hohe Sicherheit durch Verwendung aktueller kryptographischer Verfahren
- überschaubarer Code mit minimaler Angriffsfläche
- sorgfältig durchdachtes Gesamtkonzept

Für den Aufbau von VPN-Verbindungen und den Austausch von Daten greift WireGuard auf verschiedene Protokolle zurück. Die wichtigsten Protokolle sind:

- Curve25519 (ECDHE) für den Austausch von Schlüsseln
- ChaCha20 und Poly1305 für den Austausch und die Verschlüsselung der Daten
- BLAKE2s für das Hashing
- Ed25519 für das Public-Key-Authentifizierungsverfahren

Die Vorteile von WireGuard sind:

- Schnelle und einfache Einrichtung
- Schlanke Codebasis
- Fokussierung auf wenige aber moderne Kryptografiertechniken
- Unterstützt viele Betriebssystem-Varianten
- Wechsel zwischen WLAN- und Mobilfunkverbindung ohne spürbare Unterbrechung
- Sehr schneller Verbindungsaufbau
- Sehr hohe Geschwindigkeit
- Open Source

Einschränkungen gibt es bei WireGuard für VPN-Anwendungszwecke im Bereich der Anonymisierung:

- Ohne Logging nicht nutzbar.
- Keine dynamische IP-Zuweisung, jedem Client ist eine IP fest vorgegeben.



Abbildung 29: Offizielles Logo von WireGuard

7.7.5. Vergleich

Auswahlkriterium	Gewichtung	Hardware		PC-Lösung		VPN Service	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	5	40	5	40	4	32
Stabilität	8	3	24	5	40	6	48
Qualität	8	4	32	5	40	6	48
Wirtschaftliche Kriterien	24						
Kosten / Nutzen	6	4	24	5	30	2	12
Wartungskosten	6	4	24	5	30	6	36
Betriebskosten	6	4	24	4	24	5	30
Lizenzgebühren	6	4	24	4	24	5	30
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	6	24	5	20	5	20
Stabilität des Lieferanten	4	5	20	5	20	5	20
Referenzen	4	4	16	4	16	6	24
Operative Kriterien	12						
Betriebbarkeit	4	5	20	4	16	6	24
Notwendiges Know-How	4	3	12	4	16	6	24
Support	4	4	16	4	16	6	24
Organisatorische Kriterien	6						
In Prozess einfügbar	3	5	15	5	15	4	12
Kommunikationsprozesse	3	5	15	5	15	4	12
Juristische Kriterien	6						
SLA	2	6	12	6	12	6	12
Verträge	2	6	12	6	12	6	12
Gesetze	2	6	12	6	12	4	8
Ökologische Kriterien	4						
Entsorgung	2	4	8	4	8	6	12
Wiederverwendbarkeit	2	4	8	4	8	6	12
Sicherheits Kriterien	12						
Verfügbarkeit	4	6	24	6	24	6	24
Vertraulichkeit	4	6	24	6	24	5	20
Integrität	4	6	24	6	24	5	20
Total			454		486		516
Rang			3		2		1

Abbildung 30: Vergleich von drei VPN Lösungen

7.7.6. Entscheid

Wir haben uns für die PC-Lösung entschieden. Zwar wurde diese im Vergleich nur zweiter, jedoch ist diese für das Unternehmen um einiges praktischer, sicherer und günstiger zu betreiben. Wir werden auf einem PC Wireguard installieren. Sobald die Installation vorgenommen wurde, muss sich der Kunde um nichts mehr kümmern.

8. Kontrollieren

8.1. Testfälle

8.1.1. Übertragungsrate & Verfügbarkeit

8.1.1.1. Testfall 1

Testfall 1 – Vergleichsmatrix mit fünf Provider wurde erstellt.

Beschreibung	Erstellen einer Vergleichsmatrix um die fünf Provider Swisscom, Sunrise, UPC, iWay und GGA Maur zu vergleichen
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Website der Provider • Persönliche Erfahrung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Vergleichsmatrix mit Platzierung Tabelle mit den relevanten Parametern.
Tatsächliches Resultat	Es wurde eine Vergleichsmatrix erstellt, die Swisscom wurde erster. Zudem wurden die relevanten Parametern in einer übersichtlichen Tabelle zusammengefasst.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 41: Testfall 1

8.1.1.2. Testfall 2

Testfall 2 – Änderung der Anforderungen für Beispiel 1 Übertragungsrate beschrieben

Beschreibung	Es wurden zwei Fallbeispiele inhouse und beim Provider beschrieben und ausführlich erklärt.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wurde beschrieben wie sich die Übertragungsrate ändert wenn der Server inhouse und der Server beim Provider stehen würde.
Tatsächliches Resultat	Es wurden zwei Fallbeispiele beschrieben, die der Zielerwartung gerecht wurden.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 42: Testfall 2

8.1.1.3. Testfall 3

Testfall 3 – Beispiel 2 Verfügbarkeit maximale Ausfallzeit von 10 Stunden beschrieben

Beschreibung	Die Verfügbarkeit für maximal 10 h wurde kalkuliert und entsprechend dokumentiert.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Rechner • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wurde eine Verfügbarkeit von 99.89% berechnet.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 43: Testfall 3

8.1.1.4. Testfall 4

Testfall 4 – Beispiel 2 Verfügbarkeit maximale Ausfallzeit von 4 Stunden beschrieben

Beschreibung	Die Verfügbarkeit für maximal 10 h wurde kalkuliert und entsprechend dokumentiert.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Rechner • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wurde eine Verfügbarkeit von 99.95% berechnet.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 44: Testfall 4

8.1.2. WAN-Technologie

8.1.2.1. Testfall 5

Testfall 5 – Vergleich fünf WAN-Technologien	
Beschreibung	Die fünf WAN-technologien wurden dokumentiert und deren Vor- und Nachteile sind klar ersichtlich.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es werden die Themen xDSL, Fibre, Cable, Radiolink und Satellit beschrieben. Zudem werden zu jeder Technologie die Vor- und Nachteile aufgezeigt.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 45: Testfall 5

8.1.2.2. Testfall 6

Testfall 6 – Sicherste Verbindung im punkto Ausfallsicherheit	
Beschreibung	Es wird erwähnt welche die sicherste Verbindung im punkto Ausfallsicherheit ist.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wird erklärt, welche die sicherste Verbindung im punkto Ausfallsicherheit ist.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 46: Testfall 6

8.1.2.3. Testfall 7

Testfall 7 – Beste Leitung als Backup-Leitung

Beschreibung	Es wird erwähnt welche die beste Verbindung im punkto Backup-Leitung ist.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wird erklärt, welche die beste Verbindung für Backup-leitungen ist.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 47: Testfall 7

8.1.3. Internetservices

8.1.3.1. Testfall 8

Testfall 8 – Drei verschiedenen Services erarbeitet und dokumentiert

Beschreibung	Es werden inhouse, Shared Hosting und Root-Server Services aufgezeigt und deren Vor- und Nachteile nähergebracht.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es werden die Themen Inhouse, Root-Server und Shared-hosting Service beschrieben. Zudem werden zu jedem Service die Vor- und Nachteile aufgezeigt.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 48: Testfall 8

8.1.3.2. Testfall 9

Testfall 9 – Zwei Fälle erarbeitet

Beschreibung	Zwei Fälle werden aufgezeigt und analysiert.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Die Fälle «Einfache Webpräsenz und Mail» und «Komplexe DB-Anwendung mit PHP» wurden analysiert und dokumentiert.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 49: Testfall 9

8.1.4. Sicherheit

8.1.4.1. Testfall 10

Testfall 10 – Definierung von technischen sowie nicht technischen Massnahmen gemäss ISO 27000

Beschreibung	Die technischen und nicht technischen Massnahmen wurden gemäss ISO 27000 definiert.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es wurden verschiedene technische sowie nicht technische Massnahmen definiert.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 50: Testfall 10

8.1.4.2. Testfall 11

Testfall 11 – Sinnvolles Sicherheitskonzept	
Beschreibung	Es wurde ein sinnvolles Sicherheitskonzept erarbeitet.
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Das Sicherheitskonzept ist logisch und macht im Umfeld der Coffee GmbH Sinn.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 51: Testfall 11

8.1.5. Wartung und Überwachung

8.1.5.1. Testfall 12

Testfall 12 – Vergleich zwischen fünf Monitoring Tools erstellt	
Beschreibung	Vergleich von fünf Monitoring Tools
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es werden fünf verschiedene Monitoring Tools verglichen.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 52: Testfall 12

8.1.6. Firewall

8.1.6.1. Testfall 13

Testfall 13 – Vergleich zwischen drei Firewall Lösungen	
Beschreibung	Vergleich von drei Firewall Lösungen
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es werden die drei Firewall Lösungen HW, FW-OS und FWaaS verglichen.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 53: Testfall 13

8.1.7. VPN

8.1.7.1. Testfall 14

Testfall 14 – Vergleich zwischen drei VPN Lösungen	
Beschreibung	Vergleich von drei VPN Lösungen
Testszenario	<ul style="list-style-type: none"> • Bewerten des Resultat • Konsultieren einer zweiten Person (4-eye) für zweite Meinung. • Ziel überprüfen und entsprechend Ergebnis bewerten.
Involvierte Komponenten	<ul style="list-style-type: none"> • Google Recherchen • Persönliche Einschätzung • Meinung anderer Projektmitglieder
Erwartetes Resultat	Es werden Hardware, PC-Lösungen und VPN Service Lösungen verglichen.
Tatsächliches Resultat	Das Resultat entsprach dem erwarteten Resultat.
Ergebnis	Erfolgreich
Massnahmen	Keine Massnahmen erforderlich

Tabelle 54: Testfall 14

9. Auswerten

9.1. Auswerten der Testfälle

Testfall	Beschreibung	Ergebnis
1	Testfall 1	Erfolgreich
2	Testfall 2	Erfolgreich
3	Testfall 3	Erfolgreich
4	Testfall 4	Erfolgreich
5	Testfall 5	Erfolgreich
6	Testfall 6	Erfolgreich
7	Testfall 7	Erfolgreich
8	Testfall 8	Erfolgreich
9	Testfall 9	Erfolgreich
10	Testfall 10	Erfolgreich
11	Testfall 11	Erfolgreich
12	Testfall 12	Erfolgreich
13	Testfall 13	Erfolgreich
14	Testfall 14	Erfolgreich

9.2. Verbesserungsmöglichkeiten

Das Modul war unserer Meinung sehr komisch strukturiert. So wurde uns ein Skript gegeben, welches sehr unübersichtlich ist und wir mussten die einzelnen Aufgaben bearbeiten und gleichzeitig eine Dokumentation führen. Zu Beginn wurde uns gesagt man müsste einen Vortrag erstellen zu zwei Themen die gar nicht notiert wurden. Erst beim Nachfragen wurde die Aufgabenstellung für die Klasse klar. Zudem macht es unserer Meinung absolut keinen Sinn, zwei Vorträge vorzubereiten und dann am Ende nur einen vorzutragen. Eine absolute unnötige Aufgabe, der zweite Vortrag denn dieser hat weder einen informativen noch lehrreichen Charakter, da die Themen im Verlauf der LB1 sowieso bearbeitet wurden. Da würden wir uns von der Lehrperson einfach wünschen, dass man die Aufgabenstellung analysiert und sich selbst fragt wo der Sinn dahinter steckt einen zweiten kompletten überflüssigen Vortrag zu erstellen, anstelle dass jedes Team ein innerhalb der Klasse nur einmalig verteiltes Thema vorbereitet. Ansonsten waren die du bearbeitenden Aufgaben und Themen sehr interessant.

9.3. Rechnung

ICT System AG
 Ausstellungsstrasse 70
 8005 Zürich

Rechnungsnummer: 2020-187
 Rechnungsdatum: 07.12.2020
 Lieferdatum: 07.12.2020

Empfänger:

Herr
 Alan Brunner
 Altbergstrasse 19
 8953 Dietikon

Ansprechpartner: Luis Lüscher
 E-Mail: l.luescher@ictsystem.ch
 Telefon: +41 78 906 7005

Rechnung

Vielen Dank für Ihren Auftrag. Wir erlauben uns folgende Rechnung zu stellen:

Bezeichnung Artikel / Dienstleistung	Menge	Einzelpreis	Gesamtpreis in CHF
Dienstleistungen:			
Analyse IST-Zustand pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung Übertragungsrate, Verfügbarkeit pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung WAN-Technologie pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung Internetservices pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung Sicherheit pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung Wartung & Überwachung pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung Firewall pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Lösung VPN pro Stunde	2 Stück	CHF 120.00	CHF 240.00
Administrationskosten	1 Stück	CHF 180.00	CHF 180.00
Zwischensumme			2940.00 CHF
Skonto			58.80 CHF
MwSt 7.7%			226.38 CHF
Rechnungsbetrag			3107.58 CHF

CHE-123.456.789 MWST

Zahlbar bis: 7.12.2020
 Auf folgendes Konto:

UBS Switzerland AG
 BLZ 251
 Konto 12-4568-9
 IBAN CH31 8123 9000 0012 4568 9

Mit freundlichen Grüßen
 Luis Lüscher

9.4. Abnahmeprotokoll

Projektbeurteilung (Sicht des Kunden)		Datum: 07.12.2020					
	übertroffen	umfänglich	Teilweise	unzufrieden	Ja	Nein	Bemerkung
Wurde der Abgabetermin eingehalten?					<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Sind Sie mit dem Lieferobjekt zufrieden?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Sind alle Auftragspunkte vorhanden?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Funktioniert das Produkt in allen Punkten?		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Wurde das Kostendach eingehalten?					<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Müssen Sachen nachgeliefert werden?					<input type="checkbox"/>	<input checked="" type="checkbox"/>	
Wie beurteilen Sie die Zusammenarbeit mit dem Lieferanten?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Wie beurteilen Sie die *täglich" durchgeführten Sitzungen?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Wie beurteilen Sie die erhaltene Dokumentation/Informationen?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Bemerkungen:		<p>Die Arbeit der ICT System AG übertraf unsere Anforderungen und dies in einem Rahmen</p> <p>der die Kosten nicht übertrifft und der Zeitaufwand nicht höher war. In unseren Augen hat die</p> <p>ICT System AG sehr effizient gearbeitet und uns als Kunden immer wieder zum Projektstatus transparent informiert.</p>					

Abbildung 31: Abnahmeprotokoll

10. Schlusswort

Die LB1 war sehr gut durch unser Team bearbeitet. Wir sind sehr zufrieden mit unserem Resultat und hoffen, dass wir die gute Dokumentation durch einen guten Vortrag abrunden können und eine entsprechende gute Bewertung erhalten würden. Besten Dank an das gesamte Projektteam für den guten und grossartigen Einsatz und euer Engagement. Es gab einige Dinge, die aus organisatorischer Sicht seitens des Dozenten eher fragwürdig waren, aber am Ende konnte alles geklärt werden und wir konnten die Leistungsbeurteilung ohne Problem abschliessen.

11. Glossar

A-Z	Begriff	Erklärung
A	Authentisierung	Im Rahmen einer Authentisierung erbringt eine Person einen Beweis dafür, dass sie ist, wer sie zu sein vorgibt. Im Alltag geschieht dies z. B. durch die Vorlage des Personalausweises. In der IT wird hierfür häufig ein Passwort in Kombination mit einem Benutzernamen genutzt.
	Authentifizierung	Im Alltag geschieht dies z. B. durch die Prüfung des Personalausweises auf Urkundenfälschung und durch den Abgleich mit der Person. In der IT wird z. B. überprüft, ob die Kombination von Benutzernamen und Passwort im System existiert.
	Autorisierung	Im Alltag kann dies nach Vorlage des Personalausweises der Zugang zu einem Unternehmen sein, bei dem man als Gast angemeldet wurde. Aber: Vielleicht erhält man als Gast nur den Zugang zum Besprechungsraum, nicht aber zur Montagehalle. In der IT kann nach der Autorisierung in einem Benutzerkonto z. B. gearbeitet werden. Aber wenn dieses Konto nicht über Administratorenrechte verfügt, können z. B. keine neuen Programme installiert werden.
B	BIOS	Das BIOS ist die Firmware bei x86-PCs, die ursprünglich von IBM 1981 als IBM-PC und -kompatible eingeführt wurden. Es ist in einem nichtflüchtigen Speicher auf der Hauptplatine eines PC abgelegt und wird unmittelbar nach dessen Einschalten ausgeführt.
C	CIA	https://security.luis-luescher.com/documentations/cia/
D	DMZ	Eine Demilitarisierte Zone bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze abgeschirmt.
	DDoS	Denial of Service bezeichnet in der Informationstechnik die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes.
I	ISO	International Standard Organisation
	ISMS	Ein Information Security Management System ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
	ITU	Die Internationale Fernmeldeunion mit Sitz in Genf ist eine Sonderorganisation der Vereinten Nationen und die einzige völkerrechtlich verankerte Organisation, die sich offiziell und weltweit mit technischen Aspekten der Telekommunikation beschäftigt.
M	MSS	Managed Security Service
S	SLA	Ein Service-Level-Agreement bezeichnet einen Rahmenvertrag bzw. die Schnittstelle zwischen Auftraggeber und Dienstleister für wiederkehrende Dienstleistungen.

T	Terminologie	Eine Terminologie ist die Menge aller Termini eines Fachgebiets. Sie ist Teil der Fachsprache, die zusätzlich über andere charakteristische Merkmale, etwa Phraseologie oder Grammatik, verfügt. Terminologien können beispielsweise in einem Wörterbuch, einem Glossar oder einem Thesaurus formuliert sein
U	USV	Eine unterbrechungsfreie Stromversorgung stellt die Versorgung kritischer elektrischer Lasten bei Störungen im Stromnetz sicher, englisch Uninterruptible Power Supply. Davon zu unterscheiden ist die Netzersatzanlage, da diese bei der Umschaltung eine kurze Unterbrechung der Stromversorgung hat.
V	VPN	VPN bezeichnet ein virtuelles privates Kommunikationsnetz. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird.
W	WAN	Ein Wide Area Network ist ein Rechnernetz, das sich im Unterschied zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt.
	WSC	Die World Standards Cooperation ist die Arbeitsgemeinschaft dreier weltweit tätiger Organisationen der Normung. Die IEC, die ISO und die ITU schufen die WSC im Jahr 2001 zur Stärkung und Förderung des freiwilligen, auf Konsens gründenden Systems der Standardisierung.
Z	ZH	Abkürzung für Zürich. Eine Stadt in der Schweiz.

Tabelle 55: Glossar

12. Verzeichnisse

12.1. Quellenverzeichnis

Nummer	Link	Autor	Aufgerufen am
1	https://de.wikipedia.org/wiki/Scrum#Product_Owner	Wikipedia Foundation Inc.	09.11.2020
2	https://www.business-wissen.de/artikel/agiles-projektmanagement-so-funktioniert-scrum/	Dr. Jürgen Fleig	09.11.2020
3	https://www.plan42.com/index.php/de/it-security-management/iso-27000-reihe	Plan42 GmbH	30.11.2020
4	https://de.wikipedia.org/wiki/ISO/IEC-27000-Reihe	Wikipedia Foundation Inc.	30.11.2020
5	https://www.digitec.ch/de/s1/product/cisco-asa-5506-x-firewall-4656573?gclid=CjwKCAiAn7L-BRBbEiwAl9UtkCmMTYA8z7jgXX8jWITV_O2tke6PaEwPCAU3RCHRUhL266_VTJ5OhoCJ6EQA_vD_BwE&gclsrc=aw.ds	Digitec	06.12.2020
6	https://de.wikipedia.org/wiki/OPNsense	Wikipedia Foundation Inc.	06.12.2020
7	https://opnsense.org/	OPNsense Project	06.12.2020
8	https://documents.swisscom.com/product/filstore/lib/249eab45-d92c-490d-b1d6-f899c5e09c05/factsheet%20managed%20firewall-de.pdf	Swisscom (Schweiz) AG	06.12.2020
9	M145_Dokumentation_Luis_Luescher.docx	Luis Lüscher	06.12.2020
10	M145_Doku_Michalis_Chatzimichalis.docx	Michalis Chatzimichalis	06.12.2020
11	www.techradar.com	Future US Inc.	06.12.2020

Tabelle 56: Quellenverzeichnis

12.2. Tabellenverzeichnis

Tabelle 1: Beispiel für Tabelle.....	10
Tabelle 2: Leistungsbeurteilungsvorgaben.....	14
Tabelle 3: Leitfrage Grundlagen Dokumentation	18
Tabelle 4: Leitfrage Architektur Dokumentation	18
Tabelle 5: Leitfrage Entscheidungsmatrix Dokumentation	19
Tabelle 6: Leitfrage Vergleichskriterien Dokumentation	19
Tabelle 7: Leitfrage Realisation-Variante Dokumentation.....	19
Tabelle 8: Leitfrage Formale Vorgaben Dokumentation	19
Tabelle 9: Leitfrage Übertragungsrate & Verfügbarkeit Dokumentation	20
Tabelle 10: Leitfrage WAN-Technologie Dokumentation.....	21
Tabelle 11: Leitfrage Internetservices Dokumentation	22
Tabelle 12: Leitfrage Sicherheit Dokumentation	22
Tabelle 13: Leitfrage Wartung & Überwachung Dokumentation	23
Tabelle 14: Leitfrage Firewall Dokumentation	24
Tabelle 15: Leitfrage VPN Dokumentation.....	24
Tabelle 16: Leitfrage Art des Vortrages Präsentation	25
Tabelle 17: Leitfrage Einsatz von Medien Präsentation.....	25
Tabelle 18: Leitfrage Inhaltliche Dichte Präsentation	25
Tabelle 19: Leitfrag Fachliche Tiefe Präsentation	26
Tabelle 20: Leitfrage Ablauf Präsentation.....	26
Tabelle 21: Leitfrage Zeitplanung Präsentation.....	27
Tabelle 22: Leitfrage Inhaltliche Struktur Präsentation	27
Tabelle 23: Projektantrag	28
Tabelle 24: Beschreibung Namenskonvention	31
Tabelle 25: Beschreibung verschiedener Gerätetypen.....	31
Tabelle 26: Termine	32
Tabelle 27: Alle Arbeitstage der LB1.....	32
Tabelle 28: Journal Tag 1	37
Tabelle 29: Journal Tag 2	38
Tabelle 30: Journal Tag 3	38
Tabelle 31: Arbeitsjournal Tag 4.....	39
Tabelle 32: SWOT-Analyse	54
Tabelle 33: Risikoanalysetabelle.....	56
Tabelle 34: Risikomatrix.....	56
Tabelle 35: Themenübersicht	61
Tabelle 36: Beispiel Testkonzept	63
Tabelle 37: Vergleich von fünf Provider	68
Tabelle 38: Vergleichstabelle.....	75
Tabelle 39: Bewertungsmatrix für Überwachungstools	86
Tabelle 40: Beschreibung Change Management.....	87
Tabelle 41: Testfall 1	101
Tabelle 42: Testfall 2	101
Tabelle 43: Testfall 3	102
Tabelle 44: Testfall 4	102
Tabelle 45: Testfall 5	103
Tabelle 46: Testfall 6	103
Tabelle 47: Testfall 7	104
Tabelle 48: Testfall 8	104

Tabelle 49: Testfall 9	105
Tabelle 50: Testfall 10	105
Tabelle 51: Testfall 11	106
Tabelle 52: Testfall 12	106
Tabelle 53: Testfall 13	107
Tabelle 54: Testfall 14	107
Tabelle 55: Glossar	113
Tabelle 56: Quellenverzeichnis	114

12.3. Abbildungsverzeichnis

Abbildung 1: Abbildung CC BY-NC-SA.....	3
Abbildung 2: Beispiel für Abbildung	10
Abbildung 3: ICT System GmbH	15
Abbildung 4: Bearbeitung eines Ticket im Jira	16
Abbildung 5: Arbeitsplatz am Platz 11 und 12 im Schulzimmer	29
Abbildung 6: Aufbau Namenskonvention.....	31
Abbildung 7: GANTT-Plan LB1	33
Abbildung 8: Jira Scrum Board	35
Abbildung 9: Beispiel eines Jira Task.....	36
Abbildung 10: IPERKA.....	40
Abbildung 11: Scrum-Prozess von business-wissen.de	44
Abbildung 12: Kanban-Board von business-wissen.de.....	45
Abbildung 13: Projektorganigramm	46
Abbildung 14: Offerte für die Coffee GmbH	48
Abbildung 15: Auftragsbestätigung für die Coffee GmbH	49
Abbildung 16: Bewertungsmatrix für fünf Provider	67
Abbildung 17: Bewertungsmatrix WAN-Technologien	72
Abbildung 18: Matrix für Fallbeispiel 1.....	76
Abbildung 19: Matrix für Fallbeispiel 2.....	77
Abbildung 20: Offizielles Logo der ISO	78
Abbildung 21: Beispiel einer Klassifizierung in Microsoft Outlook.....	80
Abbildung 22: Funktionsumfang von Zertifikaten	82
Abbildung 23: Verhältnis Kosten und Nutzen nach der Verfügbarkeit	83
Abbildung 24: Matrix für Firewall.....	93
Abbildung 25: Einfache Erklärung von IPsec von Wikipedia	95
Abbildung 26: Site to Site VPN.....	98
Abbildung 27: End to End VPN	98
Abbildung 28: End to Site VPN	98
Abbildung 29: Offizielles Logo von WireGuard	100
Abbildung 30: Vergleich von drei VPN Lösungen	100
Abbildung 31: Abnahmeprotokoll.....	110