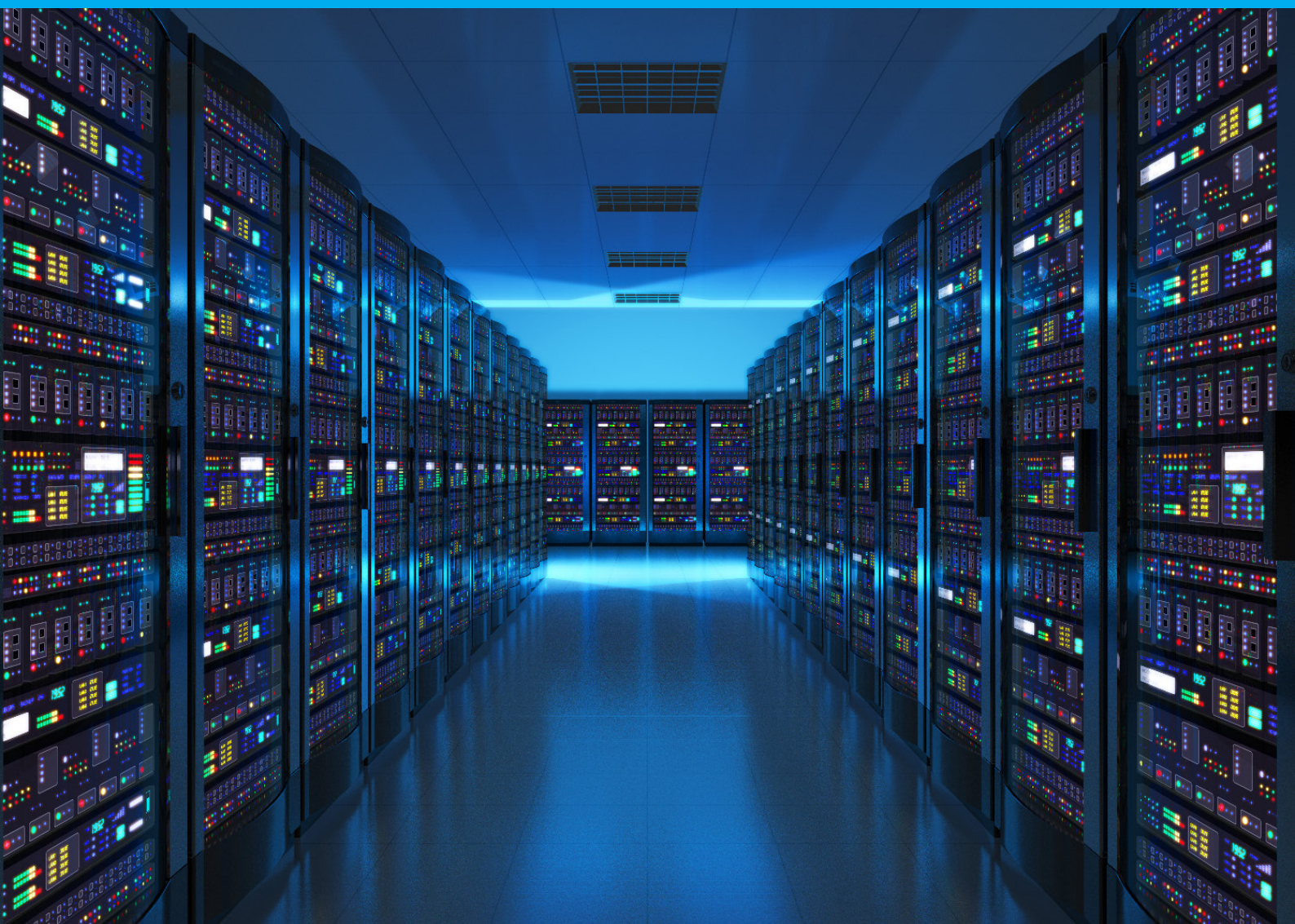


Internetanbindung für ein Unternehmen realisieren

TBZ, Johann Widmer, et. al.

Modul 146



Inhaltsverzeichnis

1.	Internetanschluss nach Kundenvorgaben	7
1.1	Anforderungen an eine Internetanbindung	7
1.2	Sicherheits- und Überwachungsmaßnahmen beim Betrieb eines Internetanschlusses	22
2.	Kundenvorgaben nach Prioritäten, Pflichtenheft	26
2.1	LB1	26
2.2	Zugangsmöglichkeiten zum Internet sowie deren Anbieter (Provider)	26
2.3	Methoden um Kundenvorgaben zu klassieren	27
2.4	Aufbau und Inhalt eines Pflichtenhefts	32
2.5	Ablauf eines Evaluationsprozesses	32
3.	Resultate der Evaluation bewerten und darstellen.	35
3.1	Die wichtigsten Kriterien für die Bewertung eines Angebotes.	35
3.2	Darstellungsarten für die Beurteilung von Offerten.	37
4.	Netzwerkplan und Netzwerkschema für die Internetanbindung erstellen oder anpassen.	39
4.1	Regeln für das Erstellen eines Namens- und Nummerierungskonzepts.	39
4.2	Funktionsweise von Firewall, DMZ, Proxy und DNS.	41
4.3	Gängige Darstellungsarten und Symbole für Netzwerkplan und Netzwerkschemata.	44
5.	Hardware- und Softwarekomponenten bestimmen und einen Beschaffungsantrag erstellen.	47
5.1	LB2	47
5.2	Aufbau und Inhalt eines Beschaffungsantrags aus der durchgeführten Evaluation.	47
5.3	Simulations-Plattformen	49
6.	Inbetriebnahme der Internetanbindung realisieren und eine Abnahme durchführen.	50
6.1	Vorgehen für die Planung und Inbetriebnahme des Internetzugangs.	50
6.2	Vorgehen für die Übergabe des Systems in den operativen Betrieb.	50
6.3	Aufbau und Inhalt eines Abnahmeprotokoll	50
	Lösungen	52
	LB1	61
	LB2	61

Anhänge

Nachrichtentechnik

Dokumentstruktur

Modulplanung

Diese Ablaufplanung soll ein Hinweis zur Durchführung des Moduls 146 darstellen. Es wird auf 9 Blöcke geplant. Der 10. Block ist Reserve oder fällt in gewissen Quartalen aus.

1. Lektionen 1 - 4

Das Kapitel 1 soll bearbeitet werden. Es wird erwartet, dass alle Aufgaben gelöst oder als Hausaufgabe erledigt werden.

2. Lektionen 5 - 8

Abgabe LB1. Das Kapitel 2 soll begleitend zu LB1 bearbeitet werden. Es wird erwartet, dass alle Aufgaben gelöst oder als Hausaufgabe erledigt werden.

3. Lektionen 9 - 12

LB 1 weiter bearbeiten. Das Kapitel 3 soll begleitend zu LB1 bearbeitet werden. Die Inhalte von Kapitel 3 helfen bei der Bearbeitung der LB1.

4. Lektionen 13 - 16

LB 1 weiter bearbeiten. Das Kapitel 4 soll begleitend zu LB1 bearbeitet werden. Die Inhalte von Kapitel 4 helfen bei der Bearbeitung der LB1.

5. Lektionen 17 - 20

LB1 präsentieren (40%, Gruppenarbeit, Themen aus Kapitel 1-3, 10 Min Präsentation und Kurz-Dokumentation) soll hier beendet sein. Anschliessend Abgabe LB2 und Arbeit an Kapitel 5.

LB2 (40%, Gruppenarbeit, Themen aus Kapitel 1 - 6 / 20% Netzwerkplanung, 50% Internetanbindung realisieren, 20% Testszenarien, 10% Abnahme).

6. Lektionen 21 - 24

LB2 (40%, Gruppenarbeit, Themen aus Kapitel 1 - 6 / 20% Netzwerkplanung, 50% Internetanbindung realisieren, 20% Testszenarien, 10% Abnahme).

7. Lektionen 25 - 28

LB2 (40%, Gruppenarbeit, Themen aus Kapitel 1 - 6 / 20% Netzwerkplanung, 50% Internetanbindung realisieren, 20% Testszenarien, 10% Abnahme).

8. Lektionen 29 - 32

LB2 (40%, Gruppenarbeit, Themen aus Kapitel 1 - 6 / 20% Netzwerkplanung, 50% Internetanbindung realisieren, 20% Testszenarien, 10% Abnahme). Abgabe LB2

9. Lektionen 33 - 36

Besprechen LB2

LB3 (20%, schriftliche Einzelarbeit mit Grundlagen aus Kapitel 1 - 6. / 40% Kundenvorgaben, 40% Netzplanung, 20% Testszenarien, Abnahme).

10. Lektionen 37 - 40

Reserve

Aufgabenverzeichnis

Aufgabe 1	9
Aufgabe 2:	12
Aufgabe 3:	13
Aufgabe 4 (nur für Cracks):	14
Aufgabe 5:	19
Aufgabe 6:	20
Aufgabe 7:	21
Aufgabe 8 (nur für Cracks):	21
Aufgabe 9:	23
Aufgabe 10 (für Cracks):	23
Aufgabe 11:	30
Aufgabe 12 (für Cracks):	31
Aufgabe 13	34
Aufgabe 14:	37

Lösungsverzeichnis

Lösungen 52

1. Aufgabe 1	52
2. Aufgabe 2	52
3. Aufgabe 3	52
4. Aufgabe 4	52
5. Aufgabe 5:	53
6. Aufgabe 6:	53
7. Aufgabe 7:	53
8. Aufgabe 8 (nur für Cracks):	54
9. Aufgabe 9:	54
10. Aufgabe 10 (für Cracks):	54
11. Aufgabe 11:	54
12. Aufgabe 12 (für Cracks):	54
13. Aufgabe 13	54
14. Aufgabe 14 (für Cracks)	54

Tabellenverzeichnis

Tabelle 1: Tätigkeiten und Übertragungsraten	9
Tabelle 2: Monitoring eines Internetzuganges	11
Tabelle 3: Vergleich der Provider	27
Tabelle 4: Nutzwertanalyse	34
Tabelle 5: Bewertungskriterien	36
Tabelle 6: Beschaffungswesen des Bundes	48

Bilderverzeichnis

Bild 1: Zusammenhang Kosten / Nutzen der Verfügbarkeit	15
Bild 2: FCAPS	23
Bild 3: Packet Firewall	42
Bild 4: Verbindungsgateway	42
Bild 5: Application Level Gateway	42
Bild 6: Stateful Inspection Firewall	43
Bild 7: Netzwerkplan	44
Bild 8: Netzwerkstruktur	45
Bild 9: Einfacher Zonenplan	45
Bild 10: komplexere Zonenpläne	46
Bild 11: Beschaffungsantrag des Bundes	47
Bild 13: Abnahmeprotokoll	51
Bild 14: Zusammenhang Übertragungsrate - Distanz	57

1. Internetanschluss nach Kundenvorgaben

Sicherheit, Performance, Verfügbarkeit und Wartung bestimmen.

Jeder Kunde hat unterschiedliche Anforderungen an die Internetanbindung. Je nach Geschäft sind die Anforderungen an die Sicherheit, die Leistungsfähigkeit, die Verfügbarkeit und die Wartbarkeit unterschiedlich gewertet.

Die Anforderung an die Internetanbindung wird durch die Anforderungen des Geschäftes bestimmt.

Alle Wünsche bezüglich der Internetanbindung, die für das Geschäft nicht benötigt werden, sollen nicht abgedeckt werden. Es ist vermutlich wünschenswert einen Anschluss mit möglichst grosser Übertragungsrate zu haben (fälschlicherweise „Bandbreite“ genannt, siehe dazu Anhang «Nachrichtentechnik» - nur für Cracks!). Falls aber lediglich einige wenige Internetabfragen pro Tag zu machen sind, um das Tagesgeschäft zu unterstützen, dann ist der grosse Anschluss sicher zu teuer und der Nutzen zu klein. Man sagt dann, dass die Wirtschaftlichkeit nicht optimal sei. (Wirtschaftlichkeit ist das Verhältnis der Kosten zum Nutzen einer Sache)

Beispiel:

Ein Bäcker in einem Dorf hat eine einfache Website bei einem Provider gehostet und ruft seine Mails mit Kundenbestellungen stündlich ab. Er bestellt auch Waren via Mail und benutzt Onlinekataloge der Lieferanten. Für eine solche Anwendung des Internet genügt sicher ein xDSL-Anschluss (zum Beispiel Swisscom-Anschluss mit 50/5 Mbit/s) oder Cable-Anschlüsse des lokalen Kabelnetzbetreibers mit einer ähnlichen Übertragungsrate. Die Verfügbarkeit dieser Anschlüsse ist genügend gut, da auch ein Ausfall des Internet über mehrere Stunden keinen geschäftskritischen Vorfall darstellt. Auch die Anforderung an eine minimale Sicherheit ist mit den handelsüblich gelieferten Geräten (Modem/Router) sicher genügend und eine Wartung der Anlagen ist nicht regelmässig notwendig.

1.1 Anforderungen an eine Internetanbindung

Übertragungsrate (Bandbreite), Verfügbarkeit, Sicherheit und Wartung

Wie leitet man nun die Anforderungen an die Internetanbindung für ein Unternehmen her? Dazu muss man zuerst das Geschäft kennen. Für jede Art Geschäft kann ein Anforderungskatalog erstellt werden. Die folgende Zusammenstellung in den Abschnitten 1.1.1 bis 1.1.4 soll Anhaltspunkte liefern für solche Anforderungskataloge.

Wie viele Mitarbeitende hat das Unternehmen pro Standort und was ist deren Haupttätigkeit im Unternehmen?

Haupttätigkeit (I): Texte, Tabellen, Mail und einfache Internetrecherchen

- A) 1 - 10 Mitarbeitende pro Standort
- B) 10 - 50 Mitarbeitende pro Standort
- C) 50 - 100 Mitarbeitende pro Standort
- D) 100 - 500 Mitarbeitende pro Standort
- E) Mehr als 500 Mitarbeitende pro Standort

Haupttätigkeit (II): Texte, Tabellen, Mail und komplexere Internetrecherchen, Multimedia

- A) 1 - 10 Mitarbeitende pro Standort
- B) 10 - 50 Mitarbeitende pro Standort
- C) 50 - 100 Mitarbeitende pro Standort
- D) 100 - 500 Mitarbeitende pro Standort
- E) Mehr als 500 Mitarbeitende pro Standort

Haupttätigkeit (III): Texte, Tabellen, PPT, Mail und komplexere Internetrecherchen, Multimedia, Informatikentwicklungen

- A) 1 - 10 Mitarbeitende pro Standort
- B) 10 - 50 Mitarbeitende pro Standort
- C) 50 - 100 Mitarbeitende pro Standort
- D) 100 - 500 Mitarbeitende pro Standort
- E) Mehr als 500 Mitarbeitende pro Standort

Wie viele Standorte hat das Unternehmen?

Haupttätigkeit (IV): Texte, Tabellen, PPT, Mail und komplexere Internetrecherchen, Multimedia, Informatikentwicklungen im Finanzdienstleistungsumfeld.

- A) 1 - 10 Mitarbeitende pro Standort
- B) 10 - 50 Mitarbeitende pro Standort
- C) 50 - 100 Mitarbeitende pro Standort
- D) 100 - 500 Mitarbeitende pro Standort
- E) Mehr als 500 Mitarbeitende pro Standort

Standorte: Wie viele Standorte hat das Unternehmen?

Fragenkataloge dieser Art erlauben es, dass man eine Aussage zur Übertragungsrate (Bandbreite) und zur Verfügbarkeit machen kann.

Die Fragenkataloge sind je nach Firma unterschiedlich. Es kann vorkommen, dass nicht nur die Anzahl der Mitarbeitenden eine Rolle spielt, sondern auch die Tätigkeit, die diese Mitarbeitenden ausführen. So benötigt ein Mitarbeiter einer Werbeabteilung mit viel Multimediainhalten sicher mehr Übertragungsrate als ein Mitarbeiter im Sekretariat.

Auch die Branche der Unternehmung spielt eine grosse Rolle. Die Finanzdienstleister sind auf eine viel grössere Verfügbarkeit angewiesen als ein einfaches Gewerbe. Für ein einfaches Gewerbe, wie zum Beispiel eine Bäckerei, ist die Internetanbindung keine zentrale Anforderung für das Geschäft. Für einen Softwareentwickler oder ein Logistikbetrieb hingegen ist diese Anbindung von grösster Bedeutung, können solche Betriebe sicher nicht ohne Internet existieren und arbeiten.

Aufgabe 1

Ordnen Sie die Übertragungsraten und Verfügbarkeiten dem Mengengerüst zu. Arbeiten Sie zu zweit. Schreiben Sie Ihre Resultate auf ein Flipchartblatt. Die Resultate werden in der Klasse diskutiert. Verwenden Sie die Übertragungsraten 50/5 Mb/s (Kupfer), 100/10 Mb/s (Kupfer), 100/100 Mb/s (Fibre), 1G/1G (Fibre), 10G/10G (Fibre). Die Verfügbarkeit kann niedrig, mittel, hoch und sehr hoch sein. Versuchen Sie auch die Technologie zu bestimmen :

Übertragungsrate /Technologie	Verfügbarkeit	Mengen	Tätigkeit
50/5 Mb/s / DSL	niedrig	1 - 10	(I)
		50 - 100	(I)
		10 - 50	(II)
		> 500	(II)
		10 - 50	(III)
		50 - 100	(III)
		100 - 500	(IV)
		> 500	(IV)

Tabelle 1: Tätigkeiten und Übertragungsraten

Besprechen Sie ihre Lösungen in der Klasse. Es gibt nicht nur eine richtige Lösung – versuchen Sie Begründungen für Ihre Lösung zu finden.

Persönliche Notizen:

1.1.2 Anforderung an die Verfügbarkeit.

Die Verfügbarkeit ist in der Informatik ein wichtiges Mass für die Betriebsbereitschaft der Anlagen. Das Geschäft muss sich darauf verlassen können, dass die Betriebsbereitschaft der Systeme und Anlagen **während der Arbeitszeiten** möglichst gross ist. Die Verfügbarkeit ist ein Mass für die Zeit, in welcher ein Dienst vollständig zur Verfügung steht.

Es befassen sich verschiedene Normen mit dieser Verfügbarkeit.

ISO 25000 (software product quality):

Availability

The degree to which data has attributes that enable it to be retrieved by authorized users and/or applications in a specific context of use.

ISO 27000 (Information security):

availability

property of being accessible and usable upon demand by an authorized entity

ISO 20000 (IT Service Management, ITSM):

Service Continuity and Availability

The two processes, availability and service continuity management, must ensure that the agreed objectives of availability and continuity for the customer can be met in every case.

Vergleiche dazu ISO Normenwerke (kostenpflichtig)

Je nach Norm werden unterschiedliche Aspekte der Verfügbarkeit stärker gewichtet. So geht es in der Norm ISO 25000 eindeutig um die Verfügbarkeit von Software. Software muss so gebaut werden, dass der Unterhalt und die Wartung so ausgeführt werden können, dass ungeplante Ausfälle minimiert werden können.

Bei der Informationssicherheit geht es vor allem um die Vermeidung von Ausfällen im Zusammenhang mit Sicherheitsrelevanten Themen, wie zum Beispiel Hackerattacken oder Virenbefall.

Beim IT Service Management, dem umfassendsten Ansatz bezüglich Verfügbarkeit, werden die ganzen IT Systeme einbezogen und es geht vor allem um die Verfügbarkeit im Sinne der Fortführungsfähigkeit des Geschäftes.

Es gilt die folgenden Begriffe zu verstehen:

Mean Time Between Failure (MTBF): Das ist die durchschnittliche Zeit zwischen zwei Ausfällen.

Mean Time To Repair (MTTR): Das ist die durchschnittliche Reparaturzeit, bis ein Ausfall behoben ist und die Anlage wieder zur Verfügung steht.

Die Verfügbarkeit errechnet sich theoretisch folgendermassen:

$$\text{Verfügbarkeit} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

Um diese Werte zu berechnen muss man den Internetzugang überwachen (monitoren). Man erfasst alle Up-Time (Zeit in welcher der Internetzugang funktionierte) und die Dauer der Ausfälle (Down-Time). Der Ausfall beinhaltet die ganze Zeit in der das System nicht verfügbar ist, also auch die Reparaturzeit. Up-Time* ist die Betriebszeit während der Arbeitszeit. Die Betriebszeiten werden in Stunden angegeben. Die Ausfälle in Minuten.

Beispiel:

Das Monitoring eines Internetzuganges liefert die folgenden Werte:

Monat	Datum / Ausfall 1	Up-Time	Up-Time*	Datum/ Ausfall 2	Up-Time	Up-Time*	Datum / Ausfall 3	Up-Time	Up-Time*	Total Ausfall	Total Up	Total Up*
Januar	3. / 10	216	72	12. / 15	648	216				25	864	288
Februar	8. / 5	120	40	13. / 20	192	64	21. / 5	192	64	30	504	168
März	1. / 5	168	56	8. / 10	96	32	12. / 15	648	216	25	912	304
April	8. / 10	816	272							10	816	272
Mai	12. / 5	144	48	18. / 20	96	32	22. / 30	240	80	55	480	160
										145	3576	1192

Tabelle 2: Monitoring eines Internetzuganges

Im Beobachtungszeitraum vom 3. Januar bis am 31. Mai betrug die gesamte Zeit zwischen zwei Ausfällen total 3360 Stunden. Die Anzahl der Intervalle der Ausfälle war 11.

Die mittlere Betriebszeit (MTBF) war somit $3360 / 11 = 325.1$ Stunden

Im Beobachtungszeitraum vom 3. Januar bis am 31. Mai betrug die gesamte Ausfallzeit 145 Minuten. Die Anzahl der Ausfälle war 12.

Die mittlere Reparaturzeit (MTTR) war somit $145 / 12 = 12.08$ Minuten oder 0.2 Stunden.

Die Verfügbarkeit errechnet sich nun folgendermassen:

Verfügbarkeit = $MTBF / (MTBF + MTTR) = 325.1 \text{ h} / (325.1 \text{ h} + 0.2 \text{ h}) = 0.999385$, in Prozenten 99.939%.

Eine solche Verfügbarkeit ist sehr gut. Da aber der Beobachtungszeitraum nur fünf Monate beträgt, ist dieser Wert mit Vorsicht zu geniessen. Ein langjähriger Wert, welcher auf guten Messreihen beruht ist sicher anzustreben.

Ein weiteres Problem dieser Berechnung ist, dass die Ausfälle teilweise in der Arbeitszeit stattfinden können. Dies wiegt sicher schwerer als ein Ausfall in der arbeitsfreien Zeit.

Führen wir also unser Beispiel weiter unter der Annahme, dass die Ausfälle alle in der Arbeitszeit stattgefunden haben:

Somit errechnet sich die MTBF mit den total 1192 Stunden Up-Time*:

$MTBF = 1192 / 11 = 108.36$ Stunden

MTTR bleibt 0.2 Stunden

Die Verfügbarkeit während der Arbeitszeit beträgt somit $108.36 \text{ h} / (108.36 \text{ h} + 0.2 \text{ h}) = 0.99816$ oder 99.816%

Oft wird diese Rechnung vereinfacht, indem man die gesamte Ausfallzeit (in unserem Beispiel 145 Minuten = 2.42 Stunden in Beziehung stellt zur gesamten Zeit einer vereinbarten Periode (meistens ein Jahr oder ein Monat). In unserem Beispiel wären das 3576 Stunden für die Zeit 3. Januar bis 31. Mai.

Die Verfügbarkeit wird dann vereinfacht berechnet mit $(3576 - 2.42) / 3576 * 100 = 99.9323 \%$ (Im Vergleich zur korrekten Berechnung mit MTBF: 99.939 % kein grosser Unterschied)

Nur für Cracks:

Erfahrene IT Fachleute besitzen Erfahrungswerte für die MTBF und MTTR oder bekommen diese Werte von ihren Internet-Providern zur Verfügung gestellt. Damit lassen sich die Verfügbarkeiten auf für die Zukunft bestimmen.

Eine weitere Anmerkung bezieht sich auf die Art der untersuchten Systeme. In unserem Beispiel haben wir uns auf den Internetzugang beschränkt. Ein Service auf einem Server ist jedoch anders zu beurteilen: Dort

muss man genau wissen, ob es sich um einen dedizierten physischen Server handelt oder um virtuelle Server! Bei virtuellen Server muss man die Verfügbarkeiten der physischen Server und der virtuellen Maschinen verknüpfen. Man muss hier die Ausfallrisiken (= 100% - Verfügbarkeit) addieren: Hat der physische Server eine Verfügbarkeit von 99.98% und der virtuelle Server eine Verfügbarkeit von 99.99 %, dann sind die Ausfallrisiken von 100 % - 99.98 % = 0.02 % respektive 100 % - 99.99 % = 0.01 % zu addieren, was 0.03 ergibt. Die Gesamtverfügbarkeit eines solchen Systems ist somit 100 % - 0.03 % = 99.97 %. Kommt noch die Verfügbarkeit der Applikation dazu, dann verkettet sich dieses Ausfallrisiko zusätzlich und die Gesamtverfügbarkeit kann dann eventuell nur noch bei 99.95 % liegen!

Redundanzen erhöhen die Verfügbarkeit, da es unwahrscheinlicher ist, dass beide Systeme gleichzeitig ausfallen. Wenn beide Systeme eine Verfügbarkeit haben von 99.98 %, also ein Ausfallrisiko von je 0.02 %, dann kann man die beiden Ausfallrisiken multiplizieren: 0.02 % x 0.02 % = 0.0004 %. Die Verfügbarkeit wäre demnach 99.9996 %.

Aufgabe 2:

Ein Internet Service Provider schreibt in seinem Vertrag zur Verfügbarkeit folgendes:

Network Availability

XXX agrees that its voice, data and dedicated Internet services will be available at least 99.99% for T-1, Fiber, EoC (Ethernet Over Copper) and Wireless (when WiMax or Point-to-Point) services and 99% for DSL/DS-0 based services of the time in a calendar month ("Network Availability"). Network Availability is defined as the number of minutes within a given calendar month that XXX's monitoring system indicates that voice, data and Internet service is available for Customer's use. Network downtime exists when a customer's circuit is unable to transmit and receive voice, data or Internet service and XXX records such a failure in the XXX trouble ticket system. Network downtime is measured from the time the trouble ticket is opened to the time Customer's service is able to transmit and receive voice and Internet data.

a) Welche Berechnungsmethode für die Verfügbarkeit wendet der Service Provider an?

.....

.....

b) Warum besteht ein Unterschied in der Verfügbarkeit zwischen Fiber (99.99 %) und DSL (99 %)?

.....

.....

.....

c) Welche Zeitspanne ist für die Berechnung der Verfügbarkeit definiert?

.....

Aufgabe 3:

Suchen Sie fünf Verfügbarkeitsrechner im Internet. Notieren Sie sich die URL.

a) Berechnen Sie bei jedem Rechner die Verfügbarkeit pro Tag, Woche, Monat und Jahr für eine Ausfallzeit von 5 Stunden und notieren Sie die Resultate.

.....

.....

.....

.....

.....

.....

b) Können diese Rechner die Verfügbarkeit auf die Arbeitszeit beschränken?

.....

.....

c) Was sind die Schwächen dieser Rechner?

.....

.....

d) Berechnen diese Rechner die exakte Verfügbarkeit?

.....

.....

Aufgabe 4 (nur für Cracks):

Eine Firma hat einen Internetzugang zu zwei Providern. Der Provider A definiert seine Verfügbarkeit mit 99.95 %. Der Provider B verspricht eine Verfügbarkeit von 99.8 %.

Die beiden Provider werden über zwei Router redundant an zwei Firewall angeschlossen. Das Corenetz ist ebenfalls redundant. Das Spanning Tree Protokoll ermöglicht eine volle Redundanz der Anlage.

Wie gross muss die Verfügbarkeit jedes Routers und jeder Firewall sein, damit nach dem Perimeter eine Gesamtverfügbarkeit von 99.5 % erreicht wird? Machen Sie eine Skizze der Anlage! Nehmen Sie an, dass die zwei Firewall und die zwei Router die gleiche Verfügbarkeit haben. Die Switches brauchen Sie in der Überlegung nicht zu berücksichtigen.

Lösung:

1.1.3 Die Sicherheit

Auch bei der Sicherheit wird die Frage nach der Verfügbarkeit gestellt, wenn auch aus spezifischen Gründen. Es geht hier vor allem um die Sicherheit nach ISO 27000, Informationssicherheit.

Die Bereitschaft der Internetanbindung kann durch Denial of Service Attacks oder anderen Attacks (zum Beispiel Viren) auf die Informationssicherheit beeinträchtigt werden. Bevor man aber hochredundante Systeme anschafft, sollte man zuerst ermitteln, welches Sicherheitsniveau gewünscht wird. Am besten macht man das mit Hilfe einer Checkliste:

Internetausfall weniger als 1 Minute: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 5 Minuten: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 15 Minuten: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 30 Minuten: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 1 Stunde: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 4 Stunden: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 8 Stunden: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall weniger als 1 Tag: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

Internetausfall mehr als 1 Tag: ☐ unbedeutend ☐ tolerierbar ☐ nicht tolerierbar ☐ katastrophal

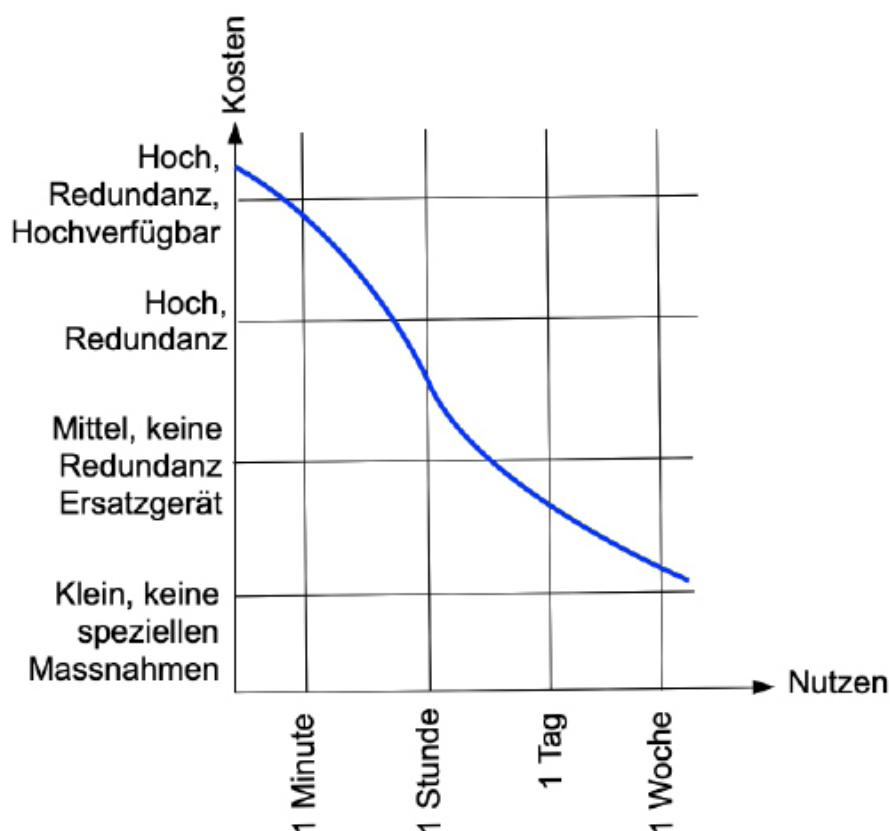


Bild 1: Zusammenhang Kosten / Nutzen der Verfügbarkeit

Bild 1 zeigt, dass eine Ausfallzeit von weniger als eine Minute nur durch hochverfügbare Systeme mit redundanter Internetanbindung und Loadbalancing erreicht werden kann. Die Kosten sind sehr hoch.

Ausfallzeiten von einer bis vier Stunden sind normal in der Industrie und können mit guten Geräten mit redundanten Netzteilen und einer Lagerhaltung von Ersatzgeräten erreicht werden. Die Kosten sind hoch bis mittel.

Ausfallzeiten von einem Tag kann man mit einfachen Mitteln erreichen. Die Kosten sind mittel bis klein.

Mehr als ein Tag Ausfall ist kaum zu erwarten und bedarf keiner Massnahme.

Man unterschätze nicht, dass heute nicht nur das Internet betroffen ist, sondern auch die Telefonie, die nun auch über das Internet läuft!

Weitere Schutzziele nach ISO/IEC 27000

Im Zusammenhang mit der Sicherheit von IT-Systemen verlangt die ISO 27000 noch weitere Schutzziele. Weil die Internetzugänge zu den IT-Systemen gehören, gelten somit die folgenden Schutzziele auch für Internetzugänge:

Vertraulichkeit:

Um die Vertraulichkeit der Schutzobjekte einer Firma zu gewährleisten sind diese zu klassieren. Eine übliche Klassierung ist «public», «internal», «confidential» und «secret». Public sind zum Beispiel Dokumente, die im Web verfügbar sind. Internal werden Dokumente klassifiziert, die nur für internen Gebrauch bestimmt sind und auf dem Web durch eine Authentisierung geschützt werden, zum Beispiel Kundenaccounts. Confidential werden Dokumente eingestuft, die nicht für Kunden oder die Allgemeinheit bestimmt sind, wie zum Beispiel Offerten. Als Geheim werden Dokumente eingestuft, die Geschäftskritische Daten beinhalten, wie zum Beispiel Rezepte oder Bilanzen der Firma.

Sind Informationen zu schützen, die mehr als public eingestuft sind, so gelangen sicher Firewall-systeme und umfangreiche weitere Sicherheitsmassnahmen zum Einsatz.

Integrität:

Um die Integrität der Daten zu gewährleisten, müssen die Internetanbindungen ebenfalls durch geeignete Massnahmen geschützt werden. Datenbanken zum Beispiel gehören nicht in Netzbereiche, auf die von aussen zugegriffen werden kann.

Im Zusammenhang mit den Internetanbindungen von Firmen muss man sich somit die folgenden Fragen stellen:

- Sind Datenbanken im Einsatz? Wenn ja, welche sind es und wie viele Mitarbeitende arbeiten damit?
- Arbeiten auch externe Personen mit den Datensätzen?
- Welche Zugriffe haben diese Externen (VPN)?

Wenn bei der Beantwortung der Fragen herauskommt, dass externe Mitarbeitende auf interne Daten zugreifen sollen, insbesondere auf Daten, die als internal, confidential oder gar secret eingestuft sind, dann muss der Internetzugang mit einem VPN abgesichert sein.

Authentizität und Authentisierung:

Beim Thema Authentisierung dürfte heute klar sein, dass die Router und andere Netzgeräte mit starken Passwörtern gesichert sein müssen. Es muss klar sein, welche Personen auf solche Systeme Zugriff haben. Man muss dies überprüfen und zudem folgende Fragen klären:

- Welche Verfahren sollen zum Einsatz kommen – User/Passwort oder drei stufiges Konzept?
- Sind Biometrische Verfahren erwünscht?

Wenn durch Antworten auf solche Fragen Anforderungen nach höherer Authentisierung deklariert werden, so muss man entsprechende Massnahmen ergreifen.

Zurechenbarkeit:

Mails, Briefe und andere Daten sollen eindeutig einem Verfasser (owner) zugeordnet werden können. Im Zusammenhang mit dem Internetzugang stellt sich hier vor allem die Frage, ob Mails signiert werden müssen. Aber auch die Zurechenbarkeit von Konfigurationsfiles der Firewalls, Switches, Accesspoints und Router muss gewährleistet sein.

Wenn die Verfasser von Konfigurationsfiles unklar sind, stellt das aus heutiger Sicht ein Sicherheitsrisiko dar!

Nicht-Abstreitbarkeit:

Dies ist eine Sicherheitsanforderung an Web-Shops. Aus Sicht der Internetanbindung kann man sich höchstens der Vollständigkeit halber fragen ob ein Web-Shop im Einsatz ist oder ob Bestellungen via Mail oder via das WEB erfolgen. Das soll man dann dokumentieren.

Verlässlichkeit:

Die Verlässlichkeit hat sehr viel mit der Wartung der Internetzugänge zu tun. Daher gelangen die folgenden Fragen zum Einsatz:

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

Kann man alle diese Fragen positiv beantworten, dann ist das System als verlässlich einzustufen. In der Praxis werden speziell ausgebildete Prüfer (Auditoren) eingesetzt um die Internetzugänge auf diese sicherheitsrelevanten Schutzziele regelmässig zu überprüfen.

Zugriffskontrolle:

Die Zugriffskontrolle schliesst im Fall der Internetanbindung neben dem physischen Zugriff auch die Bedingungen an die erlaubten Internetzugriffe mit ein. In jedem Betrieb sollte im Sicherheitsreglement (Securitypolicy) festgehalten werden, welche Dienste (Mail, Web, Facebook, Twitter, ...) für die Mitarbeitenden unter welchen Bedingungen und in welchem Umfang genutzt werden dürfen. Diese Regeln müssen überwacht werden.

Der Zugriff auf die Infrastruktur und Daten muss geregelt sein.

Achtung: Um bei diesem Thema wirklich zu verstehen, wo nun die Daten und Systeme stehen, deren Zugriff man schützen soll, muss für jeden Dienst der Ort und die Zugriffsart gut dokumentiert sein.

Es kann Sinn machen, mit Hilfe des folgenden Fragenkataloges eine grössere Klarheit über die Art der Zugriffe zu bekommen:

Welche Dienste hat die Firma intern?

- ☐ Mailserver
- ☐ Fileserver
- ☐ Datenbanken
- ☐ Web-Shop
- ☐ Web Server
- ☐ SAP / Buchhaltung / ERP
- ☐ andere:

Welche Dienste hat die Firma beim ISP gehostet?

- ☐ Mailserver
- ☐ Fileserver
- ☐ Datenbanken
- ☐ Web-Shop
- ☐ Web Server
- ☐ SAP / Buchhaltung / ERP
- ☐ andere:

Welche Dienste hat die Firma in der Cloud?

- ☐ Mailserver
- ☐ Fileserver
- ☐ Datenbanken
- ☐ Web-Shop
- ☐ Web Server
- ☐ SAP / Buchhaltung / ERP
- ☐ andere:

Mit Hilfe solcher Fragen kann man nun die Dokumentation der Zugriffskontrolle zusammenstellen und ganz klar festhalten, wo die Daten und Systeme physisch stehen, welche Dienste wo und auf welchen Systemen laufen, wer über welche Zugriffskanäle den Zugang haben darf.

Lösen Sie die folgenden Aufgaben

Aufgabe 5:

Ein kleines Unternehmen mit 20 Mitarbeitern. Das Unternehmen hat nur einen Standort. Wenn das Internet für vier Stunden ausfällt ist es nicht schlimm. Die Firma hat keine besonderen Sicherheitsanforderungen. Die Firma hat alle Internetservices beim ISP gehostet.

a) Welche Internetanbindung schlagen Sie vor? (Technologie, Sicherheit, Übertragungsrate)

.....

.....

b) Begründen Sie Ihren Vorschlag indem Sie die Aspekte der Übertragungsrate, der Verfügbarkeit und der Sicherheit in Ihrer Begründung erwähnen.

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 6:

Ein kleines Unternehmen bis 100 Mitarbeiter. Das Unternehmen hat nur einen Standort. Wenn das Internet für vier Stunden ausfällt ist es nicht schlimm. Die Firma hat erhöhte Sicherheitsanforderungen. Das Unternehmen hat alle Internetservices beim ISP gehostet.

a) Welche Internetanbindung schlagen Sie vor? (Technologie, Sicherheit, Übertragungsrate)

.....

.....

b) Begründen Sie Ihren Vorschlag indem Sie die Aspekte der Übertragungsrate, der Verfügbarkeit und der Sicherheit in Ihrer Begründung erwähnen.

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 7:

Ein Unternehmen bis 100 Mitarbeitern mit mehr als einem Standort. Wenn das Internet für 1 Stunde ausfällt wird es kritisch. Die Firma hat erhöhte Sicherheitsanforderungen. Das Unternehmen hat alle Internetservices bei sich in der Firma.

In diesem Beispiel kann eine DSL basierte Lösung nur noch knapp genügen. Für die Sicherheit soll mindestens eine managed Firewall mit DMZ (für die Server) oder ein moderner Security Gateway mit Intrusion detection and prevention (IDS/IPS) eingesetzt werden. Die Übertragungsraten soll mindestens 100/10 Mbps betragen. Ein FTTH Anschluss mit einer symmetrischen Übertragungsrate von 100/100 wäre, falls erhältlich, zu bevorzugen.

a) Welche Internetanbindung schlagen Sie vor? (Technologie, Sicherheit, Übertragungsrate)

.....

.....

b) Begründen Sie Ihren Vorschlag indem Sie die Aspekte der Übertragungsrate, der Verfügbarkeit und der Sicherheit in Ihrer Begründung erwähnen.

.....

.....

.....

.....

.....

.....

.....

.....

.....

Aufgabe 8 (nur für Cracks):

Sie sollen die Sicherheit einer Internetanbindung einer KMU beurteilen.

1.1.4 Wartung der Internetanbindung

Die Wartung sollte immer innerhalb angekündigter Wartungsfenster erfolgen. Diese sollten wenn möglich den Betrieb nicht beeinträchtigen.

Die Wartung einer Internetanbindung erfolgt unter anderem auf folgenden Ebenen:

- Wartung der Geräte
- Verwaltung der Sicherheitselemente
- Verwaltung der Konfigurationen
- Dokumentation aktuell halten

Bei der Wartung der Geräte geht es vor allem darum, dass immer die neueste Firmware eingesetzt wird und die Geräte regelmässig von Staub befreit werden. Verstaute Geräte haben eine kürzere Lebensdauer und können oft unverhofft den Dienst versagen.

Bei der Verwaltung der Sicherheitselemente geht es darum, dass die VPN-Konfigurationen und die Einstellungen der Firewall regelmässig kontrolliert werden (siehe auch Kapitel 1.2). Ein regelmässiges Studium der aktuellen Attacken auf MELANIE oder CERT ist sinnvoll.

Die Verwaltung der Konfigurationen wird auch zur Wartung gezählt, da es oft kleinere Änderungen gibt, die man in den vereinbarten Wartungsfenstern durchführen kann.

Das Nachführen der Dokumentation ist eine der wichtigsten Tätigkeiten bei der Wartung. Jede Änderung sollte protokolliert und in der Dokumentation nachgeführt sein.

1.2 Sicherheits- und Überwachungsmassnahmen beim Betrieb eines Internetanschlusses

In Kapitel 1.1.4 haben wir bereits beim Thema Wartung gelernt, dass ein Internetzugang offenbar überwacht werden muss. Diese Überwachung dient aber nicht nur der Wartung, sondern gehört zum Betrieb eines Netzes. Das zugehörige ISO-Modell ist das FCAPS-Modell, welches Fault-Management, Configuration-Management, Accounting, Performance-Management und Security-Management beschreibt. Die ITU hat darauf aufbauend eine ganze Empfehlung (ITU-T M.3400) erstellt.

Das Fault-Management soll Fehler entdecken, isolieren und die richtigen Stellen informieren. Die Fehler sollen korrigiert werden. Das Configuration-Management befasst sich mit der Verwaltung der Konfigurationsfiles, der Inventarisierung und der Verwaltung der Software (keine Applikationen). (Für Cracks: hier bestehen direkte Verbindungen zu ITIL)

Das Accounting sammelt alle Daten im Netz, die zur Abrechnung der Nutzung nötig sind. Die Geschäftszweige in einem Unternehmen sollen ja auch bezahlen, was sie benutzen.

Das Performance-Management überwacht und misst die Performance der einzelnen Netzbereiche und vergleicht diese mit vorgegebenen Sollwerten. Werden diese Sollwerte nicht erreicht, dann werden die entsprechenden Reports an die zuständigen Stellen geschickt. (Für Cracks: die Sollwerte sind in Service Level Agreements, SLA, zwischen der Firma und den Providern definiert)

Das Security-Management sichert den Zugang zu den Netzgeräten, den Netz-Ressourcen und den Netz-Services und führt die Autorisierungen durch.

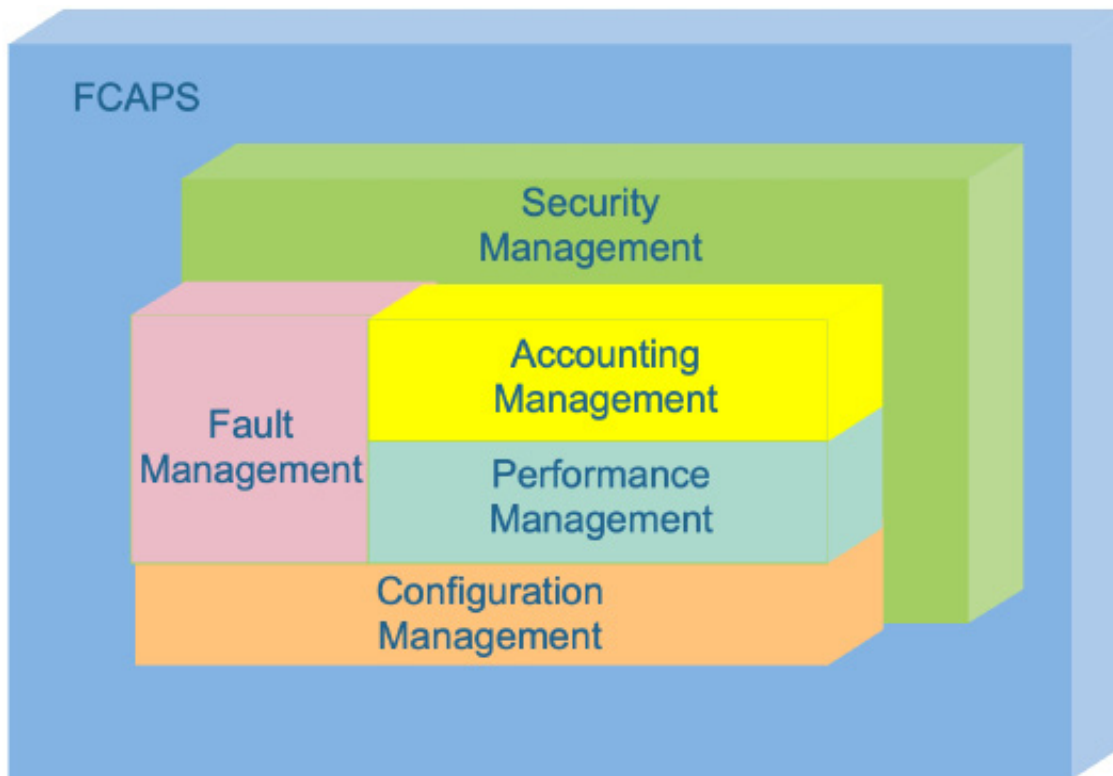


Bild 2: FCAPS

Bitte lösen Sie die folgenden Aufgaben:

Aufgabe 9:

Welche Teile des FCAPS werden für die Sicherheits- und Überwachungsfunktion eines Internetanschlusses benutzt? Begründen Sie Ihre Wahl.

.....

.....

.....

.....

.....

Aufgabe 10 (für Cracks):

Ein Betrieb hat einen Fibre-Anschluss 100/100 Mbit/s bei einem Provider. Der Provider hat dem Betrieb einen Router gestellt. Der Betrieb hat von einem anderen Anbieter eine Firewall mit Intrusion-Detection/-Prevention (IDPS) gekauft und in Betrieb genommen.

a) Welche Sicherheitsmassnahmen empfehlen Sie dem Betrieb? Nennen Sie mindestens 5 Massnahmen die Sie ergreifen müssen, um eine gute Sicherheit im Betrieb dieses Anschlusses zu gewährleisten. Hilfe: Suchen Sie Informationen zu Sicherheitsmassnahmen, securitypolicy,

Schulung der Mitarbeiter im Zusammenhang mit Gefahren aus dem Internet, Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit bei Internetanschlüssen. Antworten Sie in ganzen Sätzen und strukturieren Sie Ihre Antwort.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

b) Was würden Sie überwachen bei diesem Internetanschluss? Beschreiben Sie zuerst was Sie überwachen wollen und danach wie Sie diese Überwachung realisieren wollen.

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Kundenvorgaben nach Prioritäten, Pflichtenheft

In diesem Kapitel sollen Kundenvorgaben nach Prioritäten eruiert und klassiert werden. Die Bedeutung für das Unternehmen soll klar sein. Die Kundenvorgaben sollen in einem Pflichtenheft für die Evaluation eines Serviceproviders festgehalten werden. Die Resultate der Aufgaben sollen im Rahmen der LB1 dokumentiert werden.

2.1 LB1

Siehe dazu separates Dokument LB1 mit Bedingungen und Ablauf der Lernbeurteilung.

Die Ausgangslage für alle Aufgaben in der LB1 ist wie folgt:

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.

Erstellen Sie hier die Vorlage für das Dokument der LB1 (nach IPERKA).

2.2 Zugangsmöglichkeiten zum Internet sowie deren Anbieter (Provider)

Die Zugangsmöglichkeiten zu den verschiedenen Providern können auf verschiedenen Technologien beruhen.

Kleine KMU werden sich einen xDSL oder Cable Anschluss leisten. Falls bereits FTTH Anschlüsse vorhanden sind, werden die Provider diese Anschlüsse auf einen FTTH Anschluss migrieren. Dies, weil ein FTTH Anschluss für den Provider günstiger ist in der Bereitstellung des Dienstes und dessen Betrieb (DSL ist technologisch und betrieblich aufwendiger als das Ethernet des FTTH Anschlusses). Andere Lösungen wie PWLAN oder G5-Technologien sind heute noch wenig verbreitet.

Ihre Aufgabe besteht nun in der Recherche der aktuellen Zugangsmöglichkeiten. Füllen Sie dazu die folgende Tabelle aus. Benutzen Sie das Internet als Informationsquelle – direkte Anfragen bei den Providern sind verboten!

Provider	Angebot (Name)	Übertragungsrate	Preis	Technologie
Swisscom	Business S	40/40 Mbit/s	90 CHF/M	FTTH

Provider	Angebot (Name)	Übertragungsrate	Preis	Technologie

Tabelle 3: Vergleich der Provider

Sie können unschwer erkennen, dass sich diese Internetanschlüsse alle gleichen. Die Unterschiede sind klein und oft nicht sehr offensichtlich. Dies hat damit zu tun, dass die Swisscom die Produkte im Prinzip vorgibt und die anderen Provider in etwa das gleiche Angebot zu leicht tieferen Preisen vermarkten.

Es ist geschickter, wenn man zuerst die Anforderungen des Betriebs oder des Kunden kennt, daraus ein Lastenheft generiert, das dann der Provider als Pflichtenheft oder in Form einer Offerte ausgestalten kann.

Es gelten die folgenden Definitionen:

2.2.1 Lastenheft / Pflichtenheft

Anforderungsspezifikation (Lastenheft)

Gemäss DIN 69901-5 ist ein Lastenheft eine "vom Auftraggeber festgelegte Gesamtheit der Forderungen an die Lieferungen und Leistungen eines Auftragnehmers innerhalb eines Auftrages". Das Lastenheft enthält somit die Beschreibung, was, warum gemacht werden soll. Das Lastenheft wird in der Regel vom Auftraggeber erstellt und ist ein Bestandteil eines Vertrags.

Lösungsspezifikation (Pflichtenheft)

Das Pflichtenheft ist gemäss DIN 69901-5 definiert als "vom Auftragnehmer erarbeiteten Realisierungsvorgaben aufgrund der Umsetzung des vom Auftraggeber vorgegebenen Lastenhefts". Das Pflichtenheft enthält die Information wie und womit das Produkt gemacht werden soll.

Ein strukturiertes Vorgehen bei der Auswahl der verschiedenen Angebote (Evaluation) ist anzustreben.

Die Methoden zur Klassierung der Kundenvorgaben werden im nächsten Kapitel vorgestellt und angewendet.

2.3 Methoden um Kundenvorgaben zu klassieren

Idealerweise beschreibt der Kunde seine Wünsche bezüglich der Internetanbindung in einem Lastenheft. Dies hat den Vorteil, dass sich der Kunde bereits einmal mit seinen Wünschen auseinandersetzt. Diese Wünsche sind aber oft technisch nicht umsetzbar oder nur mit hohen Kosten realisierbar (Unwirtschaftlich). Um aus diesen Wünschen gute Kundenvorgaben abzuleiten muss

ein Informatiker alle diese Wünsche bezüglich den Anforderungen des Geschäftes klassieren und evaluieren.

Eine Anforderung ist gemäss DIN EN ISO 9000 "ein Erfordernis oder eine Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist". Allgemein beschreibt eine Anforderung, was der Auftraggeber von einem zu entwickelnden System erwartet.

Die weltweit bekannte Vorlage für die Anforderungsspezifikation ist der IEEE- Standard 8303.

Die Vorlage unten zeigt eine mögliche Kapitelstruktur auf Basis der Standards IEE839, IEEE1233, ISO 29148:

2.3.1 Vorlage normiertes Lastenheft

Titelblatt: Titel, Autor, Datum, Ersteller

1. Seite: Empfänger, Änderungshistorie, Verzeichnisse.

Inhaltsverzeichnis:

1. Einführung

Beschreibung der Aufgabe des Lastenhefts, insbesondere Veranlassung, Zielsetzung, wesentliche Aufgaben, Definitionen.

Beispiele:

- «Das vorliegende Lastenheft ist gültig für das Unternehmen [...]».
- «Dieses Lastenheft dient als technische Unterlage zur Anfrage eines Angebots für eine Entwicklungsleistung oder ist als technische Definition des Entwicklungsziels Bestandteil des Entwicklungsvertrages / Entwicklungsauftrages.».
- «Dieses Lastenheft dient als Unterlage zur Ausgestaltung eines Pflichtenheftes für die Internetanbindung der Firma Easy-Access».

Beschreibung des Ist-Zustandes (Prozessbeschreibung, bestehendes System, Organisation).

- Technischer Prozess bzw. Geschäftsmodell des Auftraggebers. Vorhandenes System: Geräte, Software, Nutzung. Organisations- Beschreibung der relevanten Bereiche beim Auftraggeber.
- Die Ausgangssituation und der Anlass zur Durchführung des Projektes. Die Defizite bzw. Probleme existierender Systeme oder auch der aktuellen Situation werden dargestellt, die zur Entscheidung geführt haben, das Projekt durchzuführen.
- Die Firma Easy-Access besitzt eine Internetanbindung mit einer Übertragungsrate von 10/1 Mb/s mit ADSL Modem. Das Routing wird vom Provider festgelegt und das NAT stellt ein internes Netz 192.168.0.0/24 zur Verfügung.

1.1 Zweck (Darstellung der Vision)

- Das Lastenheft soll erstellt werden, um die Anforderungen an eine neue Internetanbindung zu definieren.

1.2 Marktanforderungen (z.B. Markt, Bedarf, Design)

- Die neue Internetanbindung soll auf dem neuesten Stand der Access-Technologien sein und die Bedürfnisse des Geschäftes optimal abdecken.

1.3 Glossar (Definitionen, Abkürzungen) Bitte alphabetisch ordnen.

- ISP: Internet Service Provider
- Router: Vermittlungsgerät zum Internet

1.4 Referenzen

- Schreiben Sie hier, welche Referenzen Sie vom Lieferanten erwarten.

1.5 Systemübersicht (System und Kontextabgrenzung)

- Beschreiben Sie hier die aktuelle Situation am besten mit einer Skizze.

2. Beschreibung

Beschreibung des Soll-Zustandes: Anforderungen an zu-entstehendes System, Art und Weise der Durchführung.

2.1 Produktsicht

- Zeichnen Sie hier die gewünschte Internetanbindung auf. Je genauer Sie das können, desto besser werden Sie vom Lieferanten bedient.

2.2 Funktionen (Use-Cases, Feature-Baum)

- Welche Funktionen erwarten Sie von der neuen Internetanbindung? (Firewall, VPN, DHCP, IP-Konzept, ...)

2.3 Benutzer (Benutzergruppen, Profile, Szenarien)

- Wer soll das künftige System benutzen?

2.4 Rahmenbedingungen (externe Vorgaben, z.B. Protokolle, Hardware)

- Bei einer Internetanbindung ist neben der technischen Spezifikation der Anbindung auch wichtig zu wissen, wo die Services der Firma stehen (intern, ISP, cloud).
- Sind spezielle Bedingungen bezüglich Datenschutz oder anderer Gesetze notwendig?
- Wird spezielle Hardware gewünscht?

2.5 Qualitätsanforderungen (externe Vorgaben, z.B. Zuverlässigkeit)

- Welche Anforderungen an die Qualität werden verlangt?
- Software- Merkmale, -Sicherung, -Nachweise, Hardwarequalität
- "Bei Unterschreiten des technischen Nutzungsgrades von 98% hat AG das Recht auf Nachbesserung."

2.6 Annahme

- Unter welchen Bedingungen sind Sie als Kunde gewillt, das System abzunehmen (Tests, Qualität, Menge, Preis, ...)?

3 Spezifische Anforderungen

Alle Anforderungen an das neue System sollen aufgelistet werden.

3.1 Funktionale Anforderungen (z.B. Gültigkeitsprüfung, Abnahme)

- Menge (Übertragungsrate)
- Performance (Durchsatz)
- Qualität (Verfügbarkeit, Stabilität, ...)
- Sicherheit (nach ISO, Firewall)
- Anbindung externer Mitarbeiter (VPN)
- Schulung (Awareness, Funktion)
- weitere Themen

3.2 Architektur (z.B. Datenmodelle, Systemmodelle)

- Datenverarbeitung (Erfassung, Funktionen, Ausgabe), Datenspeicherung, Software, Hardware
- "Der Fernwartungszugriff erfolgt über eine browserbasierte VPN Lösung (SSL-VPN Box)".
- "Die Maschinen müssen die Möglichkeit bieten, [...] Datenerfassung als Option nachzurüsten."

- Welche Anforderungen müssen bezüglich der Architektur der Internetanbindung erfüllt sein?

3.3 Rahmenbedingungen (nicht-funktionale Anforderungen, Normen)

Anforderungen für die Inbetriebnahme und den Einsatz

- Dokumentation, Montage, Probetrieb und Abnahmen, Schulungen, Betriebsablauf, Softwarepflege
- "Für das Bedien- und Instandhaltungspersonal ist an der Maschine eine Unterweisung in deutscher Sprache durchzuführen".

Anforderungen an die Projektabwicklung einschliesslich Zeitplan

- Projektorganisation (Personal, Zuständigkeiten), Projektdurchführung (Planung, Steuerung, Überwachung), Konfigurationsmanagement (Versionsverwaltung)
- "Die vollständigen und endgültigen Unterlagen sind dem AG mindestens 14 Tage vor der Endabnahme zu übergeben".

Beschreibung der Anforderungen für die Inbetriebnahme

- "Der Signalaustausch zu anderen Maschinen, Anlagen und Einrichtungen oder übergeordneten Systemen ist zusammengefasst, einschliesslich die externen Anschlüsse, darzustellen und beschreiben".

3.5 Standards

- Welche Normen müssen erfüllt sein - allenfalls SLA

Anhänge, Index

- Dokumente der Ist-Situation
- Test-Anforderungen
- Firmeninterne Unterlagen die für das Vorhaben relevant sind

Alle diese Anforderungen sollten in einem vollständigen Lastenheft aufgeführt sein.

Nun kann es vorkommen, dass ein Kunde sehr viele Anforderungen aufschreibt! Sie sehen sofort, dass nicht alle Wünsche oder Anforderungen aus Sicht des Unternehmens des Kunden Sinn machen. Um ein unwirtschaftliches Projekt zu verhindern sollte man die Anforderungen kritisch hinterfragen.

Man klassiert daher die Anforderungen wie folgt:

2.3.2 Klassierung

Zwingend notwendig: ohne diese Anforderung kann das Geschäft den Internetzugang nicht nutzen. Das Geschäft des Kunden leidet oder wird verunmöglicht.

Notwendig: ohne diese Anforderung kann das Geschäft des Kunden den Internetzugang zwar nutzen, aber die Nutzung ist eingeschränkt oder mühsam. Das Geschäft des Kunden leidet.

Kann notwendig sein: ohne diese Anforderung kann das Geschäft des Kunden den Internetzugang nutzen. Die Nutzung ist uneingeschränkt.

Unnötig: diese Anforderung ist für das Geschäft ohne Nutzen (z.B. Zugang zu einem Pizzakurier).

Aufgabe 11:

Der Ist-Zustand eines Internetzugangs der Firma Slow ist wie folgt konfiguriert:

Eine alte asymmetrische ADSL 5/0.5 Mbit/s Verbindung wird mit einem Modem/Router des Providers in der Firma Slow terminiert. Die Website und das Mail der Firma Slow werden vom gleichen Provider betrieben.

Nun möchte die Firma Slow ein modernes FTTH-Angebot mit einer Übertragungsrate von

100/100 Mbit/s nutzen. Der Webserver mit dem Mail (MS-Exchange) soll neu in der Firma Slow aufgestellt sein und ein moderner Webshop soll Bestandteil des Internetservices der Firma Slow werden.

Welche technischen Anforderungen an die neue Internetverbindung sind technisch zwingend notwendig?

Schreiben Sie drei zwingend notwendige Anforderungen auf.

.....

.....

.....

.....

.....

.....

Beantworten und dokumentieren Sie an dieser Stelle die Fragen zum Thema 2 in der LB1.

Aufgabe 12 (für Cracks):

Der Ist-Zustand des Internetzugangs der Firma Lazy ist wie folgt konfiguriert:

Ein alter Internetzugang mit 50/5 Mbit/s ist mit einem einfachen ADSL Modem/Router terminiert.

Die Web Server der Firma und das Mail sind intern betrieben worden, was dauernd zu Sicherheitsproblemen geführt hat.

Erstellen Sie für die Firma Lazy ein vollständiges Lastenheft mit einem Soll-Zustand. Überlegen Sie bei jeder Anforderung die Klassierung. Benutzen Sie das genormte Inhaltsverzeichnis.

Geben Sie das Lastenheft praxistauglich formatiert ab. Es wird erwartet dass das Lastenheft einem Lieferanten abgegeben werden könnte.

1. Einführung

Beschreibung der Aufgabe des Lastenhefts, insbesondere Veranlassung, Zielsetzung, wesentliche Aufgaben, Definitionen.

Beschreibung des Ist-Zustandes (Prozessbeschreibung, bestehendes System, Organisation).

1.1 Zweck (Darstellung der Vision)

1.2 Marktanforderungen (z.B. Markt, Bedarf, Design)

1.3 Glossar (Definitionen, Abkürzungen) Bitte alphabetisch ordnen.

1.4 Referenzen

1.5 Systemübersicht (System und Kontextabgrenzung)

2. Beschreibung

Beschreibung des Soll-Zustandes: Anforderungen an zu-entstehendes System, Art und Weise der Durchführung.

2.1 Produktsicht

2.2 Funktionen (Use-Cases, Feature-Baum)

2.3 Benutzer (Benutzergruppen, Profile, Szenarien)

2.4 Rahmenbedingungen (externe Vorgaben, z.B. Protokolle, Hardware)

2.5 Qualitätsanforderungen (externe Vorgaben, z.B. Zuverlässigkeit)

2.6 Annahme

3 Spezifische Anforderungen

Alle Anforderungen an das neue System sollen aufgelistet werden.

3.1 Funktionale Anforderungen (z.B. Gültigkeitsprüfung, Abnahme)

3.2 Architektur (z.B. Datenmodelle, Systemmodelle)

3.3 Rahmenbedingungen (nicht-funktionale Anforderungen, Normen)

Anforderungen für die Inbetriebnahme und den Einsatz

Anforderungen an die Projektabwicklung einschliesslich Zeitplan

Beschreibung der Anforderungen für die Inbetriebnahme

3.5 Standards

Anhänge, Index

2.4 Aufbau und Inhalt eines Pflichtenhefts

Laut VDI/VDE 3694 ist die Grundlage für das Pflichtenheft das Lastenheft; ohne Lastenheft kann es kein Pflichtenheft geben. Das Pflichtenheft enthält die gleichen Punkte wie das Lastenheft und zusätzlich die folgenden Angaben:

4. Systemtechnische Lösungen

- Gliederung und Beschreibung der systemspezifischen Lösung für die Themen aus der Aufgabenstellung
- Strukturplan, Eingangsgrössen, Datenflüsse
- Funktionsbeschreibung

4.2 Systemtechnik

- Datenverarbeitungssystem, Netzwerksystem
- Datenverwaltungs- Datenbanksystem
- Gerätetechnik (Hardwareumgebung)
- Technische Angaben für das Gesamtsystem (Antwortzeit, Verfügbarkeit, Sicherheit).

2.5 Ablauf eines Evaluationsprozesses

Jeder Evaluationsprozess beinhaltet eine Beurteilung und eine Entscheidung. In der Regel ist die Beurteilung kriteriengestützt. Die Kriterien sollen aus den folgenden Kriterienfeldern stammen und je nach Situation und Projekt stärker oder weniger stark gewichtet werden.

Kriterienfelder:

- a) Technische Kriterien (Erfüllt die vorgeschlagene Lösung des Pflichtenheftes alle technischen Anforderungen aus dem Lastenheft bezüglich Qualität, Sicherheit, Performance und Menge?)
- b) Wirtschaftliche Kriterien (Nützt die Lösung dem Unternehmen mehr als sie kostet? Kann man die Projektkosten und die laufenden Kosten rechtfertigen mit Einsparungen gegenüber der alten Lösung oder mit Anforderungen aus dem Geschäft?)
- c) Strategische Kriterien (Werden die Anforderungen des Geschäftes mit der Lösung erfüllt?)
- d) Operative Kriterien (Ist die Lösung betreibbar und wartbar?)
- e) Organisatorische Kriterien (Kann die Lösung in die bestehenden organisatorischen Prozesse eingefügt werden?)
- f) Juristische Kriterien (Sind Service Level Agreements (SLA) möglich? Werden die Gesetze eingehalten?)
- g) Ökologische Kriterien (Ist die Entsorgung oder der Rückbau berücksichtigt worden?)
- h) Sicherheits Kriterien (Sind alle geforderten Sicherheitsmassnahmen umgesetzt?)

Die Beurteilung auf der Stufe der Berufsfachschule kann man mit einer einfachen Nutzwertanalyse durchführen. Wir lassen dabei die umfangreichen Theorien zur Beurteilung von Projekten und Vorhaben ausser acht, ebenso die genaue Herleitung der Kriteriengewichtung. Wir behelfen uns dabei mit dem Gesunden Menschen-Verstand (GMV).

Um eine Nutzwertanalyse durchzuführen benutzt man am besten eine Tabellenkalkulation.

Auswahlkriterium	Gewichtung	Variante 1		Variante 2		Variante 3	
		Bewertung	Teilnutzwert	Bewertung	Teilnutzwert	Bewertung	Teilnutzwert
Technische Kriterien	24	1 bis 6		1 bis 6		1 bis 6	
Übertragungsrate	8	3	24	5	40	2	16
Stabilität	8	3	24	6	48	3	24
Qualität	8	2	16	5	40	4	32
Wirtschaftliche Kriterien	24						
Kosten/Nutzen	6	6	36	4	24	4	24
Wartungskosten	6	3	18	5	30	3	18
Betriebskosten	6	4	24	5	30	5	30
Lizenzgebühren	6	2	12	3	18	6	36
Strategische Kriterien	12						
Verhalten des Lieferanten am Markt	4	2	8	5	20	2	8
Stabilität des Lieferanten	4	2	8	6	24	3	12
Referenzen	4	2	8	3	12	5	20
Operative Kriterien	12						
Betreibbarkeit	4	5	20	4	16	4	16
Notwendiges Know How	4	4	16	5	20	3	12
Support	4	5	20	6	24	4	16
Organisatorische Kriterien	6						
In Prozesse einfügbar	3	2	6	6	18	5	15
Kommunikationsprozesse	3	3	9	6	18	4	12
Juristische Kriterien	6						
SLA	2	5	10	3	6	4	8
Vorfälle	2	2	4	3	6	3	6
Gesetze	2	1	2	3	6	5	10
Ökologische Kriterien	4						
Entsorgung	2	3	6	4	8	3	6
Wiederverwendbarkeit	2	3	6	5	10	2	4
Sicherheits Kriterien	12						
Verfügbarkeit	4	2	8	3	12	4	16
Vertraulichkeit	4	2	8	3	12	3	12
Integrität	4	2	8	3	12	3	12
Total	100%		301		454		365
Rang			3		1		2

Hat man eine Beurteilung vorgenommen, so muss man nun eine Entscheidung treffen. Man kann die Teilnutzwerte zusammenzählen und so das Siegerprojekt bestimmen. Vorsicht ist aber geboten bei Resultaten, welche nur kleine Unterschiede in den Gesamtpunktzahlen ergeben! Die Regel besagt, dass ein Sieger nur sein kann, wer mindestens 20% Abstand hat zum nächst-

platzierten Projekt. Variante 2 würde diese Regel erfüllen und könnte somit als bestes Projekt gelten. Wird die Regel verletzt, muss man sich die Bewertungen nochmals anschauen und abklären, ob man nicht durch eine klarere Bewertung einen Sieger bekommt.

Tabelle 4: Nutzwertanalyse

(Für Cracks: Das macht man mit einer Sensitivitätsanalyse).

Die Evaluation (Beurteilung und Entscheidung) wäre somit abgeschlossen.

Aufgabe 13

Bearbeiten Sie hier die Themen 1 bis 5 der LB1. (6 Lektionen)

Aufgabe 14 (für Cracks)

Erweitern Sie Ihr Lastenheft zu einem Pflichtenheft. Sie sollen dazu die Rolle des von Ihnen gewählten Internetproviders aus Aufgabe 13 schlüpfen und die Aufgabe aus dieser Sicht lösen.

3. Resultate der Evaluation bewerten und darstellen.

In diesem Kapitel sollen die Resultate einer Evaluation unter Berücksichtigung des Pflichtenheftes und der wirtschaftlichen Aspekte an einem praktischen Beispiel bewertet und dargestellt werden.

3.1 Die wichtigsten Kriterien für die Bewertung eines Angebotes.

In Kapitel 2 haben wir bereits Kriterien für die Evaluation einer Internetanbindung benutzt. Es wurde damit eine Evaluation durchgeführt, das heisst, es wurde ein geeigneter Internetanbieter gefunden.

Die dort verwendeten Kriterien sind in der Praxis oft in der gezeigten Art in die erwähnten Kriterienfelder gruppiert. Solche Vorgehen eignen sich vor allem für interne Evaluationen aus dem Internet, wenn ein neues Auto gekauft werden soll, wenn neue Hardware angeschafft werden soll oder wenn erste Projektkosten abgeschätzt werden sollen.

Handelt es sich aber um ein grösseres Vorhaben, so werden die Arbeiten oder Beschaffungsvorhaben ausgeschrieben (Submission, Tender). Unter gewissen Umständen und für grosse Projekte ist eine Submission nach WTO (World Trade Organisation) sogar vorgeschrieben. Staatliche Stellen oder grosse Firmen müssen die Projekte ab einer gewissen Grösse ausschreiben (zum Beispiel ab CHF 100'000).

Bei einer Submission werden entweder Firmen eingeladen (Submission auf Einladung) oder die Ausschreibung wird auf Internetplattformen publiziert (offene Submission). Eine Submission enthält das Lastenheft und zwingend die Bewertungskriterien für die Offerten.

Die Firmen, die an einer Submission teilnehmen, werden ihre Offerten unter Bezugnahme auf diese Kriterien abgeben.

Ein Beispiel von solchen Bewertungskriterien für die Auswertung der eingegangenen Angebote für eine Breitband-Internetanbindung (dies ist ein echtes Praxis-Beispiel):

Kriterium	Gewichtung	Bewertung
1. Preis	55%	Punkte = $2 + (\text{niedrigster Preis} / \text{Preis des Angebotes})$
2. Personal/Büro Projektteam, Nachweis der fachlichen Leistungsfähigkeit Ingenieure und technische Zeichner für die Erstellung v. Abfragen und Auswertungen Nachweis der wirtschaftlichen Leistungsfähigkeit (regelmässige Zahlung von Abgaben, Steuern, Krankenkassenbeiträgen; Gesamtumsätze/Umsätze f. vergleichbare Leistungen der letzten drei abgeschlossenen Geschäftsjahre; Berufshaftpflichtversicherung) ISO 9000/9001 oder gleichwertiges Qualitätssystem	15%	Summe der vergebenen Punkte = <ul style="list-style-type: none"> • für jeden nachgewiesenen Unterpunkt 2 Punkte, • nachgewiesen durch Fremdleistungen 1 Punkt, • sonst 0 Punkte. Ermittlung des Durchschnittswertes: $DW = \text{Summe der vergebenen Punkte} / \text{Anzahl (5) der Unterpunkte}$

Kriterium	Gewichtung	Bewertung
3. Umsetzungskonzept (Erläuterungsbericht) max. zweiseitiger Erläuterungsbericht Musterbogen für Befragung/Erhebung/ Auswertung	15%	Die Bewertung erfolgt durch eine dreiköpfige Jury nach folgendem Schema: <ul style="list-style-type: none"> Die Darstellung entspricht den Anforderungen 2 Punkte, mit Einschränkungen 1 Punkt, nicht den Anforderungen 0 Punkte; Ermittlung des Durchschnittswertes (DW=Summe der vergebenen Punkte je Bewerber / Anzahl der Jurymitglieder). Ein DW < 0,6 führt zum Ausschluss des Angebotes.
4. Referenzen - Kenntnisse Breitband Befragung/Erhebung/Auswertung Ingenieurleistungen Fördermittelantrag/Ergebnisberichte Vorbereitung und Mitwirkung der Vergabe	10%	Zu jedem Unterpunkt sind mindestens 3 Referenzen abzugeben. Sind zu einem Unterpunkt keine Referenzen/Kenntnisse vorhanden, führt dies zum Ausschluss des Angebotes. Summe der vergebenen Punkte = <ul style="list-style-type: none"> für jeden nachgewiesenen Unterpunkt 2 Punkte, nachgewiesen durch Fremdleistungen 1 Punkt. Ermittlung des Durchschnittswertes: DW=Summe der vergebenen Punkte / Anzahl (5) der Unterpunkte.
5. Fremdleistungen	5%	Sind keine Fremdleistungen erforderlich: <ul style="list-style-type: none"> 2 Punkte, sonst 0 Punkte.

Hinweis: Lassen Sie nur offerieren, wenn Sie auch die Absicht haben etwas zu kaufen! Anfragen für Offerten aus dem schulischen Umfeld sind verboten. Grund: Das Erstellen von Offerten ist eingrosser Aufwand. Wenn dann gar nichts gekauft werden kann, weil es sich ja um ein Schulprojekt handelt, dann ist das für die Firmen enorm ärgerlich.

Tabelle 5: Bewertungskriterien

Der Bund hat ein Merkblatt für die Arbeit von Evaluatoren herausgegeben (Es handelt sich um ein Merkblatt, wie man Leute, die Evaluationen im Gesundheitswesen durchführen, auswählen soll): «Beurteilung von Offerten für Evaluationsmandate». Darin wird jede Offerte einzeln beurteilt bevor ein Quervergleich gemacht wird. «Die Hauptkriterien für den Zuschlag einer Arbeit (Zuschlagskriterien) sind: Zweckmässigkeit der Leistung, Preis, Termine, Anbieterbezogene Kriterien sowie der Gesamteindruck, den eine Offerte hinterlässt.»

In diesem Merkblatt heisst es weiter:

«Eine Offerte soll primär Folgendes aufzeigen oder bewirken: Der Auftrag ist richtig verstanden und das Vorgehen ist nachvollziehbar.

- Die Datenerhebungen sind in Bezug auf die Beantwortung der Fragestellungen zweckmässig.
- Die Datenauswertung und die Analyse der Resultate sind zweckmässig.
- Die Produkte der Evaluation sind angemessen präzisiert.
- Das Preis-Leistungsverhältnis ist insgesamt angemessen.
- Der Zeitplan ist realistisch.
- Das Evaluationsteam erfüllt die Voraussetzungen für die Auftragserfüllung.
- Der Gesamteindruck ist überzeugend.

Solche und ähnliche Merkblätter oder gar Reglemente haben Firmen, öffentliche Ämter oder andere Stellen, die grosse Projekte mit grossen Budgets zu vergeben haben.

Aufgabe 14:

Suchen Sie im Internet Musterofferten (zum Beispiel https://www.idparc.ch/files/documents/Muster_Offerte.pdf) wählen Sie eine aus.

Beantworten Sie die folgenden Fragen:

- Finden Sie die Kriterien 1 bis 5 der Tabelle oben in diesen Musterofferten? Was steht da konkret zu diesen Kriterien (Sie sollen genau schreiben was da steht und nicht einfach ja oder nein)-
- Welche der Punkte oben sind in der gewählten Offerte drin? Schreiben sie ganz genau auf, was Sie gefunden haben und was Ihrer Meinung nach fehlt.

3.2 Darstellungsarten für die Beurteilung von Offerten.

Wenn man eine Ausschreibung macht, dann soll die Form der Offerte möglichst genau vorge-schrieben sein. Je mehr Freiraum man den offerierenden Firmen gibt, desto unvergleichbarer werden die Offerten. Es macht also Sinn, dass man mindestens eine Tabelle in der Art wie oben gezeigt abgibt, mit möglichst klaren Fragestellungen.

Beispiel für eine Internetanbindung:

1. Umsetzungskonzept

Geben Sie einen Netzwerkplan ab, der aufzeigt, wie die Internetanbindung technisch realisiert ist. Erwartet wird ein Plan, in welchem alle Elemente angeschrieben sind, alle Verbindungen ein-gezeichnet und alle Elemente in einer Legende genau spezifiziert sind.

Was würden Sie da noch hinzufügen? Versuchen Sie das noch genauer zu beschreiben:

.....

.....

.....

2. Personal / Büro

Wie viele Netzingenieure beschäftigen Sie?

Wie viele Supportangestellte beschäftigen Sie?

Zahlen Sie Ihre Sozialversicherungsbeiträge regelmässig?

Ist Ihr Umsatz grösser als 1 Million CHF / Jahr?

Ist Ihr Umsatz grösser als 10 Mio CHF / Jahr?

Ist Ihr Umsatz grösser als 100 Mio CHF / Jahr?

Haben Sie eine Berufshaftpflichtversicherung?

Sind Sie ISO 9000 zertifiziert?

Welche Punkte würden Sie noch im Fragebogen festhalten?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Wie Sie nun unschwer feststellen konnten, ist die Evaluation und die Beurteilung von Internetanbindungen und Providern keine einfache Sache und braucht viel Erfahrung.

4. Netzwerkplan und Netzwerkschema für die Internetanbindung erstellen oder anpassen.

In diesem Kapitel wenden wir uns der Praxis zu. Sie müssen sich nun vorstellen, dass Sie bei einem Provider zuständig sind für den Aufbau eines Internetanschlusses eines Kunden. Zu den Kapiteln 4, 5 und 6 gehört die LB2.

4.1 Regeln für das Erstellen eines Namens- und Nummerierungskonzepts.

Alle Geräte an einem Netz haben einen Namen. Die Vergabe und der Gebrauch dieser Namen im Netz sind in RFC beschrieben.

Man unterscheidet grundsätzlich zwischen reinen Gerätenamen für beispielsweise Server, Workstations, Printer, Router, Gateways, Firewalls, Switches, Scanner im Netz (LAN, enterprise network) und den Hostnamen oder den vollständigen Domain Namen (Fully Qualified Domain Name (FQDN)).

In jedem Fall muss ein Name so aufgebaut sein, dass er im DNS eingetragen werden und von allen Betriebssystemen erkannt werden kann. Zudem sollen Gerätenamen für interne Personen leicht verständlich sein und Hinweise liefern zur Art, Standort und Domäne des Gerätes.

4.1.1 Hostnamen (FQDN)

Schauen wir zuerst die RFC zu den Hostnamen an. Der Name des Servers (Gerätes) wird als «hostname» bezeichnet. Der hostname kann ein Domänenname und ein Topleveldomainname mit je einem Punkt beinhalten (zum Beispiel «jupiter.tbz.ch.». **Man beachte den Punkt am Schluss des FQDN!** Diese Namensgebung führt zu einem Fully Qualified Domain Name (FQDN) und ist für Server in Domänen sehr geeignet. Im Internet sind diese FQDN zusammen mit den zugeteilten IP-Adressen im Domain Name System (DNS) gespeichert.

Der Fully qualified Host Name (FQHN) beschreibt noch den Namen des Servers in einem Subnetz: (zum Beispiel srv01.admin.tbz.ch)

In den RFC 952, RFC 1123 und RFC 2965 ist geregelt, welche Zeichen für die Benennung von Hosts erlaubt sind:

«A «name» (Net, Host, Gateway, or Domain name) is a text string up to 24 characters drawn from the alphabet (A-Z), digits (0-9), and the minus sign (-) and period (.). No blank or space characters are permitted as part of a name. No distinction is made between upper and lower case. The first character must be a letter. The last character must not be a minus sign or period. A host which serves as a GATEWAY should have «-GATEWAY» or «-GW» as part of its name. A host which is a TIP or a TAC should have «-TIP» or «-TAC» as part of its host name, if it is an ARPANET or DoD host.

Host software MUST handle host names of up to 63 characters and SHOULD handle host names of up to 255 characters.»

4.1.2 Gerätenamen

Für Computernamen gibt es best practice RFC 1178 und Guidelines for computer naming standards

In Windowsumgebungen haben alle Computer einen eindeutigen Namen. Dieser Name identifiziert den Computer im WINS oder DNS im ganzen Netz. Diese Namen sollten nicht mehr als 15 Zeichen lang sein.

Erlaubte Zeichen und einige Anweisungen sind:

- Buchstaben A-Z und Ziffern 0-9 (andere Zeichen könnten im DNS Probleme verursachen).
- Der Computernamen sollte nicht mit einer Zahl beginnen - nicht alle DNS-Server können damit umgehen.
- Möglichst keine hexadezimalen Namen benutzen - diese sind schwer verständlich.
- Namen sollten kürzer als 15 Zeichen sein. Active Directory könnte damit Probleme bekommen und längere Namen sind schwerer zu merken.
- Namen sollten den Mitarbeitern etwas sagen - unverständliche oder kryptische Namen sollten vermieden werden.
- Usernamen sollten nicht als Computernamen dienen - wenn der User sein Gerät zurückgibt, muss der Name geändert werden, was schwierig sein könnte. Besser sind Computernamen welche aus Serie-Nummern und der Lokation zusammengesetzt sind.
- Möglichst keine falsche Rechtschreibung - auch keine Substitutionen wie 0 (Null) statt O oder 3 statt E.
- Gerätenamen möglichst am Gerät anschreiben.

Damit die Namensgebung skalierbar bleibt, sind Planetennamen und andere namensgebende Ideen nicht unbedingt sinnvoll.

Besser sind Konzepte die sich aus Gerätetyp, Nummer (kann die Seriennummer sein), Ort zusammensetzen:

SV	Servers
WS	Workstations
PR	Printers
RT	Router
SW	Switch
FW	Firewall
TS	Terminal Servers
DC	Domain Controllers
IIS	Web Servers
MSX	Mail Servers
SQL	SQL Servers
SMS	SMS Servers
APP	Application Servers

So könnte zum Beispiel ein Server Nummer 1 im Rechenzentrum im Rack 005 an der Zentralstrasse in Zürich folgendermassen benannt werden:

SV001ZHZenR005

In Windows können die Computer auch automatisch benannt werden - der Nutzen davon muss aber sehr sorgfältig abgeklärt werden.

Siehe zum Beispiel folgenden Beitrag dazu: <http://labmice.techtarget.com/articles/computernaming.htm>

4.2 Funktionsweise von Firewall, DMZ, Proxy und DNS.

LB1 Themen 6 und 7 (2 Lektionen)

Firewalls können, in der einfachsten Form, nur Pakete nach bestimmten Regeln filtern (Packet Filter). Dies kann in Layer 3 Geräten (Router) erfolgen.

Möchte man auf Layer 4 die TCP (UDP) Verbindung überwachen, muss man Verbindungs Gateways einsetzen.

Genügt dies noch nicht und möchte man im Layer 7, dem application layer, in die Kommunikation hineinschauen, so muss man Application Level Gateways benutzen.

Diese Application Layer Firewall kann die Netzbelastung massiv erhöhen und daher ist häufig eine Kombination aus Paketfilter und Gateway im Einsatz, die sogenannte Stateful Inspection Firewall.

Möchte man die Pakete noch eingehender inspizieren, muss man Next-Generation Firewalls (NGFW) mit Deep Packet Inspection einsetzen. Diese Firewall kann auch den Inhalt der Nachrichten anschauen und somit gefährlichen Code entdecken.

Egal welche Art von Firewall eingesetzt wird: Eine falsch konfigurierte Firewall oder eine Firewall die nicht gewartet wird, deren Regeln also nicht permanent auf die neuesten Bedrohungen angepasst wird, kann in gewisser Weise schlimmer sein als eine fehlende Firewall. Dies, weil sie den gefährlichen Eindruck von Sicherheit vermittelt, während sie wenig oder gar keine bietet.

Daher gibt es heute Ansätze, die Intrusion Detection (IDS) oder gar Intrusion Prevention (IPS) implementiert haben. Solche Ansätze erlauben es auch, die Gesamtsicherheit eines Netzes (gegen interne und externe Angriffe) zu gewährleisten. Diese werden als Bedrohungsorientierte NGFW und Unified Threat Management (UTM) bezeichnet.

Ein modernes Schutzsystem für das Netz gegen innere und äussere Bedrohungen weist somit die folgenden Eigenschaften auf:

Intrusion Detection and Prevention

Managed Security (im Sinne von Wartung und Unterhalt der Firewallregeln)

Zentrale Wartung aller Sicherheitsrelevanten Parameter

Verbindung zu Vulnerabilitätsdatenbanken wie zum Beispiel <https://cve.mitre.org>. Auch die Analyse der Sicherheitsmeldungen in Melani des Bundes (<https://www.melani.admin.ch/melani/de/home.html>) hilft bei der Wartung der Sicherheitssysteme im Netz.

Im Folgenden werden die Firewall-Typen genauer erklärt.

4.2.1 Packet filter Firewalls

Dieser Firewall-Typ arbeitet auf Routern oder wird auf Linux/Unix-Systemen (zum Beispiel kleinen «embedded systems» wie Banana Pi Router R2) als Software installiert (zum Beispiel pfsense oder IPFire).

Das Grundprinzip dieser Variante ist, dass die Pakete mit bestimmten Regeln verglichen werden. Sollte die Prüfung eine Verletzung einer Regel bemerken, wird das Paket nicht weitergeleitet.

Überprüft werden die Ziel- und Ursprung-IP-Adressen, die Portnummern (siehe Liste der standardisierten Ports für UDP und TCP, zum Beispiel 22 für Secure Shell, SSH) und die Protokollnummern (siehe Liste der Protokollnummern, zum Beispiel Protokollnummer 1 für das ICMP-Protokoll).

Bei diesen Firewall wird bevorzugt das Prinzip eingesetzt, dass grundsätzlich alle Ports geschlossen sind und nur das Erlaubte geöffnet wird.

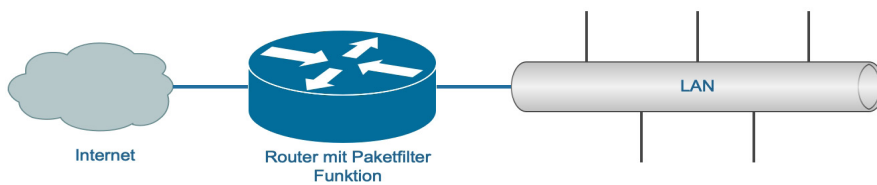


Bild 3: Packet Firewall

4.2.2 Verbindungs Gateways (Circuit Level Gateways)

Dieser Typ Firewall trennt zwei Netze auf Layer 4 des ISO-OSI-Layern. Zum Beispiel wird das Interne LAN vom Internet oder zwei LAN-Subnetze die unterschiedliche Sicherheitsanforderungen haben getrennt.

Sie überwachen die TCP-Daten im gesamten Netzwerk und identifizieren bösartige Inhalte relativ schnell. Sie basieren darauf, dass sie eine gestartete Sitzung überprüfen und das Zielsystem als vertrauenswürdig angesehen wird. Damit lassen sich auf einer Firewall beliebige IP-Adressen und Ports sperren oder freischalten. Sie sind allerdings nicht in der Lage, die Paketinhalte selbst zu kontrollieren. Man kombiniert solche Gateways daher oft mit Paketfiltern oder anderen Firewall-Typen.

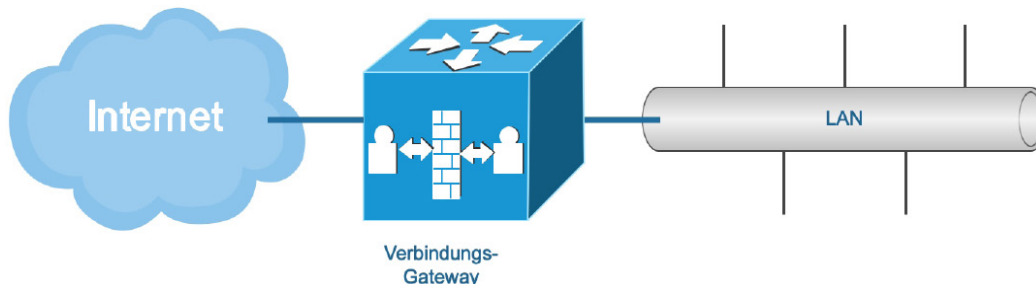


Bild 4: Verbindungsgateway

4.2.3 Application Level Gateways

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.

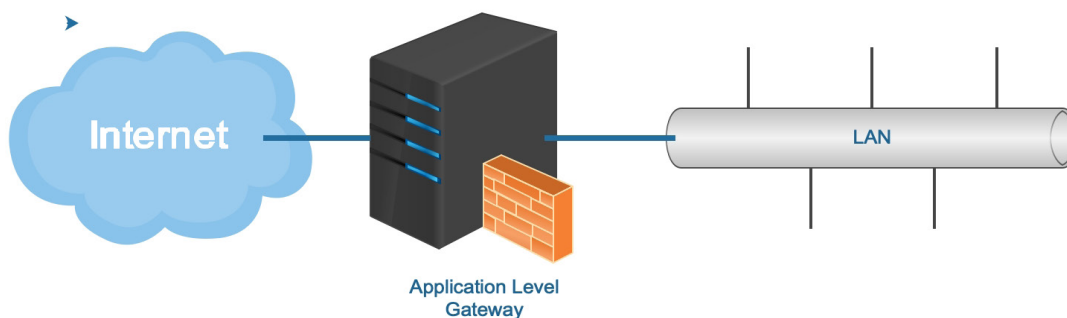


Bild 5: Application Level Gateway

4.2.4 Stateful Inspection Firewalls

Man kann diesen Typ Firewall als Kombination der Paketfilter mit den Gateways betrachten. Sie untersuchen daher nicht nur jedes Paket, sondern auch, 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 benutzt Regeln auf der Basis von Protokoll, Port sowie Quell- und Zieladresse. Die Firewall kann schnell verifizieren, ob neue eingehende Pakete den Kriterien für autorisierten Verkehr entsprechen oder nicht. Pakete, die nicht Teil einer autorisierten Sitzung sind, werden abgewiesen.

Solche Firewalls sind oft so aufgebaut, dass ein erster Gateway die Demilitarized Zone (DMZ) schützt und eine weiterer, nachgeschalteter Gateway dann das LAN abschirmt. In der DMZ werden dann die von aussen sichtbaren Services (Webserver, Mailserver) betrieben.

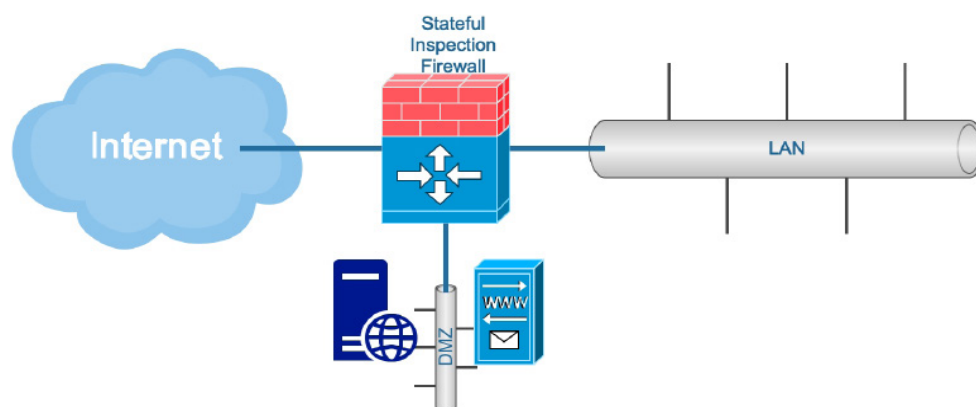


Bild 6: Stateful Inspection Firewall

4.2.5 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.

4.2.6 Bedrohungsorientierte NGFW und Unified Threat Management (UTM).

UTM Systeme können die folgenden Features beinhalten:

- Firewalls
- Intrusion Detection Systeme (IDS)
- Intrusion Prevention Systeme (IPS)
- Antiviren-Gateways, -Scanner und -Protectionssysteme
- Internet-Gateways

- VPN Gateways (Virtual Private Network Gateways)
- Spamfilter
- Contentfilter
- Proxy-Funktionen
- Network Address Translation (NAT)
- Authentifizierungssysteme
- Verschlüsselungssysteme
- Quality of Service Funktionen (QoS)
- Reportingfunktionen

Grundsätzlich sind Bedrohungsorientierte Next Generation Firewall und UTM Systeme sehr weit entwickelte Gesamtsicherheitslösungen für Netze, die nur noch von Spezialisten gewartet werden können und teilweise direkten On-line Zugang haben zu Vulnerabilitätsdatenbanken und Warnsystemen bezüglich Internetattacken. Auch gegen interne Hackereien sind diese Firewalls sehr gut geschützt.

4.3 Gängige Darstellungsarten und Symbole für Netzwerkplan und Netzwerkschemata.

LB1: Präsentationen erstellen und halten. (2 Lektionen)

Logische Netzwerkschemata sind möglichst hierarchisch darzustellen. Entweder von oben nach unten oder von links nach rechts. Sich kreuzende Linien bei den Verbindungsleitungen sind unschön und zu vermeiden.

Die Hierarchie besteht in einem Datacenter oder Enterprise Network immer aus den Core-Komponenten, den Aggregation/Distribution-Komponenten und den Access-Komponenten. Komponenten können sowohl Router wie auch Switches oder Firewall sein.

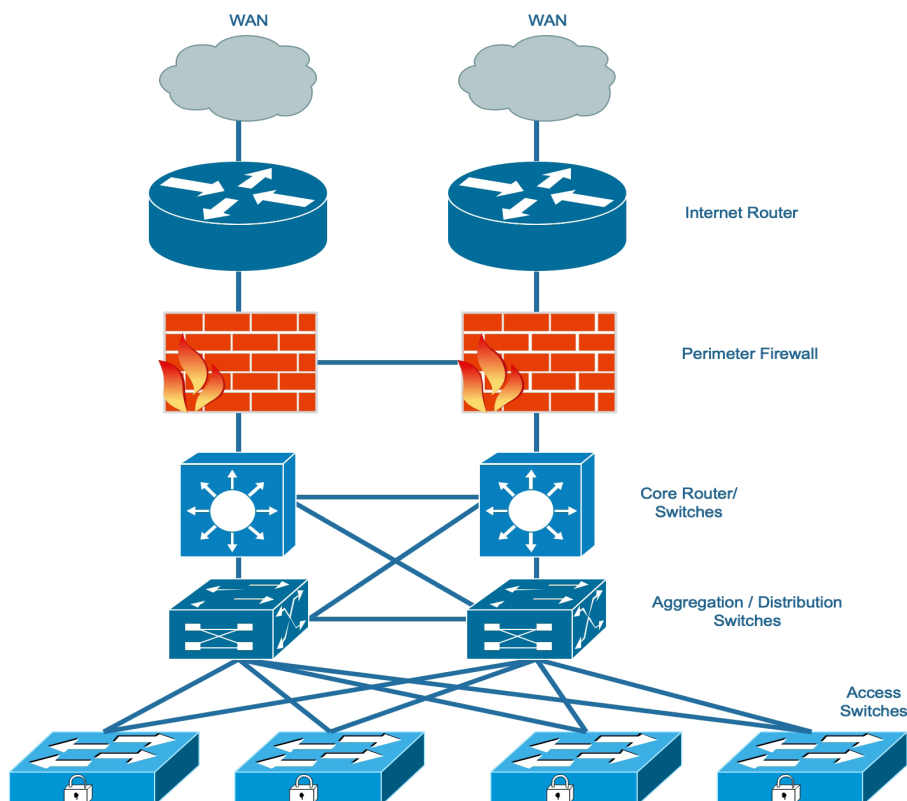


Bild 7: Netzwerkplan

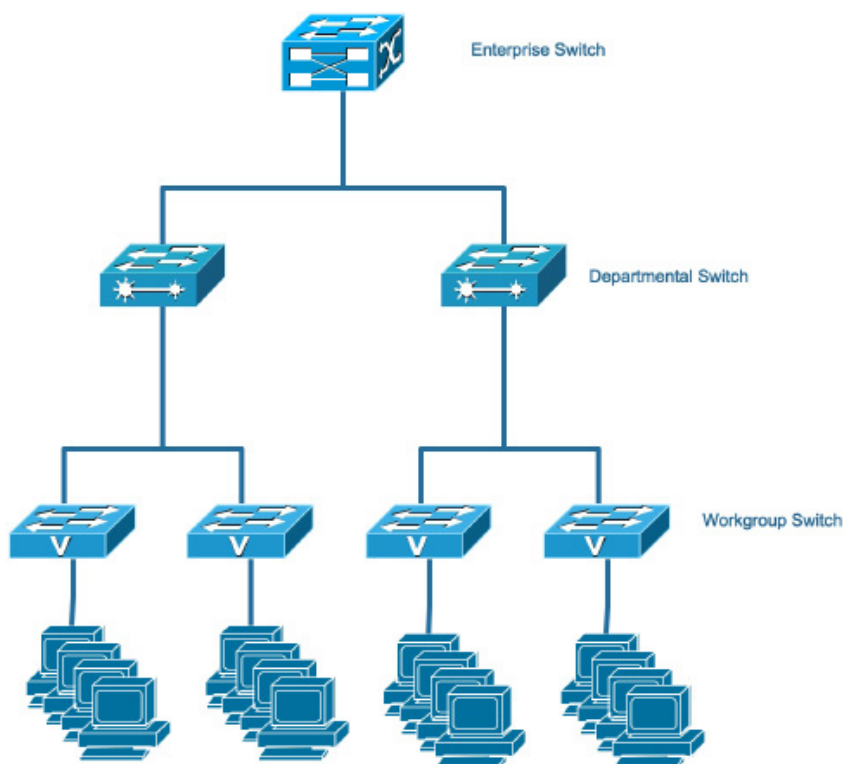
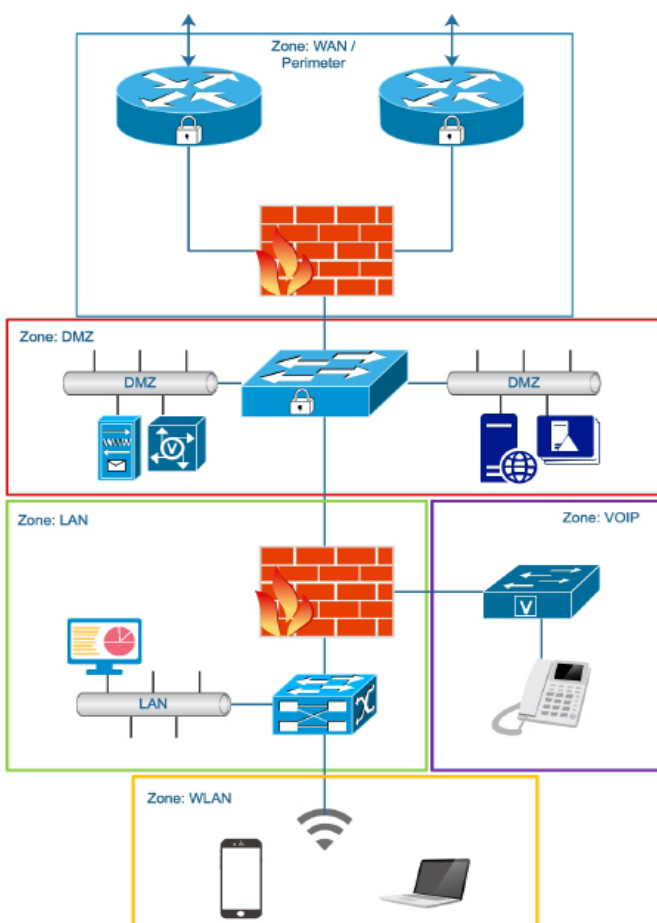


Bild 8: Netzwerkstruktur

In kleineren Netzen werden Hub-Tree (Baumstrukturen) gezeichnet. Meistens sind diese Baumstrukturen 2 Stufig und nur in grösseren Netzen 3-Stufig ausgeführt. Man spricht dann von Enterprise Switches in der obersten Hierarchiestufe, von Departmental Switches in der mittleren Hierarchiestufe und von Workgroup Switches in der untersten Hierarchiestufe.



Hier ein einfacher Zonenplan einer kleinen Firma mit einer stateful inspection Firewall. Die 5 Zonen Wide Area Network (WAN), Demilitarised Zone (DMZ), Local Area Network (LAN) Voice over IP (VOIP) und Wireless LAN (WLAN) bezeichnen vier unterschiedliche Sicherheitszonen.

In der DMZ befinden sich in der Regel die Server, die von aussen gut zugreifbar sein müssen, deren Regeln somit einen Zugriff von aussen erlauben, wie zum Beispiel Webserver, Mailserver und Intrusion Detection.

Bild 9: Einfacher Zonenplan

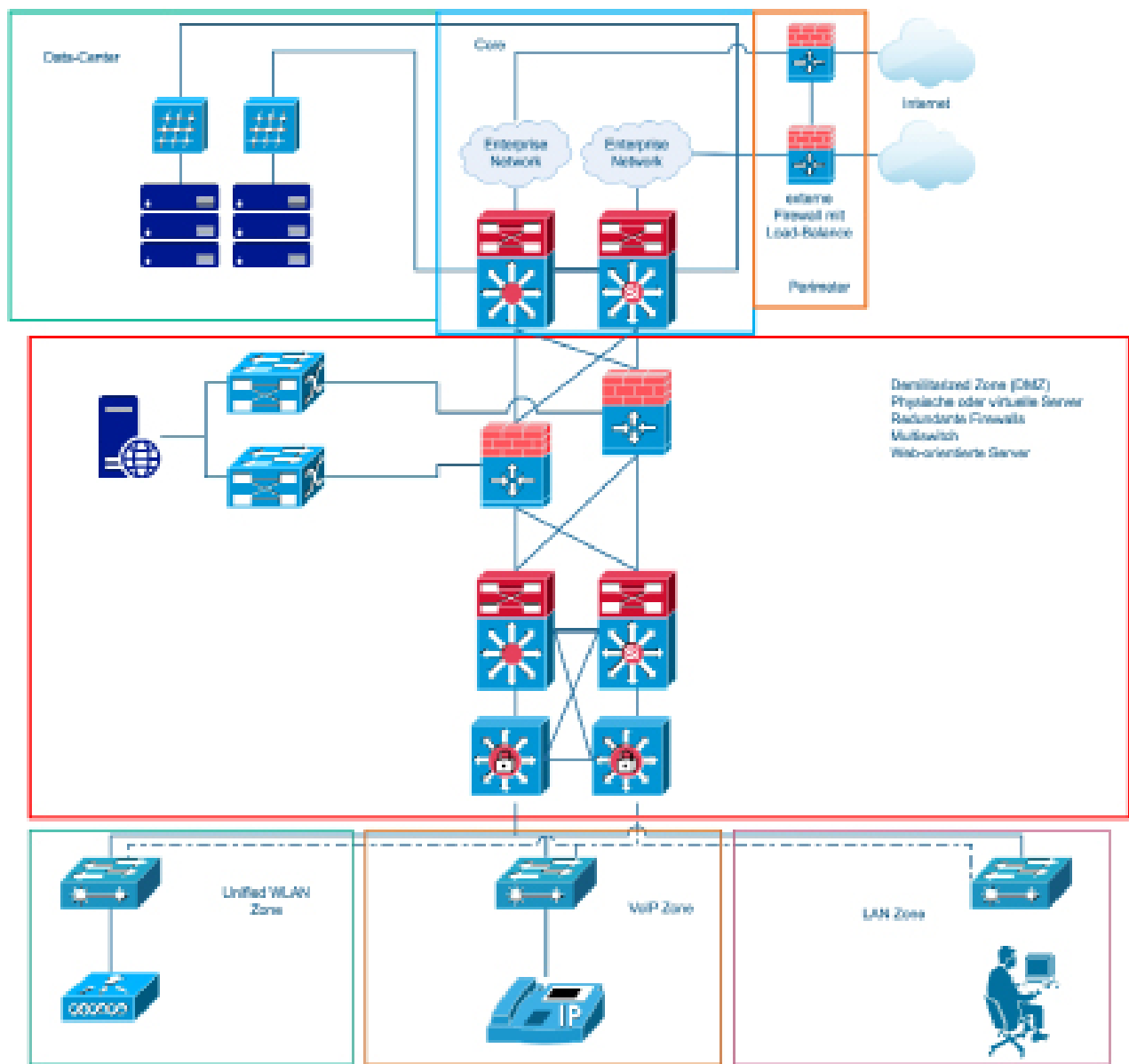


Bild 10: komplexere Zonenpläne

Sollen Zonenpläne gezeichnet werden gilt diese Regel der Hierarchie weiterhin. Innerhalb der Zonen soll es ebenfalls keine gekreuzten Linien geben.

Solche komplexen Zonenpläne finden sich in grösseren Firmen und dienen dazu, die unterschiedlichen Sicherheitszonen oder VLAN-Zonen zu unterscheiden.

5. Hardware- und Softwarekomponenten bestimmen und einen Beschaffungsantrag erstellen.

Hardware- und Software-Komponenten bestimmt man erst, wenn man eine Umsetzungsvariante gefunden hat. Die Umsetzungsvariante findet man durch eine Evaluation (siehe Kapitel 2).

5.1 LB2

An dieser Stelle wird die LB2 abgegeben.

5.2 Aufbau und Inhalt eines Beschaffungsantrags aus der durchgeführten Evaluation.

Zu beachten gilt, dass öffentliche Stellen die Beschaffung unter Umständen ausschreiben müssen, das heisst, dass je nach Grösse der Beschaffung ein Beschaffungsverfahren durchgeführt werden muss. Die folgende Bilder sind ein Beispiel des Bundesamtes für Strassen (ASTRA). Versuchen Sie ein ähnliches Formular zu erstellen für die KMU oben.


 Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra		Bundesamt für Strassen ASTRA	
Beschaffungsantrag			
Laufweg:	Antragsteller/in: <input type="text"/>		Abt./Bereich: <input type="text"/>
	Datum: <input type="text"/>		<input type="checkbox"/> DL/Produkt
	<input type="checkbox"/> Informatik		<input type="checkbox"/> Nachtrag
	1. Was soll beschafft werden?		
	Beschreibung der zu beschaffenden Dienstleistung / des zu beschaffenden Produktes: <input type="text"/>		
	Kostenvoranschlag CHF inkl. 8% MwSt: <input type="text"/> [Betrag]		
	Vorschlag Lieferant/en: <input type="text"/> [Vorschlag Lieferanten]		
	Kredit:		
	<input type="checkbox"/> A6100.0001 Globalbudget Erfolgsrechnung (ER) <input type="text"/> (Kostenart/Sachkto. Budget)		
	<input type="checkbox"/> A8100.0001 Globalbudget Investitionsrechnung (IR) <input type="text"/> (Kostenart/Sachkto. Budget)		
<input type="checkbox"/> andere: <input type="text"/> [Beschrieb] (Kostenart/Sachkto. Budget)			
Abwicklung via:		<input type="checkbox"/> TDcost (nur Nationalstrassenrechnung)	
		<input type="checkbox"/> SRM (bundesintern, z.B. BIT, BBL)	
		<input type="checkbox"/> SAP (für alle sonstigen Fälle)	
Beschaffungsverfahren: <input type="checkbox"/> Freihändig <input type="checkbox"/> Einladung <input type="checkbox"/> Selektiv <input type="checkbox"/> Offen			
<input type="checkbox"/> Begründung für freihändiges Verfahren liegt bei (wenn Betrag ≥ CHF 50'000 bei Lieferungen; ≥ CHF 150'000 bei Bau- oder Dienstleistungen Ausnahmen Art 13 bzw. 36 VoeB)			
Für den Antrag: Datum/Visum Antragsteller/in: <input type="text"/>			
Vorge-setzer	Linienvorgesetzter <input type="text"/>		FC / L VMZ <input type="text"/>
	immer (Datum/Visum): <input type="text"/>		(Datum/Visum): <input type="text"/>
Achtung: wenn Antragsteller = Filiale od. VMZ + Papier-Laufweg erwünscht: weiterleiten via Fabasoft an Ass AC UN (diese druckt aus und führt d. Beschaffungsantrag über Laufweg, inkl. Beilagen).			

Bild 11: Beschaffungsantrag des Bundes

Ab hier **entweder** von Hand ausfüllen (Papier-Laufweg) **oder** auf Fabasoft-Laufweg senden!

*A Fachbereich Beschaffungs- und Vertragswesen (FBV)	Immer: (Stellungnahme mit Handlungsanweisungen, Datum, Visum):	
Kreditinhaber	Sind diese Aufwendungen budgetiert? (Datum, Visum):	<input type="checkbox"/> ja <input type="checkbox"/> nein
Informatik-Controlling-Beauftragter	Immer: Betrifft die Beschaffung Informatik? (Handlungsanweisung, Datum, Visum)	<input type="checkbox"/> ja <input type="checkbox"/> nein Sachkontonummer:
Finanzen + Controlling	Immer: (Freigeben und Auftragsnummer eintragen, Datum, Visum)	

Retour an Antragsteller (wenn Filiale/VMZ: retour an Ass AC IN, diese führt nach Rücksprache mit Antragsteller mit Punkt 2 weiter).

Ab hier in jedem Fall von Hand ausfüllen und auf Papier-Laufweg senden (kein Fabasoft-Laufweg!)

2. Freigabe Beschaffungsverfahren (nicht nötig bei freihändigem Verfahren)

AC	Einverstanden (Datum/Visum):	
Direktor	Einverstanden (nur wenn gem. UKR Vertragsunterzeichnender):	

Retour an Antragsteller (wenn Filiale/VMZ: retour an Ass AC IN) zur Durchführung des Beschaffungsverfahrens.

FBV	(nur wenn nicht Freihändig) bestätigt <input type="checkbox"/> ja <input type="checkbox"/> nein (siehe Beilage)
BL SI	Nur bei Informatikbeschaffungen: (Datum/Visum):
AC	Einverstanden (Datum/Visum):
Direktor	(Datum/Visum, nur wenn durch UKR verlangt):

*C FBV	4. Vertragsfreigabe	Vertrag i.O. zur Unterschrift gemäss UKR: (Datum/Visum FBV):
--------	---------------------	--

Vertrag mit Beschaffungsantrag retour an Antragsteller (wenn Filiale/VMZ: retour an Ass AC IN). Weiter wie folgt: Vertrag unterzeichnen lassen und unterschriebenen Vertrag einscannen und in Fabasoft ablegen, Original-Vertrag und Original-Beschaffungsantrag immer an F+C leiten

Einzureichende Unterlagen und Hinweise zu den einzelnen Unterschriften des Fachbereichs Beschaffungs- und Vertragswesen (FBV)

Unter-schrift FBV	Freihändiges Verfahren			Einladungs-Verfahren	Offenes/selektives Verfahren
	bis CHF 50'000 (Lieferung) resp. bis CHF 150'000 (Dienstleistung)	ab CHF 50'000 (Lieferung) resp. ab CHF 150'000 (Dienstleistung) bis CHF 230'000	ab CHF 230'000	ab CHF 50'000 (Lieferung) resp. ab CHF 150'000 (Dienstleistung) bis CHF 230'000	ab CHF 230'000 (Dienstleistung, Lieferung)
*A	<input type="checkbox"/> Offerte	<input type="checkbox"/> - Offerte - Begründung Art. 13/36 VoeB	<input type="checkbox"/> - Offerte - Begründung Art. 13/36 VoeB - Hinweis: Publikation notwendig!	<input type="checkbox"/> - Namen der Anbieter - Pflichtenheft	<input type="checkbox"/> - Ausschreibungsunterlagen - SIMAP-Ausschreibungstext
*B			<input type="checkbox"/> - Zuschlagspublikation (PDF) - Hinweis: Einsicht FBV vor Publikation!	<input type="checkbox"/> - Offerten - Evaluationsbericht und Beilagen	<input type="checkbox"/> - Offerten - Evaluationsbericht und Beilagen - SIMAP-Text des Zuschlages - Hinweis: für Debriefing FBV beziehen
Achtung: Vertragsunterzeichnung nur bei vollständigen Visas auf Beschaffungsantrag!					
*C	<input type="checkbox"/> Vertrag	<input type="checkbox"/> Vertrag	<input type="checkbox"/> Vertrag (nicht unterschreiben, bevor die Rechtsmittelfrist abgelaufen ist [20 Tage Beschwerdefrist, 1 Woche Zuwartefrist])	<input type="checkbox"/> Vertrag	<input type="checkbox"/> Vertrag (nicht unterschreiben, bevor die Rechtsmittelfrist abgelaufen ist [20 Tage Beschwerdefrist, 1 Woche Zuwartefrist])

Tabelle 6: Beschaffungswesen des Bundes

Eine mittelständische Firma hat einen neuen Bedarf betreffend der Internetanbindung. Die aktuelle Konfiguration ist schon einige Jahre in Betrieb und wurde für ca. 20 PCs ausgelegt. Bis heute ist die Firma sehr gewachsen und hat gemäss Inventar 72 PCs, 36 WLAN Devices (Laptop, Tablets und Smartphones) und eine TVA für den gesamten Gesprächsverkehr intern und extern (nur VoIP mit fixen Geräten über LAN und Funktelefone über WLAN).

Auch sollen die intern neu installierten Dienste wie einfachen Webaufttritt, Web-Shop mit Datenabgleich zu interner Finanz-Applikation und einem E-Mail-Server mit integriert werden. Dabei hat die Sicherheit höchste Priorität.

Alle angeschlossenen PC's und WLAN Devices haben Zugriff auf die Shares (SMB) und die Printer. Auch sind die neuen oben beschriebenen Dienste von überallher erreichbar.

Ihre Rolle ist es, als Beauftragten diese Arbeiten auszuführen. Das beinhaltet die Planung, den Einkauf, die Realisierung, das Testen und die Abgabe an den Kunden.

Die Anbindung an das Internet wurde mit dem ISP folgendermassen vereinbart.

- FTTH über Swisscom
- 250/250 Mbit/s Übertragungsrate
- UTM Security Device
- LAN Switch mit 48 Ports, VLAN für Internet, VLAN für Voice, VLAN für internen IP Traffic, VLAN für Management.

Formulieren Sie einen Beschaffungsantrag für die KMU oben. Bestimmen Sie geeignete Komponenten für die Internetanbindung der KMU in der LB2.

5.3 Simulations-Plattformen

Die folgenden Simulationsplattformen sind zur Lösung der LB2 zu empfehlen:

EVE NG: <https://www.eve-ng.net>

Filius: <http://www.lernsoftware-filius.de>

GNS3: <https://www.gns3.com>

Firewalls:

OPNSENSE: <https://opnsense.org>

PFSense: <https://www.pfsense.org>

6. Inbetriebnahme der Internetanbindung realisieren und eine Abnahme durchführen.

Dies ist der Praxisteil, der mit Hilfe der LB2 bearbeitet werden soll. Die Anmerkungen zu den einzelnen

6.1 Vorgehen für die Planung und Inbetriebnahme des Internetzugangs.

Die Planung soll grundsätzlich mit einer in der Praxis gebräuchlichen Projektmanagementmethode erfolgen. Wir benutzen IPERKA falls keine andere Methode zur Wahl steht.

Geplant und begründet werden müssen mindestens die folgenden Punkte:

- Netzwerkplan eventuell mit Zonenplan
- Ressourcen: wer macht was?
- Zeitplan: wann soll was gemacht werden?
- Materialliste: Welche Geräte und welches Material wird benutzt und muss zur Verfügung stehen?
- Konfigurationsfiles für die Router, Switches und Firewall
- Beschaffungsantrag

6.2 Vorgehen für die Übergabe des Systems in den operativen Betrieb.

Zu einer erfolgreichen Übergabe gehört, dass eine Schulung erfolgt, dass die notwendigen Anleitungen vorliegen, dass Wartung und Support bekannt sind und dass die Sicherheit der Installation gewährleistet ist.

Beachten Sie diese Punkte in Ihrem Abnahmeprotokoll in LB2.

6.3 Aufbau und Inhalt eines Abnahmeprotokoll

Die Übergabe an den Betrieb erfolgt mit Hilfe eines User Acceptance Tests. Der Test weist mindestens nach, dass alle Funktionen einwandfrei zur Verfügung stehen. Die User entlasten die Projektverantwortlichen danach mit einem Abnahmeprotokoll. Dieses Abnahmeprotokoll soll die Testergebnisse festhalten und zusammen mit den oben erwähnten Übergabetätigkeiten dem Kunden überreicht werden.

Abnahmeprotokolle können etwa folgendermassen aussehen:

Abnahmeprotokoll		Datum:	Uhrzeit	von - bis
Bauvorhaben:			Auftrag vom:	

Gewerk:		Beginn:	
Auftraggeber:		Fertigstellung:	
Auftragnehmer:		Vertragl. vereinb. Fertigstellung:	
Teilnehmer:		Terminüberschreitung:	

Lfd. Nr.	Übergabe folgender Unterlagen, Plänen, Schlüssel usw.
	<input type="checkbox"/> weiteres siehe Anlage

Bei der Abnahme wurden die folgenden Mängel festgestellt. Diese Mängel sind unverzüglich spätestens bis zum zu beseitigen. Sofern der Auftragnehmer nicht innerhalb der vorgenannten Frist die Mängel beseitigt, ist der Auftraggeber berechtigt, auf Kosten des Auftragnehmers die Mängelbeseitigung vorzunehmen bzw. durch Dritte vornehmen zu lassen. Alle Ansprüche des Auftraggebers auf Gewährleistung und Schadenersatz bleiben unberührt.

Lfd. Nr.	Mangel bzw. unvollständige Leistung
	<input type="checkbox"/> weitere Mängel siehe Anlage

☐ Die Abnahme der Leistungen wird wegen der vorgenannten Mängel verweigert.
☐ Der Auftraggeber behält sich die Geltendmachung der vereinbarten Vertragsstrafe vor.
☐ Die Leistungen werden abgenommen unter Vorbehalt der aufgeführten Mängel.
☐ Frist für die Gewährleistung der abgenommenen Leistung: Beginn: Ende:

den

Auftraggeber:	Auftragnehmer:
---------------	----------------

Bild 13: Abnahmeprotokoll

Lösungen

1. Aufgabe 1

Übertragungsrate /Technologie	Verfügbarkeit	Mengen	Tätigkeit
50/5 Mb/s / DSL	niedrig	1 - 10	(I)
50/5 Mb/s / DSL	niedrig	50 - 100	(I)
100/10 Mb/s / DSL	mittel	10 - 50	(II)
500/500 Mb/s / Fibre	mittel	> 500	(II)
100/100 Mb/s / Fibre	hoch	10 - 50	(III)
100/100 Mb/s / Fibre	hoch	50 - 100	(III)
500/500 Mb/s / Fibre	sehr hoch	100 - 500	(IV)
1000/1000 Mb/s / Fibre	sehr hoch	> 500	(IV)

2. Aufgabe 2

a) Abgekürzte Formel ohne MTBF

b) DSL ist eine Technologie, die eine schlechte Verfügbarkeit hat.

c) 1 Monat

3. Aufgabe 3

a) Es sind 5 URL gesucht und die jeweiligen Berechnungen. Die meisten URL werden das folgende Resultat berechnen:

pro Tag	pro Woche	pro Monat	pro Jahr
79,16667 %	97,02381 %	99,30556 %	99,94292 %

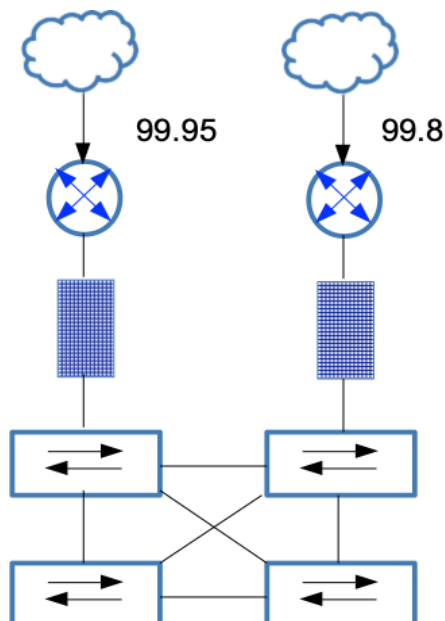
b) nicht beschränkt auf die Arbeitszeit

c) Alle diese Rechner basieren nicht auf gemessenen Zahlen, sondern nur auf dem Verhältnis der Ausfallzeiten pro Monat oder Jahr.

d) Nein, keine Berechnung auf Grund MTBF und MTTR.

4. Aufgabe 4

Skizze:



Geräte hintereinander:

Ausfallrisiko links (AL):

$$AL = 0.05 + x + x$$

Ausfallrisiko rechts (AR):

$$AR = 0.2 + x + x$$

Redundanz:

$$AL * AR = 0.5 = (0.05 + 2x) * (0.2 + 2x) = 0.05 * 0.2 + 0.05 * 2x + 0.2 * 2x + 2x * 2x =$$

$$AL * AR = 0.01 + 2x * (0.05 + 0.2) + 4x^2 = 0.5$$

$$4x^2 + 0.5x - 0.49 = 0$$

$$x_1 = (-0.5 + (0.5^2 - 4 * 4 * -0.49)^{1/2}) / 2 * 4 = (-0.5 + (0.25 + 7.84)^{1/2}) / 8 = 0.293$$

$$x_2 = (-0.5 - (0.5^2 - 4 * 4 * -0.49)^{1/2}) / 2 * 4 = (-0.5 - (0.25 + 7.84)^{1/2}) / 8 = -0.418$$

Das mögliche Gesamtausfallrisiko ist demnach 0.293 pro Router oder Firewall.

Die Verfügbarkeit dieser Geräte kann demnach bis $100 - 0.293 = 99.707\%$ sein.

5. Aufgabe 5:

a) In diesem Beispiel wird eine DSL basierte Lösung mit einem Packet-Filter-Router genügen, mit einer Übertragungsrate von 50/5 Mbps.

b) Für 20 Mitarbeitende genügen 50/5 Mbit/s Übertragungsrate, da keine besonders anspruchsvollen Dienste genutzt werden sollen und alle Services beim ISP gehostet sind. Die Verfügbarkeit des Internetanschlusses ist mit dieser einfachen Anschlussart gewährleistet, da notfalls die Services via Hotspot erreicht werden können. Da die Services beim Provider laufen, ist deren Verfügbarkeit gegeben. Eine einfache Packet Filter Firewall ist genügend, weil die Services durch den ISP geschützt werden.

6. Aufgabe 6:

a) Eine DSL basierte Lösung kann immer noch genügen. Die Übertragungsraten soll mindestens 100/10 Mbps betragen. Ein FTTH Anschluss mit einer symmetrischen Übertragungsrate von 100/100 wäre, falls erhältlich, zu bevorzugen. Für die Sicherheit soll eine managed Firewall oder ein moderner Security Gateway eingesetzt werden.

b) Für 100 Mitarbeitende genügen 50/5 Mbit/s Übertragungsrate nur knapp, da hier allenfalls besonders anspruchsvollen Dienste genutzt werden sollen. Die Verfügbarkeit des Internetanschlusses ist mit dieser einfachen Anschlussart trotzdem gewährleistet. Ein FTTH Dienst würde eine bessere Verfügbarkeit bieten. Da die Services beim Provider laufen, ist deren Verfügbarkeit gegeben. Eine managed Firewall ist genügend, weil die Services durch den ISP geschützt werden.

7. Aufgabe 7:

a) Welche Internetanbindung schlagen Sie vor? (Technologie, Sicherheit, Übertragungsrate)

Diese Aufgabe ist individuell zu lösen und basiert auf der Theorie in Kapitel 1.

b) Begründen Sie Ihren Vorschlag indem Sie die Aspekte der Übertragungsrate, der Verfügbarkeit und der Sicherheit in Ihrer Begründung erwähnen.

Begründung: Es wurde die Technologie (z.B. FTTH) gewählt, weil die Übertragungsrate von 100/100 Mbps für die beschriebene Umgebung gefordert wird. Die Sicherheit muss mit einer Firewall und Sicherheitsvorschriften geregelt werden, weil das Unternehmen kritische Daten besitzt. Die Verfügbarkeit soll mit Redundanzen erreicht werden, weil die Firma bereits bei einem Ausfall von 1 Minute einen kritischen Zustand erreicht.

8. Aufgabe 8 (nur für Cracks):

Sie sollen die Sicherheit einer Internetanbindung einer KMU beurteilen.

Hier müssen alle Aspekte im Buch hinreichend erläutert werden. Lösung individuell.

9. Aufgabe 9:

Welche Teile des FCAPS werden für die Sicherheits- und Überwachungsfunktion eines Internetanschlusses benutzt? Begründen Sie Ihre Wahl.

Faultmanagement, weil es die Fehler erkennt, Accounting, weil dort auch Unregelmässigkeiten in der Nutzung festgestellt werden können. Performance, weil Unregelmässigkeiten in der Performance oft einen Hinweis geben auf sicherheitsrelevante Vorkommnisse. Security Management, weil dieses die Sicherheit überwacht.

10. Aufgabe 10 (für Cracks):

Ein Betrieb hat einen Fibre-Anschluss 100/100 Mbit/s bei einem Provider. Der Provider hat dem Betrieb einen Router gestellt. Der Betrieb hat von einem anderen Anbieter eine Firewall mit Intrusion-Detection/-Prevention (IDPS) gekauft und in Betrieb genommen.

a) Welche Sicherheitsmassnahmen empfehlen Sie dem Betrieb? Nennen Sie mindestens 5 Massnahmen die Sie ergreifen müssen, um eine gute Sicherheit im Betrieb dieses Anschlusses zu gewährleisten. Hilfe: Suchen Sie Informationen zu Sicherheitsmassnahmen, securitypolicy, Schulung der Mitarbeiter im Zusammenhang mit Gefahren aus dem Internet, Sicherung der Vertraulichkeit, Integrität und Verfügbarkeit bei Internetanschlüssen. Antworten Sie in ganzen Sätzen und strukturieren Sie Ihre Antwort.

Es wird hier erwartet, dass Sie eine Lösung auf der Basis ISO 27000 oder BSI abliefern, individuell.

b) Was würden Sie überwachen bei diesem Internetanschluss? Beschreiben Sie zuerst was Sie überwachen wollen und danach wie Sie diese Überwachung realisieren wollen.

Überwacht werden muss der interne und der externe Verkehr. Dies wird heute mit IDPS und NGFM/UTM erreicht.

11. Aufgabe 11:

Zwingend notwendig: Lastenheft/Pflichtenheft, Projektorganisation (Ressourcen, Budget, Termine), Netzplanung, SLA, Wartung/Support-organisation, Betriebsorganisation.

12. Aufgabe 12 (für Cracks):

individuell, bitte mit Lehrer besprechen.

13. Aufgabe 13

Individuell - siehe Lösung LB1

14. Aufgabe 14 (für Cracks)

individuell.

Anhang Nachrichtentechnik

Bandbreite, Übertragungsrate

Leider bieten die Internet Service Provider (ISP) die Übertragungsrate, also die Geschwindigkeit mit der Daten vom Endkunden zum oder vom ISP transportiert werden als «Bandbreite» an.

Diese Angabe ist aber falsch.

Die Übertragungsrate (data transfer rate) ist gemäss «ITU Terms and Definitions» definiert als:

«Sector : Standardization (ITU-T)

Abbreviation : None

Term : effective data transfer rate

Definition : The average number of bits, characters, or blocks per unit time transferred from a data source to a data sink and accepted as valid. It is expressed in bits, characters, or blocks per second, minute, or hour.»

Somit hat die Übertragungsrate die Einheit Bit pro Sekunde oder oft Megabit pro Sekunde (bit/s oder Mbit/s).

Bandbreite hingegen ist ein Begriff aus der Nachrichtentechnik und ist gemäss ITU Terms and Definitions definiert als:

«Sector : Radiocommunication (ITU-R) - Recommended

Abbreviation : None

Term : (frequency) bandwidth

Definition : Rec. ITU-R V.662-3 - The quantitative difference between the limiting frequencies of a frequency band. Note 1 - The term «bandwidth» is usually associated with a qualification, for example: - baseband bandwidth - necessary bandwidth - bandwidth of an amplifier or other device. Note 2 - A bandwidth is defined by a single value and does not depend upon the position of the band in the frequency spectrum. This usage is not recommended.»

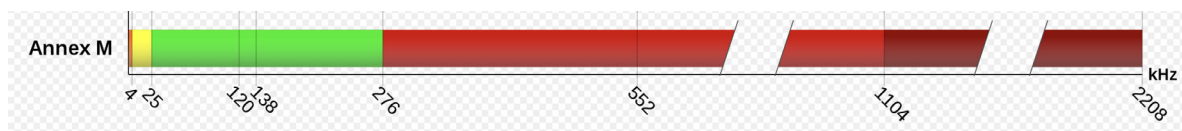
Die Einheit der Bandbreite ist Herz (Hz).

Der Zusammenhang zwischen Bandbreite und Übertragungsrate besteht darin, dass ein Telekommunikationsanbieter die Nachrichtentechnik (Bandbreite) benutzt um auf zwei Kupferdrähten oder einem Koaxialkabel oder neuerdings auf Glasfaserleitungen eine Übertragungsrate für Ethernet und TCP/IP Signale zum Modem des Kunden bereitzustellen.

Zwei Kupferdrähte (zum Beispiel mit ADSL):

Ein Modem beim Provider (Digital Subscriber Line Access Multiplexer, DSLAM) benutzt die Bandbreiten xxx bis zum Modem des Benutzers (das Modem ist im DSL-Router integriert und befindet sich gleich hinter dem Anschluss der Telefondrähte).

Die Bandbreiten (Frequenzbereiche) die ein DSL nach ITU-T G.992.5 Annex M benutzt wäre zum Beispiel:



Die ersten 4 kHz werden von der alten Telefonie belegt, bis 25 kHz wird nicht verwendet, damit die Telefonie und die Datenübertragung sich nicht stören. Von 25 kHz bis 276 kHz steht ein Kanal für den Upstream mit einer Bandbreite von 251 kHz zur Verfügung. Von 276 kHz bis 2208 kHz, also mit einer Kanal-Bandbreite von 1932 kHz, befindet sich der Downstream. Das macht deutlich, warum der Upstream und der Downstream bei DSL nicht symmetrisch sein kann. Auf der Upstreambandbreite von 251 kHz können 3.5 Mbit/s übertragen werden und auf der Downstre-

ambandbreite von 1932 kHz werden gemäss Norm 24 Mbit/s übertragen.

Normalerweise kann man mit einem Hz ein Bit übertragen (Nyquist-Shannon-Abtasttheorem). Nachrichtentechnische Methoden wie Quadratur Amplituden Modulation (QAM) oder Kanalbündelung erlauben es aber, dass pro Hz mehrere Bit übertragen werden können und somit höhere Übertragungsraten erzielt werden können.

Wichtig ist noch, dass die 24 Mbit/s nur in der Nähe der Zentrale des Providers erreicht werden können. Aus physikalischen Gründen nimmt die erzielbare Übertragungsrate mit der >Distanz rasch ab.

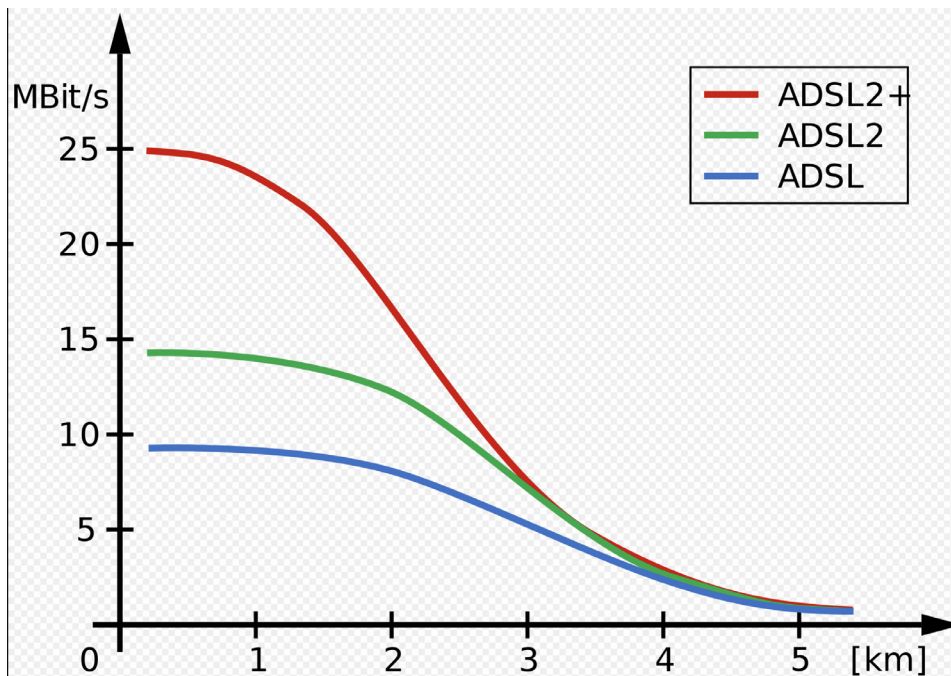


Bild 14: Zusammenhang Übertragungsrate - Distanz

Beim Data Over Cable Service Interface Specification (DOCSYS) Kabelmodem ist die Art der Übertragung ähnlich. Ein TV Kanal hat eine Bandbreite von ca 8 MHz. Durch Kanalbündelung und QAM-4096 Technologien und 20 kHz bis 50 kHz Trägerbandbreite erzielt man hier momentan bis 10 Gbit/s Downstream-Übertragungsraten. Der Upstream ist allerdings nur bei etwa 1 Gbit/s. Die Übertragungsdistanz kann hier bis 150 km betragen.

Die effektiven Übertragungsraten hängen aber stark von der Qualität der jeweiligen Netze der Provider ab und betragen heute 500 Mbit/s Downstream und ca 50 Mbit/s im Upstream.

Beide Kupferbasierten Technologien haben aber den Nachteil, dass die Aufbereitung der Transportstreams sehr aufwendig ist und gegenüber dem im LAN verbreiteten Ethernet somit zu teuer ist. Die Provider suchen daher Möglichkeiten, kostengünstigere Technologien einzusetzen.

Bei Lichtwellenleitern ist eine kostengünstigere Transportmöglichkeit gegeben. Auf Glasfaser kann Ethernet und TCP/IP sehr einfach auf grosse Distanzen transportiert werden. Die Verbreitung der Fiber to the Home Netze (Ftth) nimmt aus diesem Grund stark zu.

Anhang Dokumentstruktur (Minimalanforderung)

Titelblatt:

Titel, eventuell Untertitel, Namen der Verfasser, Erstellungsdatum oder Zeitraum, Logo der Firma, Adresse.

Revision-History.

Tabelle mit:

Datum / Änderung / Seite, Kapitel / Name (wer hat es geändert?) /

Diverse Verzeichnisse

Bild-, Tabellenverzeichnis, Glossar, ... (kann auch am Ende des Dokumentes stehen)

Quellenverzeichnis (kann auch am Ende des Dokumentes stehen)

Inhalt: Inhaltsverzeichnis (Dokumentstruktur):

1. Klären des Auftrages

- 1.1 Beschreiben des Auftrages in eigenen Worten
- 1.2 Machbarkeit (kann die Aufgabe überhaupt gelöst werden? Machbar aus Sicht Technik, Betrieb, Organisation, Strategie, Wirtschaftlichkeit, Juristisch, Security, Ökologisch, Umfeld,
- 1.3 Ziele (Muss und Kann-Ziele)
- 1.4 Recherche in Quellen (Informationsbeschaffung, Anleitungen, ...)
- 1.5 Methoden (welche Methoden werden benutzt (IPERKA, Scrum, SWOT, Systems-Engineering, ...))

2. Planung

- 2.1 Zeitplan
- 2.2 Ressourcen Plan (wer macht was)
- 2.3 Budget (nur in echten Projekten)

3. Varianten

- 3.1 Drei Varianten machen Sinn bei Projekten (Geräte, Konzepte, Schema, ...) (wenn Aufgabenserien mit mehreren Aufgaben vorliegen, dann sollen hier nur die Entscheidungskriterien aufgelistet werden die im Auftrag eingesetzt werden.
- 3.2 Entscheidung

4. Umsetzung

- 4.1 Vorgehen festhalten (Dokumentation der Abläufe, Lösungen von Teilaufgaben.)
Mehrere Aufgaben werden dann so beschrieben:
 - 4.1 Aufgabe 1. Lösung
 - 4.2 Aufgabe 2. Lösung
 -

5. Testen

5.1 Vollständigkeitstest (haben Sie alle Aufgaben gelöst?)

5.2 Technische Tests.

Es wird immer ein 3-Plattformenansatz eingesetzt: Development, Integration, Production
Development: Unit-Tests

Integration: Performancetests, Functional Tests, Security Tests, User-Acceptance Tests, ...

Produktion: keine Tests! Wenn Performance und Security überprüft werden müssen, dann nur in Randstunden!

Testszenarios müssen die vier Fälle *true positive*, *true negative*, *false positive*, *false negative* diskutieren!

Anmerkung: Ein Test beruht immer auf einer Methode (noch besser auf einem Standard). Diese Methode kann selbst auch ein Problem haben. Es kann vorkommen, dass ein Test auf Grund einer fehlerhaften Testmethode ein falsches Resultat liefert.

Methoden können sein: Ping (ICMP), Startabläufe mit walk trough, provozieren von Fehlern, ...

Ein Testszenario sagt ein Resultat vorher (Prediction).

Man unterscheidet:

Es kann sein, dass das erhaltene Testresultat die Vorhersage erfüllt und das Resultat auch wirklich mit der Realität übereinstimmt (true positive)

Es kann sein, dass das erhaltene Testresultat die Vorhersage erfüllt, das Resultat aber nicht mit der Realität übereinstimmt – der Test ist also falsch (false positive)

Es kann sein, dass das erhaltene Testresultat die Vorhersage nicht erfüllt und das Testresultat auch mit der Realität übereinstimmt (das System läuft wirklich nicht) (true negative)

Es kann sein, dass das erhaltene Testresultat die Vorhersage nicht erfüllt, das Resultat in der Realität aber falsch ist (das System läuft in Tat und Wahrheit obschon der Test sagt es laufe nicht) (false negative)

6. Projektabschluss

6.1 Erreichen der oben genannten Ziele

6.2 Reflexion pro Teilnehmer

6.3 Allenfalls Budgetkontrollen, Zeitkontrollen, ...

6.4 Empfehlungen an den Kunden / Management

6.5 Ausblick – in gewissen Fällen ist es sinnvoll, wenn man beschreibt, was man als Erweiterung, Verbesserung, ... in einem neuen Projekt machen sollte oder könnte.

LB1

siehe Ablage TBZ

LB2

siehe Ablage TBZ

