



Fachinformatiker für Anwendungsentwicklung
Dokumentation zur schulischen Projektarbeit im Fach P/LZ

Aufbau einer DMZ in einem mittelständischen Unternehmen

Arbeitsgruppe 9: Rico Krüger, Andreas Biller



Abbildung 1: DMZ zwischen Nord- und Südkorea

Abgabetermin: Berlin, den 25.06.2017



Oberstufenzentrum Informations- und Medizintechnik
Haarlemer Str. 23-27, 12359 Berlin

Dieses Werk einschließlich seiner Teile ist **urheberrechtlich geschützt**. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Autors unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen sowie die Einspeicherung und Verarbeitung in elektronischen Systemen.

Inhaltsverzeichnis

Abbildungsverzeichnis	IV
Tabellenverzeichnis	V
Listings	VI
Abkürzungsverzeichnis	VII
1 Einleitung	1
1.1 Projektumfeld	1
1.2 Projektziel	1
1.3 Projektbegründung	2
1.4 Projektschnittstellen	2
1.5 Projektabgrenzung	3
2 Projektplanung	3
2.1 Projektphasen	3
2.2 Zeitplanung	4
2.3 Abweichungen vom Projektantrag	4
2.4 Ressourcenplanung	4
2.5 Entwicklungsprozess	5
3 Analysephase	5
3.1 Ist-Analyse	5
3.2 Wirtschaftlichkeitsanalyse	6
3.2.1 „Make or Buy“-Entscheidung	6
3.2.2 Projektkosten	6
3.2.3 Amortisationsdauer	7
3.3 Nutzwertanalyse	7
3.4 Anwendungsfälle	7
3.5 Qualitätsanforderungen	7
3.6 Fachkonzept	8
3.7 Zwischenstand	8
4 Entwurfsphase	8
4.1 Zielplattform	8
4.2 Netzwerkplan	9
4.3 Maßnahmen zur Qualitätssicherung	9
4.4 Pflichtenheft/Datenverarbeitungskonzept	10
4.5 Zwischenstand	10

5	Implementierungsphase	11
5.1	Implementierung der Virtuellen Maschinen	11
5.2	Konfiguration der Router	11
5.2.1	Konfiguration der Interfaces	11
5.2.2	Konfiguration der statischen Routern	12
5.2.3	Konfiguration von NAT und Port-Forwarding	12
5.2.4	Konfiguration des DNS-Server	12
5.2.5	Konfiguration des Zeitserver	12
5.3	Implementierung der physischen Hosts	13
5.3.1	Konfiguration der Interfaces	13
5.4	Implementierung der Geschäftslogik	13
5.5	Zwischenstand	13
6	Abnahmephase	14
6.1	Zwischenstand	14
7	Einführungsphase	14
7.1	Zwischenstand	14
8	Dokumentation	15
8.1	Zwischenstand	15
9	Fazit	15
9.1	Soll-/Ist-Vergleich	15
9.2	Lessons Learned	16
9.3	Ausblick	16
	Literaturverzeichnis	17
	Eidesstattliche Erklärung	18
A	Anhang	i
A.1	Schritt-für-Schritt Anleitung	i
A.2	Detaillierte Zeitplanung	vi
A.3	Lastenheft	vii
A.4	Use Case-Diagramm	ix
A.5	Pflichtenheft (Auszug)	ix
A.6	Netzplan	xi
A.7	Oberflächenentwürfe	xii
A.8	Screenshots der Anwendung	xiv
A.9	Entwicklerdokumentation	xvi
A.10	Testfall und sein Aufruf auf der Konsole	xviii
A.11	Klasse: ComparedNaturalModuleInformation	xix

Inhaltsverzeichnis

A.12	Klassendiagramm	xxii
A.13	Benutzerdokumentation	xxiii

Abbildungsverzeichnis

1	DMZ zwischen Nord- und Südkorea	1
2	Netzplan DMZ Arbeitsgruppe 9	9
3	Use Case-Diagramm	ix
4	Netzplan der DMZ (Arbeitsgruppe 9)	xi
5	Liste der Module mit Filtermöglichkeiten	xii
6	Anzeige der Übersichtsseite einzelner Module	xiii
7	Anzeige und Filterung der Module nach Tags	xiii
8	Anzeige und Filterung der Module nach Tags	xiv
9	Liste der Module mit Filtermöglichkeiten	xv
10	Aufruf des Testfalls auf der Konsole	xix
11	Klassendiagramm	xxii

Tabellenverzeichnis

1	Zeitplanung	4
2	Kostenaufstellung	7
3	Zwischenstand nach der Analysephase	8
4	Zwischenstand nach der Entwurfsphase	11
5	Zwischenstand nach der Implementierungsphase	13
6	Zwischenstand nach der Abnahmephase	14
7	Zwischenstand nach der Einführungsphase	14
8	Zwischenstand nach der Dokumentation	15
9	Soll-/Ist-Vergleich	16

Listings

Listings/tests.php	xviii
Listings/cnmi.php	xix

Abkürzungsverzeichnis

DMZ	Demilitarisierte Zone
FA54	Klassenbezeichnung am OSZ IMT)
ITS	Informationstechnische Systeme
P/LZ	Projekt/Linux-Zertifizierung
API	Application Programming Interface
CSV	Comma Separated Value
PHP	Hypertext Preprocessor
UML	Unified Modeling Language

1 Einleitung

1.1 Projektumfeld

Unternehmen: "Das OSZ IMT in der Haarlemer Straße in Berlin-Britz im Bezirk Neukölln ist eines von 36 Oberstufenzentren in Berlin. Es vereint das Berufliche Gymnasium, die Berufsoberschule, die Fachoberschule, die Berufsfachschule, die Fachschule und die Berufsschule. (...) [An ihm] arbeiten etwa 160 Lehrkräfte und nichtpädagogisches Personal in Laboren, Werkstätten, Lernbüros und allgemeinen Unterrichtsräumen. (...) [Es] hat rund 3000 Schüler (...) [und] ist die größte Schule Berlins für Informationstechnik und Deutschlands größte Schule für Medizintechnik."¹ Wir besuchen dort seit 2 bzw. 1.5 Jahren den Unterricht der Klasse Klassenbezeichnung am OSZ IMT) (FA54).

Auftraggeber: Als angehende Fachinformatiker für Anwendungsentwicklung am OSZ IMT sollen wir nun im Rahmen des Faches Projekt/Linux-Zertifizierung (P/LZ) ein auf mittelständige Unternehmen anwendbares IT-Sicherheitskonzept entwickeln. Dazu werden wir im Verlauf des Projektunterrichtes eine Demilitarisierte Zone (DMZ) unter Verwendung des zuvor in Informationstechnische Systeme (ITS) erlernten Wissens über Netzwerktechnik einrichten. Gleichzeitig erarbeiten wir uns Anhand eines Online-Kurses der Cisco-Networking-Academy die für das Projekt benötigten Grundkenntnisse im Umgang mit Linux.

Verantwortlicher Auftraggeber und unser Ansprechpartner für dieses Projekt ist **Herr Ralf Henze**, Netzwerktechniker und Lehrer am OSZ IMT in den Unterrichtsfächern ITS und P/LZ.

1.2 Projektziel

Projekthintergrund: Neben dem offensichtlichen Ziel dieses Projektes, ein DMZ-Netzwerk unter Linux einzurichten, will es uns als Teil des Berufsschulunterrichtes natürlich vor allem etwas beibringen. So ist die eigentliche Projektarbeit durchzogen von unterschwelligem Langzeitnutzen für unsere berufliche Entwicklung. Das Wissen, wie und wo man jederzeit Befehle nachschlagen kann, die beidenswerten Möglichkeiten mit grep, pipes und kleinen Tools wie xargs erstaunlich komplizierte Probleme lösen zu können. Auch die bewusst schon fast aufs Niveau der IHK angehobenen Anforderungen an die Projektdokumentation und das Nahelegen, für deren Erstellung mit einer Sprache wie L^AT_EX zu arbeiten, anstelle dies mit gängigen Office Paketen zu tun, waren eine gute Vorbereitung und hervorragende Übung. So konnte Gelerntes durch praktisches Anwenden gefestigt und Neues sinnvoll ausprobiert werden.

¹Pressemappe, "Porträt des OSZ IMT"?

1 Einleitung

Ziel des Projekts: Die eigentliche Kernaufgabe des Projektes ist die Planung und praktische Umsetzung eines grundlegenden IT-Sicherheitskonzeptes mit Hilfe eines DMZ-Netzwerkes und dessen Absicherung durch das Setzen bzw. Löschen von Firewall-Regeln über ein Shell-Script. Die demilitarisierte Zone soll zwischen den Windows-Clients des Kunden im internen Netz und den potentiell schädlichen Anfragen der restlichen Welt aus dem externen Netzwerk liegen. Hier steht auch der Windows-Webserver des Kunden, welcher sowohl von Innen (zur Wartung) wie auch von Außen (für Besucher) erreichbar sein muss. Zwei virtuelle Linuxmaschinen sollen als Router zwischen den Netzen konfiguriert werden, wobei der Äußere sowohl das NATen als auch die Funktion der Firewall übernehmen soll. Planung und Umsetzung sollen umfassend Dokumentiert werden. Jedes Gruppenmitglied soll ein Kompetenzportfolio führen, in dem er seine Kenntnisse, Gelerntes und Probleme vor, während und nach den Aufgaben der Projektarbeit sammelt und kritisch analysiert.

1.3 Projektbegründung

Nutzen des Projekts: Neben dem bereits mehrfach erwähnten Lerneffekt für uns als Schüler, sowohl in den Grundlagen der IT-Sicherheit, des Arbeitens auf dem Linux-Filesystem mit Hilfe der CLI, wie auch der Wiederholung der Befehle zur Konfiguration von Netzwerken und Schnittstellen in einer neuen leicht anderen Syntax, liegt der Projektnutzen wohl vor Allem auf dem Verstehen der Arbeitsweise von Access-Control-Listen, der Bedeutung der drei Chains sowie eines besseren Einblicks in die Welt der Linux-Distributionen, deren Stärken und Schwächen sowie deren Konfiguration. Und da das Projekt den Auftraggeber faktisch nichts kostet, uns aber fachlich weiter bringt, ist dessen Durchführung für beide Seiten ein Win-Win-Geschäft.

Motivation: Grundlegende Motivation ist wohl für jeden Bereiligten an diesem Projekt seine ganz eigene Sache. Der Auftraggeber ist daran interessiert, ein fertiges, funktionierendes System zu erhalten, welches seine Wünsche und Anforderungen erfüllt, aber er und auch wir können darüber hinaus uns und uns gegenseitig an greifbaren Indikatoren bezüglich unserer Fachkompetenz bewerten. Wir stellen uns somit einer solchen Aufgabe, um etwas neues zu lernen, etwas zu wiederholen und uns zu verbessern. Oder einfach, weil wir es können. Manchmal auch, um uns auf eine Zertifizierung vorzubereiten.

1.4 Projektschnittstellen

Technisch gesehen interagieren in unserem Projekt zwei oder mehrere Windows-Rechner, welche über das Labornetzwerk des Raumes 3.1.01 verbunden sind. Auf beiden läuft jeweils eine Linux Debian Distribution in einer virtuellen Umgebung durch den VMWare Player. Die Schnittstellen der virtuellen Linuxdistributionen wiederum sind über den Bridged Modus in den Netzwerkeinstellungen des VMWare Players mit einer der physikalischen Netzwerkschnittstelle des Host-PCs verbunden. Über das Labornetz kann Verbindung zu den Rechnern der anderen Gruppen aufgenommen werden.

2 Projektplanung

Die Unterrichtszeit für das Projekt, sowie die Infrastruktur (Pro Gruppe 2 Rechner + benötigte Peripherie, 2 virtuelle Maschinen und alle sonst benötigten Ressourcen, Zugang zum Internet und ins Labornetz) und alles weitere wird uns im Rahmen des P/LZ-Unterrichtes zur Verfügung gestellt.

Dank der theoretischen Natur des Projektes sind die einzigen Benutzer unseres Projektes wir, evtl. unsere Mitschüler während des Erfahrungsaustausches untereinander, sowie unser Auftraggeber, Herr Henze, der sich immer wieder über den aktuellen Stand informiert und auch die finale Abnahme des Projektes übernimmt.

Zur finalen Abnahme durch den Kunden sollen sowohl die Funktionalität der Firewall-Regeln nachweislich testbar sein, als auch die Projektdokumentation inkl. einer Kopie des verwendeten Firewall-Scriptes, den tabellarisch erfassten Testresultaten sowie je eines Kompetenzportfolios pro Gruppenmitglied zur Abgabe vorliegen.

1.5 Projektabgrenzung

Was dieses Projekt nicht bietet: Dieses Projekt will auf keinen Fall den Anspruch erheben, durch die verwendeten Techniken ein Netzwerk oder System perfekt und allumfassend vor unbefugtem Eindringen schützen zu können. Es vermittelt nur Einblicke in die Grundlagen der Netzwerktechnik und IT-Sicherheit. Ein perfektes und vor allen schädlichen Einflüssen geschütztes System kann es nicht geben. Weiterführende Informationen zur Verbesserung der Systemsicherheit können aber der im Quellverzeichnis angegebenen Literatur entnommen werden.

2 Projektplanung

Da unser Projekt über die Dauer eines ganzen Schuljahres angelegt ist und wir die Unterrichtszeit zum Teil mit dem Erlernen von Fertigkeiten im Umgang mit Linux verbringen werden, muss der Ablauf genau geplant werden. Im folgenden erläutern wir die einzelnen Projektphasen, welche Ressourcen genutzt wurden und wann die Durchführung von der Planung abgewichen ist.

2.1 Projektphasen

Im Rahmen des P/LZ Unterrichts erhalten wir in jeder Schulwoche meist Freitags für je zwei Blöcke a 90 Minuten Zugang zum Labor 3.1.01 am OSZ IMT in Berlin. Das Schuljahr umfasst 14 Schulwochen in denen das Projekt durchgeführt werden muss. Außerhalb der Schulzeit können wir Private Ressourcen nutzen und planen pro Schulwoche jeweils 6 Stunden Freizeit am Wochenende als zusätzliche Pufferzeit ein. Die 42 Laborstunden und die Pufferzeit von 84 Stunden ergeben eine Gesamtzeit von 126 Stunden bis zur Projektabgabe.

2 Projektplanung

Wir gehen davon aus die grundlegende Planung und Analyse in den ersten beiden Schulwochen durchzuführen, die nächsten drei Schulwochen sollte das Netzwerk entworfen und erstellt werden. Anschließend wollen wir mit der Implementierung der Firewall beginnen, wofür wir ca. vier Schulwochen einplanen. Die Restliche Schulzeit wird für die Erstellung der Dokumentation und eine Stunde für die Abnahme durch den Kunden verplant. Je nach Bedarf kann die Pufferzeit zu weiterer Recherche zuhause genutzt werden.

2.2 Zeitplanung

Tabelle 1 zeigt unsere Zeitplanung für die einzelnen Projektphasen:

Projektphase	Geplante Zeit
Analysephase	6 h
Entwurfsphase	9 h
Implementierungsphase	12 h
Abnahmetest der Fachabteilung	1 h
Erstellen der Dokumentation	14 h
Pufferzeit	84 h
Gesamt	126 h

Tabelle 1: Zeitplanung

2.3 Abweichungen vom Projektantrag

Aufgrund unserer Unerfahrenheit im Umgang mit \LaTeX gestaltet sich die Erstellung der Projektdokumentation leider schwieriger als vermutet. Zudem konnten die Funktionstests an unserer Firewall nicht bis zum Ende des letzten Unterrichtsblockes abgeschlossen werden, worauf Herr Krüger viel Zeit damit verbracht hat, eine zweite Testumgebung für unser Firewall-Script mit Windows Server 2016 zu virtualisieren, deren Installation und Konfiguration im Anhang dokumentiert wurde. Deshalb erbaten wir eine kurzzeitige Verlängerung der Abgabefrist und konnten nur die während des Unterrichtes erstellte und benutzte Dokumentation einsenden, zu finden im Anhang [A.1: Schritt-für-Schritt Anleitung](#) auf Seite i.

2.4 Ressourcenplanung

Für die Durchführung im Labor werden benötigt: 2 Rechner mit Windows (und einem Benutzeraccount mit Adminrechten), die Software VMWare Player, eine Distribution von Debian für die virtuelle Maschine, Zugang zum Labornetz, ein Webserver und ein Editor zum Bearbeiten von HTML, Zugang zum Internet für Recherche, Software zum Festhalten der Ergebnisse, Software zum Durchführen von Tests. Zusätzlich bedarf es der Unterstützung durch fachkundige Mitschüler wie den Herren Habekost, Schernekau und Mahnke sowie Hilfe durch Herrn Henze bei schwereren Problemen.

3 Analysephase

Für die Arbeit außerhalb der Schule haben wir zur Recherche und für weitere Versuche sowohl Rechner mit Ubuntu 14.04 als auch Rechner mit Windows 7 und 10 und eigene Heimnetzwerke mit Internetanbindung. Auch die benötigte Software sowie L^AT_EX und Editoren um die Dokumentation anzufertigen sind vorhanden. Dank einer während des Projektes angelegten Schritt-für-Schritt Anleitung zum Einrichten des Netzwerks, sowie der Möglichkeit virtuelle Maschinen zu kopieren bzw. das Versuchsnetzwerk selbst zu virtualisieren, kann auch zuhause gearbeitet werden.

2.5 Entwicklungsprozess

Um unser Projekt durchzuführen benutzen wir einen auf dem Wasserfallmodel basierenden Entwicklungsprozess und den üblichen Stufen Anforderung, Entwurf, Implementation, Überprüfung und Wartung.

3 Analysephase

Im Nachfolgenden verzichten wir auf einen Großteil der üblichen Berechnungen zur Wirtschaftlichkeit des Projektes, da dieses zum Großteil unserer fachlichen Kompetenzbildung dienen soll. Darüber hinaus wäre für ein fiktives mittelständisches Unternehmen ein bereits existierendes Produkt sowohl vom zu erwartenden Arbeitsaufwand wie auch finanziell deutlich günstiger. Es wird daher lediglich eine beispielhafte Kostenberechnung für die Umsetzung der Planung durch uns erstellt und dafür ein größeres Augenmerk auf Anforderungen und Nutzen des Projekts gelegt.

3.1 Ist-Analyse

Was ist vorhanden: Im Labor sind für jedes Gruppenmitglied vorhanden: ein Bildschirmarbeitsplatz, Windows 7, Adminrechte, zwei physikalische Netzwerkinterfaces, Anschluß an Labornetzwerk und Internet, die Software VMWare Player, Debian Images auf einem Netzlaufwerk sowie ein Webserver.

Was ist zu erstellen: Zuerst muss nun von jeder Gruppe ein Netzplan erstellt werden. Dann gilt es, die Debian 7 (Wheezy) Linux-Images in virtuellen Maschinen auf beiden Rechnern mit Hilfe des VMWare Players aufzusetzen. Diese werden zu einem Outside- und einem Inside-Router konfiguriert und die geplanten Netzwerk- und Routingeeinstellungen müssen sowohl an den virtuellen wie auch physikalischen Schnittstellen durchgeführt werden. Auf dem Rechner des Outside-Routers muss ein Webserver eingerichtet werden, wofür NAT und Port-Forwarding nötig sind. Zwischendurch wird es immer wieder der gezielten Recherche bedürfen. Um schließlich Zugriffe von außen zu regulieren, muss eine Firewall mit entsprechenden Regeln erstellt werden, die per Skript an- und abschaltbar ist. Die Funktionalität muss getestet werden und Projekt und Tests sind zu dokumentieren. Unser

3 Analysephase

Lernfortschritt ist in einem Kompetenzportfolio niederzuschreiben. Gleichzeitig sind Laborübungen und Tests zu Linux-Kenntnissen zu absolvieren.

3.2 Wirtschaftlichkeitsanalyse

Wie bereits Anfänglich erwähnt, lohnt sich das Projekt für ein fiktives mittelständisches Unternehmen nur bedingt.

3.2.1 „Make or Buy“-Entscheidung

Die Kosten für eine qualifizierte Kraft zur ständigen Wartung des Servers, die durch Dauerbetrieb anfallenden Stromkosten sowie die zusätzlichen Hardwarekosten bei einem zukünftigen Upscaling übersteigen bei weitem die Kosten für einen fachkundig und sicher Administrierten Server bei einem seriösen Hosting-Anbieter.

Da unsere Empfehlung an den Kunden ein Produkt eines anderen Anbieters wäre, wird das Projekt nur zu unserem Nutzen und der Erfahrung willen, die wir damit gewinnen, umgesetzt.

3.2.2 Projektkosten

Da es sich nur um ein fiktives Projekt handelt, verzichten wir auf eine detaillierte Berechnung mit Stromkosten innerhalb des Labors, den Gehältern der Lehrkräfte oder etwaiger Lizenzgebühren. Wir beschränken uns auf eine fiktive Beispielrechnung mit unserem Stundenlohn während der Projektdauer.

Beispielrechnung (verkürzt) Die realen Kosten für die Durchführung des Projekts setzen sich sowohl aus Personal-, als auch aus Ressourcenkosten zusammen. Wir rechnen hier lediglich mit dem fiktiven Gehalt eines Auszubildenden im zweiten Lehrjahr von ca. 800 € Brutto pro Monat.

$$3 \cdot 800 \text{ €/Monat} \div 13 \div 40 \text{ h/Monat} \approx 4,62 \text{ €/h} \quad (1)$$

Es ergibt sich also ein Stundenlohn von 4,62 €. Die Durchführungszeit des Projekts beträgt 42 Stunden. Die Nutzung von Ressourcen² sowie die Kosten durch andere Mitarbeiter werden hier nicht mit eingerechnet. Eine Aufstellung der Kosten befindet sich in Tabelle 2 und sie betragen insgesamt 388,08 €.

²Räumlichkeiten, Arbeitsplatzrechner etc.

Vorgang	Zeit	Kosten pro Stunde	Kosten
Entwicklungskosten	42 h	$4,62 \text{ €} \times 2 = 9,24 \text{ €}$	388,08 €
			388,08 €

Tabelle 2: Kostenaufstellung

3.2.3 Amortisationsdauer

Aufgrund unserer „Make or Buy“-Entscheidung und da das Projekt nur zu Lernzwecken umgesetzt wird verzichten wir hier auf die Berechnung eines fiktiven Rentabilitätszeitpunktes. Das gelernte wird sich spätestens zur IHK-Prüfung und bei der Anfertigung der Dokumentation des IHK-Abschlussprojektes auszahlen.

3.3 Nutzwertanalyse

Durch den Aufbau einer DMZ können wir die Zugriffe auf unsere Server, in diesem Fall ein einfacher Webserver, von Außen und Innen reglementieren. So wird über den Routern mit einer konfigurierten Firewall ein sicherer Zugang zu unserem Webserver ermöglicht. Die Aufteilung in unterschiedliche Netzwerke ermöglicht den Administratoren eine einfachere Verwaltung der Berechtigungen für die Mitglieder des Firmennetzes.

3.4 Anwendungsfälle

.....

Beispiel Ein Beispiel für ein Use Case-Diagramm findet sich im Anhang [A.4: Use Case-Diagramm](#) auf Seite [ix](#).

3.5 Qualitätsanforderungen

Der Webserver soll von Außen (über die öffentliche IP des Outside-Routers) und Innen erreichbar, aber vor potentiellen Angreifern bestmöglich mit den zur Verfügung stehenden Mitteln geschützt sein. Es muss sichergestellt werden, dass kein unberechtigter Dritter Zugriff auf die Geräte und deren Konfiguration hat. Dabei ist darauf zu achten, dass die Mitarbeiter weiterhin wie gewohnt Zugriff auf das Internet und den Webserver haben.

3.6 Fachkonzept

Die Mitarbeiter sollen untereinander, mit dem Webserver und dem Internet kommunizieren können, dabei jedoch bestmöglich geschützt werden.

Die Administrator sollen zusätzlich die Möglichkeit haben, die Server und Router aus der Ferne zu warten. Dabei sollte es unerheblich sein, wie viele Clients und Server sich im internen bzw. DMZ-Netz befinden.

3.7 Zwischenstand

Tabelle 3 zeigt den Zwischenstand nach der Analysephase.

Vorgang	Geplant	Tatsächlich	Differenz
1. Analyse des Ist-Zustands	3 h	4 h	+1 h
2. „Make or buy“-Entscheidung und Wirtschaftlichkeitsanalyse	1 h	1 h	
3. Erstellen eines „Use-Case“-Diagramms	2 h	2 h	
4. Erstellen des Lastenhefts	3 h	3 h	

Tabelle 3: Zwischenstand nach der Analysephase

4 Entwurfsphase

Da unsere Hard- und Software von unserem Auftraggeber gestellt und vorgegeben wird, erübrigt seine ausführliche Begründung, weshalb wir diese Materialien verwendet haben. Zudem wird so sichergestellt, dass während unserer Projektzeit alle benötigten Mittel zur Verfügung stehen.

4.1 Zielplattform

Hardware: Die uns zur Verfügung stehenden Desktop PCs bleiben unverändert. Die Leistungsdaten derer genügen für den Aufbau einer einfachen DMZ.

Software: Für die Implementation eines Routers als virtuelle Maschine nutzen wir den vorinstallierten VMWare Player. Dieser ist kostenlos und berechtigt uns zum Virtualisieren einer Linux Distribution. Des Weiteren werden wir auch das beigefügte Debian benutzen. Auf den VMs wird mit BASH und Linux-Befehlen gearbeitet, da wir nur kleinere Konfigurationen und Scripts schreiben. Um die Konfiguration zu testen, die Router per Remote zu konfigurieren und eventuell Dateien auszutauschen, wird noch SSH- und FTP-Client-Software benötigt. Dafür werden wir Putty und winscp verwenden. Diese Tools sind kompakt und beeinträchtigen nicht die Leistung der Hosts.

4.2 Netzwerkplan

Abbildung 2 zeigt die grundsätzliche IP-Adressverteilung in den geplanten Netzwerken. Unser Konzept teilt sich grundsätzlich in das Labornetz (hier symbolisch für den Rest der Welt), das interne Netz (mit den Windows-Clients unseres Kunden) und das von der Außenwelt abgeschottete DMZ-Netzwerk, welches nur über spezielle Berechtigungen zu erreichen und für spezielle Dienste (Webserver) zu verwenden ist.

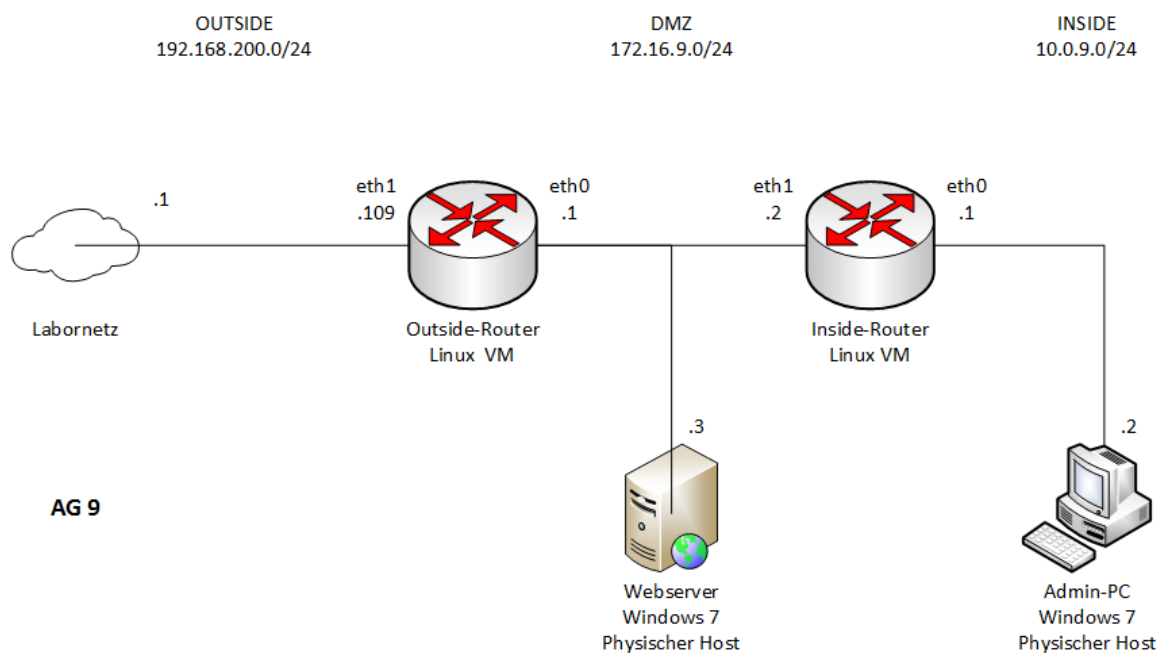


Abbildung 2: Netzplan DMZ Arbeitsgruppe 9

4.3 Maßnahmen zur Qualitätssicherung

Bei jeder Veränderungen der Konfiguration werden Tests durchgeführt. Diese sollen gewährleisten, dass das **Fachkonzept** eingehalten wird. Vorgenommene Konfigurationen werden notiert und das Firewall-Script wird zusätzlich auf einen externen Datenträger kopiert. So wird sichergestellt, dass bei einem Defekt die ursprüngliche Konfiguration schnell wieder verfügbar ist.

4.4 Pflichtenheft/Datenverarbeitungskonzept

1. Musskriterien

- Das DMZ-Netz erhält die Netzmaske 172.16.9.0/24
- Das intere Netz erhält die Netzmaske 10.0.9.0/24
- Die öffentliche Schnittstelle des Outside-Router erhält die IP 192.168.200.109
- Der Outside-Router erhält als Standard-Gateway die IP 192.168.200.1
- Der Outside-Router erhält eine statische Route für das interne und DMZ-Netz
- Der Inside-Router erhält als Standard-Gateway das Interface des Outside-Routers, welches in die DMZ zeigt
- Der Webserver ist über die öffentliche IP des Outside-Routers über HTTP/S von außen erreichbar
- Der Webserver ist über die lokale IP 172.16.9.3 über HTTP/S aus dem internen Netzwerk erreichbar
- Die Router und Windows-Clients bekommen als DNS-Server die IPs 192.168.95.40 und 192.168.95.41
- Die Router und Windows-Clients bekommen als NTP-Server die IP 192.168.200.1
- Die Firewall verhindert unrechtmäßigen Datentransfer zwischen den Netzen und auf den Routern
- Der Admin-PC mit der IP 10.0.9.2 ist berechtigt mittels SSH auf die Router zuzugreifen

2. Kannkriterien

- Die Firewall lässt sich mit den Optionen `start` und `stop` bzw. ausschalten
- Die Firewall-Skripts der Router befinden sich im Verzeichnis `/root/bin`
- Die Veränderung der Firewall-Konfiguration befindet sich jeweils im Verzeichnis `/var/log/-firewall`
- Der Admin-PC mit der IP 10.0.9.2 ist berechtigt mittels RDP auf den Webserver zuzugreifen

4.5 Zwischenstand

Tabelle 4 zeigt den Zwischenstand nach der Entwurfsphase.

Vorgang	Geplant	Tatsächlich	Differenz
1. Prozessentwurf	2 h	3 h	+1 h
2. Datenbankentwurf	3 h	5 h	+2 h
3. Erstellen von Datenverarbeitungskonzepten	4 h	4 h	
4. Benutzeroberflächen entwerfen und abstimmen	2 h	1 h	-1 h
5. Erstellen eines UML-Komponentendiagramms	4 h	2 h	-2 h
6. Erstellen des Pflichtenhefts	4 h	4 h	

Tabelle 4: Zwischenstand nach der Entwurfsphase

5 Implementierungsphase

...immer testen usw.

5.1 Implementierung der Virtuellen Maschinen

Eine Debian Distribution als virtuelle Maschine ist bereits auf beiden Rechnern vorhanden. Diese wird kopiert und dann mit dem VMWare Player gestartet. Wir überbrücken die physischen Netzwerkadapter der Windows Hosts auf die virtuellen Adapter der Linux Distribution. So haben die designierten Router über die physischen Interfaces Zugriff auf das Netzwerk.

5.2 Konfiguration der Router

Über dem VMWare Player auf den Windows Hosts verbinden wir uns auf die Router und können diese dann über das Terminal konfigurieren. Die Passwörter, die wir vom Kunden erhalten haben, lassen wir unverändert. Als erstes werden die Hostnamen angepasst. Dazu ersetzt man den alten Namen in den Dateien `/etc/hostname` und `/etc/hosts`. Danach sollte die Maschine neu gestartet werden.

Diese und alle weiteren von uns benötigten Dateien lassen sich über einen vorinstallierten Editor öffnen und bearbeiten, z. B. mit vi:

```
vi /etc/hostname.
```

5.2.1 Konfiguration der Interfaces

Für die Konfiguration der Interfaces halten wir uns an den erstellten Netzplan (Siehe ??). Um die Interfaces zu konfigurieren, wird die Datei `/etc/network/interfaces` geöffnet.

Inside-Router Für den Inside-Router tragen wir neben den IP-Adressen seiner Schnittstellen als Standard-Gateway das Interface des Outside-Routers ein, welches sich in der DMZ befinden soll. (Siehe Anhang InideRouterInt.png)

Outside-Router Der Outside-Router erhält zusätzlich zu seinen IP-Adressen als Gateway die IP-Adresse 192.168.200.1 (Standard-Gateway Labornetz). (Siehe Anhang OutsideRouterInt.png)

5.2.2 Konfiguration der statischen Routern

Wir benötigen zwei statische Routen auf dem Outside-Router, eine für die DMZ und eine für das LAN. (Siehe Anhang OuoutsideRouterInt.png)

5.2.3 Konfiguration von NAT und Port-Forwarding

Weiterhin konfigurieren wir in der interfaces-Datei vom Outside-Router NAT für die DMZ und das LAN sowie Port-Forwarding zu unserem Webserver ein. (Siehe Anhang OuoutsideRouterInt.png) Um jedoch NAT und Port-Forwarding auf beiden Routern nutzen zu können, müssen wir dies erst aktivieren. Dies geschieht mit dem Befehl `echo 1 > /proc/sys/net/ipv4/ip_forward`.

Dies ist jedoch nur eine temporäre Lösung und geht nach einem Neustart verloren. Damit der Prozess mit dem Systemstart geladen wird, tragen wir (, nachdem unsere Tests erfolgreich waren,) setzen wir den Wert in der Datei `/etc/sysctl.conf` von `#net.ipv4.ip_forward` auf 1 und kommentieren diese Zeile aus.

5.2.4 Konfiguration des DNS-Server

In der Datei `/etc/resolv.conf` tragen wir für beide die IP-Adresse der von unserem Auftraggeber bereitgestellten DNS-Server ein.

```
nameserver 192.168.200.40
nameserver 192.168.200.41
```

5.2.5 Konfiguration des Zeitserver

Um einen Zeitserver angeben und nutzen zu können, installieren wir mit `apt-get install ntp` den ntp-Dienst. Danach fügen wir die IP-Adresse des bereitgestellten NTP-Servers (Standard-Gateway) in die Datei `/etc/ntp.conf` ein: `server 192.168.200.1 iburst`. (Siehe NTP.conf)

5.3 Implementierung der physischen Hosts

Bevor die Schnittstellen auf die Router angepasst werden, werden noch evtl. benötigte Dateien und Programme (notepad++, putty, winscp) heruntergeladen. Im Gegensatz zu Router-Konfiguration wird hier fast ausschließlich mit der GUI gearbeitet

5.3.1 Konfiguration der Interfaces

Für die IP-Adressierung halten wir uns ebenfalls an den Netzplan (Siehe Netzplan Produktionsumgebung).

5.4 Implementierung der Geschäftslogik

- Beschreibung des Vorgehens bei der Umsetzung/Programmierung der entworfenen Anwendung.
- Ggfs. interessante Funktionen/Algorithmen im Detail vorstellen, verwendete Entwurfsmuster zeigen.
- Quelltextbeispiele zeigen.
- Hinweis: Wie in Kapitel 1: [Einleitung](#) zitiert, wird nicht ein lauffähiges Programm bewertet, sondern die Projektdurchführung. Dennoch würde ich immer Quelltextausschnitte zeigen, da sonst Zweifel an der tatsächlichen Leistung des Prüflings aufkommen können.

Beispiel Die Klasse `ComparedNaturalModuleInformation` findet sich im Anhang [A.11: Klasse: ComparedNaturalModuleInformation](#) auf Seite [xix](#).

5.5 Zwischenstand

Tabelle 5 zeigt den Zwischenstand nach der Implementierungsphase.

Vorgang	Geplant	Tatsächlich	Differenz
1. Anlegen der Datenbank	1 h	1 h	
2. Umsetzung der HTML-Oberflächen und Stylesheets	4 h	3 h	-1 h
3. Programmierung der PHP-Module für die Funktionen	23 h	23 h	
4. Nächtlichen Batchjob einrichten	1 h	1 h	

Tabelle 5: Zwischenstand nach der Implementierungsphase

6 Abnahmephase

- Welche Tests (z. B. Unit-, Integrations-, Systemtests) wurden durchgeführt und welche Ergebnisse haben sie geliefert (z. B. Logs von Unit Tests, Testprotokolle der Anwender)?
- Wurde die Anwendung offiziell abgenommen?

Beispiel Ein Auszug eines Unit Tests befindet sich im Anhang [A.10: Testfall und sein Aufruf auf der Konsole](#) auf Seite [xviii](#). Dort ist auch der Aufruf des Tests auf der Konsole des Webserverns zu sehen.

6.1 Zwischenstand

Tabelle 6 zeigt den Zwischenstand nach der Abnahmephase.

Vorgang	Geplant	Tatsächlich	Differenz
1. Abnahmetest der Fachabteilung	1 h	1 h	

Tabelle 6: Zwischenstand nach der Abnahmephase

7 Einführungsphase

- Welche Schritte waren zum Deployment der Anwendung nötig und wie wurden sie durchgeführt (automatisiert/manuell)?
- Wurden ggfs. Altdaten migriert und wenn ja, wie?
- Wurden Benutzerschulungen durchgeführt und wenn ja, Wie wurden sie vorbereitet?

7.1 Zwischenstand

Tabelle 7 zeigt den Zwischenstand nach der Einführungsphase.

Vorgang	Geplant	Tatsächlich	Differenz
1. Einführung/Benutzerschulung	1 h	1 h	

Tabelle 7: Zwischenstand nach der Einführungsphase

8 Dokumentation

- Wie wurde die Anwendung für die Benutzer/Administratoren/Entwickler dokumentiert (z. B. Benutzerhandbuch, [API-Dokumentation](#))?
- Hinweis: Je nach Zielgruppe gelten bestimmte Anforderungen für die Dokumentation (z. B. keine IT-Fachbegriffe in einer Anwenderdokumentation verwenden, aber auf jeden Fall in einer Dokumentation für den IT-Bereich).

Beispiel Ein Ausschnitt aus der erstellten Benutzerdokumentation befindet sich im Anhang [A.13: Benutzerdokumentation](#) auf Seite [xxiii](#). Die Entwicklerdokumentation wurde mittels PHPDoc³ automatisch generiert. Ein beispielhafter Auszug aus der Dokumentation einer Klasse findet sich im Anhang [A.9: Entwicklerdokumentation](#) auf Seite [xvi](#).

8.1 Zwischenstand

Tabelle 8 zeigt den Zwischenstand nach der Dokumentation.

Vorgang	Geplant	Tatsächlich	Differenz
1. Erstellen der Benutzerdokumentation	2 h	2 h	
2. Erstellen der Projektdokumentation	6 h	8 h	+2 h
3. Programmdokumentation	1 h	1 h	

Tabelle 8: Zwischenstand nach der Dokumentation

9 Fazit

9.1 Soll-/Ist-Vergleich

- Wurde das Projektziel erreicht und wenn nein, warum nicht?
- Ist der Auftraggeber mit dem Projektergebnis zufrieden und wenn nein, warum nicht?
- Wurde die Projektplanung (Zeit, Kosten, Personal, Sachmittel) eingehalten oder haben sich Abweichungen ergeben und wenn ja, warum?
- Hinweis: Die Projektplanung muss nicht strikt eingehalten werden. Vielmehr sind Abweichungen sogar als normal anzusehen. Sie müssen nur vernünftig begründet werden (z. B. durch Änderungen an den Anforderungen, unter-/überschätzter Aufwand).

³Vgl. PHPDOC.ORG [2010]

9 Fazit

Beispiel (verkürzt) Wie in Tabelle 9 zu erkennen ist, konnte die Zeitplanung bis auf wenige Ausnahmen eingehalten werden.

Phase	Geplant	Tatsächlich	Differenz
Entwurfsphase	19 h	19 h	
Analysephase	9 h	10 h	+1 h
Implementierungsphase	29 h	28 h	-1 h
Abnahmetest der Fachabteilung	1 h	1 h	
Einführungsphase	1 h	1 h	
Erstellen der Dokumentation	9 h	11 h	+2 h
Pufferzeit	2 h	0 h	-2 h
Gesamt	70 h	70 h	

Tabelle 9: Soll-/Ist-Vergleich

9.2 Lessons Learned

- Was hat der Prüfling bei der Durchführung des Projekts gelernt (z. B. Zeitplanung, Vorteile der eingesetzten Frameworks, Änderungen der Anforderungen)?

9.3 Ausblick

- Wie wird sich das Projekt in Zukunft weiterentwickeln (z. B. geplante Erweiterungen)?

Literaturverzeichnis

phpdoc.org 2010

PHPDOC.ORG: *phpDocumentor-Website*. Version: 2010. <http://www.phpdoc.org/>, Abruf:
20.04.2010

Eidesstattliche Erklärung

Wir, Rico Krüger und Andreas Biller, versichern hiermit, dass wir unsere **Dokumentation zur schulischen Projektarbeit im Fach P/LZ** mit dem Thema

Aufbau einer DMZ in einem mittelständischen Unternehmen

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt haben, wobei wir alle wörtlichen und sinngemäßen Zitate als solche gekennzeichnet haben. Die Arbeit wurde bisher keinem anderen Lehrer vorgelegt und auch nicht veröffentlicht.

Berlin, den 25.06.2017

ANDREAS BILLER, RICO KRÜGER

A Anhang

A.1 Schritt-für-Schritt Anleitung

FA54

P / LZ

Herr Henze

Gruppe 9

Andreas Biller, Rico Krüger

Thema: Aufbau einer DMZ

1. Aufsetzen der virtuellen Maschinen

Auf zwei Clients je eine virtuelle Maschine mit Linux-OS (Debian) aufsetzen (mit VM-Ware Player). Falls VM bereits vorhanden, diese in eigenen Benutzer-Ordner kopieren. Sonst über Linux mit VM-Ware Player installieren.

Rolle	Name	Passwort
Benutzer	user	oszimt
Administrator	root	osz

2. Änderung des Modus der Netzwerkschnittstellen

Wir öffnen VM-Ware Player und starten Linux. Dann versetzen wir in den Einstellungen die Netzwerkschnittstellen in den **Bridge-Modus**.

3. Erstellung Netzwerkplan

Wir erstellen einen Netzplan und vergeben die benötigten IP-Adressen.

4. Konfiguration Schnittstellen und NAT der Linux-VMs als Router

Die Schnittstellen werden auf beiden Debian-Systemen in der Datei „*/etc/network/interfaces*“ konfiguriert.

4.1. Konfiguration Inside-Router

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 10.0.9.1
netmask 255.255.255.0

# The second interface
allow-hotplug eth1
iface eth1 inet static
address 172.16.9.2
netmask 255.255.255.0
gateway 172.16.9.1
```

4.2. Konfiguration Outside-Router

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 172.16.9.1
netmask 255.255.255.0

# second interface
allow-hotplug eth1
iface eth1 inet static
address 192.168.200.109
netmask 255.255.255.0
gateway 192.168.200.1

### static routing ###
post-up route add -net 10.0.9.0 netmask 255.255.255.0 gw 172.16.9.2
pre-down route del -net 10.0.9.0 netmask 255.255.255.0 gw 172.16.9.2

### NAT and Port-Forwarding ###
```

FA54

P / LZ

Herr Henze

Gruppe 9

Andreas Biller, Rico Krüger

Thema: Aufbau einer DMZ

```
post-up iptables -A FORWARD -o eth1 -s 172.16.9.0/24 -m conntrack --ctstate NEW -j ACCEPT
post-up iptables -A FORWARD -o eth1 -s 10.0.9.0/24 -m conntrack --ctstate NEW -j ACCEPT
post-up iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE

post-up iptables -A PREROUTING -t nat -i eth1 -p tcp --dport 80 -j DNAT --to-destination 172.16.9.3:80
post-up iptables -A FORWARD -p tcp -d 172.16.9.3 --dport 80 -j ACCEPT
post-up iptables -A POSTROUTING -t nat -s 172.16.9.3 -o eth1 -j MASQUERADE
```

5. Aktivierung IP-Forwarding

Temporäre Aktivierung:

Ausführen des Befehls: `echo „1“ > /proc/sys/net/ipv4/ip_forward`

Permanente Aktivierung:

In der Datei „`/etc/sysctl.conf`“ den Wert von „`#net.ipv4.ip_forward`“ auf **1** setzen und die Auskommentierung aufheben: `net.ipv4.ip_forward=1`

6. Neustarten der Schnittstellen zum Übernehmen der Konfiguration

Dafür werden folgende Befehle nacheinander ausgeführt:

```
ifdown eth0
ifdown eth1
ifup eth0
ifup eth1
```

7. Konfiguration der physikalischen Netzwerk-Schnittstellen der Windows-Clients

Die physikalischen Schnittstellen der Hosts von den beiden Linux-VMs werden über „Systemsteuerung“ -> „Netzwerk- und Freigabecenter“ -> „Adaptoreinstellungen ändern“ -> „Ethernet-Adapter“ -> „Eigenschaften“ -> „Internetprotokoll, Version 4 (TCP/IPv4)“ -> „Eigenschaften“ geändert.

7.1. Konfiguration Host Inside-Router



7.2. Konfiguration Host Outside-Router



8. Deaktivierung der Windows-Firewall

Firewall auf den Windows-Clients deaktivieren.

9. Bereitstellung des Webserver

Auf dem physischen Host des Outside-Routers wird ein einfacher Webserver auf Port 80 gestartet. **Index.htm** in das Root-Verzeichnis des Webserver kopieren / aktualisieren.

10. Testen der Konfigurationen

- Zugriff auf das Internet vom Client aus dem Inside-Netz testen.
- Zugriff auf das Internet vom Client aus dem Outside-Netz testen
- Zugriff auf den Webserver aus dem Inside- und Labornetz (192.168.200.0/24) testen.

11. Einrichten der Firewall

Outside-Router:

Wir erstellen mit `mkdir /root/bin` den Ordner, wechseln dorthin und erstellen `touch firewall.sh` im Ordner **/root/bin/** als root folgendes **firewall.sh** Script und machen dieses mit `chmod 700 firewall.sh` ausführbar:

```
#!/bin/sh
case "$1" in
stop)
    echo
    echo "Stopping Firewall..."
    echo
    iptables -F
    iptables -P INPUT ACCEPT
```

FA54

P / LZ

Herr Henze

Gruppe 9

Andreas Biller, Rico Krüger

Thema: Aufbau einer DMZ

```
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
;;
start)
echo
echo "Starting Firewall..."
echo
iptables -A OUTPUT -p icmp --icmp-type 8 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p icmp --icmp-type 0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
;;
*)
echo "Es wurde kein oder ein falscher Parameter übergeben"
echo "start: Zum Starten der Firewall."
echo "stop: Zum Beenden der Firewall."
esac
iptables -L
```

Dann fügen wir den Ordner **/root/bin** zur PATH-Variablen hinzu, um das Script von überall ausführbar zu machen:

```
PATH=$PATH:/root/bin
```

Inside-Router:

Wir erstellen mit `mkdir /root/bin` den Ordner, wechseln dorthin und erstellen `touch firewall.sh` im Ordner **/root/bin/** als root folgendes **firewall.sh** Script und machen dieses mit `chmod 700 firewall.sh` ausführbar:

```
#!/bin/bash
if [ -z "$1" ]; then
echo ""
echo "enter \"start\" or \"stop\" as an argument to start or stop the
firewall"
echo "enter \"show\" as an argument to display the current configuration"
echo ""
exit 1
else
if [ "$1" = "start" ]; then
echo ""
echo "starting firewall..."
echo ""
# set default policy to drop everything
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
# flush all filter table rules
iptables -F
# flush all user defined filter table rules
# iptables -X
# allow outgoing ping request
iptables -A OUTPUT -p icmp --icmp-type 8 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
```

FA54

P / LZ

Herr Henze

Gruppe 9

Andreas Biller, Rico Krüger

Thema: Aufbau einer DMZ

```
iptables -A INPUT -p icmp --icmp-type 0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
# allow incoming ping request
iptables -A INPUT -p icmp --icmp-type 8 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type 0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
elif [ "$1" = "stop" ]; then
    echo ""
    echo "stopping firewall..."
    echo ""
    # allow everything
    iptables -P INPUT ACCEPT
    iptables -P FORWARD ACCEPT
    iptables -P OUTPUT ACCEPT
    # flush all filter table rules
    iptables -F
elif [ "$1" = "show" ]; then
    echo ""
    echo "showing iptables:"
    echo ""
    iptables -L
else
    echo ""
    echo "unrecognized argument: $1"
    echo "exiting script..."
    echo "enter \"start\" or \"stop\" as argument to start or stop the
firewall"
    echo ""
    exit 1
fi
# show iptables
iptables -L
echo ""
echo "Good job! All done."
echo ""
exit 0
fi
```

Dann fügen wir den Ordner **/root/bin** zur PATH-Variablen hinzu, um das Script von überall ausführbar zu machen:

```
PATH=$PATH:/root/bin
```

TODO: allow `ssh` for using `puTTY` and `xming` through **firewall.sh**, DNS mit NAMESERVER `ip-dns-labornetz` (inside und outside) in die `/etc/resolv.conf`

A.2 Detaillierte Zeitplanung

Analysephase	9 h
1. Analyse des Ist-Zustands	3 h
1.1. Fachgespräch mit der EDV-Abteilung	1 h
1.2. Prozessanalyse	2 h
2. „Make or buy“-Entscheidung und Wirtschaftlichkeitsanalyse	1 h
3. Erstellen eines „Use-Case“-Diagramms	2 h
4. Erstellen des Lastenhefts mit der EDV-Abteilung	3 h
Entwurfsphase	19 h
1. Prozessentwurf	2 h
2. Datenbankentwurf	3 h
2.1. ER-Modell erstellen	2 h
2.2. Konkretes Tabellenmodell erstellen	1 h
3. Erstellen von Datenverarbeitungskonzepten	4 h
3.1. Verarbeitung der CSV-Daten	1 h
3.2. Verarbeitung der SVN-Daten	1 h
3.3. Verarbeitung der Sourcen der Programme	2 h
4. Benutzeroberflächen entwerfen und abstimmen	2 h
5. Erstellen eines UML-Komponentendiagramms der Anwendung	4 h
6. Erstellen des Pflichtenhefts	4 h
Implementierungsphase	29 h
1. Anlegen der Datenbank	1 h
2. Umsetzung der HTML-Oberflächen und Stylesheets	4 h
3. Programmierung der PHP-Module für die Funktionen	23 h
3.1. Import der Modulinformationen aus CSV-Dateien	2 h
3.2. Parsen der Modulquelltexte	3 h
3.3. Import der SVN-Daten	2 h
3.4. Vergleichen zweier Umgebungen	4 h
3.5. Abrufen der von einem zu wählenden Benutzer geänderten Module	3 h
3.6. Erstellen einer Liste der Module unter unterschiedlichen Aspekten	5 h
3.7. Anzeigen einer Liste mit den Modulen und geparsen Metadaten	3 h
3.8. Erstellen einer Übersichtsseite für ein einzelnes Modul	1 h
4. Nächtlichen Batchjob einrichten	1 h
Abnahmetest der Fachabteilung	1 h
1. Abnahmetest der Fachabteilung	1 h
Einführungsphase	1 h
1. Einführung/Benutzerschulung	1 h
Erstellen der Dokumentation	9 h
1. Erstellen der Benutzerdokumentation	2 h
2. Erstellen der Projektdokumentation	6 h
3. Programmdokumentation	1 h
3.1. Generierung durch PHPdoc	1 h
Pufferzeit	2 h
1. Puffer	2 h
Gesamt	70 h

A.3 Lastenheft

Es folgt unser Lastenheft mit Fokus auf den Anforderungen:

Die Umsetzung muss folgende Anforderungen erfüllen:

1. DMZ

- 1.1. Die DMZ soll aus zwei virtuellen, zu Routern konfigurierten Linux-Distributionen bestehen, welche die Netze INSIDE, OUTSIDE und das DMZ-Netz miteinander verbinden.
- 1.2. Die Router sollen entsprechend des Netzplanes eingerichtet und konfiguriert werden.
- 1.3. Die DMZ soll Zugriffe auf den Webserver erlauben, aber Zugriffe auf das INSIDE-Netz verhindern. Hierzu soll auf dem Outside-Router NAT, Portforwarding und eine Firewall laufen.
- 1.4. Die Router sollen nur vom Client-Rechner her fernadministrierbar sein.

2. Client-Rechner

- 2.1. Der Client-Rechner im INSIDE-Netz nutzt das Betriebssystem Windows.
- 2.2. Der Webserver soll eine Webseite mit dem aktuellen Stand der Gruppe anzeigen.

3. Webserver

- 3.1. Der Webserver nutzt das Betriebssystem Windows. Er wird über das Tool Mini-Webserver vom Auftraggeber bereitgestellt.
- 3.2. Der Webserver im DMZ-Netz muss vom OUTSIDE-Netz über Port 80 erreichbar sein. Hierzu soll auf dem Outside-Router NAT und Port-Forwarding eingerichtet werden.
- 3.3. Der Webserver soll eine Webseite mit dem aktuellen Stand der Gruppe anzeigen.

4. Firewall

- 4.1. Die Firewall soll den Webserver in der DMZ über Port 80 erreichbar sein lassen.
- 4.2. Die Firewall soll SSH nur vom Admin-PC zulassen.
- 4.3. Die Firewall soll ICMP zulassen.
- 4.4. Die Firewall soll DNS zulassen.
- 4.5. Die Firewall soll RDP zulassen.
- 4.6. Die Firewall soll per Script an- und ausschaltbar sein. Hierzu muss an diversen Stellen per Script die Linux-Systemkonfiguration verändert werden

5. Sonstige Anforderungen

- 5.1. Das Projekt soll unter Berücksichtigung der von der IHK ausgegebenen Richtlinien für eine Projektdokumentation dokumentiert werden.
- 5.2. Es soll ein logischer Netzplan in Papierform erstellt und der Dokumentation angefügt werden.

- 5.3. Pro Person soll ein ausführliches Kompetenzportfolio erstellt werden, welches einen kritischen Überblick über unsere individuellen Kompetenzstände vor, während und nach dem Projekt liefert. Diese sollen der Dokumentation angehängt werden.
- 5.4. Die Funktionalität der Firewall soll getestet und die Ergebnisse in zwei Testprotokollen festgehalten werden. Diese sind der Dokumentation anzuhängen.

A.4 Use Case-Diagramm

Use Case-Diagramme und weitere UML-Diagramme kann man auch direkt mit L^AT_EX zeichnen, siehe z. B. <http://metauml.sourceforge.net/old/usecase-diagram.html>.

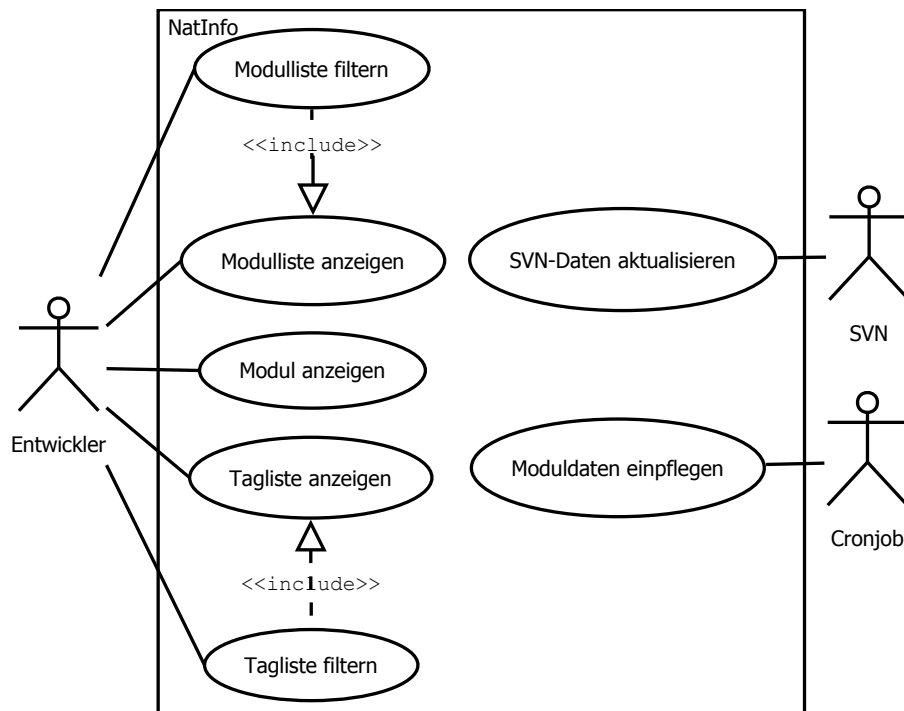


Abbildung 3: Use Case-Diagramm

A.5 Pflichtenheft (Auszug)

Zielbestimmung

1. Musskriterien

1.1. Modul-Liste: Zeigt eine filterbare Liste der Module mit den dazugehörigen Kerninformationen sowie Symbolen zur Einhaltung des Entwicklungsprozesses an

- In der Liste wird der Name, die Bibliothek und Daten zum Source und Kompilat eines Moduls angezeigt.
- Ebenfalls wird der Status des Moduls hinsichtlich Source und Kompilat angezeigt. Dazu gibt es unterschiedliche Status-Zeichen, welche symbolisieren in wie weit der Entwicklungsprozess eingehalten wurde bzw. welche Schritte als nächstes getan werden müssen. So gibt es z. B. Zeichen für das Einhalten oder Verletzen des Prozesses oder den Hinweis auf den nächsten zu tätigenden Schritt.
- Weiterhin werden die Benutzer und Zeitpunkte der aktuellen Version der Sourcen und Kompilate angezeigt. Dazu kann vorher ausgewählt werden, von welcher Umgebung diese Daten gelesen werden sollen.

- Es kann eine Filterung nach allen angezeigten Daten vorgenommen werden. Die Daten zu den Sourcen sind historisiert. Durch die Filterung ist es möglich, auch Module zu finden, die in der Zwischenzeit schon von einem anderen Benutzer editiert wurden.
- 1.2. Tag-Liste: Bietet die Möglichkeit die Module anhand von Tags zu filtern.
- Es sollen die Tags angezeigt werden, nach denen bereits gefiltert wird und die, die noch der Filterung hinzugefügt werden könnten, ohne dass die Ergebnisliste leer wird.
 - Zusätzlich sollen die Module angezeigt werden, die den Filterkriterien entsprechen. Sollten die Filterkriterien leer sein, werden nur die Module angezeigt, welche mit einem Tag versehen sind.
- 1.3. Import der Moduldaten aus einer bereitgestellten [CSV](#)-Datei
- Es wird täglich eine Datei mit den Daten der aktuellen Module erstellt. Diese Datei wird (durch einen Cronjob) automatisch nachts importiert.
 - Dabei wird für jedes importierte Modul ein Zeitstempel aktualisiert, damit festgestellt werden kann, wenn ein Modul gelöscht wurde.
 - Die Datei enthält die Namen der Umgebung, der Bibliothek und des Moduls, den Programmtyp, den Benutzer und Zeitpunkt des Sourcecodes sowie des Kompilats und den Hash des Sourcecodes.
 - Sollte sich ein Modul verändert haben, werden die entsprechenden Daten in der Datenbank aktualisiert. Die Veränderungen am Source werden dabei aber nicht ersetzt, sondern historisiert.
- 1.4. Import der Informationen aus SVN. Durch einen „post-commit-hook“ wird nach jedem Einchecken eines Moduls ein [PHP](#)-Script auf der Konsole aufgerufen, welches die Informationen, die vom SVN-Kommandozeilentool geliefert werden, an NatInfo übergibt.
- 1.5. Parsen der Sourcen
- Die Sourcen der Entwicklungsumgebung werden nach Tags, Links zu Artikeln im Wiki und Programmbeschreibungen durchsucht.
 - Diese Daten werden dann entsprechend angelegt, aktualisiert oder nicht mehr gesetzte Tags/Wikiartikel entfernt.
- 1.6. Sonstiges
- Das Programm läuft als Webanwendung im Intranet.
 - Die Anwendung soll möglichst leicht erweiterbar sein und auch von anderen Entwicklungsprozessen ausgehen können.
 - Eine Konfiguration soll möglichst in zentralen Konfigurationsdateien erfolgen.

Produkteinsatz

1. Anwendungsbereiche

Die Webanwendung dient als Anlaufstelle für die Entwicklung. Dort sind alle Informationen

für die Module an einer Stelle gesammelt. Vorher getrennte Anwendungen werden ersetzt bzw. verlinkt.

2. Zielgruppen

NatInfo wird lediglich von den Natural-Entwicklern in der EDV-Abteilung genutzt.

3. Betriebsbedingungen

Die nötigen Betriebsbedingungen, also der Webserver, die Datenbank, die Versionsverwaltung, das Wiki und der nächtliche Export sind bereits vorhanden und konfiguriert. Durch einen täglichen Cronjob werden entsprechende Daten aktualisiert, die Webanwendung ist jederzeit aus dem Intranet heraus erreichbar.

A.6 Netzplan

Der Netzplan unserer [DMZ](#)

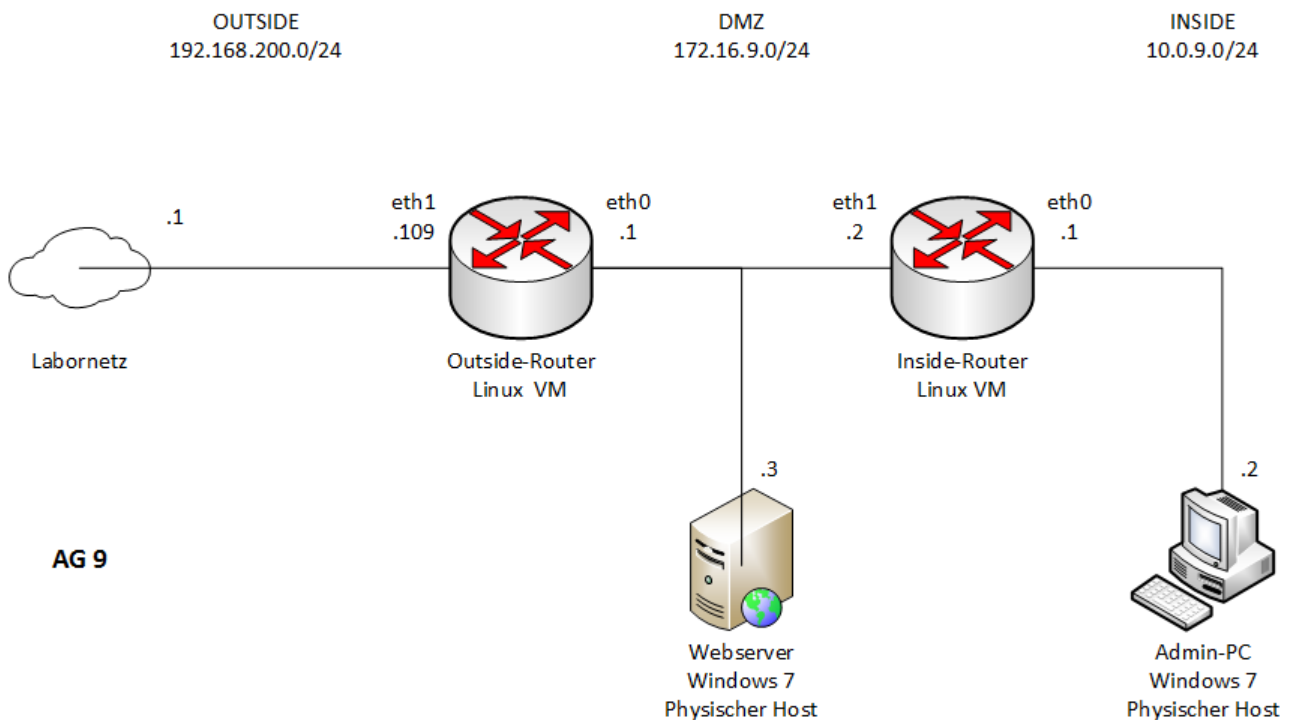


Abbildung 4: Netzplan der DMZ (Arbeitsgruppe 9)

A.7 Oberflächenentwürfe

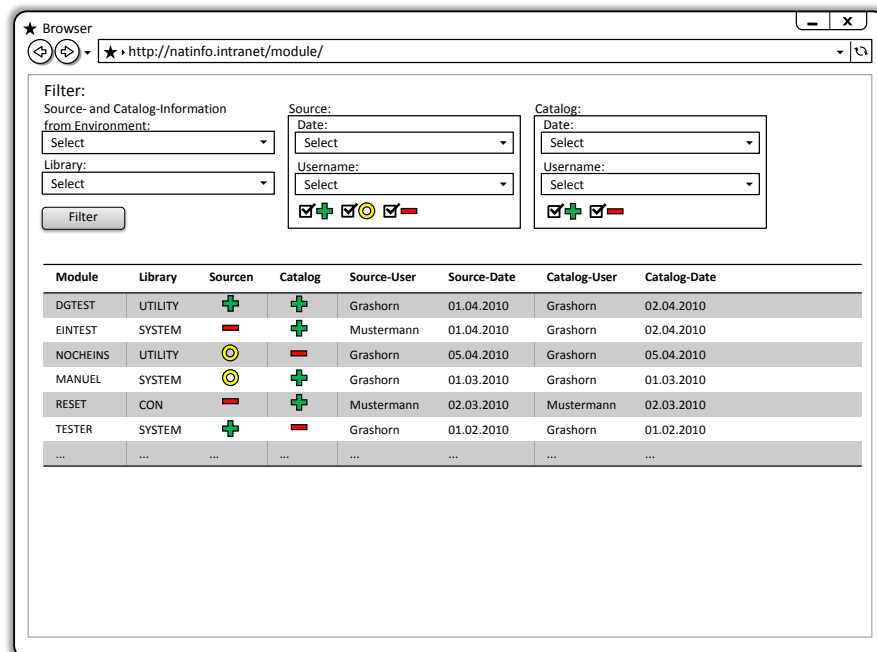


Abbildung 5: Liste der Module mit Filtermöglichkeiten

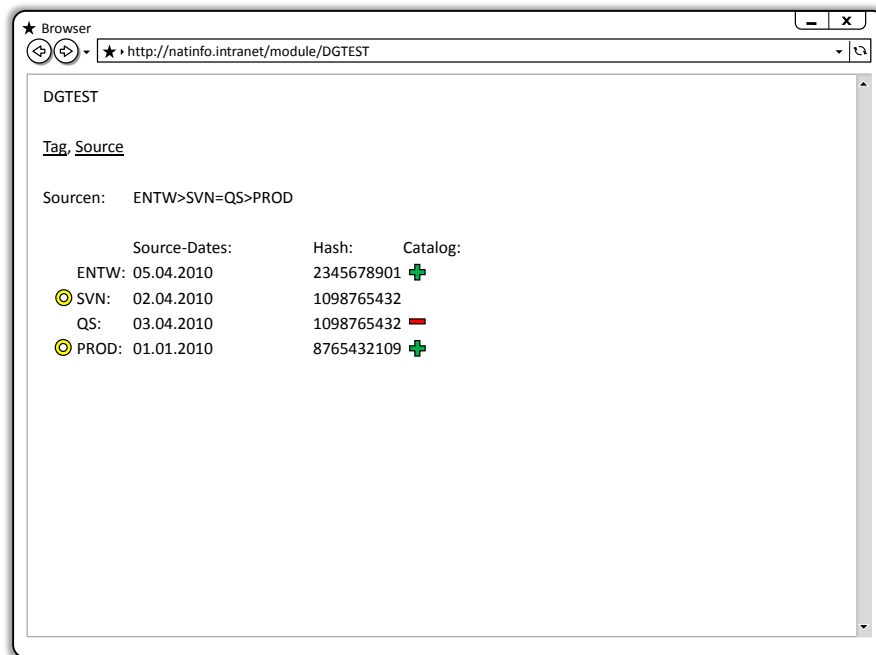


Abbildung 6: Anzeige der Übersichtsseite einzelner Module

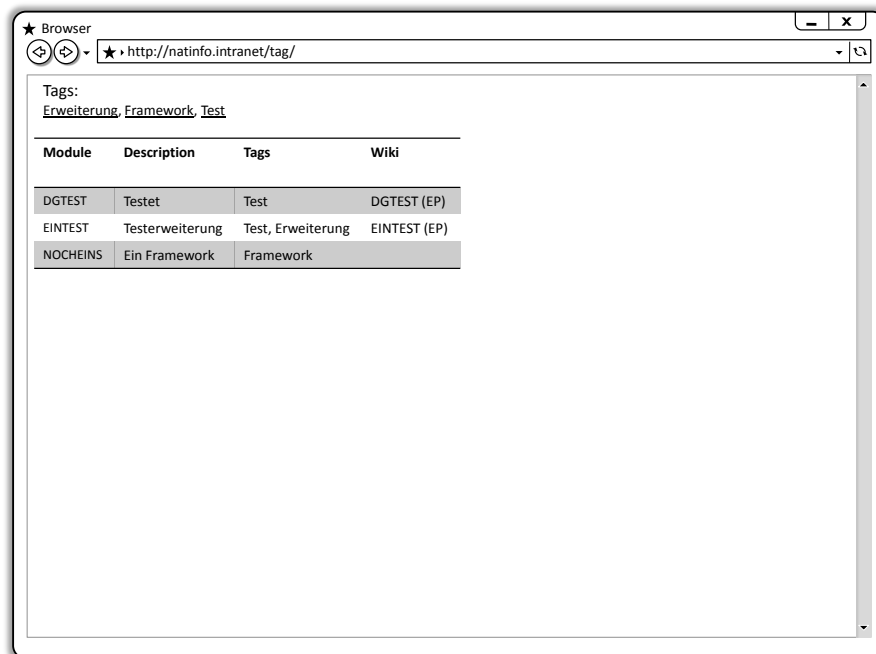
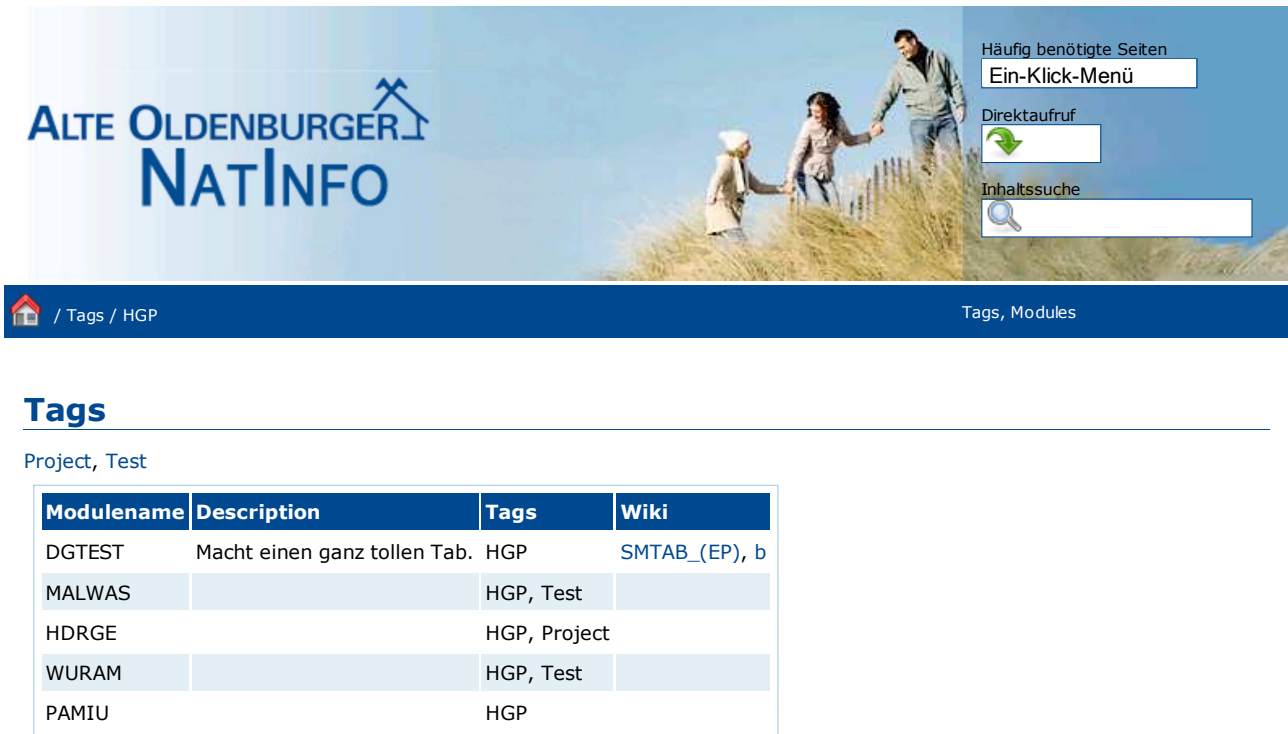


Abbildung 7: Anzeige und Filterung der Module nach Tags

A.8 Screenshots der Anwendung



The screenshot shows the website 'ALTE OLDENBURGER NATINFO'. The header features a blue sky background with a family walking on a grassy dune. On the right, there are links for 'Häufig benötigte Seiten', 'Ein-Klick-Menü', 'Direktaufruf', and 'Inhaltssuche'. Below the header, a blue navigation bar shows the breadcrumb '/ Tags / HGP' and the text 'Tags, Modules'. The main content area is titled 'Tags' and displays a table of modules filtered by the tag 'HGP'.

Modulename	Description	Tags	Wiki
DGTEST	Macht einen ganz tollen Tab.	HGP	SMTAB_(EP), b
MALWAS		HGP, Test	
HDRGE		HGP, Project	
WURAM		HGP, Test	
PAMIU		HGP	

Abbildung 8: Anzeige und Filterung der Module nach Tags



Modules

Environment	ENTW
Library	Select
Catalog user	Select
Catalog date	Select
Source user	Select
Source date	Select
Reset Filter	











Name	Library	Source	Catalog	Source-User	Source-Date	Catalog-User	Catalog-Date
SMTAB	UTILITY			MACKE	01.04.2010 13:00	MACKE	01.04.2010 13:00
DGTAB	CON			GRASHORN	01.04.2010 13:00	GRASHORN	01.04.2010 13:00
DGTEST	SUP			GRASHORN	05.04.2010 13:00	GRASHORN	05.04.2010 13:00
OHNETAG	CON			GRASHORN	05.04.2010 13:00	GRASHORN	01.04.2010 15:12
OHNEWIKI	CON			GRASHORN	05.04.2010 13:00	MACKE	01.04.2010 15:12

Abbildung 9: Liste der Module mit Filtermöglichkeiten

A.9 Entwicklerdokumentation

lib-model

[class tree: lib-model] [index: lib-model] [all elements]

Packages:
lib-model

Files:
Naturalmodulename.php

Classes:
Naturalmodulename

Class: Naturalmodulename

Source Location: /Naturalmodulename.php

Class Overview

BaseNaturalmodulename
|
--Naturalmodulename

Subclass for representing a row from the
'NaturalModulename' table.

Methods

- [__construct](#)
- [getNaturalTags](#)
- [getNaturalWikis](#)
- [loadNaturalModuleInformation](#)
- [__toString](#)

Class Details

[line 10]
Subclass for representing a row from the 'NaturalModulename' table.

Adds some business logic to the base.

[\[Top \]](#)

Class Methods

constructor [__construct](#) [line 56]

Naturalmodulename [__construct](#)()

Initializes internal state of Naturalmodulename object.

Tags:

see: parent::__construct()
access: public

[\[Top \]](#)

method [getNaturalTags](#) [line 68]

array [getNaturalTags](#)()

Returns an Array of NaturalTags connected with this Modulename.

Tags:

return: Array of NaturalTags
access: public

[\[Top \]](#)

method getNaturalWikis [line 83]

```
array getNaturalWikis( )
```

Returns an Array of NaturalWikis connected with this Modulename.

Tags:

return: Array of NaturalWikis
access: public

[\[Top \]](#)

method loadNaturalModuleInformation [line 17]

```
ComparedNaturalModuleInformation  
loadNaturalModuleInformation( )
```

Gets the ComparedNaturalModuleInformation for this NaturalModulename.

Tags:

access: public

[\[Top \]](#)

method __toString [line 47]

```
string __toString( )
```

Returns the name of this NaturalModulename.

Tags:

access: public

[\[Top \]](#)

Documentation generated on Thu, 22 Apr 2010 08:14:01 +0200 by [phpDocumentor 1.4.2](#)

A.10 Testfall und sein Aufruf auf der Konsole

```

1 <?php
2 include(dirname(__FILE__).'/../bootstrap/Propel.php');
3
4 $t = new lime_test(13);
5
6 $t->comment('Empty Information');
7 $emptyComparedInformation = new ComparedNaturalModuleInformation(array());
8 $t->is($emptyComparedInformation->getCatalogSign(), ComparedNaturalModuleInformation::EMPTY_SIGN, '
    Has no catalog sign');
9 $t->is($emptyComparedInformation->getSourceSign(), ComparedNaturalModuleInformation::SIGN_CREATE, '
    Source has to be created');
10
11 $t->comment('Perfect Module');
12 $criteria = new Criteria();
13 $criteria->add(NaturalmodulePeer::NAME, 'SMTAB');
14 $moduleName = NaturalmodulePeer::doSelectOne($criteria);
15 $t->is($moduleName->getName(), 'SMTAB', 'Right module name selected');
16 $comparedInformation = $moduleName->loadNaturalModuleInformation();
17 $t->is($comparedInformation->getSourceSign(), ComparedNaturalModuleInformation::SIGN_OK, 'Source sign
    shines global');
18 $t->is($comparedInformation->getCatalogSign(), ComparedNaturalModuleInformation::SIGN_OK, 'Catalog sign
    shines global');
19 $infos = $comparedInformation->getNaturalModuleInformations();
20 foreach($infos as $info)
21 {
22     $env = $info->getEnvironmentName();
23     $t->is($info->getSourceSign(), ComparedNaturalModuleInformation::SIGN_OK, 'Source sign shines at ' . $env);
24     if ($env != 'SVNENTW')
25     {
26         $t->is($info->getCatalogSign(), ComparedNaturalModuleInformation::SIGN_OK, 'Catalog sign shines at ' .
            $info->getEnvironmentName());
27     }
28     else
29     {
30         $t->is($info->getCatalogSign(), ComparedNaturalModuleInformation::EMPTY_SIGN, 'Catalog sign is empty
            at ' . $info->getEnvironmentName());
31     }
32 }
33 ?>

```



```

ao-suse-ws1.ao-dom.alte-oldenburger.de - PuTTY
ao-suse-ws1:/srv/www/symfony/natural # ./symfony test:unit ComparedNaturalModuleInformation
1..13
# Empty Information
ok 1 - Has no catalog sign
ok 2 - Source has to be created
# Perfect Module
ok 3 - Right modulename selected
ok 4 - Source sign shines global
ok 5 - Catalog sign shines global
ok 6 - Source sign shines at ENTW
ok 7 - Catalog sign shines at ENTW
ok 8 - Source sign shines at QS
ok 9 - Catalog sign shines at QS
ok 10 - Source sign shines at PROD
ok 11 - Catalog sign shines at PROD
ok 12 - Source sign shines at SVNENTW
ok 13 - Catalog sign is empty at SVNENTW
# Looks like everything went fine.
ao-suse-ws1:/srv/www/symfony/natural #

```

Abbildung 10: Aufruf des Testfalls auf der Konsole

A.11 Klasse: ComparedNaturalModuleInformation

Kommentare und simple Getter/Setter werden nicht angezeigt.

```

1 <?php
2 class ComparedNaturalModuleInformation
3 {
4     const EMPTY_SIGN = 0;
5     const SIGN_OK = 1;
6     const SIGN_NEXT_STEP = 2;
7     const SIGN_CREATE = 3;
8     const SIGN_CREATE_AND_NEXT_STEP = 4;
9     const SIGN_ERROR = 5;
10
11     private $naturalModuleInformations = array();
12
13     public static function environments()
14     {
15         return array("ENTW", "SVNENTW", "QS", "PROD");
16     }
17
18     public static function signOrder()
19     {
20         return array(self::SIGN_ERROR, self::SIGN_NEXT_STEP, self::SIGN_CREATE_AND_NEXT_STEP, self::SIGN_CREATE, self::SIGN_OK);
21     }
22
23     public function __construct(array $naturalInformations)
24     {
25         $this->allocateModulesToEnvironments($naturalInformations);

```

A Anhang

```

26     $this->allocateEmptyModulesToMissingEnvironments();
27     $this->determineSourceSignsForAllEnvironments();
28 }
29
30 private function allocateModulesToEnvironments(array $naturalInformations)
31 {
32     foreach ($naturalInformations as $naturalInformation)
33     {
34         $env = $naturalInformation->getEnvironmentName();
35         if (in_array($env, self::environments()))
36         {
37             $this->naturalModuleInformations[array_search($env, self::environments())] = $naturalInformation;
38         }
39     }
40 }
41
42 private function allocateEmptyModulesToMissingEnvironments()
43 {
44     if (array_key_exists(0, $this->naturalModuleInformations))
45     {
46         $this->naturalModuleInformations[0]->setSourceSign(self::SIGN_OK);
47     }
48
49     for ($i = 0; $i < count(self::environments()); $i++)
50     {
51         if (!array_key_exists($i, $this->naturalModuleInformations))
52         {
53             $environments = self::environments();
54             $this->naturalModuleInformations[$i] = new EmptyNaturalModuleInformation($environments[$i]);
55             $this->naturalModuleInformations[$i]->setSourceSign(self::SIGN_CREATE);
56         }
57     }
58 }
59
60 public function determineSourceSignsForAllEnvironments()
61 {
62     for ($i = 1; $i < count(self::environments()); $i++)
63     {
64         $currentInformation = $this->naturalModuleInformations[$i];
65         $previousInformation = $this->naturalModuleInformations[$i - 1];
66         if ($currentInformation->getSourceSign() <> self::SIGN_CREATE)
67         {
68             if ($previousInformation->getSourceSign() <> self::SIGN_CREATE)
69             {
70                 if ($currentInformation->getHash() <> $previousInformation->getHash())
71                 {
72                     if ($currentInformation->getSourceDate('YmdHis') > $previousInformation->getSourceDate('YmdHis'))
73                     {
74                         $currentInformation->setSourceSign(self::SIGN_ERROR);
75                     }
76                 }
77             }
78         }
79     }
80 }

```

A Anhang

```

76         else
77         {
78             $currentInformation->setSourceSign(self::SIGN_NEXT_STEP);
79         }
80     }
81     else
82     {
83         $currentInformation->setSourceSign(self::SIGN_OK);
84     }
85 }
86 else
87 {
88     $currentInformation->setSourceSign(self::SIGN_ERROR);
89 }
90 }
91 elseif ($previousInformation->getSourceSign() <> self::SIGN_CREATE && $previousInformation->
    getSourceSign() <> self::SIGN_CREATE_AND_NEXT_STEP)
92 {
93     $currentInformation->setSourceSign(self::SIGN_CREATE_AND_NEXT_STEP);
94 }
95 }
96 }
97
98 private function containsSourceSign($sign)
99 {
100     foreach($this->naturalModuleInformations as $information)
101     {
102         if($information->getSourceSign() == $sign)
103         {
104             return true;
105         }
106     }
107     return false ;
108 }
109
110 private function containsCatalogSign($sign)
111 {
112     foreach($this->naturalModuleInformations as $information)
113     {
114         if($information->getCatalogSign() == $sign)
115         {
116             return true;
117         }
118     }
119     return false ;
120 }
121 }
122 ?>

```

A.12 Klassendiagramm

Klassendiagramme und weitere UML-Diagramme kann man auch direkt mit \LaTeX zeichnen, siehe z. B. <http://metauml.sourceforge.net/old/class-diagram.html>.

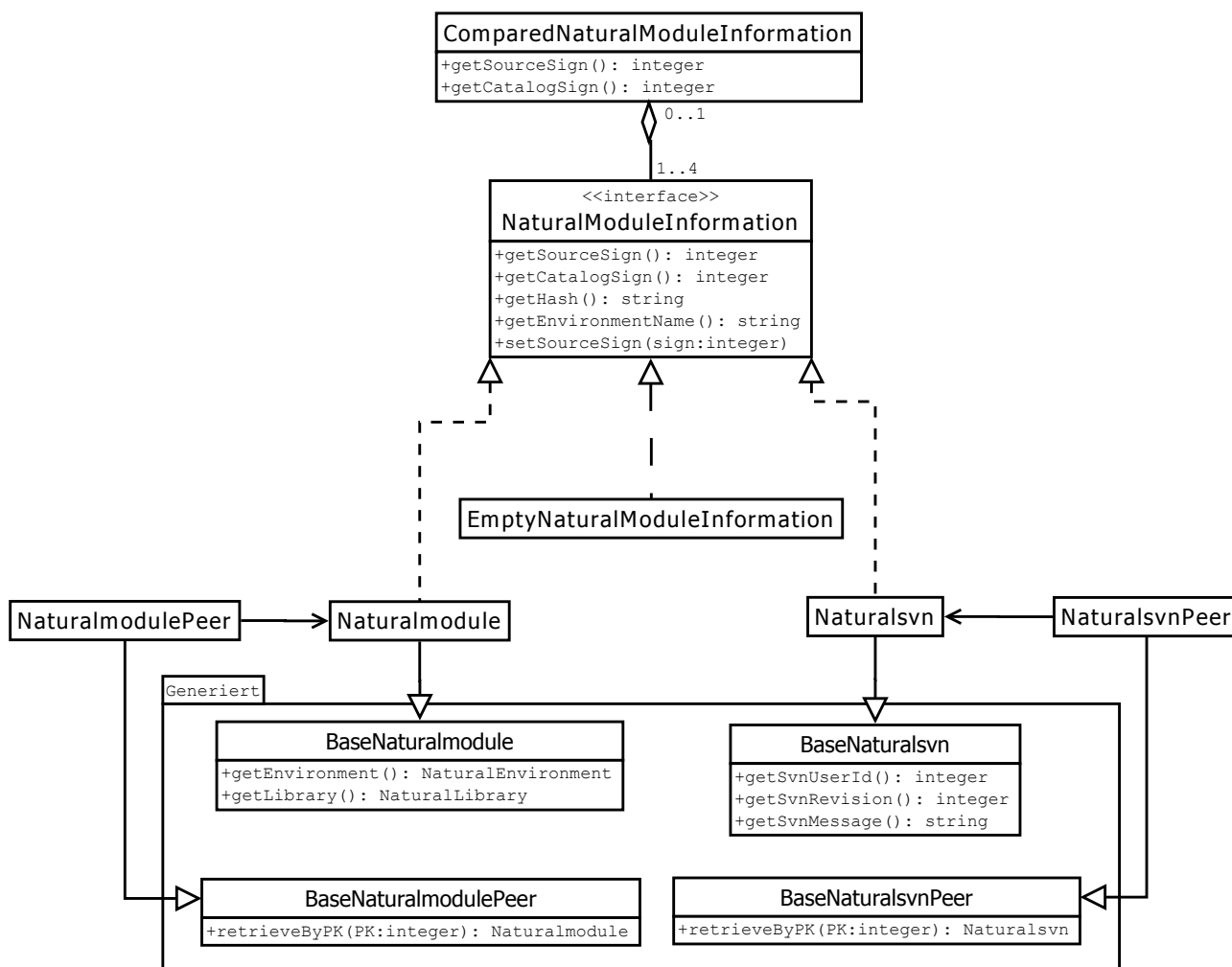







Abbildung 11: Klassendiagramm

A.13 Benutzerdokumentation

Ausschnitt aus der Benutzerdokumentation:

Symbol	Bedeutung global	Bedeutung einzeln
	Alle Module weisen den gleichen Stand auf.	Das Modul ist auf dem gleichen Stand wie das Modul auf der vorherigen Umgebung.
	Es existieren keine Module (fachlich nicht möglich).	Weder auf der aktuellen noch auf der vorherigen Umgebung sind Module angelegt. Es kann also auch nichts übertragen werden.
	Ein Modul muss durch das Übertragen von der vorherigen Umgebung erstellt werden.	Das Modul der vorherigen Umgebung kann übertragen werden, auf dieser Umgebung ist noch kein Modul vorhanden.
	Auf einer vorherigen Umgebung gibt es ein Modul, welches übertragen werden kann, um das nächste zu aktualisieren.	Das Modul der vorherigen Umgebung kann übertragen werden um dieses zu aktualisieren.
	Ein Modul auf einer Umgebung wurde entgegen des Entwicklungsprozesses gespeichert.	Das aktuelle Modul ist neuer als das Modul auf der vorherigen Umgebung oder die vorherige Umgebung wurde übersprungen.