IT-Sicherheitslabor – Ein praxisorientierter Ansatz zur Zusammenarbeit von Hochschule und Industrie in der Lehre

Sebastian Abeck, Robert Reutter, Aleksander Dikanski, Philipp Schleier
Forschungsgruppe Cooperation & Management, Karlsruher Institut für Technologie (KIT)
{abeck, aleksander.dikansk}@kit.edu, {robert.reutter, philipp.schleier}@student.kit.edu

Jürgen Biermann, Ingo Pansa
iC Consult GmbH
{juergen.biermann, ingo.pansa}@ic-consult.de

Zusammenfassung

Das IT-Sicherheitslabor ist ein sowohl von Hochschulseite als auch von Industrieseite aktiv unterstützter Ansatz, eine wissenschaftlich fundierte und praxisorientierte Ausbildung in einem bedeutenden Teilbereich der Informatik, der Sicherheit von Informationstechnologie, voranzutreiben. Im Labor werden praktische Fragestellungen, die in gemeinsamen Kooperationsprojekten gesammelt wurden, in einer pädagogisch angemessenen Form aufbereitet. Die am Labor teilnehmenden Studierenden werden so an die Praxis herangeführt. Durch den Ansatz wird eine enge Verzahnung von Lehre und Praxis erreicht, indem das in den Kooperationsprojekten erworbene Wissen wieder zurück in das Labor und damit unmittelbar in die Lehre einfließt.

1. Einleitung

Damit die universitäre Bachelorausbildung den Anforderungen eines berufsqualifizierenden Abschlusses in Zukunft auch tatsächlich gerecht wird, müssen verstärkt praxisorientierte Elemente in die entsprechenden Studiengänge einbezogen werden. Ein Beispiel eines solchen Angebots ist das am Karlsruher Institut für Technologie (KIT) aufgebaute IT-Sicherheitslabor. Hierin werden Informatik-Bachelor-Studierende im Rahmen eines Praktikums an konkrete Sicherheitsfragestellungen herangeführt, die sich in realen Unternehmensumgebungen stellen. Das Innovative an diesem Labor ist die direkte Einbeziehung eines Industriepartners in die Konzeption der zu lösenden Praktikumsaufgaben, wodurch der industrielle Praxisbezug von Anfang an hergestellt wird. Der Industriepartner ist im Fall des IT-Sicherheitslabors das Unternehmen iC Consult[1], das als Integrationsdienstleister im Kontext komplexer Identitätsmanagement- und Zugriffskontrollfragestellungen jeweils die am besten geeigneten Lösungen entwickelt. In der Vergangenheit hat der Lehrstuhl, an dem das IT-Sicherheitslabor entwickelt wurde, in Kooperation mit dem Industriepartner zahlreiche dieser Projekte im Rahmen von Diplom- bzw. Masterarbeiten durchgeführt. Die aus pädagogischer Sicht besonders wertvollen Projektlösungen werden für das Labor so aufbereitet, dass ein Bachelor-Studierender systematisch an die Problemstellung herangeführt wird und im Rahmen von Aufgaben Teile der Lösung entwickelt und praktisch anwendet.

Das IT-Sicherheits-Laborsystem ist ein Vorgehensmodell zur Überführung konkreter industrieller Problemstellung in die praxisorientierte Lehre. Durch die Zusammenarbeit mit dem Partner iC Consult eröffnet sich die Möglichkeit, aktuelle Problemstellungen zu beziehen, die die Industrie beschäftigen. Diese werden dann innerhalb der C&M Forschungsgruppe[2] als Praktikum angeboten.

Aufgrund der Komplexität derartig konkreter Problemstellungen ist es nötig, diese zur Bearbeitung vom konkreten Anwendungsfall auf die übergeordneten Fragestellungen zu abstrahieren. Die so entstandenen allgemeinen Fragestellungen bilden jeweils ein im Sicherheitslabor zu bearbeitendes Sicherheitsszenario. Dieses wird zur Ausarbeitung in seine Kernpunkte unterteilt, die jeweils den

[1] iC Consult Gesellschaft für Systemintegration und Kommunikation mbH. Kooperationspartner der C&M-Forschungsgruppe. Web-Adresse: http://www.ic-consult.com/
[2] Die Forschungsgruppe Cooperation und Management (C&M) ist Teil des Instituts für Telematik an der Fakultät für Informatik der Universität Karlsruhe. Web-Adresse: http://www.cm-tm.uka.de/

Ausgangspunkt für ein Lernziel bilden. Anhand praktischer Aufgaben sollen die Studierenden die entsprechenden Kompetenzen zum Erreichen des Lernziels aufbauen. Bei der Bearbeitung wird von Seiten der Betreuung ein Lösungsleitfaden zur Verfügung gestellt, der die Studierenden bei der zielgerichteten Lösung des gestellten Problems unterstützen soll. Dieser Leitfaden, sowie die von den Studierenden zu erarbeitende Dokumentation, ist ein spezielles wissenschaftliches Dokument, das von der Forschungsgruppe erarbeitete Konventionen erfüllt. Diese wurden durch den Lehrstuhl entwickelt und sind ein seit Jahren erprobtes Mittel, das im Bereich der Informatik zu hohem Lernerfolg führt und die Wiederverwendbarkeit der Dokumente gewährleistet.

2. Eigenschaften und Einordnung des IT-Sicherheitslabors

An das im IT-Sicherheitslabor verwendete Lehrmaterial wird die Anforderung gestellt, dass es von den Laborteilnehmern weitestgehend im Selbststudium bearbeitet werden kann. Daher wird bei der Beschreibung der durchzuführenden praktischen Aufgaben viel Wert auf eine präzise Darstellung der durchzuführenden Schritte gelegt, um den jeweiligen Versuchsaufbau selbstständig durchführen zu können. Der Versuchsaufbau besteht dabei aus verschiedenen Arten von (System-, Sicherheits- und Anwendungs-) Softwaresystemen, die auf virtuellen Maschinen zu installieren und auf geeignete Weise zu konfigurieren sind. Dieser Teil der Beschreibungen des IT-Sicherheitslabors weist Ähnlichkeiten mit den sowohl zu OpenSource-Softwareprodukten als auch zu kommerziellen Softwareprodukten bestehenden Tutorien auf. Beispiele solcher Tutorien sind [Li05], [JB+07], [Ru02].

Dieser auf Selbststudium und selbstständigen Aufbau des Versuchsaufbaus ausgelegte Teil des IT-Sicherheitslabors ist der virtuelle Anteil des Labors; das Praktikum wird daher teilweise als eine virtuelle Lehrveranstaltung [Br03] angeboten. Der Praktikumsteilnehmer soll dabei lernen, die notwendigen Schritte zur Lösung des gestellten Sicherheitsproblems ausschließlich auf der Grundlage der vorgegebenen Beschreibungen und zunächst ohne Inanspruchnahme eines Betreuers selbstständig durchzuführen – eine Fähigkeit, die von jedem Ingenieur / Informatiker in der industriellen Praxis als eine Selbstverständlichkeit gefordert wird. Ein vergleichbarer Ansatz, der ebenfalls im Bereich der IT-Sicherheit angesiedelt ist und auf den Konzepten des Tele-Tutoring und des virtuellen Labors aufsetzt, ist das in [HM+04] beschriebene Tele-Lab.

Eine spezifische Eigenschaft des IT-Sicherheitslabors besteht darin, dass das Konzept bereits in seinem Kern eine enge Verzahnung mit einem Industriepartner und den gemeinsam durchgeführten Industrieprojekten vorsieht. An der Gestaltung des Lehr- und Lernkonzepts waren von Anfang an sowohl Mitarbeiter des Lehrstuhls, das das Praktikum anbietet als auch Mitarbeiter des Industriepartners beteiligt. Hierdurch wird sichergestellt, dass der Industriepartner aktiv zur praxisorientierten Ausbildung beiträgt. Die das Labor durchlaufenden Studierenden werden an die sich in der Praxis stellenden Projektaufgaben etappenweise herangeführt, wie Abbildung 1 des folgenden Abschnitts verdeutlicht. Dies ist tatsächlich die große Stärke des verfolgten IT-Sicherheitslabor-Ansatzes.

3. Einordnung des Labors in den Studiengang eines Studierenden

Der Studierende kommt mit dem Labor in Kontakt, wenn er ein zur Vorlesung "Web-Anwendungen und Serviceorientierte Architekturen" (WASA, [Ab12]) begleitendes Praktikum belegt und sich im Bereich der Sicherheit von Web-Anwendungen vertiefen möchte.

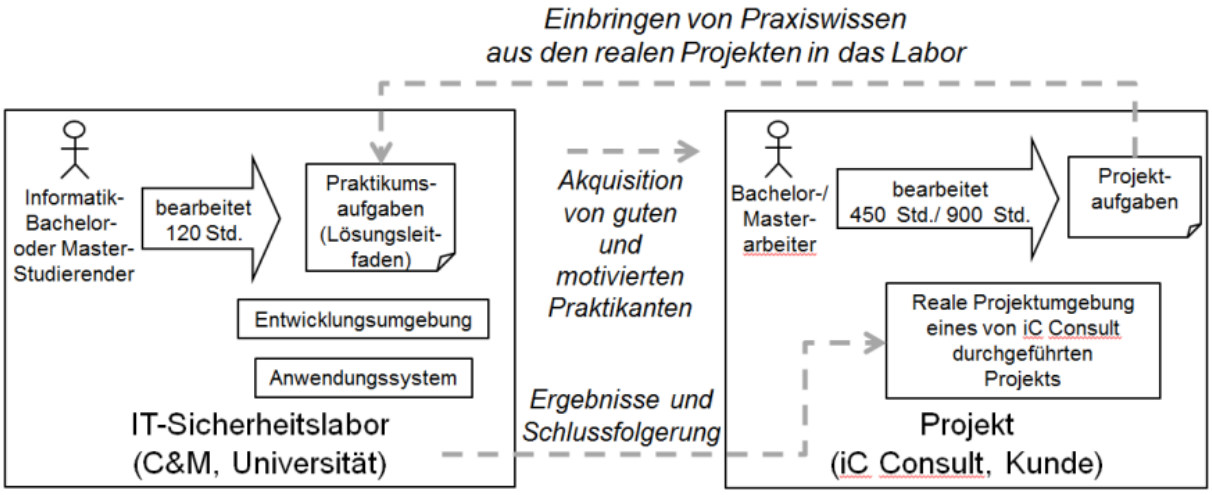

Abbildung 1: Einordnung des Labors in die Arbeiten der Studierenden

Das Praktikum hat einen Umfang von 4 Leistungspunkten, wobei ein Leistungspunkt einem Umfang von 30 Arbeitsstunden entspricht. Die Praktikumsaufgaben sind Teil des sog. Lösungsleitfadens. Der Lösungsleitfaden wird zu einem im Labor zu behandelnden Thema mit einem praktischen Szenario eingeführt. Außerdem werden Lernziele formuliert, zu denen Aufgaben gestellt werden, die zur Erreichung dieser Lernziele beitragen. Ferner wird ein Weg zur Lösung der Aufgaben angegeben, damit der Studierende die Aufgaben in angemessener Zeit durchführen kann. Die Vorbereitung eines Studierenden auf eine Bachelor-/Masterarbeiter auf dem Gebiet der IT-Sicherheit ist neben der praxisnahen Ausbildung ein wesentliches Ziel des IT-Sicherheitslabors.

Ein Ziel des Konzepts ist, die Inhalte des IT-Sicherheitslabors ständig aktuell zu halten, um die neuen Studierenden möglichst nahe an die in den aktuell laufenden Projekten behandelten Fragestellungen heranzuführen. Die Rückführung der Projektinhalte in das Labor gehört zu den Aufgaben der Bachelor-/Masterarbeiter, die bei C&M die Rolle eines sog. SeniorStudents einnehmen und eine Ko-Betreuung der Praktikanten (JuniorStudents) übernehmen. Die Ergebnisse der Labor-Experimente sowie die gewonnenen Erfahrungen werden dem Industriepartner (iC Consult) präsentiert. In Form einer Bachelor- oder Master-Arbeit oder durch den Industriepartner selbst können die Ergebnisse bzw. die analysierten Schlussfolgerungen in die reale Projektumgebung und somit in das Projekt des Industriepartners zurückgeführt werden.

4. Die wesentlichen Bestandteile und Artefakte des Labors

Das IT-Sicherheitslabor besteht aus einer Reihe von wiederverwendbaren Bestandteilen, die in ihrer Gesamtheit das Labor bilden. Es ist eine Arbeitsstätte für technische Arbeiten, Untersuchungen und Versuche. Die genaue Beschreibung der einzelnen Komponenten, deren Einsatzmöglichkeiten und Zusammenspiel, sind Teil des sogenannten Laborsystems. Diese Beschreibungen, zusammen mit einem Laborsystem-Entwicklungsprozess, bilden ein Vorgehensmodell zur Erstellung von Laboratorien [Re12]. Als Beispiel für konkrete Komponenten ist hier das Laborthema "Sichere Java Web-Komponenten" (siehe auch Kapitel 5) dargestellt. Dies ist das erste aufgestellte IT-Sicherheitslabor, die Problemstellung ist in diesem Fall, anstatt wie im Regelfall von einem Industriepartner überliefert, dem C&M-Umfeld entnommen worden.

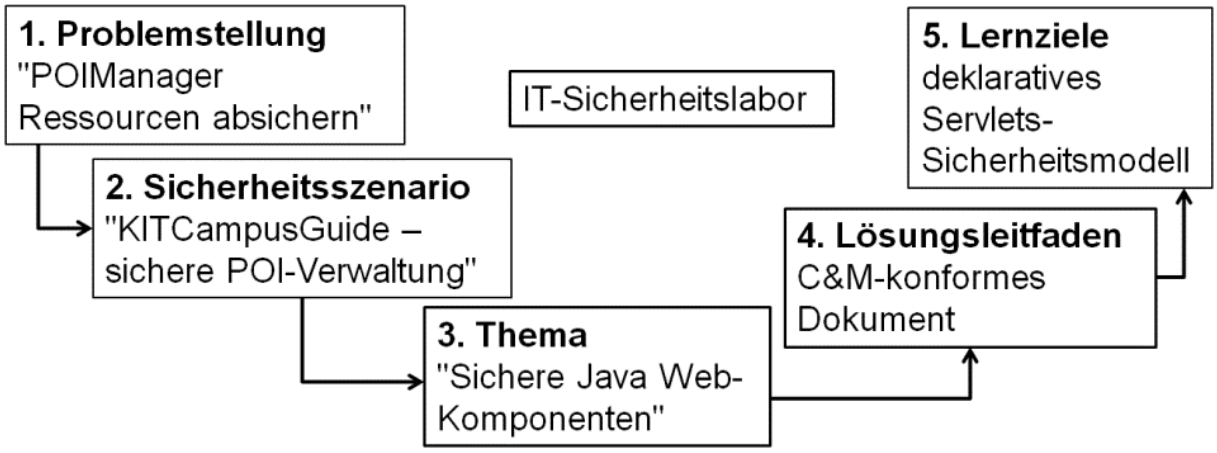

Abbildung 2: Bestandteile des Labors

Die **Problemstellung** wird von dem Industriepartner des Labors gestellt. Neben einer Beschreibung des Problems wird in der Regel eine Reihe von Anforderungen beschrieben. Die Problemstellung wird zur Behandlung innerhalb des Labors in ein **Sicherheitsszenario** abstrahiert. Das Sicherheitsszenario ist eine weiterführende Analyse der Problemstellung, die in der Regel bereits einen Lösungsansatz beschreibt. Das Szenario kann durch Fließtext, Grafiken und UML-Verhaltensdiagramme beschrieben werden. Innerhalb eines Labors können mehrere **Themen** behandelt werden. So wird innerhalb des IT-Sicherheitslabors das Thema "Sichere Java Web-Komponenten" behandelt, dieses leitet sich direkt aus dem Sicherheitsszenario „KITCampusGuide – sichere POI-Verwaltung“ ab. Ein zu jedem Thema bestehender **Lösungsleitfaden** beinhaltet die Beschreibung des Sicherheitsszenarios sowie die Ausformulierung der **Lernziele** und der praktischen Aufgabenstellungen. Damit der Laborant die Aufgaben korrekt und Zeitnahe lösen kann, sind die benötigten theoretischen Grundlagen im Lösungsleitfaden enthalten. Ebenfalls ist die Dokumentation und Installationsanleitung des eingesetzten Softwaresystems und der Entwicklungsumgebung enthalten. Der Laborant wird innerhalb des Lösungsleitfadens durch eine Art Musterlösung der Aufgaben geleitet. Dabei werden auch bestimmte Abschnitte des Leitfadens abstrahiert, damit der Laborant gezwungen ist, eigenständige Lösungen zu erstellen. Passend zu dem Sicherheitsszenario und dessen Problemstellung werden dem Laboranten klar formulierte Lernziele vorgegeben. Sie beschreiben die Kompetenzen, die der Laborant durch das Laborsystem erlernen oder verbessern soll.

Die Kapitelstruktur eines Lösungsleitfadens kann wie folgt aufgebaut werden [Re12]:

1. **Einführung**: Diese beinhaltet eine Motivation, die Zielvorstellungen und Einleitung in das Sicherheitsszenario.
2. **Organisation**: Dieses Kapitel beinhaltet einen Zeitplan, die geplanten Präsentationen und Präsenzphasen, die Kommunikationsregeln, die eingesetzten Teamprozesse und Dokumentationskonventionen.
3. **Entwicklung**: Hier wird die Entwicklungsumgebung des Labors vorgestellt, sowie die benötigten Werkzeuge und Konventionen zur Softwareentwicklung.
4. **Aufgabenbeschreibung**: Praktische Aufgaben werden einem übergeordneten Lernziel zugeordnet. Eine Aufgabenstellung verweist gleichzeitig auf eine Lösungsbeschreibung, eine geschätzte Bearbeitungszeit sowie die nötigen Installationsanweisungen der benötigten Software-Komponenten.
5. **Evaluation**: In diesem Kapitel werden die Laboranten dazu aufgefordert, das abgehaltene Labor zu bewerten. Dabei sollen konkrete Verbesserungsvorschläge ausgearbeitet und die erlernten Fähigkeiten der Laboranten dokumentiert werden.
6. **Zusammenfassung und Ausblick:** In diesem Kapitel werden die behandelten Themen und die ausgearbeiteten Lösungen zusammengefasst. Den Laboranten wird ein Ausblick präsentiert, wie die behandelten Themen und die erlernten Fähigkeiten erweitert werden können bzw. wie sie in der Industrie zum Einsatz kommen.

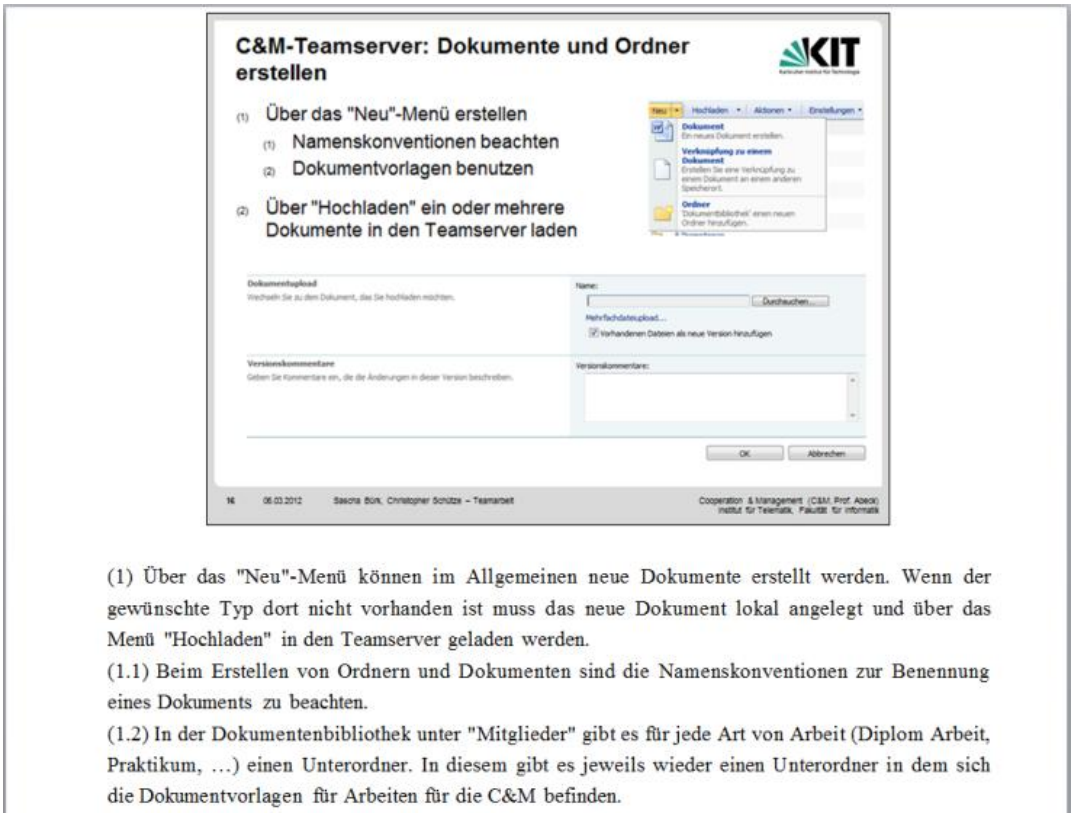

Abbildung 3: Beispielausschnitt - C&M-konformes Dokument

Das Format und das Vorgehen innerhalb des Lösungsleitfadens orientiert sich an dem Konzept der praktischen Aufgaben der Vorlesung „Web-Anwendungen und Serviceorientierte Architekturen" [Ab12]. Für das Format wird als Grundlage ein C&M-konformes Dokument eingesetzt (siehe Abbildung 3). Diese sind mittels Powerpoint erstellte Dokumente, die im Notizenseitenformat (DIN A4) erstellt werden, aber auch im Präsentationsmodus eingesetzt werden können. Die obere Hälfte einer Seite beinhaltet eine Präsentationsfolie, darin enthalten sind unter anderem Überschriften, Notizen, Stichwörter, Codezeilen, Grafiken und Screenshots. Die untere Hälfte einer Seite beinhaltet Fließtext zur Beschreibung der Folieninhalte sowie Abkürzungen und Quellenangaben. Diese Mischung aus Präsentationsfolie und wissenschaftlich aufbereitetem Fließtext wird bei C&M seit Jahren für die Dokumentation der Vorlesungen, Seminararbeiten, Praktika usw. mit Erfolg eingesetzt. Gerade im Bereich der Informatik, in dem Softwareartefakte wie UML-Diagramme, Prozessdiagramme oder Programm-Screenshots eingesetzt werden, können diese Grafiken mit ausgiebigen Zusatzinformationen in Textform ergänzt werden. Der große Vorteil der Verwendung des C&M-konformen Dokuments besteht darin, dass die Dokumente innerhalb der Forschungsgruppe im Format und den Konventionen einheitlich gehalten sind. Da die Folienseiten jeweils Grafiken, Text, Kurzbeschreibungen und Referenzen enthalten, stellen sie atomare Komponenten dar. Diese Komponenten können in den verschiedenen Dokumenten innerhalb der Forschungsgruppe mit minimalem Aufwand wiederverwendet bzw. ausgetauscht werden. So kann z.B. eine ausgearbeitete Komponente eines Praktikums in eine Präsentation für den Industriepartner eingebaut oder etwa in ein Vorlesungsskript integriert werden.

5. Im IT-Sicherheitslabor behandelte Inhalte

Zur Einführung des Laborsystems am Lehrstuhl wurden unter anderem Sicherheitsbetrachtungen an einer universitätsinternen Anwendung zur Navigation auf dem Campus durchgeführt. Unter dem Titel

"Sichere Java Web-Komponenten" wurden am sogenannten KITCampusGuide[3] (KCG) Kernaspekte sicherer Verbindungen sowie der abgesicherten Identifizierung gegenüber einer Java-basierten Web-Anwendung betrachtet. Der KCG ist eine zu Lehr- und Forschungszwecken am Lehrstuhl eingesetzte Web-Anwendung auf Java-Basis. Um den Fokus stärker auf die im Praktikum bearbeiteten Sicherheitsfragestellungen zu lenken, wurde speziell die Komponente „POI[4]-Verwaltung“ des KCG betrachtet. Für die Erstellung des Themas wurde auf eine frühere Arbeit am Lehrstuhl zurückgegriffen, die die Absicherung dieser Komponente zum Inhalt hatte [Ho11]. Die POI-Verwaltungs-Komponente bietet registrierten Benutzern unter anderem die Möglichkeit, die Zugriffsrechte erstellter POI´s zu bearbeiten. Dieses Szenario bietet eine Reihe von sicherheitsspezifischen Anforderungen, die durch eine Sicherheitsanforderungsanalyse anhand von Missbrauchsfällen [SO04] identifiziert wurden. Den Laboranten wurde eine eigens dafür erstellte Webanwendung namens „POIManager“[5] bereitgestellt. Mithilfe des Lösungsleitfadens konnten die Laboranten die benötigte Entwicklungs- und Anwendungs-Umgebung auf einen beliebigen Computer installieren, um damit anschließend die praktischen Aufgaben (siehe Abbildung 4) auszuarbeiten. Für das Erreichen des Lernziels „Absicherung von Java Web-Komponenten“ wurde die praktische Aufgabe „Architektur- und Code-Review“ gestellt. Die Aufgabe sah vor verschiedene Sicherheitsmuster wie z.B. das Secure-Channel-Muster (siehe [SN+05] und [SF+06]) zu identifizieren und deren Funktionsweise am POIManager nachzuvollziehen. Anschließend musste das Deklarative Sicherheitsmodell [Mo09] des POIManagers überprüft und erweitert werden. Je nach Motivation und verbleibender Zeit konnten die Laboranten entscheiden, die Web-Anwendung weiter zu entwickelt bzw. um ein programmatisches Sicherheitsmodell [Mo09] zu ergänzen.

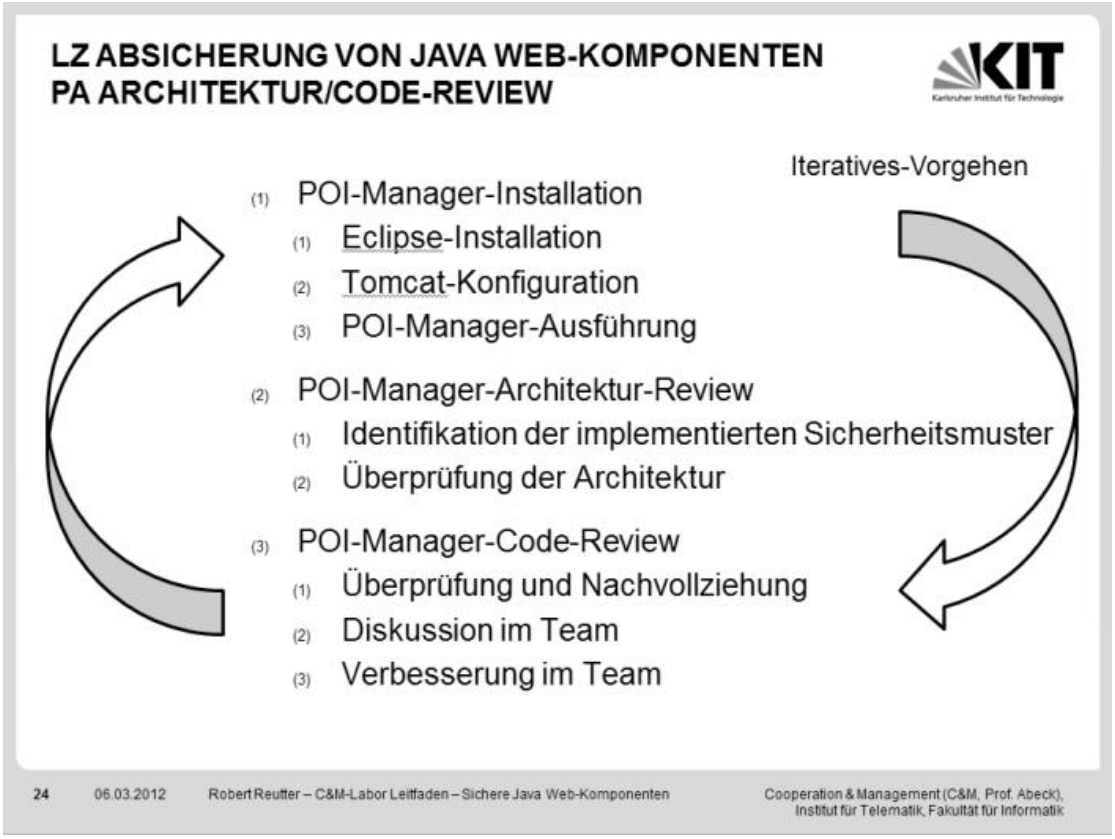

Abbildung 4: Praktische Aufgabe - Leitfaden „Sichere Java Web-Komponenten“

[3] Der KITCampusGuide ist zu finden unter http://code.google.com/p/kitcampusguide/.
[4] „POI“ steht für „Point of Interest“.
[5] Der POIManager ist zu finden unter http://code.google.com/p/icconsult-sicherheitslabor/.

Auf diesem Thema aufbauend wurde eine weitere, vom Industriepartner eingebrachte, Problemstellung betrachtet. Diese ist im Cloud-Computing-Umfeld angesiedelt und befasst sich mit der sicheren Migration einer bestehenden Web-Anwendung unter der Prämisse, dass Benutzerdaten weiterhin in einem Active Directory lokal vorgehalten werden sollten. Das vom Industriepartner eingebrachte Thema „Absicherung einer in die Cloud migrierten Web-Anwendung“ [Pa11] wurde für die Lehre in ein Sicherheitsszenario umgewandelt [Si10]. Die theoretischen Hintergründe sowie die Analyse des Sicherheitsszenarios wurden den Laboranten in wissenschaftlicher Form aufbereitet [Re12]. Aus dem vorbereiteten Szenario ließen sich wiederum die Lernziele und die praktischen Aufgaben ableiten. Ziel war es, Methoden zur Absicherung kritischer Unternehmensdaten bei der Migration eines Geschäftsprozesses auf das Angebot eines Cloud-Plattform-Anbieters zu erarbeiten. Die praktischen Aufgaben, also der Aufbau einer Testumgebung - was bei IT-Systemen Installation und Einrichtung umfasst - wurden dabei jeweils vor Ort in den Laborräumen des Lehrstuhls durchgeführt. Zu diesem Zweck wurde vonseiten der Universität eine entsprechende Ausrüstung zur Verfügung gestellt, die es ermöglicht, jeweils in Teams praktische Fortschritte im Labor zu erzielen.

Diese von den Studierenden durchgeführten Arbeiten wurden in einer entsprechenden Dokumentation festgehalten. Diese erfüllt mehrere Zwecke: Einerseits bearbeitet nicht jeder Praktikant jede Aufgabe, sondern erweitert nach und nach eine gemeinsame Plattform. Um trotzdem stets über den Gesamtfortschritt des Praktikums informiert zu sein, wird von den Praktikanten erwartet, dass sie ihre geleisteten Arbeiten dokumentieren bzw. anhand der Dokumentation den aktuellen Stand nachvollziehen. Zum anderen dient die Dokumentation als Grundgerüst für nachfolgende Praktika und somit als Grundlage für das Verständnis der nachfolgenden Praktikanten. Die dokumentierten Lösungen der Studierenden sowie Erfahrungen beim Umgang mit den eingesetzten Technologien können ebenfalls vom Industriepartner als Grundlage weiterer Betrachtungen genutzt werden. Neben der Funktion einer Ergebnisdokumentation für den Industriepartner repräsentiert die erarbeitete Dokumentation aber auch die praktisch erbrachten Leistungen und den durch das Praktikum erzielten Lernerfolg bei den Studierenden.

Die theoretischen Arbeiten werden, im Gegensatz zum praktischen Teil, von jedem Studierenden durchgeführt, um das Verständnis sowohl für die praktisch erbrachten Leistungen, als auch für die zugrunde liegenden Konzepte und Vorgehensweisen sicherzustellen. Die Ergebnisse dieser theoretischen Betrachtungen werden ebenfalls in die gemeinsame Dokumentation eingearbeitet, um zu gewährleisten, dass bei Fortsetzung des Praktikums durch andere Studierende die bisher erarbeiteten Inhalte verstanden werden. Unter diesen Bedingungen ist gewährleistet, dass sich die Laborthemen durch den Einsatz der Studierenden ständig weiterentwickeln.

6. Ausblick

Die Aufbau- und erste Erprobungsphase des IT-Sicherheitslabors hat gezeigt, dass eine Zusammenarbeit zwischen Hochschule und Industrie nicht nur in der Forschung, sondern auch in der Lehre erfolgreich sein kann. Der Anreiz des Industriepartners, in die Lehre zu "investieren", besteht darin, Studierende heranzuziehen, die neben dem zwingend notwendigen theoretischen Rüstzeug auch Praxiskenntnisse erworben haben, die für deren gezielten Einsatz in Industrieprojekten benötigt werden.

Zur Förderung der Teamarbeit innerhalb des Praktikumsteams wurde von Anfang an auf die durch die Internet-Technologie ermöglichten neuen Kommunikationsformen gesetzt. Den Studierenden steht ein Team-Server zur Ablage aller laborbezogenen Dokumente zur Verfügung, außerdem werden regelmäßig Video- und Audiokonferenzen mit dem Industriepartner iC Consult abgehalten. Weiterhin werden fortlaufend innovative Technologien erprobt. Diese Kommunikationsformen werden aber das persönliche Gespräch niemals verdrängen. Das Konzept sieht im Gegenteil die persönliche Zusammenarbeit zwischen Betreuer und Praktikanten bzw. zwischen den Praktikanten untereinander als die Basis an, die durch die "Kommunikation über das Netz" ergänzt wird.

Zentrales Ziel des Laborsystems ist es, erarbeitete Lösungen sowie deren Dokumentation als Grundlage für Folgepraktika oder Bachelor- und Masterarbeiten zu verwenden. So können die Studierenden erlernte Kompetenzen und Erfahrungen in die weiteren Projekte und Industrielösungen des Partners mit einbringen.

Auch wenn das Laborsystem zunächst am Lehrstuhl nur im Zusammenhang mit IT-Sicherheit eingesetzt wird, eignet es sich auch zur Erarbeitung diverser praxisorientierter Fragestellungen in anderen Bereichen der Informatik. Bereiche, zu dem der Lehrstuhl weitere Labore plant, sind die Entwicklung von Web-Service-orientierten Softwaresystemen und das Projekt- und Portfolio-Management.

Referenzen

[Ab12] Sebastian Abeck: Web-Anwendungen und Serviceorientierte Architekturen, Lehrveranstaltung, Karlsruher Institut für Technologie (KIT), C&M (Prof. Abeck), 2012.
Web-Adresse: http://www.cm-tm.uka.de/study_wasa1.php.

[Br03] Claudia Bremer: Online Lehren leicht gemacht! Leitfaden für die Planung und Gestaltung von virtuellen Hochschulveranstaltungen, 2003.

[HM+04]: Ji Hu, Christoph Meinel, Michael Schmitt: Tele-Lab IT Security: An Architecture for Interactive Lessons for Security Education, SIGCSE'04, March 3–7, 2004, Norfolk, Virginia, USA.

[Ho11] Hedayatollah Hosseini: Analyse und Entwurf von Sicherheitsmaßnahmen am Beispiel des KITCampusGuides, Studienarbeit, Karlsruher Institut für Technologie (KIT), C&M (Prof. Abeck), 2011.

[JB+07] Eric Jendrock, Jennifer Ball, Debbie Carson, Ian Evans, Scott Fordin, Kim Haase: The Java EE 5 Tutorial, Web-Adresse: http://docs.oracle.com/javaee/5/tutorial/doc/.

[Li05] Y. Daniel Liang: Installing and Configuring JDK 1.6, Supplement for Introduction to Java Programming
Web-Adresse: http://cs.armstrong.edu/liang/intro7e/supplement/Supplement1bInstallingJDK6.pdf.

[Mo09] Rajiv Mordani: Java™ Servlet Specification, Version 3.0, Java Community Process, Sun Microsystems, Inc., 2009.
Web-Adresse: http://jcp.org/aboutJava/communityprocess/final/jsr315/index.html

[Pa11] Ingo Pansa: Szenario-Beschreibung: Migration einer Web-Anwendung auf die Microsoft Azure Plattform, Szenario und erste Arbeitspakete, iC Consult GmbH, 2011.

[Re12] Robert Reutter: Entwicklung eines IT-Sicherheits-Laborsystems, Masterarbeit, Karlsruher Institut für Technologie (KIT), C&M (Prof. Abeck), 2012.

[Ru02] Brad Rubin: Java security, Part 2: Authentication and authorization, developerWorks, IBM
Web-Adresse: http://www.ibm.com/developerworks/java/tutorials/j-sec2/.

[SO04] Guttorm Sindre, Andreas L. Opdahl: Eliciting security requirements with misuse cases, Requirements Engineering, Springer-Verlag London Limited, 2004.

[Si10] Holger Sirtl: Cloud Computing mit der Windows Azure Platform: Entwicklung, Integration und Betrieb Cloud-basierter Software, CTP Edition, Microsoft Press, 2010.

Vita

Sebastian Abeck hat an der TU München promoviert und habilitiert. Seit 1996 ist er Professor am Karlsruher Institut für Technologie (KIT). Dort leitet er die Forschungsgruppe Cooperation & Management, mit der er im Bereich der serviceorientierten Web-Anwendungen Forschungs- und Industrieprojekte durchführt. Eines dieser Projekte hat den Aufbau eines IT-Sicherheitslabors zum Ziel, an dem **Aleksander Dikanski** im Rahmen seiner Dissertation und **Robert Reutter** im Rahmen seiner Masterarbeit maßgeblich beteiligt sind. **Philipp Schleier** hat ein Praktikum im Rahmen des IT-Sicherheitslabors durchgeführt und plant die Durchführung einer Bachelorarbeit in dem Industrieprojekt „*Lightweight and Flexible Identity Management LaFIM*“, zu dem er sich im Praktikum die notwendigen Kompetenzen erworben hat.

Jürgen Biermann hat Physik studiert, ist Mitbegründer der iC Consult und leitet das Unternehmen erfolgreich seit nun 15 Jahren. Er begleitet verschiedene Integrationsprojekte deutschlandweit und sucht darüber hinaus den direkten Kontakt zu Hochschulen mit dem Ziel der Steigerung der Ausbildungsqualität. **Ingo Pansa** hat am Karlsruher Institut für Technologie (KIT) promoviert. In seiner wissenschaftlichen Arbeit befasst er sich mit der dienstorientierten Integration von IT-Management-Werkzeugen. Bei iC Consult ist er als Senior Consultant tätig und fokussiert hierbei auf Identitätsmanagement- und Zugriffskontrollfragestellungen in komplexen verteilten Unternehmensanwendungen.