Wie lehrt man IT-Sicherheit am Besten? Eine empirische Studie

Frank van der Beek
RWTH Aachen
frank.beek at onlinehome.de

Martin Mink
Lehrstuhl für Praktische Informatik 1
Universität Mannheim
mink at informatik.uni-mannheim.de

Abstract: Eine Betrachtung der aktuellen IT-Sicherheitslehre an Universitäten zeigt, dass Studenten nicht nur Techniken zum Schutz von IT-Systemen erlernen, sondern vermehrt auch Angriffsmethoden vermittelt bekommen, d.h. wie IT-Systeme kompromittiert und Schwachstellen ausgenutzt werden können. Aber wie ist diese Entwicklung zu bewerten? Um diese Frage zu beantworten wird die Hypothese untersucht, dass die Vermittlung offensiver Techniken, wie sie von Angreifern angewendet werden, zu einem höheren Verständnis von IT-Sicherheit führt als eine klassische defensive Lehre. Im Rahmen einer empirischen Studie wurden zwei IT-Sicherheitskurse mit einem offensiven bzw. defensiven Lehransatz durchgeführt und die Ergebnisse eines abschließenden Experiments miteinander verglichen, um Rückschlüsse auf das IT-Sicherheitsverständnis der Kursteilnehmer zu ziehen.
Die bei der ersten Durchführung der Studie erlangten Daten unterstützen die Hypothese, jedoch zeigt die Auswertung auch, dass die Konzeption der Studie überarbeitet werden muss, um eine aussagekräftigere Entscheidung über die Gültigkeit der Hypothese treffen zu können.

1 IT-Sicherheitslehre an Universitäten

Die Gefährdungen, denen IT-Systeme ausgesetzt sind, unterliegen einem kontinuierlichen Veränderungsprozess und derzeit nicht nur einer wachsenden Quantität, sondern auch einer wachsenden Qualität. Verfolgten Angreifer bis vor einigen Jahren noch das Ziel, sich mit ihren Fähigkeiten zu rühmen, steht heute vor allem eine anhaltende Präsenz des Angreifers auf einem kompromittierten Rechner im Vordergrund, um finanzielle Interessen zu verfolgen, bewusst Schaden zu verursachen oder wichtige Informationen auszuspähen.

Dabei liegen die Ursachen für solche Angriffe meist nicht am Ausfall technischer Schutzmaßnahmen wie Firewalls oder Intrusion Detection Systeme, sondern an menschlichem Versagen, sei es durch Fehlverhalten von Mitarbeitern in einer bestimmten Situation, Fahrlässigkeit durch mangelnde Einstellung gegenüber IT-Sicherheit oder die nicht konsequente Einhaltung von Sicherheitsregeln bzw. Vorschriften.

Insbesondere in der Industrie ist der Bedarf nach erfahrenen IT-Sicherheitskräften sehr hoch. Jedoch sind nur wenige Hochschulabsolventen ausreichend dafür qualifiziert, was vor allem daran liegt, dass in der Hochschulausbildung zu wenig Informationssicherheit gelehrt und praktiziert wird und viele Studenten dadurch zu wenig Kenntnisse auf diesem Gebiet erlangen. Dies wird durch eine von der Universität Regensburg durchgeführten Studie belegt [DFNP06], in welcher die befragten Studenten IT-Sicherheit zwar als sehr wichtig einstuften, es sich aber auch zeigte, dass sie nicht genügend Wissen und praktische Erfahrungen haben, um bestimmte Sachverhalte entsprechend zu beurteilen und in die Realität umzusetzen. So hat auch jüngst die Gesellschaft für Informatik (GI) empfohlen, IT-Sicherheit in der schulischen und akademischen Ausbildung aller Studiengänge stärker im Curriculum zu berücksichtigen, wobei auch die Einführung eines expliziten Studiengangs „Informationssicherheit“ diskutiert wurde [Ges06]. Diese Arbeit konzentriert sich auf die Lehre im akademischen Bereich, in welchem zwei Lehransätze für IT-Sicherheit zu unterscheiden sind, ein *offensiver* und ein *defensiver* Lehransatz:

Defensiver Ansatz Vermittelt die Techniken, die dem Schutz eines Systems und der enthaltenen Informationen dienen, z.B. durch kryptographische Protokolle, Firewalls, Intrusion Detection Systeme oder Zugriffskontrollen.

Offensiver Ansatz Beschreibt die Vermittlung von Techniken, die darauf abzielen, *etwas kaputt zu machen*. Dabei geht es vorwiegend um Angriffe auf die drei Grundpfeiler der IT-Sicherheit: *Verfügbarkeit*, *Vertraulichkeit* und *Integrität*, z.B. durch Denial of Service-Angriffe oder das Mitlesen (Sniffen) von Informationen im Netzwerk. Die Intention des offensiven Lehransatzes liegt darin, die Methoden der Angreifer kennenzulernen.

Während anfangs ausschließlich Verteidigungsmaßnahmen gelehrt wurden, scheint an vielen Hochschulen eine Veränderung bezüglich des Lehransatzes stattzufinden, da immer häufiger auch offensive Aspekte an Universitäten vermittelt werden. In der Lehrtätigkeit des Lehrstuhls an der RWTH Aachen bzw. seit zwei Jahren an der Universität Mannheim liegt der Schwerpunkt in der IT-Sicherheitslehre auf der Vermittlung von offensiven Techniken. Dazu gehört u.a. ein regelmäßig stattfindendes sog. *Hacker-Praktikum*, in welchem die Teilnehmer sowohl Angriffstechniken als auch Verteidigungsmaßnahmen in einem geschlossenen Netzwerk praktisch ausprobieren können [DFMP05]. Eine Fortführung des Hacker-Praktikums ist die bisher zweimal angebotene *Summer School*, in welcher über mehrere Wochen fortgeschrittene Angriffstechniken begleitet von Vorlesungen und Vorträgen analysiert und in praktischen Übungen erprobt wurden [DGHM05].

Des Weiteren nimmt ein studentisches Team der RWTH Aachen regelmäßig und erfolgreich an IT-Sicherheitswettbewerben, wie dem *Capture the Flag* der University of California, Santa Barbara (UCSB)[1] oder dem *Cipher*[2] *Capture the Flag Wettbewerb* (CTF) teil, in welchem weltweit verteilte Teams von Universitäten gegeneinander antreten mit dem Ziel, die Server der anderen Teams anzugreifen und gleichzeitig den eigenen Server zu verteidigen.

[1] http://www.cs.ucsb.edu/ vigna/CTF/

[2] http://www.cipher-ctf.org, **C**hallenges in **I**nformatics: **P**rogramming, **H**osting and **E**xplo**R**ing

Im Bereich der offensiven Kurse und Lehrmethoden existiert eine Anzahl von Veröffentlichungen, wie [SMR00], [SJ03], [Vig03] und [DRR03], aber nach Wissen der Autoren existiert kein Ansatz für eine *Bewertung* des offensiven Ansatzes durch wissenschaftliche Methoden.

Motiviert durch die positiven Erfahrungen mit dem offensiven Lehransatz wird in dieser Arbeit im Rahmen einer empirischen Studie die offensive und die defensive IT-Sicherheitslehre miteinander verglichen und bewertet.

Überblick Im folgenden Abschnitt wird eine Einführung in die empirische Methodik gegeben, die grundlegend für das Verständnis der Durchführung der Studie ist, welche in Abschnitt 3 vorgestellt wird. Nach der Schilderung des Aufbaus der im Rahmen der Studie durchgeführten IT-Sicherheitskurse in Abschnitt 4, wird in Abschnitt 5 die Auswertung der Studie vorgestellt. Der abschließende Abschnitt 6 betrachtet die Durchführung der Studie kritisch und gibt einen Ausblick.

2 Grundlagen der empirischen Methodik

Der folgende Abschnitt vermittelt zunächst die Grundlagen der in empirischen Studien angewendeten Methoden, bevor die konkrete Durchführung der Studie beschrieben wird.

Die Durchführung einer Studie läuft unter dem Oberbegriff eines Experiments. Nach einer Definition von Wundt [Kla05] handelt es sich dabei um die systematische Beobachtung eines planmäßig herbeigeführten und wiederholbaren Vorgangs, wie sich unter Konstanthaltung anderer Bedingungen mindestens eine abhängige Variable ändert, nachdem mindestens eine unabhängige Variable manipuliert worden ist. Die grundsätzlichen Schritte bei der Durchführung eines Experiments bestehen aus dem Aufstellen einer *Hypothese*, dem Feststellen der relevanten *Variablen* und der Entwicklung der Versuchsanordnung mit einem abschließenden Vergleich der gemessenen Ergebnisse.

Hypothesen Zu den wichtigsten Aufgaben der empirischen Forschung gehört die Überprüfung von Hypothesen. Diese bezeichnen unbewiesene Annahmen oder Behauptungen, dass ein Sachverhalt oder ein Ereignis eintritt, wenn bestimmte Bedingungen vorliegen [BD06]. Die empirischen Daten, die im Laufe einer Studie gesammelt werden, können selber keine Auskunft darüber geben, ob eine Hypothese bestätigt oder widerlegt werden kann, sondern bieten nur eine Entscheidungsgrundlage für oder gegen die Hypothese. Dabei besteht auch, wie bei jeder Entscheidung, die Gefahr, sich falsch zu entscheiden. Daher erfolgt die Prüfung von Hypothesen in der empirischen Methodik in der Regel durch statistische Hypothesentests, die auch als Signifikanztests bezeichnet werden und die Wahrscheinlichkeit für eine Fehlentscheidung bezüglich der Gültigkeit einer Hypothese berechnen.

Variablen Bei einer Hypothese wird ein allgemein gültiger Zusammenhang zwischen mindestens zwei Variablen vermutet, der in der Form „Wenn ..., dann ..." ausgedrückt werden kann. Variablen beschreiben in der empirischen Methodik Eigenschaften von Menschen oder Objekten, die verschiedene Werte (Ausprägungen) annehmen können. Variablen, die in einem Experiment variiert werden, um die Effekte, die sich daraus ergeben, zu betrachten und dadurch Rückschlüsse auf die aufgestellte Hypothese zu ziehen, werden als *unabhängige* Variablen bezeichnet, während die Auswirkungen einer Veränderung an der *abhängigen* Variablen geprüft werden.

Versuchsplanung Der Versuchsplan ist ein standardisiertes Schema, welches die Basis jeder wissenschaftlichen Untersuchung bildet und beschreibt, wie eine empirische Fragestellung untersucht werden soll. Diese Planung ist entscheidend dafür, wie aussagekräftig später die Untersuchungsergebnisse sind. In diesem Zusammenhang spricht man auch von der Validität, der Gültigkeit der Ergebnisse, welche je nach Konzeption des Versuchsplans variieren kann

Dabei wird unterschieden zwischen interner und externer Validität. *Interne Validität* ist dann erreicht, wenn die Veränderung der abhängigen Variable eindeutig auf die Manipulation der unabhängigen Variablen zurückgeführt werden kann, also neben der Untersuchungshypothese keine besseren Alternativerklärungen existieren. Die Anzahl plausibler Alternativerklärungen nimmt dabei durch zusätzliche Faktoren (Störvariablen) zu, die einen Einfluss auf das Ergebnis ausüben, zum Beispiel durch eine sinkende Aufmerksamkeit der Probanden oder eine ungenaue bzw. fehlerhafte Messung der Merkmale. *Externe Validität* hingegen ist dann erreicht, wenn das Ergebnis einer Stichprobe auf andere Personen, Zeitpunkte oder Situationen übertragen und verallgemeinert werden kann. Diese ist eventuell gefährdet, wenn eine Untersuchungsumgebung zu sehr von natürlichen Gegebenheiten distanziert oder eine ausgewählte Stichprobe nicht repräsentativ genug ist.

3 Durchführung der Studie

Um den offensiven mit dem defensiven Lehransatz vergleichen und wissenschaftlich überprüfen zu können, wurden zwei Kompaktkurse für IT-Sicherheit konzipiert, von denen ein Kurs den offensiven Ansatz verfolgt und der zweite Kurs den defensiven Ansatz. Die Idee, die Studie als Kompakt- bzw. Crashkurs durchzuführen, hat den Vorteil, dass ein Kompaktkurs im Gegensatz zu einer Vorlesung über IT-Sicherheit oder einem mehrwöchigen Praktikum in kürzerer Zeit (hier dreitägig) durchgeführt und damit auch häufiger wiederholt werden kann, um mehr Daten für die Studie erfassen zu können und eventuelle Planungsfehler zu korrigieren. Ausgehend von der Behauptung, dass der offensive Lehransatz *besser* ist, ergibt sich für die Studie die folgende Forschungshypothese:

„Studenten, die eine offensive Ausbildung in IT-Sicherheit erhalten, haben ein besseres Verständnis von IT-Sicherheit als Studenten, die eine defensive Ausbildung erhalten."

Besser kann in diesem Zusammenhang u.a. bedeuten, dass die Studenten durch die erlernten Angriffstechniken mehr Kenntnisse von potentiellen Schwachstellen in sicherheitskri-

tischen Systemen haben und auch weniger Zeit in Anspruch nehmen müssen, um sicherheitsbezogene Aufgaben ordnungsgemäß durchzuführen [Min07].

Da in dieser Studie die Auswirkungen der beiden Lehransätze auf das *IT-Sicherheitsverständnis* beobachtet und gemessen werden sollen, handelt es sich hierbei um die abhängige Variable des Experiments. Die Kurszuordnung (offensiv, defensiv) wird zu diesem Zweck variiert und gehört damit zu den unabhängigen Variablen. Dabei bilden die Teilnehmer des Kurses mit dem offensiven Lehransatz die Experimentalgruppe und die Teilnehmer des defensiv ausgelegten Kurses die so genannte Kontrollgruppe, eine Gruppe, welche die spezielle zu untersuchende Maßnahme, nämlich die offensive Lehre, nicht erhält.

Neben der unabhängigen Variable der Kurszuordnung wurde eine weitere unabhängige Variable, das Vorwissen der Untersuchungsteilnehmer, welches den Kenntnisstand der Teilnehmer bezüglich IT-Sicherheit *vor* der Kursdurchführung repräsentiert, berücksichtigt. In Kombination ergeben sich insgesamt vier Stichprobengruppen, wie sie in Tab. 1 dargestellt sind.

	Offensiver Kurs	Defensiver Kurs
Wenig Vorwissen	Experimentalgruppe - (EG 1)	Kontrollgruppe - (KG 1)
Viel Vorwissen	Experimentalgruppe - (EG 2)	Kontrollgruppe - (KG 2)

Tabelle 1: Die vier Stichprobengruppen für die Durchführung der Studie

Um das Auftreten möglicher Störfaktoren zu minimieren, wurde das Prinzip des statistischen Fehlerausgleichs verfolgt und die Studenten **zufällig** auf die Kurse verteilt. Abb. 1 veranschaulicht den Vorgang der Teilnehmerauswahl und der Gruppenzuordnung grafisch.

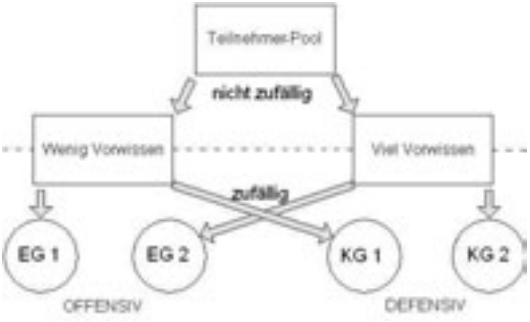


Abbildung 1: Auswahl und Zuordnung der Teilnehmer auf die Gruppen

Die Zielgruppe dieser Studie und damit die zu untersuchende Gesamtpopulation besteht ausschließlich aus Hochschulstudenten. Bereits kurz nach Ausschreibung der Kompaktkurse im Internet und in Newsgroups erhielten die Versuchsleiter über 100 Bewerbungen für eine Teilnahme an den Kursen, von denen letztendlich 42 Teilnehmer ausgewählt wurden. Es handelte sich hauptsächlich um Studenten der RWTH Aachen, aber auch von weiteren Universitäten in Deutschland, wie Berlin, Oldenburg, Bremen, Bochum oder Köln. Auch bezüglich der Studienfachrichtungen waren sehr viele unterschiedliche Bereiche ver-

treten, was nochmals aufzeigt, dass das Interesse an IT-Sicherheit nicht nur im Studiengang Informatik, sondern auch in anderen Bereichen sehr hoch ist. So waren in den Kursen u.a. Studenten aus den Studiengängen Informatik, Elektrotechnik, Mathematik, BWL, Maschinenbau und Medienwissenschaften vertreten.

Der schwierigste Part der empirischen Forschung besteht nun darin, die zu untersuchenden Merkmale in eine messbare Form zu bringen, also an Daten zu gelangen. Dieser Schritt wird auch als *Operationalisierung* bezeichnet und beinhaltet zum Beispiel die Datenerhebung durch Interviews, Fragebögen oder Tests. Bei einem psychologischen Test handelt es sich nach [LR98] um ein wissenschaftliches, also nach bestimmten Regeln durchgeführtes, Routineverfahren zur Operationalisierung von Merkmalen, um eine quantitative oder qualitative Aussage über den relativen Grad der Merkmalsausprägung zu machen. Das Ziel psychologischer Tests ist, je nach Reaktion der Teilnehmer auf Testaufgaben oder Fragen auf Persönlichkeitsmerkmale wie Fähigkeiten, Wissen oder Verhalten zu schließen [Büh04].

Für dieses Experiment wurden insgesamt drei verschiedene Tests konstruiert, um die Auswirkungen der beiden Lehransätze zu vergleichen und damit das IT-Sicherheitsverständnis der Studenten messen zu können: Ein Wissenstest, ein Fragebogen zur Selbsteinschätzung und ein praktischer Test. Diese werden im folgenden kurz vorgestellt.

Wissenstest Der Wissenstest soll die IT-Sicherheitskenntnisse der Studenten sowohl vor als auch nach dem Kurs messen. Dieser Wissenstest war als Multiple-Choice-Test aufgebaut und enthält Fragen wie „Was wissen Sie über Buffer Overflows?“ oder „Wie wird ein Syn-Flood-Angriff durchgeführt?“. Da eine abgegebene Leistung im Wissenstest nach bestimmten Kriterien eindeutig als richtig oder falsch klassifiziert werden kann, liegt ein rein objektiver Maßstab zu Grunde, was eine gute Auswertbarkeit des Tests und Vergleichbarkeit der Ergebnisse gewährleistet. Das Testergebnis wurde außerdem für die Zuordnung der Teilnehmer auf die beiden Vorwissensgruppe verwendet.

Selbsteinschätzungstest Bei einem Selbsteinschätzungstest handelt es sich um einen psychologischen Fragebogen, um Personen bezüglich ihrer Einstellung zu einem bestimmten Betrachtungsgegenstand zu befragen. Dabei spielen objektive Maßstäbe wie bei einem Wissenstest keine Rolle mehr und es existieren auch keine richtigen oder falschen Antworten, sondern die Bewertung erfolgt nach einem rein subjektiv festgelegten Bewertungsmaßstab des Testerstellers. Der hier erstellte Fragebogen zur Selbsteinschätzung (im Folgenden auch als Awarenesstest bezeichnet) befragte die Teilnehmer nach ihrer Einstellung zu sicherheitsrelevanten Themen wie Kryptographie, Sicherheitsupdates oder Passwortsicherheit und beinhaltete u.a. Fragen nach E-Mail- und Festplattenverschlüsselungen oder ihrem Update- und Backupverhalten. Dabei handelte es sich überwiegend um Fragen mit mehr als zwei Antwortkategorien, die eine gewisse Rangordnung darstellen (Ratingskala), z.B. „sehr gut – gut – weniger gut – schlecht“.

Abschlusstest Der Abschlusstest bildete das entscheidende Messinstrument dieser Studie, um die beiden Kurse und damit die Lehransätze miteinander zu vergleichen und zu

bewerten.

Die Idee, einen praktischen Abschlusstest durchzuführen, basiert auf der Tatsache, dass die bisher vorgestellten Tests keine qualitative Bewertung des IT-Sicherheitsverständnisses erlauben. Der letzte Teil der Kompaktkurse sollte genau an dieser Schwachstelle anknüpfen und auch die Fähigkeit der Teilnehmer bewerten, das Gelernte praktisch anwenden und übertragen zu können. Dieser Test war für den offensiven und defensiven Kurs identisch ausgelegt und stellte die Teilnehmer vor die Aufgabe, innerhalb einer festgelegten Zeit von 50 Minuten, auf einem von den Versuchsleitern präparierten Linux-System Anzeichen für Kompromittierungen bzw. Konfigurationsfehler zu identifizieren und das System in einen sicheren Zustand zu überführen. So waren u.a. Rootkits installiert, Benutzer mit schwachen Passwörtern vorhanden und unsichere Dienste gestartet. Anhand der Anzahl der gefundenen Kompromittierungen bzw. gelöster Aufgaben jedes Teilnehmers konnten somit Rückschlüsse auf das IT-Sicherheitsverständnis gezogen und die Lehransätze bewertet werden.

Wie in Abb. 2 zu erkennen ist, interessierte die Versuchsleiter auch die unterschiedlichen Strategien, wie die Teilnehmer bei der Analyse des Systems vorgegangen waren. Zu diesem Zweck mussten die Probanden die identifizierten Probleme, Lösungsvorschläge zu deren Behebung sowie die darauf verwendete Zeit protokollieren. Als zusätzliche Kontrolle wurden sämtliche Tastatureingaben der Teilnehmer mit einem Keylogger aufgezeichnet, um diese mit ihren Angaben vergleichen zu können.

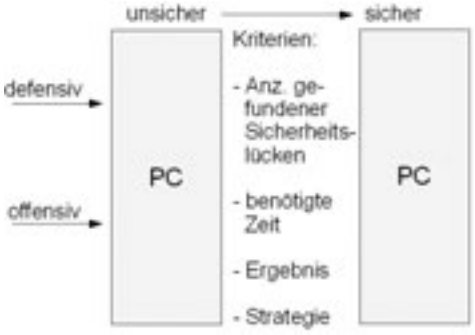


Abbildung 2: Aufbau des Abschlusstests

4 Inhalt der Kompaktkurse

Die Durchführung der beiden Kompaktkurse erfolgte vom 20.-22.März 2007, sowie vom 27.-29.März 2007 im Rechenzentrum der RWTH Aachen. Damit die Teilnehmer nicht direkt auf der Hard- und Software der Kursrechner arbeiten, wurde die vorinstallierte Virtualisierungssoftware *Virtual PC 2007* von Microsoft verwendet. Als Betriebssystem wurde von den Versuchsleitern ein *Linux Debian System* gewählt und entsprechend für die Kurse vorkonfiguriert, welches als virtuelle Festplatte auf alle Kursrechner verteilt wurde und

somit jeder Versuchsteilnehmer auf einem identischen System arbeiten konnte.

Der Inhalt der Kurse setzte sich aus sieben Modulen aus dem Bereich IT-Sicherheit, einem Einführungsmodul, sowie dem bereits beschriebenen praktischen Abschlusstest zusammen, deren Durchführung auf drei aufeinanderfolgende Tage verteilt wurde. Eine Übersicht über die Kursinhalte ist in Tabelle 2 dargestellt.

Tag 1	Tag 2	Tag 3
1. **Einführung**: Ethik/Rechtliches Linux-Grundlagen Programmierung in C Netzwerk-Grundlagen	4. **Netzwerksicherheit 1**: Sniffen Port Scanning	7. **Websicherheit**: Command/SQL Injection Cross Site Scripting Authentifikation
2. **Unixsicherheit**: Passwortsicherheit Zugriffskontrolle Kompromittierungen	5. **Netzwerksicherheit 2**: Spoofing TCP-Hijacking Denial of Service SSH	8. **Malware**: Viren Würmer Trojaner Rootkits
3. **Softwaresicherheit**: Speicherorganisation Buffer Overflows Format Strings Race Conditions	6. **Firewalls**: Konzept Architektur Konfiguration	**Abschlusstest**

Tabelle 2: Überblick über die Kursinhalte

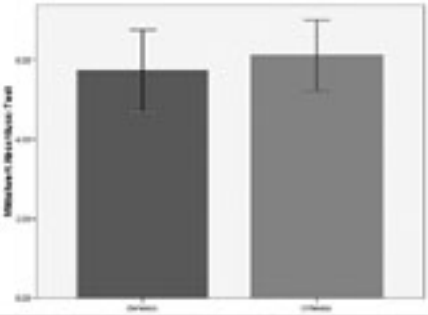
In jedem Modul wurden zu Beginn in einem ca. 30-minütigen Vortrag die theoretischen Konzepte des jeweiligen Themas vorgestellt, gefolgt von einer einstündigen praktischen Bearbeitung eines Aufgabenblattes (jeder Teilnehmer hatte einen Computer zur Verfügung) mit anschließender Besprechung der Übungsaufgaben. Der Theoriepart wurde für beide Kurse identisch gehalten, da eine Differenzierung zwischen dem offensiven und defensiven Lehransatz ausschließlich in den Übungen erfolgen sollte. Beispielhaft wird dies hier anhand der Übung zum Thema Malware gezeigt: Der gemeinsame Teil in beiden Kursen bestand aus der Integritätsüberprüfung von Systemdateien mithilfe des Werkzeugs Tripwire[3] und der Suche nach installierten Rootkits mit Werkzeugen wie RootkitHunter. Die Unterscheidung bestand zum einen darin, dass dies im defensiven Kurs ausführlicher behandelt wurde als im offensiven und zum anderen der Quellcode eines Internet-Wurms analysiert wurde. Im Gegensatz dazu beschäftigten sich die Teilnehmer des offensiven Kurses detaillierter mit der Funktionalität, Installation und den Einsatzmöglichkeiten von Rootkits sowie der Analyse und Verwendung eines Trojanisches Pferds, welches einen unprivilegierten Remote-Login ermöglichte.

[3] http://www.tripwire.com/

5 Ergebnisse der Studie

Die Überprüfung der Hypothese und somit der direkte Vergleich der beiden Lehransätze erfolgte durch die Auswertung der beiden Fragebögen und des praktischen Abschlusstests. Diese Auswertung und anschließende Interpretation der Ergebnisse wurde untermauert durch Verwendung der Statistiksoftware SPSS[4]. Die Auswahl der jeweiligen statistischen Analysen richtete sich dabei nach der Anzahl Variablen und dem gewählten Versuchsplan. In dieser Studie wurden mittels SPSS u.a. Signifikanztests oder Varianzanalysen durchgeführt, um Rückschlüsse über die Auswirkung der Kurszuordnung, der Vorwissenszuordnung bzw. einer Kombinationswirkung dieser beiden Effekte auf die Kursresultate zu ziehen.

Im Folgenden sollen zunächst die Resultate des Abschlusstests betrachtet werden. Das Gesamtergebnis ohne eine Unterscheidung nach viel oder wenig Vorwissen ist in Abb. 3 dargestellt. Auf der y-Achse sind dabei die durchschnittlich erreichten Punkte aus dem Test dargestellt, deren genauen Werte aus der Tabelle entnommen werden können.



	Punkte	in %	Konfidenzintervall
Defensivkurs	5,7	38,07%	4,7 ; 6,75
Offensivkurs	6,11	40,73%	5,2 ; 7

Abbildung 3: Ergebnisse des Abschlusstest (Durchschnitt)

Wie an den Ergebnissen zu erkennen ist, haben die Teilnehmer des Offensivkurses im Abschlusstest mit durchschnittlich 40,73% der maximal erreichbaren Punkte bessere Ergebnisse erzielt als die Teilnehmer des Defensivkurses mit 38,07%. Anhand dieser Resultate allerdings bereits zu folgern, dass der offensive Lehransatz besser sei als der defensive Ansatz, wäre zum einen verfrüht und zum anderen mit einer hohen Irrtumswahrscheinlichkeit verbunden. Es ist offensichtlich, dass der Unterschied, der gerade einmal einer Differenz von 0,41 Punkten im Abschlusstest entspricht, äußerst knapp ist. Hinzu kommt die Unschärfe des Ergebnisses, welche durch eine Betrachtung der Konfidenzintervalle (in Abb. 3 als Intervalle um den Mittelwert eingezeichnet) festgestellt werden kann. Ein Konfidenzintervall wird auch als Vertrauensintervall bezeichnet und schätzt den Bereich, in welchem der Mittelwert der Testresultate (hier: zu 95%) liegen kann. Je kleiner dieses Intervall ist, desto präziser ist der Mittelwert und somit auch das gesamte Testergebnis.

[4] http://www.spss.com

In Abb. 3 sind allerdings relativ breite Konfidenzintervalle zu erkennen, die sich zu einem großen Teil überlappen. Da somit keine eindeutige Aussage über die exakte Lage des Mittelwertes gemacht werden, handelt es sich um ein nicht ausreichend signifikantes Testergebnis.

Interessant und aussagekräftiger ist hingegen die Betrachtung der Strategien, welche die Teilnehmer bei der Analyse des Systems verfolgt haben. Diese Vorgehensweise konnte sowohl durch die Angaben der Teilnehmer auf dem Lösungsblatt als auch durch eine Analyse der Protokolldateien des Keyloggers rekonstruiert werden.

Wie Abb. 4 zu entnehmen ist, suchten die Teilnehmer des Defensivkurses früher nach Benutzern mit schwachen Passwörtern und erkannten das Problem der offenen Ports, also von laufenden unsicheren Dienste. Dem gegenüber steht die Bearbeitungsstrategie der Offensivteilnehmer, welche zuerst nach Malware, also hier den beiden Rootkits, suchten. Zudem identifizierten sie häufiger und früher das Vorhandensein eines aktiven Netzwerk-Sniffers und der Netzwerkschnittstelle im promiscuous mode. Auffallend ist dabei, dass obwohl die Versuchsteilnehmer des Defensivkurses diese Kenntnisse ebenfalls vermittelt bekommen haben, um z.B. nach Rootkits auf dem System zu suchen, diese erst sehr spät oder gar nicht nachprüften. Dabei gehört die Verbreitung von Malware oder das Ausspähen von Informationen zu den größten realen Gefahren für IT-Systeme, was die Vermutung zulässt, dass die Teilnehmer des Offensivkurses eher die konkreten Bedrohungspotentiale für IT-Sicherheit einschätzen können und nach diesen suchen.

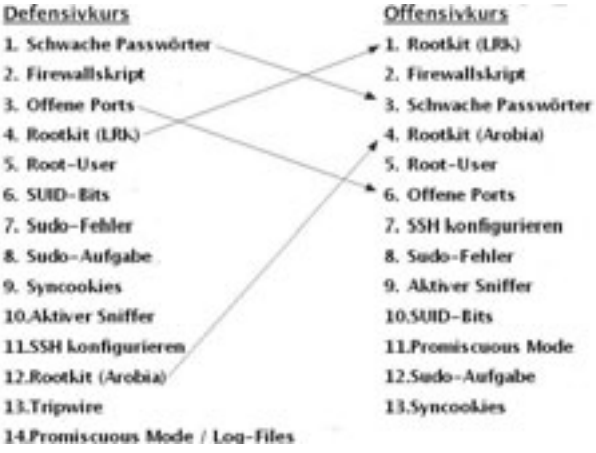
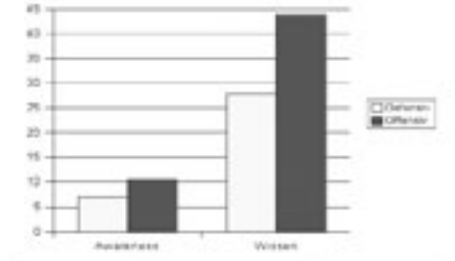


Abbildung 4: Strategie der Bearbeitung

Auch die Analyse der weiteren Ergebnisse aus dem Wissenstest bzw. Awarenesstest, wie sie in Abb. 5 dargestellt sind, lassen bezüglich des IT-Sicherheitswissens der Teilnehmer weitere signifikante Unterschiede zwischen dem Defensiv- und dem Offensivkurs erkennen. So konnten die Offensivkursteilnehmer ihre Ergebnisse aus dem Wissenstest um 43,85% zum Vorwert verbessern, die Teilnehmer aus dem Defensivkurs lediglich um 27,88%. Das entspricht, wie in Abb. 6 dargestellt, einem 57,28% besseren Ergebnis als der Defensivkurs.

Bezüglich der Awareness, also der Einstellung der Teilnehmer gegenüber IT-sicherheitsrelevanten Themen, ist ebenfalls eine klare Tendenz erkennbar. So scheinen die Studenten des Offensivkurses durch die direkte Konfrontation mit Angriffstechniken mehr dazu hingezogen zu sein, ihr gegenwärtiges „PC-Verhalten“ zu überdenken und z.B. mehr auf die Verschlüsselung von E-Mails und Daten zu achten oder häufiger Backups durchzuführen. Wie Abb. 6 zeigt, wurden sie durch die Kursdurchführung um 45,7% stärker bezüglich potentieller IT-Sicherheitsrisiken sensibilisiert als die Teilnehmer des Defensivkurses.



	Awarenesstest	Wissenstest
Defensivkurs	+7,09%	+27,88%
Offensivkurs	+10,33%	+43,85%

Abbildung 5: Fortschritte der Teilnehmer

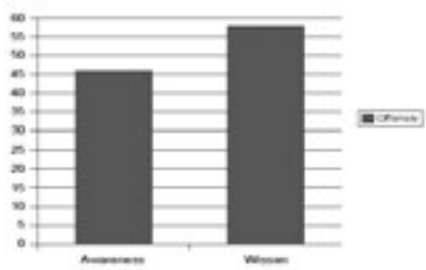


Abbildung 6: Relativer Unterschied der Teilnehmerfortschritte

Eine ausführlichere Beschreibung der Ergebnisse und des Aufbaus der Studie, sowie der Kursinhalte, findet sich in [vdB07].

6 Kritische Reflexion der Studiendurchführung und Ausblick

Trotz der auffallenden Unterschiede bei den Arbeitsstrategien, Wissens- und Persönlichkeitstests ist, wie bei der Betrachtung des Ergebnisses des Abschlusstests bereits deutlich wurde, die abschließende Gesamtbewertung der Studie kritisch zu betrachten und die Aussagekraft der obigen Ergebnisse zu relativieren. So ist unklar, inwieweit technische oder inhaltliche Probleme bei dieser Durchführung der Studie die Ergebnisse zugunsten des Offensivkurses beeinflusst haben könnten:

Technische Probleme Sinkende Motivation und schlechte Arbeitsbedingungen, hervorgerufen durch Soft- und Hardwareprobleme wie Systemabstürze oder Speicherplatzprobleme waren ein großes Problem im ersten, dem defensiven, Kurs. Die technischen Probleme führten vor allem zu Verzögerungen im Tagesablauf, wodurch Vorträge verspätet begannen, die praktischen Übungen kürzer ausfielen oder die Besprechung der Aufgaben am Ende der Module teilweise entfallen musste. Im offensiven Kurs bestanden zwar auch Probleme durch gelegentliche Systemabstürze, jedoch konnten die Versuchsleiter durch die Erfahrungen aus der Vorwoche den Speicherplatzproblemen frühzeitig entgegenwirken, wodurch es keine Verzögerungen im Kursablauf gab und auch genügend Zeit für die

Besprechung der Übungen blieb.

Inhaltliche Probleme Bezüglich der inhaltlichen Planung der Übungen war es schwer, eine sinnvolle und eindeutige Abgrenzung zwischen offensiven und defensiven Methoden zu finden, da viele Angreifertechniken ebenfalls von Administratoren zur Erhöhung der IT-Sicherheit angewendet werden. So existierten viele Gemeinsamkeiten zwischen den Übungen, weswegen kein Kurs als klar offensiv oder defensiv bezeichnet werden kann. Für eine Wiederholung der Studie kommt daher – neben einer eindeutigeren Abgrenzung – auch eine Anpassung der theoretischen Inhalte in Betracht, welche bisher identisch gehalten wurden. Eine Auswahl geeigneter offensiver bzw. defensiver Kursthemen könnte der Arbeit zur Klassifikation von IT-Sicherheitsveranstaltungen entnommen werden [Mer07].

Feedback der Kursteilnehmer Die Kursteilnehmer erhielten zum Abschluss des Kurses einen Kursbewertungsbogen, in welchem sie zunächst anonym die Durchführung des Kurses bewerten und ihre persönliche Meinung niederschreiben konnten, gefolgt von einer offenen Diskussion mit allen Teilnehmern. Sowohl im Bewertungsbogen, als auch in der Diskussionsrunde äußerten sich fast alle Teilnehmer, auch die des Defensivkurses trotz der technischen Probleme, sehr zufrieden über die Kursdurchführung und bestätigten, einen guten und umfassenden Einblick in das Gebiet der IT-Sicherheit erhalten zu haben. Vor allem die Kombination von Theorie und direktem Anschluss der praktischen Übungen, um das Gelernte anwenden zu können, wurde äußerst positiv aufgenommen und hat den Teilnehmern auch sichtlich Spaß gemacht.

Abschließend lässt sich feststellen, dass die aufgestellte Forschungshypothese nicht als bestätigt angesehen werden kann. Sie ist allerdings auch nicht widerlegt, sondern die hier festgestellte Tendenz für die offensive Lehre muss durch mehr Datenmaterial und größere Stichproben erneut überprüft werden. Offen ist jedoch die Frage, inwieweit die Gesetzeslage solche Veranstaltungen in Zukunft zulässt. So wurde Anfang Juli diesen Jahres das neue Strafrechtänderungsgesetz zur Bekämpfung der Computerkriminalität im Bundesrat verabschiedet, wonach das Herstellen, Verbreiten oder Besitzen von „Hackertools“ unter Strafe gestellt wurde. Dabei sind zwar eher Schwierigkeiten im privaten Bereich zu erwarten als in der IT-Sicherheitslehre an Hochschulen, jedoch sind die zukünftigen Entwicklungen und Auswirkungen dieses Gesetzes noch nicht abzusehen.

Literatur

[BD06] Jürgen Bortz und Nicola Döring. *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler*. Springer, 2006.

[Büh04] Bühner. *Einführung in die Test- und Fragebogenkonstruktion*. Pearson Studium, 2004.

[DFMP05] Maximillian Dornseif, Felix Freiling, Martin Mink und Lexi Pimenidis. Teaching Data Security at University Degree Level. In *Proceedings of the Fourth World Conference on Information Security Education*, Seiten 213–222, 2005.

[DFNP06] Dimler, Federrath, Nowey und Plößl. Awareness für IT-Sicherheit und Datenschutz in der Hochschulausbildung - Eine empirische Untersuchung. In *Beiträge der 3. Jahrestagung des GI-Fachbereichs Sicherheit*, Seiten 18–21, 2006.

[DGHM05] Maximillian Dornseif, Felix C. Gärtner, Thorsten Holz und Martin Mink. An Offensive Approach to teaching Information Security: "Aachen Summer School Applied IT Security". Bericht AIB-2005-02, RWTH Aachen, Januar 2005.

[DRR03] R. Dodge, D.J. Ragsdale und C. Reynolds. Organization and Training of a Cyber Security Team. In *Proceedings of the 2003 IEEE International Conference on Systems, Man & Cybernetics*, 2003.

[Ges06] Gesellschaft für Informatik e.V. IT-Sicherheit in der Ausbildung – Empfehlung zur Berücksichtigung der IT-Sicherheit, 2006.

[Kla05] Klauer. *Das Experiment in der pädagogisch-psychologischen Forschung*. Waxmann, 2005.

[LR98] Lienert und Raatz. *Testaufbau und Testanalyse*. Beltz, 6. Auflage, 1998.

[Mer07] Christian Mertens. Wie lehrt man IT-Sicherheit am Besten - Übersicht, Klassifikation und Basismodule. Diplomarbeit, RWTH Aachen, 2007.

[Min07] Martin Mink. Ist Angriff besser als Verteidigung? Der richtige Weg für IT-Sicherheitsausbildung. In *Innovationsmotor IT-Sicherheit - Tagungsband zum 10. Deutschen IT-Sicherheitskongress*, 2007.

[SJ03] W.J. Schepens und J. James. Architecture of a Cyber Defense Competition. In *Proceedings of the 2003 IEEE International Conference on Systems, Man & Cybernetics*, 2003.

[SMR00] Markus Schumacher, Marie-Luise Moschgath und Utz Roedig. Angewandte Informationssicherheit: Ein Hacker-Praktikum an Universitäten. *Informatik Spektrum*, 6(23), Juni 2000.

[vdB07] Frank van der Beek. Wie lehrt man IT-Sicherheit am Besten? Eine empirische Studie. Diplomarbeit, RWTH Aachen, 2007.

[Vig03] Giovanni Vigna. Teaching Network Security Through Live Exercises. In *World Conference on Information Security Education*, Jgg. 253 of *IFIP Conference Proceedings*, Seiten 3–18. Kluwer, 2003.