

# Ist Angriff besser als Verteidigung?

## Der richtige Weg für IT-Sicherheitsausbildung

Martin Mink  
Universität Mannheim  
mink@informatik.uni-mannheim.de

### Kurzfassung:

Aktuelle Trends in der IT-Sicherheitsausbildung gehen in die Richtung, offensive Techniken zu lehren, die ursprünglich von Hackern entwickelt wurden. Dies reflektiert Ansätze der Unternehmenswelt, in der offensive Sicherheitstest (*penetration testing*) rasch allgemeine Anerkennung finden. Dieser Beitrag beruht auf den Erfahrungen mit einem Sicherheitslehrplan an einer deutschen Universität, der offensive Techniken gegenüber defensiven bevorzugt. Wir stellen die Behauptung auf, dass das Lehren von offensiven Methoden zu besseren Sicherheitsexperten führt, als nur das Lehren von defensiven Techniken allein. Es wird ein experimenteller Aufbau vorgestellt, mit dem diese Behauptung näher untersucht werden soll. Der experimentelle Aufbau greift auf Konzepte aus den Human- und Sozialwissenschaften zurück, um den Nutzen offensiven Lehrens empirisch zu bewerten.<sup>1</sup>

## 1. Einführung

### Motivation

IT-Infrastrukturen werden von ständig wechselnden Gefahren bedroht. Ein Bericht von der „security threat trend front“ des Internets [SH04] zeigt eine Tendenz hin zu höherem Kenntnisstand der Angreifer und Professionalität der Angriffe. Hacker wählen ihre Ziele mit wesentlich mehr Sorgfalt aus als zuvor und verwenden das komplette Waffenarsenal, wie mit Keyloggern ausgestattete Trojanische Pferde, um in Unternehmens- oder Verwaltungsnetzwerke einzudringen. Auf der Gegenseite verstärkt sich ebenfalls der Trend zu ganzheitlicher ausgerichteten Ansätzen. Dies bedeutet, dass technische Lösungen wie Firewalls und Systeme zur Schutzzielverletzungserkennung (IDS) in eine Sicherheits- und Risikomanagementperspektive integriert werden müssen. Erstaunlicherweise jedoch nennt Peter G. Neumann, Gründer und Moderator des bekannten *Risks Digest* [RFD], Management nicht als eine der acht wichtigsten aktuellen Herausforderungen von IT-Sicherheit [N04]: Neben praktischen Erfahrungen in Systementwicklung und Schutz der Privatsphäre (engl. „privacy“) wird das Thema *Sicherheitsausbildung* ebenfalls aufgeführt.

Die Sicherheitsausbildung an Universitäten ist geprägt von defensiven Techniken wie Kryptographie, Firewalls, Zugriffskontrolle und Erkennung von Schutzzielverletzungen. Aber auch hier lässt sich eine Tendenz in Richtung offensiverer Methoden erkennen [SMR00, V03]. In der wissenschaftlichen Literatur erfahren offensive Techniken ebenfalls allgemeine Anerkennung [AB05, FV93, AG04]. Die *Association for Computing Machinery* (ACM) widmete sogar eine gesamte Sonderausgabe ihres Magazins „Communications of the ACM“ dem Thema „Hacking and Innovation“ [C06].

---

<sup>1</sup> Eine vorläufige Version dieser Arbeit ist erschienen im Tagungsband der Konferenz *Information Security Curriculum Development* [MF06]

Was ist der Grund dafür? In einem kürzlich erschienenen Artikel argumentiert Conti [C05], dass Akademiker, die sich mit IT-Sicherheit beschäftigen, viel von Hackern und deren Sicherheitsdenken lernen können, indem sie ihre Versammlungen besuchen (wie *DEFCON* [DC] oder *Black Hat* [BH]). Dieser Ansatz stimmt mit der Entwicklung im professionellen Bereich überein, offensivere Methoden in Sicherheitstests einzusetzen, speziell in der prominenten Variante *Penetration Testing*, welche den Einsatz von Hacker-Werkzeugen wie Netzwerk-Sniffern, Passwort-Crackern und Disassemblierern, sowie von aktivem Testen von Unternehmensnetzwerken in Echtzeit beinhaltet. Betrachtet man diese Anzeichen, dann scheint es einen wesentlichen Vorteil zu geben, Sicherheit in offensiver Weise zu behandeln. Aber gibt es wirklich einen Vorteil? Und falls ja, ist dieser irgendwie quantifizierbar?

## Eigener Beitrag

Basierend auf den Erfahrungen mit der Sicherheitsausbildung von Studenten sind wir<sup>2</sup> davon überzeugt, dass das Lehren von offensiven Methoden im universitären Lehrplan einen beachtlichen Vorteil hat. Kurz gefasst: Wir vertreten die Meinung, dass mehr Zeit auf den Angriff als auf die Verteidigung in Lehrveranstaltungen verwendet werden sollte: Angriff ist besser als Verteidigung. Diese Feststellung führt jedoch zu einer grundlegenden Forschungsfrage: Lässt sich diese Hypothese objektiv messen?

In diesem Beitrag beschreiben wir einen experimentellen Aufbau mit dem die Hypothese „Angriff besser als Verteidigung“ überprüft werden soll. Für die Untersuchung ist eine genauere Definition erforderlich, was „besser“ in diesem Zusammenhang bedeutet. Im Kontext der IT-Sicherheitsausbildung von Studenten kann „besser“ auf mehrere Arten verstanden werden:

- ein besseres Verständnis der Schwachpunkte von Sicherheitssystemen
- ein geringerer Zeitaufwand, um sicherheitsbezogene Aufgaben zu erledigen
- eine kontinuierlichere Laufzeit eines administrierten Systems oder
- eine bessere Fähigkeit, sichere Software zu programmieren.

Dies setzt eine gründliche empirische Untersuchung voraus, um die Hypothese zu beurteilen. Wir beziehen uns zu diesem Zweck auf allgemein anerkannte Methoden aus den Human- und Sozialwissenschaften.

Häufig wird das Lehren offensiver Methoden als falsch kritisiert, weil dadurch die Anzahl der „bösen Hacker“ ansteige und folglich der Sicherheitsstand im Internet nicht erhöht, sondern im Gegenteil erniedrigt werde. Wir meinen jedoch, dass dieser Ansatz fehlerbehaftet ist. Jede Sicherheitstechnik kann sowohl für gute als auch für schlechte Zwecke genutzt werden. Die Tendenz hin zu Penetration Testing in Unternehmen zeigt, dass offensive Techniken eingesetzt werden können, um den Grad der Sicherheit einer Organisation zu erhöhen. Dies bedeutet, dass Studenten mit Erfahrung in Angriffstechniken nicht notwendigerweise zu *Black Hats* (Jargon für böartige Hacker, die „Bösen“) werden müssen, sondern eher *White Hats* (die „Guten“) werden. Wir stimmen jedoch zu, dass offensive Techniken nicht für sich allein gelehrt werden dürfen. Genauso wie bei Verteidigungstechniken sollte jede Veranstaltung zu IT-Sicherheit von einer elementaren Diskussion rechtlicher Auswirkungen und Ethik begleitet werden.

---

<sup>2</sup> Mitglieder des „Laboratory for Dependable Distributed Systems“ der RWTH Aachen, jetzt Universität Mannheim

## Übersicht

Abschnitt 2 gibt einen Überblick über die im Sicherheitslehrplan der Forschungsgruppe des Autoren angebotenen Veranstaltungen und geht auf vergleichbare Aktivitäten im Bereich offensiver Ausbildung ein. Abschnitt 3 zeigt dann einen Ansatz, die Effekte offensiven Lehrens im Vergleich zu defensivem Lehren zu messen. Der Beitrag schließt mit Abschnitt 4, in dem eine Zusammenfassung und Ausblick gegeben werden.

## **2.Lehrplan und verwandte Arbeiten**

### Lehrplan

Im Folgenden wird ein zweisemestriger universitärer Lehrplan für IT-Sicherheit vorgestellt (siehe Abb. 1 und [DFMP05]). Dieser Lehrplan wurde in den Jahren 2003 bis 2005 durch das „Laboratory for Dependable Distributed Systems“ an der RWTH Aachen angeboten. Durch den Wechsel der Forschungsgruppe an die Universität Mannheim im Herbst 2005 befindet sich der Lehrplan erneut im Aufbau, wird aber in ähnlicher Form fortgesetzt werden. Es wird jetzt kurz auf die Inhalte der einzelnen Kurse eingegangen, unter besonderer Beachtung der offensiven Bestandteile. Am Anfang der Veranstaltungen – speziell der offensiv orientierten – erhalten die Teilnehmer eine Einführung in rechtliche Implikationen ihres Handelns und über ethisches Verhalten.

- Das erste Semester hat drei Elemente: (1) eine Vorlesung zu *angewandter IT-Sicherheit*, (2) eine Vorlesung zu *Computerforensik* und (3) ein *Seminar* zu aktuellen Entwicklungen in der Computersicherheit.
- Das zweite Semester besteht aus (1) einer Vorlesung zu *Schwachstellen in Webanwendungen* und (2) einem intensiven *Praktikum*, in dem Studenten in einem geschlossenen Netzwerk praktische Erfahrungen mit offensiven und defensiven Techniken sammeln können. Das Semester endet mit (3) einer *Sommerschule*, in der fortgeschrittene Angriffstechniken trainiert und analysiert werden.

### **Vorlesung zur angewandten IT-Sicherheit**

Die Vorlesung *Angewandte IT-Sicherheit* wird mit 4 Semesterwochenstunden (SWS) angeboten und führt in grundlegende Konzepte der Informationssicherheit ein. Nach der Besprechung der zugrunde liegenden Terminologie werden zuerst Sicherheitskonzepte betrachtet, die auf einem Einzelplatzrechner mit UNIX- oder Linux-Betriebssystem vorhanden sind (Authentifizierungsmethoden, Zugriffskontrolle, kryptographische Grundlagen, Datensicherung und physische Sicherheit, um nur einige zu nennen). Der zweite Teil der Vorlesung behandelt Netzwerk- und Internet-Sicherheit, u.a. das Absichern von Netzwerkdiensten-Diensten und Schwachstellen der TCP/IP-Protokollfamilie. Als neuere Entwicklung wird ein stärkerer Akzent auf Softwaresicherheit gesetzt. Wo immer möglich werden Schwachstellen und Angriffstechniken diskutiert um auf Schwachpunkte derzeitiger Technologien aufmerksam zu machen. So werden im Abschnitt zu Passwort-basierten Authentifizierungsmethoden Angriffe auf Passwortdateien mittels sog. Passwort-Cracker oder im Rahmen von sicheren Programmierstechniken die Auswirkungen von Buffer Overflows vorgestellt. Die Vorlesung dient als „Mind-Opener“ für eine Vielzahl von Aspekten der Computersicherheit.

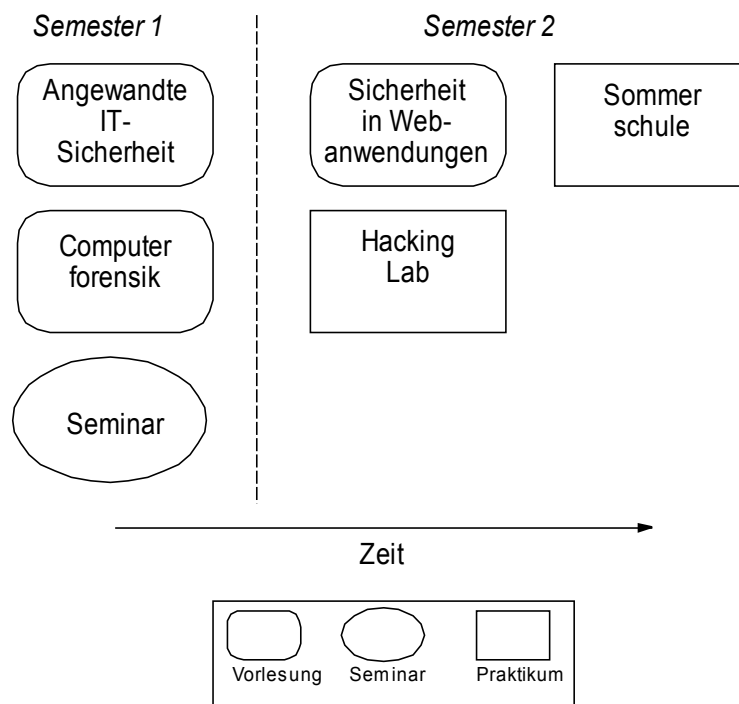


Abbildung 1: Lehrplan IT-Sicherheit

### Vorlesung zur Sicherheit in Webanwendungen

*Common Failures in Internet Applications* (oder „How web servers get Owned“) ist eine Vorlesung mit 1 SWS, deren Ziel ist aufzuzeigen, wie unsichere Webapplikationen angegriffen und für Angriffe genutzt werden können. In einer Fallstudie wird beispielhaft demonstriert, welche Problematiken sich durch den Einsatz von Webservern oder Mailservern und die Verwendung von Konzepten wie PHP, Datenbanken oder HTTP-Cookies und -Authentifizierung in Webanwendungen ergeben. Dazu zählen SQL-Injektionen, Cross site scripting (XSS), die Übernahme von Sitzungen oder die Manipulation von versteckten Feldern in HTML-Formularen. Ebenso gezeigt wird das Aufspüren von unsicheren Webdiensten mithilfe von Internet-Suchmaschinen (z.B. Datenbank- oder Druckeradministrationsseiten, die über das Internet zugänglich sind) und verfügbare Software-Werkzeuge (z.B. zur Manipulation des HTTP-Verkehrs).

### Vorlesung zu Computerforensik

Die klassische Computerforensik beinhaltet das Sammeln, die Interpretation/Aufbereitung und die Präsentation von auf Computern gefundenen Beweisen zur Unterstützung des juristischen Systems. In der Vorlesung *Computerforensik* (2 SWS) wird diese Definition von Computerforensik erweitert zu einer eher wissenschaftlich orientierten Definition: Computerforensik wird hier nicht primär als Unterstützung für das juristische System verstanden, sondern als Hilfsmittel zum Verstehen von Sicherheit. Die Veranstaltung definiert Computerforensik als den „Versuch, die Ursachen für eine Richtlinienverletzung in einem Datenverarbeitungssystem zu ermitteln“. Demzufolge beinhaltet Computerforensik auch die Analyse von sicherheitskritischen Vorfällen, um die Werkzeuge, Vorgehensweise und Techniken von Angreifern kennenzulernen und damit ähnliche Fehler in der Zukunft zu vermeiden. Die Vorlesung und die begleitende Übung zielt darauf ab, Studenten das Extrahieren und Interpretieren von potentiellem Beweismaterial und das Einschätzen der Gültigkeit dieser Informationen zu vermitteln. Großer Wert wird dabei auf Wissen über Dateisysteme gelegt, aber auch Themen wie Netzwerke und Prozessmanagement werden behandelt. Der Umgang mit kommerzieller forensische Software wird in der Veranstaltung nicht vertieft; Ziel ist, die Studenten zu

befähigen, notwendige forensische Tools selbst zu entwerfen und – basierend auf dem dafür nötigen Verständnis – die Fähigkeit zu haben, sich in die am Markt vorhandenen Softwarelösungen schnell einzuarbeiten zu können.

### **Praktikum**

Das *Hacking Lab* ist eine praktische Einführung in sowohl defensive als auch offensive Sicherheitsmethoden (4 SWS). Es bietet Studenten die Möglichkeit, beide Seiten der IT-Sicherheit kennenzulernen: mit der Anwendung offensiver Techniken die Rolle des Angreifers und mit defensiven Techniken die Rolle des Administrators von Computersystemen. Die Teilnehmer des Praktikums arbeiten in Teams. Jedes Team administriert eine Anzahl von Computern, auf denen unterschiedliche Betriebssysteme laufen (hauptsächlich Linux und MS Windows). Die Computer sind untereinander vernetzt und haben keine oder nur sehr eingeschränkte Verbindung ins Internet, sodass die Praktikumssteilnehmer Angriffe ausprobieren können, ohne dass es zu Auswirkungen auf andere Netzwerke oder deren Computer kommen kann. Durch die Anwendung der Methoden von Angreifern sammeln die Studenten Erfahrung mit Schwachstellen und Angriffspunkten von Software und Netzwerken. Dieses Wissen versetzt sie in die Lage, ihre Systeme besser gegen Angriffe zu schützen.

Im Laufe der Zeit wurden verschiedene Ansätze getestet und weiterentwickelt: Ausgehend von einem nur wenig angeleiteten Szenario, in dem die Studenten auf den von ihnen verwalteten Computer veraltete<sup>3</sup> Versionen von Betriebssystemen installierten, und dann – während sie die sicherheitsrelevante Konfiguration ihrer Systeme im Verlauf des Praktikums schrittweise erhöhten – Angriffe auf die Computer der anderen Teams ausprobierten, über vorinstallierte Betriebssysteme und eine stärkere Anleitung durch zu bearbeitende Aufgabenblätter, hin zu mehr und obligatorischen Aufgabenblättern und die Durchführung eines sog. Capture-The-Flag-Wettbewerbs<sup>4</sup> (CTF) als Teil des Praktikums. In dem letzten an der RWTH Aachen durchgeführten Praktikum war das Praktikumsnetzwerk über ein virtuelles privates Netzwerk (VPN) mit vier anderen deutschen Universitäten verbunden, um so das Erforschen und Angreifen unbekannter Netzwerke und Computer zu ermöglichen – aber gleichzeitig auch die Notwendigkeit, die eigenen Systeme gegen Angriffe aus den anderen Netzen zu schützen.

### **Sommerschule**

In der mehrwöchigen *Summerschool „Applied IT Security“* (2 bis 3 Wochen in den Semesterferien) wird den Teilnehmern die Möglichkeit geboten, Fehler in Hard- und Softwaresysteme zu induzieren und die Auswirkungen zu untersuchen. Die Veranstaltung dient als Fortführung des Hacking Labs, in der fortgeschrittene Angriffstechniken trainiert und analysiert werden. Um Studenten im Hauptstudium an wissenschaftliche Arbeitsweisen heranzuführen, werden sowohl diese als auch Promotionsstudenten zur Teilnahme ausgewählt. Zusätzlich stammt ein großer Anteil der Teilnehmer aus dem Ausland, um das Arbeiten in internationalen Teams und Wissenstransfer zu fördern.

Ein Tag in der Sommerschule beginnt mit einem Vortrag zu einem bestimmten Thema (z.B. forensische Methoden, Malware, Webanwendungen, Honeynets). Im daran anschließenden praktischen Teil bearbeiten die Teilnehmer den Rest des Tages dieses Thema, indem sie die vorgestellten Techniken anwenden und weiterentwickeln. Unterbrochen wird die Arbeit von einem sog. *Coffee Table Talk* am Nachmittag, in dem ein Gast aus einem Unternehmen oder einer Organisation ein Thema aus seinem Arbeitsgebiet vorstellt. Der Sinn des Vortrags ist es, den Teilnehmern einen Blick über den Tellerrand zu ermöglichen und die Aufmerksamkeit auf Themen zu lenken, die in der Praxis relevant sind. Der Tag endet mit einem Plenumstreffen, in dem jeder vorstellt, womit er sich an diesem Tag beschäftigt hat. Für mehr Informationen zu Ablauf und Planung der Sommerschule siehe [DGHM05].

---

<sup>3</sup> Um die Recherche nach Sicherheitslücken zu erleichtern, da diese hier bereits gut dokumentiert sind

<sup>4</sup> Siehe dazu den Abschnitt „Verwandte Arbeiten“

## Verwandte Arbeiten

Verschiedene Lehransätze beschäftigen sich mit offensiven Methoden in der Lehre. So wird an der TU Darmstadt von dem *IT Transfer Office* (ITO) des Fachbereichs Informatik seit 1999 jährlich ein *Hacker Contest* genanntes Praktikum angeboten [SMR00]. Vergleichbare Praktika sind mittlerweile auch an anderen deutschen Universitäten Teil des Lehrangebots.

Es existieren weitere Projekte, die offensive Techniken als Lehrmethode einsetzen, aber keines dieser Projekte behandelt offensive Techniken derart wissenschaftlich, wie es in der Sommerschule der Fall ist. Zu erwähnen sind hier die sog. *Wargames*, die bereits eine lange Tradition unter Sicherheitsinteressierten haben. Für ein Wargame erstellt ein Organisator eine Reihe von herausfordernden Aufgaben, die von den Teilnehmern gelöst werden müssen. Diese sind meist levelbasiert und können – je nach Art – im Webbrowser oder auf der Kommandozeile bearbeitet werden. Die Aufgaben orientieren sich an Problemen, die ein Angreifer bei dem Versuch einer Systemkompromittierung typischerweise überwinden muss. Bekannte Wargames finden sich unter [DE, HTP]. Etwas wettbewerbs-orientierter als Wargames sind *Capture-The-Flag-* (CTF) oder *Deathmatch*-Wettbewerbe, in denen die teilnehmenden Teams versuchen, in die Computer der anderen Teams einzudringen, um sog. *flags* (engl. „Flaggen“) zu erobern und gleichzeitig den eigenen Server gegen Angriffe zu verteidigen. Vermutlich am bekanntesten ist der internationale CTF (iCTF) der University of California at Santa Barbara (UCSB), in dem weltweit verteilte Teams gegeneinander antreten [UCSB, V03]. Aber auch in Europa werden derartige Wettbewerbe organisiert, so z.B. der *Cipher*-Wettbewerb an der RWTH Aachen [RWTH].

Im Militärbereich lassen sich ähnliche Ansätze offensiver Ausbildung finden, z.B. im US-amerikanischen Militär [WN98]. Das *Information Technology and Operations Center* der Militärakademie West Point (USA) verwendet ebenfalls offensive Methoden in seinem Lehrplan. Das Zentrum organisiert jährlich eine sog. *Cyber Defense Exercise*, die Ähnlichkeiten mit den CTF-Wettbewerben hat. Einheiten der US-Streitkräfte mit einem Bereich in Sicherheitsausbildung wie die Militärakademie West Point, die U.S. Airforce Academy und die Naval Postgraduate School nehmen an dieser Übung teil. Von den Teilnehmern verwaltete Computer werden von der 92<sup>nd</sup> *Information Warfare Aggressor Squadron* der *National Security Agency* (NSA) über einen Verlauf von mehreren Tagen angegriffen und müssen von den Teilnehmern verteidigt werden [DRR03, SJ98].

## **3. Angriff kontra Verteidigung**

Keine der oben erwähnten verwandten Arbeiten versucht, den Vorteil der Verwendung von offensiven Methoden in der universitären Lehre gegenüber defensiven Methoden abzuschätzen. Ausgehend von der These, dass es einen Vorteil gibt, bleibt die Frage, wie sich dies auf wissenschaftlichem Wege überprüfen lässt. Dem Autor ist kein solcher Ansatz in der Sicherheits-Community bekannt. Aber in anderen Wissenschaftsdisziplinen wie der Psychologie oder den Erziehungswissenschaften existiert eine lange Geschichte von und Methoden für das Messen von Wissen. Diese sollen genutzt werden, um die beiden Ansätze zu vergleichen.

Der folgende Abschnitt gibt eine kurze Einführung in Methoden, die in empirischen Untersuchungen genutzt werden. Danach wird der gewählte Aufbau der Studie vorgestellt, mit der die Effekte von offensiver und defensiver Lehre verglichen werden soll.

## Einführung in empirische Forschung

Um eine gemeinsame Grundlage zu bieten und für diejenigen, die nicht mit empirischer Forschung vertraut sind, wird hier eine kurze Einführung in die empirischen Methoden gegeben, die für den vorliegenden Fall relevant sind.

Eine Studie beginnt mit einer *Hypothese*, die den Sachverhalt ausdrückt, der im Interesse des Forschenden liegt. Bei der Hypothese kann es sich um eine *einseitige* (bzw. *direktionale*) Hypothese (die Richtung etwaiger Unterschiede ist spezifiziert) oder eine *zweiseitige* (bzw. *ungerichtete*) Hypothese (die Richtung ist nicht spezifiziert) handeln. In beiden Fällen wird ein allgemein gültiger Zusammenhang zwischen mindestens zwei Variablen vermutet, der in der Form „Wenn ..., dann ...“ ausgedrückt werden kann. Eine *Variable* dient in einer Studie zur Beschreibung von Merkmalsunterschieden einer Gruppe von (Untersuchungs-)Objekten. Sie ist ein Symbol für die Menge der Ausprägungen eines Merkmals (z.B. Variable Geschlecht={männlich, weiblich}). Eine Hypothese drückt die vermutete Auswirkung einer *unabhängigen Variablen* auf eine *abhängige Variable* aus. Wichtig für die Gültigkeit einer Studie sind die *interne Validität* und die *externe Validität*: eine Studie hat eine hohe interne Validität, wenn Veränderungen in den abhängigen Variablen eindeutig auf den Einfluss der unabhängigen Variablen zurückzuführen sind. Externe Validität bezieht sich auf den Grad, mit dem das in einer Stichprobe gefundene Ergebnis auf andere Personen, Situationen oder Zeitpunkte generalisiert werden kann. Die Validität wird hauptsächlich durch folgende zwei untersuchungstechnische Maßnahmen beeinflusst: Feld- gegenüber Laboruntersuchung und quasiexperimenteller Aufbau gegenüber experimentellem Aufbau. Eine *Felduntersuchung* findet in einer vom Untersucher möglichst unbeeinflussten, natürlichen Umgebung statt (z.B. auf einem Spielplatz) während eine *Laboruntersuchung* in Umgebungen durchgeführt wird, die eine weitgehende Ausschaltung oder Kontrolle von Störgrößen ermöglichen (z.B. in einem schallisolierten Raum). Generell kann festgehalten werden, dass eine Felduntersuchung eine geringere interne Validität besitzt als eine Laboruntersuchung (da eine Kontrolle von Störgrößen nur bedingt möglich ist), aber eine höhere externe Validität (da die Ergebnisse in der Regel praxisbezogener sind). Wenn in einer Studie eine natürlich gewachsene Gruppe betrachtet wird (z.B. eine Schulklasse), wird der Aufbau *quasiexperimentell* genannt, während in einem experimentellen Aufbau zufällig zusammengestellte Gruppen verglichen werden (die randomisierte Verteilung der Objekte auf die zu untersuchenden Gruppen stellt die Vergleichbarkeit der Gruppen sicher). In einem Experiment variiert der Versuchsleiter systematisch mindestens eine unabhängige Variable und registriert, welchen Effekt diese aktive Veränderung auf die abhängige Variable bewirkt. Die vom Versuchsleiter ausgeübte Variation wird als *Treatment* bezeichnet. [BD03, R05] geben mehr Informationen zu der Thematik.

## Empirische Studie

Als Szenario für die Untersuchung gehen wir von einem praktischen IT-Sicherheitskurs mit offensiver Orientierung aus, wie dem Hacking Lab oder der Sommerschule. Um zu zeigen, dass die in einem solchen Kurs gelehrt offensive Ausbildung zu einem besseren Verständnis von Computersicherheit führt, wäre ein Ansatz, bei dem nur der Effekt dieses Kurses gemessen wird (Fallstudie) nicht empfehlenswert, da dieser nur eine geringe interne Validität bietet. Stattdessen findet ein Vergleich mit einer weiteren Gruppe statt, die eine rein defensive Ausbildung erhalten hat. Dies impliziert, dass ein vergleichbarer Kurs angeboten werden muss, der dem klassisch defensiven Ansatz folgt.

Die Hypothese wird damit präzisiert zu:

Studenten, die eine offensiv orientierte Ausbildung in Computersicherheit erhalten haben, haben ein tiefergehendes Verständnis für IT-Sicherheit als Studenten, die rein defensiv ausgebildet wurden.

Bei dieser Hypothese handelt es sich um eine Unterschiedshypothese, die zwei Gruppen erfordert: eine mit offensiver, die andere mit klassisch defensiver Ausbildung, was zu einem Zwei-Gruppen-Plan führt. Diese beiden Gruppen werden mithilfe empirischer Methoden untersucht und verglichen. Die unabhängige Variable ist die *Art der Lehre* (nämlich die Menge {offensiv, defensiv}), als abhängige Variable ergibt sich *Verständnis von IT-Sicherheit*.

Für die Durchführung der Studie gibt es zwei Ansätze: zum einen die Untersuchung von Studenten, die einen der beiden Kurse als Teil ihres Studienplans besuchten. Es handelt sich um den quasiexperimentellen Ansatz. Da in diesem Fall die Studenten selbst einen der Kurse auswählen, gibt es keine Kontrolle über personenbezogene Störvariablen, und die interne Validität der Studie ist gefährdet. Zum anderen existiert der experimentelle Ansatz: Die Aufteilung der Studenten auf die beiden Gruppen erfolgt nach dem Zufallsprinzip; die Randomisierung minimiert Unterschiede bzw. neutralisiert personenbezogene Störvariablen und erhöht damit die interne Validität.  $n$  Teilnehmer werden gleichmäßig auf zwei Experimentalgruppen  $S_1$  und  $S_2$  der Größe  $n_1$  bzw.  $n_2$  verteilt (idealerweise gilt  $n_1 = n_2$ ). Auf Gruppe  $S_1$  wird das eine Treatment angewendet (hier: offensive Ausbildung), auf  $S_2$  das andere (hier: defensive Ausbildung). Für den vorliegenden Fall wird der zweite Ansatz gewählt. Er bietet eine bessere Kontrolle über die interne Validität, erfordert aber, dass zwei dafür konzipierte Kurse angeboten werden. Eine weiterführende Möglichkeit besteht darin, eine zusätzliche Gruppe, die kein Treatment erfahren hat (d.h. ohne Sicherheitsausbildung), in die Studie einzubeziehen/zu berücksichtigen. Diese Möglichkeit wird im vorliegenden Versuchsplan nicht berücksichtigt, kann jedoch in einer zukünftigen Untersuchung eingesetzt werden.

Um zu überprüfen, ob weitere unabhängige Variablen relevant sind, kann ein mehrfaktorielles Design verwendet werden. So kann z.B. eine zweite unabhängige Variable hinzugefügt werden; im vorliegenden Fall z.B. „Vorwissen“, „Motivation“, „Intelligenz“ oder „Grad der Anleitung“ (hoch, niedrig). Unter der Annahme, dass die zweite unabhängige Variable ebenfalls zwei Ausprägungen hat, ergeben sich vier Experimentalgruppen  $S_{11}$ ,  $S_{12}$ ,  $S_{21}$  und  $S_{22}$ , auf die die Studienteilnehmer gleichmäßig verteilt werden müssen.

### **Experiment**

Das Experiment wird als Laboruntersuchung, d.h. als experimentelles Design angelegt. Es werden zwei Kurse angeboten, einer defensiv orientiert, der andere offensiv. Es handelt sich um mehrtägige Kompaktkurse, um den Aufwand sowohl für die Versuchsleitung als auch die Teilnehmer in Grenzen zu halten. Außerdem lässt sich die Studie so einfacher wiederholen, als wenn die Kurse im Verlauf eines Semesters angeboten werden. Die Entscheidung fiel auf jeweils einen 3-tägigen, praktischen Kurs, in dem jedes Thema mit einem Vortrag eingeführt und danach Aufgaben von den Teilnehmern praktisch bearbeitet werden. Für den Vergleich wird am Ende des Kurses eine Messung des Sicherheitsstandes und Verständnisses der einzelnen Gruppenmitglieder durchgeführt. Da es sich um einen größtenteils praktischen Kurs handelt fiel die Wahl dafür auf einen praktischen Test. In der derzeitigen Variante konfrontiert der Test die Untersuchungsteilnehmer mit einem Computersystem mit Sicherheitslücken und Fehlkonfigurationen, welche erkannt und korrigiert werden müssen. Dabei gemessene Kriterien (z.B. Anzahl der gefundenen Sicherheitslücken und benötigte Zeit) werden als Maß für den Vergleich herangezogen (siehe Abb. 2). Um zusätzlich den Wissensstand der einzelnen Teilnehmer vor und nach den Kursen vergleichen zu können, erhalten die Studenten vor Beginn und nach Ende der Kurse einen Fragebogen, evtl. auch nochmal einige Zeit danach, um die Langzeitwirkung zu überprüfen. Der Fragebogen ist aus zwei Teilen aufgebaut: der eine Teil soll das Sicherheitsbewusstsein abfragen (z.B. Selbsteinschätzung, Login am eigenen Computer als Administrator?), der andere Wissen über Sicherheitstechnologien überprüfen (z.B. Kenntnisse über E-Mail-Verschlüsselung oder Buffer Overflows). Die Problematik des Fragebogens ist, dass die Fragen so ausgewählt sein müssen, dass sie das gewünschte Ziel erreichen. Der Theorie des Fragebogenentwurfs folgend, muss dieser überprüft und getestet werden.

Die Fragestellung wird seit Anfang diesen Jahres auch in zwei Diplomarbeiten bearbeitet: Die eine Arbeit – mit dem Titel „Wie lehrt man IT-Sicherheit am besten? - IT-Sicherheitskurse weltweit: Überblick, Klassifikation und Basismodule“ – analysiert und klassifiziert eine weltweite Auswahl von Kursen zur Computersicherheit. Anhand der Klassifikation soll ermittelt werden, welche Themen eher offensiv und welche eher defensiv einzuordnen sind. Basierend darauf werden dann zwei Kurse konzipiert, einer mit defensiver, der andere mit offensiver Ausrichtung. Die zweite Arbeit – mit dem

Titel „Wie lehrt man IT-Sicherheit am besten? - Eine empirische Studie “ – bildet die Grundlage für die Durchführung der geplanten Studie und nutzt die Erkenntnisse und Ergebnisse der ersten Arbeit.

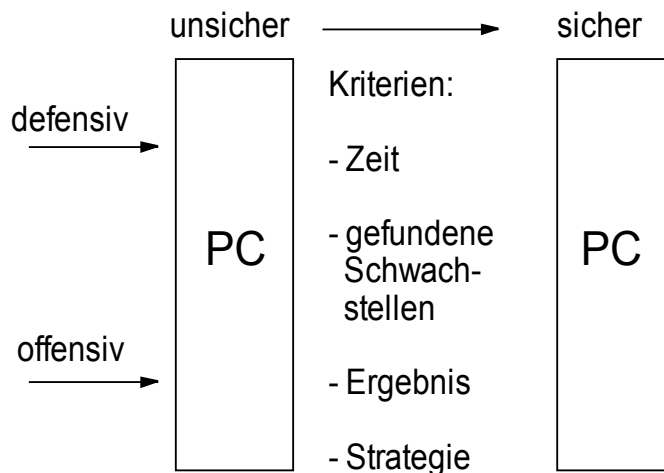


Abbildung 2: Versuchsdurchführung

#### 4. Zusammenfassung und Ausblick

Dieser Beitrag stellt einen Ansatz vor, um die Auswirkung offensiver Lehre auf Universitätsstudenten zu messen. Um nachzuweisen, dass offensive Lehre Vorteile gegenüber einer rein defensiven Ausbildung hat, werden Methoden aus den Human- und Sozialwissenschaften für den Entwurf eines Experiment eingesetzt.

Die Untersuchung wird im März 2007 erstmalig an Universitätsstudenten durchgeführt; auf dem Kongress im Mai können voraussichtlich erste Ergebnisse vorgestellt werden. Bis dahin muss der Versuchsplan weiterentwickelt, konkretisiert und überprüft werden.

Gefährdet wird der Einsatz offensiver Methoden in Lehre und Penetration Tests durch den Entwurf zur Änderung des Strafrechts zur Bekämpfung der Computerkriminalität, den das Bundeskabinett am 20. September 2006 beschlossen hat. Hier besteht Unsicherheit, inwieweit der Besitz und die Verwendung von potentiellen Hacker-Werkzeugen strafbar sein wird.

#### 5. Literaturhinweise

- [SH04] T. Slewe und M. Hoogenboom. Who will rob you on the digital highway? *Communications of the ACM*, 47(5):56–60, Mai 2004.
- [RFD] P. G. Neumann. The risks-forum digest. <http://catless.ncl.ac.uk/risks>.
- [N04] P. G. Neumann. Inside risks: the big picture. *Communications of the ACM*, 47(9):112, Sept. 2004.
- [SMR00] M. Schumacher, M.-L. Moschgath, und U. Roedig. Angewandte Informationssicherheit: Ein Hacker-Praktikum an Universitäten. *Informatik Spektrum*, 6(23), Juni 2000.
- [V03] G. Vigna. Teaching network security through live exercises. World Conference on Information Security Education, *IFIP Conference Proceedings*, pages 3–18. Kluwer, 2003.
- [AS05] K. P. Arnett und M. B. Schmidt. Busting the ghost in the machine. *Communications of the ACM*, 48(8):92–95, Aug. 2005.

- [FV93] D. Farmer und W. Venema. Improving the security of your site by breaking into it. Usenet Posting auf comp.security.unix, 3. Dez. 1993.
- [AG04] I. Arce und G. McGraw. Guest Editors' introduction: Why attacking systems is a good idea. *IEEE Security & Privacy*, 2(4):17–19, Juli/Aug. 2004.
- [C06] G. Conti. Hacking and innovation (guest editor's introduction). *Communications of the ACM*, Juni 2006.
- [C05] G. Conti. Why computer scientists should attend hacker conferences. *Communications of the ACM*, 48(3):23–24, März 2005.
- [R05] D. Rost. *Interpretation und Bewertung pädagogisch-psychologischer Studien*. Beltz, 2005.
- [SJ98] W. Schepens und J. James. Architecture of a cyber defense competition. In *Proceedings of the 2003 IEEE International Conference on Systems, Man & Cybernetics*, 1998.
- [BH] Black Hat briefings, training and consulting. <http://www.blackhat.com>. Letzter Zugriff Jan. 2007.
- [DC] DEFCON hacking event. <http://www.defcon.org>. Letzter Zugriff Jan. 2007.
- [BD03] J. Bortz und N. Döring. *Forschungsmethoden und Evaluation für Human- und Sozialwissenschaftler*. Springer, 3. Auflage, 2003.
- [DE] Digital Evolution. Wargames "Digital Evolution". <http://wargames.dievo.org>. Letzter Zugriff Jan. 2007.
- [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.
- [DFMP05] M. Dornseif, F.C. Freiling, M. Mink und L. Pimenidis. Teaching data security at university degree level. In *Proceedings of the IFIP Fourth World Conference on Information Security Education*, S. 213–222, 2005.
- [DGHM05] M. Dornseif, F.C. Gärtner, T. Holz, and M. Mink. An Offensive Approach to teaching Information Security: "Aachen Summer School Applied IT Security". Technischer Bericht AIB-2005-02, RWTH Aachen, Jan. 2005.
- [HTP] Hack this page. Homepage "Hack this page". <http://www.hackthispage.tk>. Letzter Zugriff Dez. 2006.
- [UCSB] G. Vigna. Homepage "UCSB Capture The Flag". <http://www.cs.ucsb.edu/~vigna/CTF/>. Letzter Zugriff Dez. 2006.
- [RWTH] L. Pimenidis. Homepage „Cipher Capture The Flag“. <http://www.cipher-ctf.org>. Letzter Zugriff Jan. 2007.
- [WN98] G. White und G. Nordstrom. Security across the curriculum: Using computer security to teach computer science principles. In *Proceedings of the 19th International Information Systems Security Conference*, S. 519–525, 1998.
- [MF06] F.C. Freiling und M. Mink. Is Attack Better Than Defense? Teaching Information Security the Right Way. In *Proceedings of the 2006 Information Security Curriculum Development Conference*, Sept. 2006.