

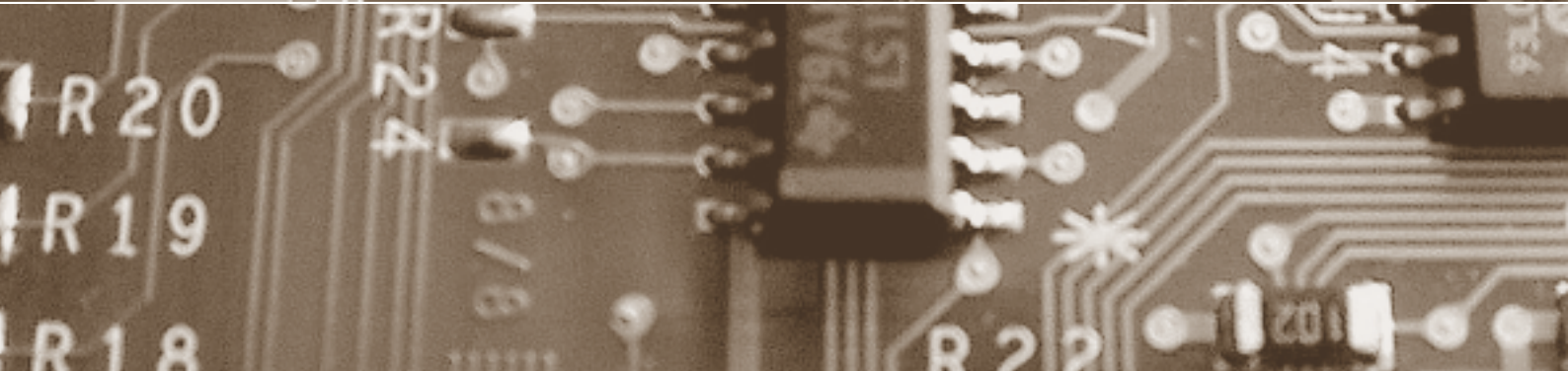
Schwerpunkt:

Suchen – Vergessen

fokus: Suchmethoden im Netz: heute – morgen

fokus: Wer sucht, der findet (nicht immer): Internetzensur

report: BWIS-II-Reform: kritische Bemerkungen



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

fokus

Schwerpunkt:

Suchen – Vergessen

auftakt

Geschürte Ängste – gleichgültige

Menschen

von Gerhart R. Baum

Seite 101

Vergessen – nicht vergessen –

nicht finden

von Beat Rudin

Seite 104

Suchmethoden im Netz: heute – morgen

von Felix-Robinson Aschoff

und Abraham Bernstein

Seite 106

Daten «löschen» oder wirksam
entfernen?

von Thomas Burris

Seite 110

Wer sucht, der findet (nicht immer)

von Daniel Zinn

Seite 114

Best Practices for Social Networks

von Giles Hogben

Seite 120

zwischenakt

Weit vom (Daten-)Geschütz ...

von Frank U. Frey

Seite 123

Die Entwicklung von Suchtechnologien für das World Wide Web gehört heute zu den zentralen Herausforderungen der Informatik. Eine Alternative zu den heutigen Algorithmen-basierten Suchmaschinen stellen hierbei Social-Search-Ansätze dar. Das Semantic Web beinhaltet schliesslich die Vision, komplexe natürlichsprachige Anfragen beantworten zu können.

**Suchmethoden
im Netz: heute –
morgen**

Nicht alles, was im Internet steht, ist gut. Es kann zutiefst menschenunwürdig und rechtswidrig sei (wie Kinderpornografie) oder auch bloss einem Regime nicht gefallen. Aus diesem Grund gibt es rund um den Erdball Internetzensur – zum Teil mit Unterstützung der Betreiber von Internet-suchmaschinen.

**Wer sucht,
der findet
(nicht immer)**

«Social Networks» erleben einen regelrechten Boom und können neben gewünschten Effekten auch unerwünschte Nebenwirkungen zeitigen. Die ENISA (European Network and Information Security Agency) hat ein Papier erarbeitet, worin einerseits die Bedrohungen dargestellt und andererseits Empfehlungen für Betreiber und Nutzer aufgestellt werden.

**Best Practices for
Social Networks**

impresum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer, J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Rubrikenredaktor: Dr. iur. Amédéo Wermelinger

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Kirschgartenstrasse 7, CH-4010 Basel
Tel. +41 (0)61 270 17 70, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 112.00 (inkl. Versandkosten), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtchenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Druck AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

BWIS-II-Reform: kritische Bemerkungen Mit der beabsichtigten Reform des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS) sollen dem Staatsschutz weitreichende Eingriffsbefugnisse zugestanden werden. Der Beitrag setzt sich kritisch mit den heiklen Aspekten des Entwurfs auseinander.

OpenID: Single-Sign-On-Spezifikation OpenID ist ein dezentral angelegtes Single-Sign-On-System, bei welchem der Benutzer über seine Identitäten und über die Weitergabe seiner Identitäts-Attribute entscheidet, wobei die Unabhängigkeit von Identity Providern gewährleistet wird.

Schmerzvolle Erfahrung Die Einwilligung in Persönlichkeitsverletzungen gehört zur Ausübung der höchstpersönlichen Rechte, welche der urteilsfähigen minderjährigen Person zustehen, wie das Bundesgericht im Fall der schmerzhaften Behandlung einer 13-jährigen festgehalten hat. Was heisst das z. B. bei Facebook-Eintragungen, die sich bei einer Stellenbewerbung negativ auswirken können?

Videoüberwachung im Lichte der Verfassung Die Datenschutzkommission des Fürstentums Liechtenstein hat entschieden, dass eine flächendeckende Videoüberwachung in der Fussgängerzone der Hauptstadt Vaduz rund um die Uhr zur Vermeidung von Vandalenakten und Straftaten unverhältnismässig sei.

report

GESETZGEBUNG

BWIS-II-Reform: kritische Bemerkungen

von Lucien Müller, Nina Widmer und Rainer J. Schweizer

Seite 124

IT-SICHERHEITSAUSBILDUNG

Über den Nutzen offensiver Lehre von Martin Mink

Seite 130

TECHNIK

von Robert Ott

Seite 134

RECHTSPRECHUNG

Verwaltungsrat lebenslang auf dem Web?

von Amédéo Wermelinger

Seite 138

RECHTSPRECHUNG

von Amédéo Wermelinger

Seite 139

RECHTSPRECHUNG

Videoüberwachung im Lichte der Verfassung

von Philipp Mittelberger

Seite 140

TRANSFER

Zugriffschutz: eine technische Herausforderung

von Roland Portmann

Seite 144

forum

ISSS

Am Puls der Informationssicherheit

von Bernhard Hämmerli

Seite 146

agenda

Seite 147

schlussakt

Nachträgliche zusätzliche «Sicherheit»?

von Bernhard Hämmerli

Seite 148

Cartoon

von Hanspeter Wyss

IT-Sicherheitsausbildung

Über den Nutzen offensiver Lehre



Dipl.-Inform.
Martin Mink,
Doktorand am
Lehrstuhl für
Praktische
Informatik 1,
Universität
Mannheim,
Mannheim/
Deutschland
mink@
uni-mannheim.de

In der Nacht vom 7. auf den 8. Dezember 2007 sassen 22 Studenten und Mitarbeiter der Universität Mannheim dicht gedrängt in einem Raum vor Computern und arbeiteten fieberhaft. Sie hatten sich hier versammelt, um von fünf Uhr nachmittags bis zwei Uhr morgens gegen 34 andere Teams aus Europa, den USA, Australien, Russland und Indien anzutreten. Weitere Studenten betraten den Raum als Zuschauer und beobachteten interessiert das Geschehen. Als nach langem und spannendem Kampf um kurz vor drei Uhr morgens das Ergebnis verkündet wurde und das Mannheimer Team den zweiten Platz erreicht hatte, brach Jubel los. Was war hier los? Ein Wettbewerb in IT-Sicherheit, genannt *Capture-The-Flag* (CTF), veranstaltet von der Universität in Santa Barbara, Kalifornien (UCSB), USA¹. Als Nebeneffekt dieser ausgezeichneten Platzierung erhielt das Team in den nächsten Tagen Jobangebote und Interviewanfragen.

IT-Sicherheitsausbildung an Universitäten

Der Wettbewerb entstammt einem Trend in der Ausbildung in IT-Sicherheit an Universitäten. Im klassischen, defensiven Ansatz steht die Lehre von Schutz- und Verteidigungsmassnahmen im Vordergrund. Typischerweise wird hier viel Kryptografie gelehrt, ausserdem Konzepte wie Firewalls oder Intrusion-Detection-Systeme.

Im Gegensatz dazu werden im neueren, offensiven Ansatz existierende Systeme und Software auf ihre Sicherheit untersucht. Die dabei erkannten Schwachstellen können einerseits zur Verbesserung dieser Systeme und den Entwurf von neuen Systemen genutzt werden. Andererseits soll das Wissen über Angriffsmethoden zu einer verbesserten Strategie in der Abwehr von Angriffen beitragen.

Diese Entwicklung fand zuerst in der Praxis statt: Administratoren nutzten die Methoden von Angreifern, um die Sicherheit ihrer Netzwerke zu überprüfen, indem sie mit entsprechenden Software-Werkzeugen den Netzwerkverkehr beobachteten oder die Passwörter der Benutzer ihrer Systeme auf schwache Passwörter testeten. Solches Vorgehen war jedoch anfangs stark umstritten. Der Vorwurf lautete, dass mit derartigen Werkzeugen Angriffsmethoden für jedermann zugänglich gemacht werden. So wurde Dan Farmer im Jahr 1995 von seinem damaligen Arbeitgeber gekündigt, weil er die Software SATAN veröffentlichte. Mit diesem Werkzeug konnten Administratoren automatisiert nach Schwachstellen auf vernetzten Computern suchen².

Mittlerweile hat sich die Ansicht gewandelt, wird jedoch immer noch diskutiert, und der offensive Ansatz ist vor einigen Jahren auch in die universitäre Lehre eingezogen. Vorreiter in diesem Bereich in Deutschland

ist die TU Darmstadt, die seit acht Jahren den sogenannten *Hacker Contest* anbietet. Dabei handelt es sich um ein Praktikum, in dem die Teilnehmer sowohl die Rolle eines Administrators als auch eines Angreifers einnehmen. In einem abgeschotteten Netzwerk sichern sie von ihnen administrierte Computer gegen Angriffe ab und versuchen gleichzeitig, die Computer der anderen Praktikumsteilnehmer anzugreifen. Ähnliche praktische Veranstaltungen werden mittlerweile auch von anderen deutschen Universitäten angeboten. In der Schweiz veranstaltet die Hochschule Luzern ein Sicherheitspraktikum, dessen Unterlagen seit kurzem frei verfügbar sind³. Der Autor dieses Artikels führte an der RWTH Aachen erstmals im Wintersemester 2004 ein sogenanntes *Hacker-Praktikum* durch und seit dem Sommersemester 2007 an der Universität Mannheim. An vielen Universitäten in den USA sind derartige Praktika bereits üblich.

Die Akzeptanz des offensiven Ansatzes lässt sich u.a. in der Literatur an Beiträgen und Artikeln wie denen von Conti sowie Arce und McGraw erkennen. Dem Vorwurf der Gefahr einer illegalen Verwendung des erlernten Wissens muss jedoch immer noch begegnet werden. Ein Werkzeug, mit dem sich ein Administrator schützen kann, kann von einem Angreifer zum Angriff genutzt bzw. missbraucht werden – und umgekehrt. Für die Sicherheitsaus-

bildung bedeutet das: Die Studenten müssen über die rechtlichen und ethischen Implikationen ihres Handelns aufgeklärt werden. Zu den in Deutschland rechtlich relevanten Regelungen gehören die Paragraphen des Strafgesetzbuches: § 202a (*Ausspähen von Daten*), § 202b (*Abfangen von Daten*), § 303a (*Datenveränderung*) und § 303b (*Computersabotage*) sowie seit August 2007 der umstrittene sogenannte «Hackerparagraf», § 202c (*Vorbereiten des Ausspähens und Abfangens von Daten*). In den Veranstaltungen des Lehrstuhls an der Universität Mannheim erfolgt dies durch eine Besprechung der rechtlichen und ethischen Grundsätze zu Veranstaltungsbeginn.

Ausser den Praktika existiert ein weiteres, eher spielerisches Konzept in der offensiven IT-Sicherheitsausbildung: die eingangs erwähnten Capture-Flag-Wettbewerbe. Der Name leitet sich ab von dem Ziel des Wettbewerbs, «Flaggen» zu erobern. Bei den Flaggen handelt es sich um Zeichenketten, die vom Veranstalter auf Servern abgelegt werden. Jedes teilnehmende Team verwaltet einen Server, alle Teams verwenden den gleichen Server und die Server sind über Netzwerk miteinander verbunden. Auf den Servern laufen vom Veranstalter erstellte Dienste, die Sicherheitslücken enthalten. Jedes Team muss seinen Server gegen Angriffe der anderen Teams schützen und gleichzeitig die Server der anderen Teams angreifen, um Flaggen zu erobern.

Positive Erfahrungen

Die am Lehrstuhl mit der offensiven Lehre gemachten Erfahrungen sind äusserst positiv – sowohl in der Zeit an der RWTH Aachen als auch derzeit an der Universität Mannheim. Die Studenten sind sehr inter-

essiert und investieren viel Zeit. Das Hacker-Praktikum ist regelmässig ausgebucht. Die Teilnahme an CTF-Wettbewerben verursacht viel Begeisterung – nicht nur bei den Teilnehmern, sondern auch bei den Zuschauern. Daraus ergab sich die Frage: Lässt sich der Nutzen des offensiven Lehransatzes bewerten?

Abgesehen von einer Veröffentlichung von MICHAEL NAEF und DAVID BASIN (ETH Zürich) ist dem Autor keine Untersuchung des offensiven Ansatzes in der IT-Sicherheitsausbildung an Hochschulen bekannt. In dem Beitrag der ETHZ findet jedoch lediglich ein konzeptioneller Vergleich statt. Um den Nutzen der offensiven Ausbildung zu evaluieren, muss das Wissen über IT-Sicherheit gemessen werden. Aber wie lässt sich Wissen messen? Hierfür finden sich Methoden im Bereich der Human- und Sozialwissenschaften, die im Rahmen einer empirischen Studie angewendet werden sollen.

Planung und Durchführung der Studie

Für die Bewertung des offensiven Lehransatzes erfolgt ein Vergleich mit einer Kontrollgruppe. Die Wahl fiel auf den defensiven Ansatz. In der Studie werden somit zwei Gruppen von Universitätsstudenten, von denen die eine offensiv, die andere defensiv ausgebildet wurde, miteinander verglichen – in Bezug auf verschiedene Kriterien wie Wissensstand und Fähigkeit der Anwendung des erlernten Wissens. Die gesammelten Daten ermöglichen eine empirische Bewertung des offensiven Ansatzes.

Für die Studie wurden zwei IT-Sicherheitskurse entworfen. Einer der Kurse ist offensiv, der andere defensiv orientiert. Die Kurse umfassen drei Tage und bestehen aus neun Modulen. Bei dem ersten Modul handelt

es sich um eine Einführung in Linux-Administration, Netzwerke und C-Programmierung, bei den Modulen 2 bis 8 um Themen aus der IT-Sicherheit, und das neunte Modul ist der Test für den Vergleich. Als Themen werden u.a. Passwort-, Netzwerk-, Software- und Webanwendungssicherheit sowie Firewalls und Malware behandelt. Jedes Modul besteht aus einem Vortrag zur Einführung in die Thematik, dem anschließenden praktischen Bearbeiten eines Aufgabenblatts sowie der abschliessenden Besprechung der Aufgaben. Der Theorieteil ist für beide Gruppen identisch gehalten, die Unterscheidung zwischen offensiv und defensiv liegt im praktischen Teil.

Der Vergleich selbst erfolgt mithilfe eines Wissenstests, eines Tests zum Sicherheitsbewusstsein (Awareness) sowie eines Abschlusstests. Letzterer ist als praktischer Test konzipiert. Dies entspricht einerseits der praktischen Ausrichtung der Kurse. Andererseits lässt sich durch Beobachten des konkreten Handelns eine bessere Aussage treffen als durch Angaben der Teilnehmer zu ihrem vermutlichen Verhalten. Der Wissens- und der Awareness-Test werden in Form eines Fragebogens durchgeführt, der zu Beginn und zu Ende der Massnahme erhoben wird. Damit lässt sich die Veränderung des Wissens bzw. der Awareness durch den Kurs feststellen.

Kurz & bündig

An Universitäten werden vermehrt nicht nur Techniken zum direkten Schutz von IT-Systemen gelehrt, sondern auch Angriffsmethoden vermittelt. Im Rahmen einer empirischen Studie wird untersucht, ob der offensive Ansatz bessere Resultate für die Verteidigung bringt als der defensive. Die bei der ersten Durchführung der Studie erlangten Daten unterstützen diese Vermutung; es zeigt sich jedoch auch, dass für eine Aussage mehr Daten erhoben werden müssen.

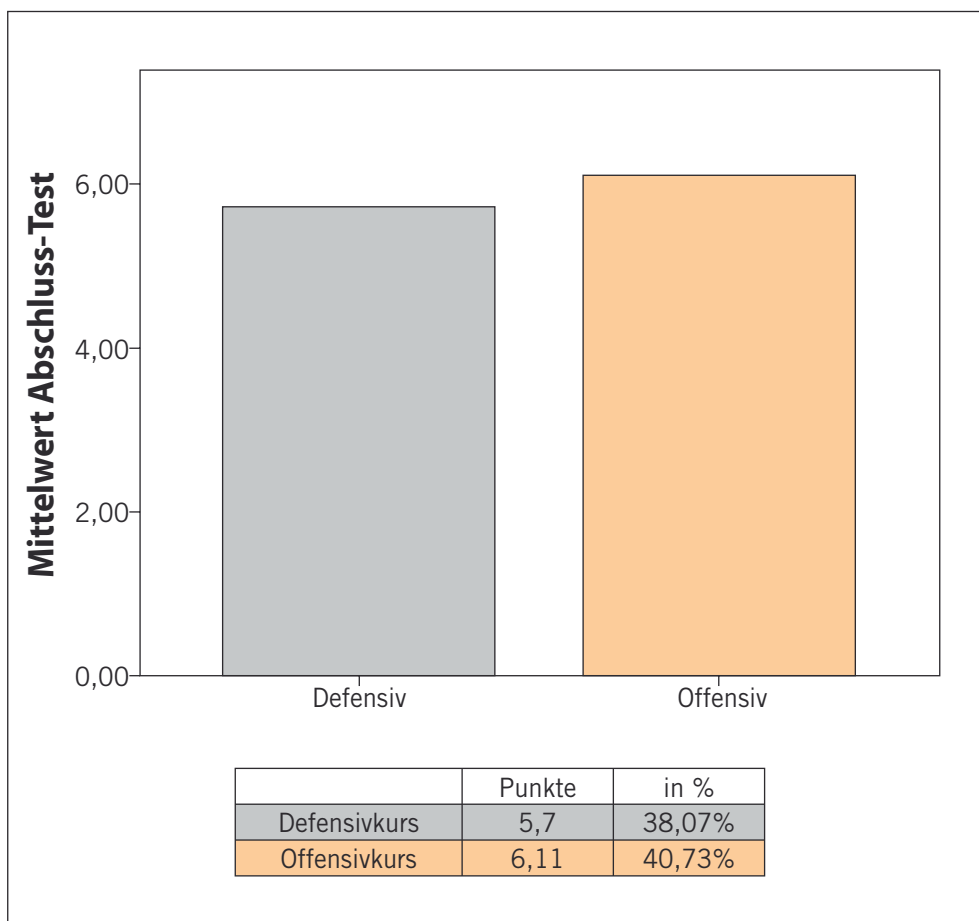


Abb. 1: Ergebnis des Abschlusstests

Der Abschlusstest war für den offensiven und defensiven Kurs identisch ausgelegt. Er stellte die Teilnehmer vor die Aufgabe, innerhalb einer festgelegten Zeitspanne auf einem von den Versuchsleitern präparierten Linux-System Anzeichen für erfolgte Angriffe (Kompromittierungen) und Konfigurationsfehler zu identifizieren. Es waren u.a. Rootkits installiert, Benutzer mit schwachen Passwörtern vorhanden und von Vorgaben abweichende Dienste

gestartet. Ziel war es, das System in einen sicheren Zustand zu überführen.

Die Studie wurde zum ersten Mal im März 2007 an der RWTH Aachen durchgeführt und zwei weitere Male im Frühjahr 2008. Letztere müssen noch ausgewertet werden; die Angaben in diesem Artikel beziehen sich deswegen auf die Studiendurchführung im Jahr 2007. Hier nahmen 42 Studenten teil; hauptsächlich von der RWTH Aachen, aber auch von

anderen deutschen Universitäten. Neben Informatikstudierenden waren auch weitere Studiengänge vertreten. Das Vorwissen der Teilnehmer wurde zum Zeitpunkt der Kursanmeldung durch den Wissenstest erfasst. Die Bewerber wurden dann zufällig derart auf die beiden Termine verteilt, dass in jedem Termin jeweils zur Hälfte Teilnehmer mit geringem und mit hohem Vorwissen vorhanden waren. Durch diese Zuteilung konnte das Vorwissen als ein zusätzliches Kriterium erfasst werden, und die randomisierte Aufteilung auf die beiden Gruppen ist Grundlage für die Vergleichbarkeit der Gruppen.

Auswertung und Ergebnisse

Für die Auswertung des Abschlusstests wurden Aufzeichnungen der Probanden genutzt. Darin hatten sie während des Tests die identifizierten Probleme, die Lösungsvorschläge zu deren Behebung sowie die darauf verwendete Zeit protokolliert. Zusätzlich waren alle Tastatureingaben der Teilnehmer mit einem Keylogger aufgezeichnet worden. Als Mass für das IT-Sicherheitsverständnis der beiden Gruppen diente die Anzahl der gefundenen Kompromittierungen, die benötigte Zeit und die Strategie (Reihenfolge der Bearbeitung).

Die Auswertung des Abschlusstests ergab, dass die Teilnehmer des Offensivkurses mit durchschnittlich 40,73% der maximal 15 erreichbaren Punkte ein besseres Ergebnis erzielten als die Teilnehmer des Defensivkurses mit 38,07% (siehe Abb. 1). Schlüsselte man den Abschlusstest nach Vorwissen auf, dann ergibt sich, dass die Teilnehmer mit wenig Vorwissen in etwa gleich abschneiden. Die Teilnehmer mit viel Vorwissen holen erwartungsgemäss mehr Punkte (siehe Abb. 2). Eine interessante

Literatur, weiterführende Links

- I. ARCE/G. MCGRAW, Why attacking systems is a good idea, IEEE Security & Privacy, Juli/Aug. 2004, 17–19.
- G. CONTI, Hacking and Innovation, Communications of the ACM, Juni 2006.
- J. MARKOFF, Dismissal of Security Expert Adds Fuel to Internet Debate, The New York Times, 22. März 1995, <<http://query.nytimes.com/gst/fullpage.html?res=990CE7D81739F931A15750COA963958260>> (10.04.2008).
- M. NAEF/D. BASIN, Conflict or Review – Two Approaches to an Information Security Laboratory, Communications of the ACM, 2008 (noch nicht veröffentlicht).
- F. VAN DER BEEK, Wie lehrt man IT-Sicherheit am besten? – Eine empirische Studie, Diplomarbeit, RWTH Aachen, 2007.

Beobachtung hierbei ist, dass Teilnehmer mit viel Vorwissen im Offensivkurs ein besseres Ergebnis erreichen als im Defensivkurs.

Im Wissenstest konnten die Offensivkursteilnehmer ihre Ergebnisse im Mittel um knapp 44% verbessern, die des Defensivkurses lediglich um knapp 28%. Bezüglich der Awareness ist ebenfalls eine klare Tendenz erkennbar. Die offensive Gruppe wurde wesentlich stärker bezüglich potenzieller IT-Sicherheitsrisiken sensibilisiert als die Teilnehmer des Defensivkurses.

Ebenfalls interessant ist die Betrachtung der Strategien, welche die Teilnehmer bei der Analyse des Systems verfolgten. Die Teilnehmer des Defensivkurses suchten früher nach Benutzern mit schwachen Passwörtern und erkannten das Problem von Diensten, die ohne Vorgabe gestartet waren. Demgegenüber steht die Bearbeitungsstrategie der Offensivgruppe, welche zuerst nach Rootkits suchte. Zudem identifizierten sie häufiger und früher das Vorhandensein eines aktiven Netzwerk-Sniffers und der Netzwerkschnittstelle im *promiscuous mode*. Auffallend ist, dass die Versuchsteilnehmer des Defensivkurses die Präsenz eines Rootkits erst sehr spät oder gar nicht überprüften. Dieser Schritt sollte jedoch als erstes erfolgen. Offenbar konnten die Teilnehmer des Offensivkurses die konkreten Bedrohungspotenziale für IT-Sicherheit eher einschätzen.

Eine ausführlichere Beschreibung der Ergebnisse sowie des Aufbaus der Studie findet sich in der in der Litera-

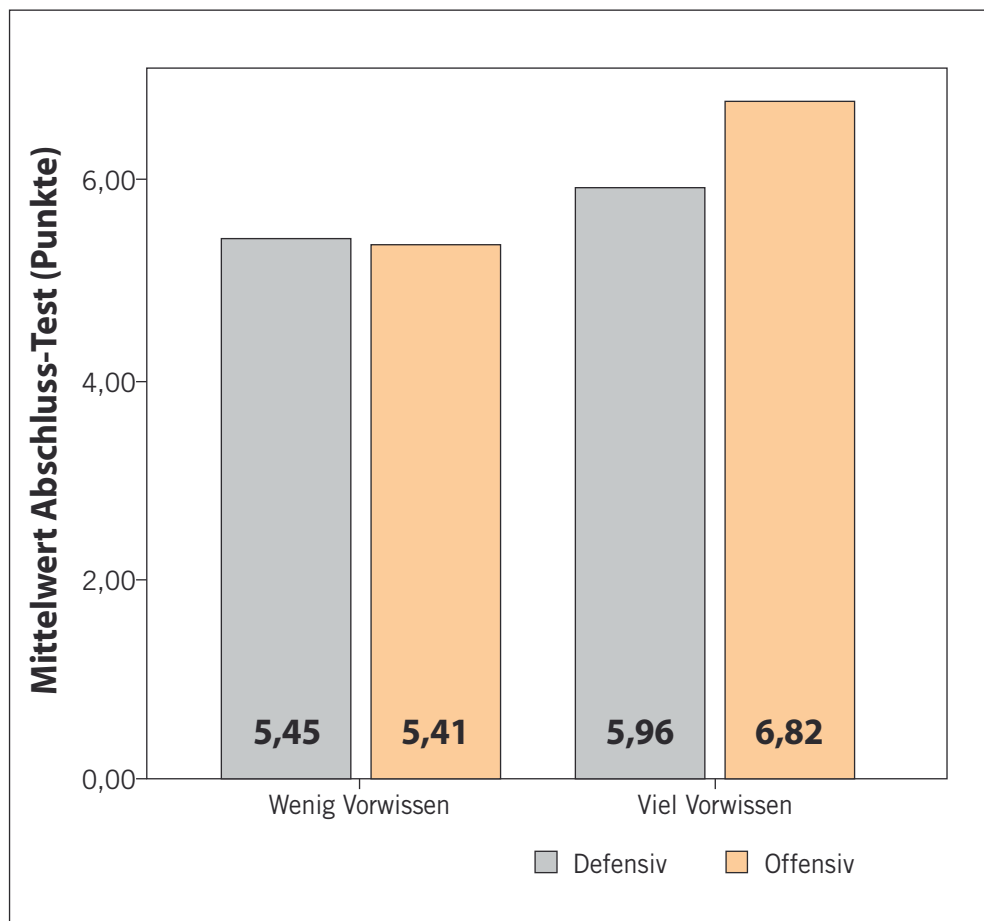


Abb. 2: Abschlusstest nach Vorwissen

turliste genannten Diplomarbeit von F. VAN DER BEEK.

Ist Angriff besser als Verteidigung?

Die in der vorgestellten Studie untersuchte These, dass der offensive Ansatz bessere Ergebnisse für die IT-Sicherheitsausbildung an Hochschulen bringt als der defensive, kann anhand der vorliegenden Daten nicht beantwortet werden. Im Wis-

sens- und Awareness-Test zeigen sich zwar Vorteile für die offensive Gruppe, aber im Abschlusstest ist der Unterschied zwischen beiden Gruppen mit nur 0,41 Punkten zu gering. Mithilfe wiederholter Durchführungen der Studie wie der im Jahr 2008 müssen mehr empirische Daten gesammelt werden, um eine aussagekräftige Entscheidung treffen zu können. ■

Fussnoten

- ¹ <<http://www.cs.ucsb.edu/~vigna/CTF/>> (14.12.2007).
- ² Siehe Artikel von JOHN MARKOFF in der New York Times (Literaturverzeichnis).
- ³ Security-Labor der Hochschule Luzern: <<http://www.securitylabor.ch>> (1.4.2008).

Meine Bestellung

- 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name _____ Vorname _____

Firma _____

Strasse _____

PLZ _____ Ort _____ Land _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:

Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich

Telefon +41 44 200 29 19

Telefax +41 44 200 29 18

E-Mail: zs.verlag@schulthess.com

Homepage: www.schulthess.com

Schulthess 