Security Awareness Kampagne als Element aktiven Lernens – ein Erfahrungsbericht

Marietta Spangenberg[1]

Abstract: Das Thema "Entwicklung von IT-Sicherheitsbewusstsein an der Hochschule Zittau/Görlitz" wurde im Modul IT-Sicherheitsmanagement der Masterausbildung Informatik als Projektaufgabe bearbeitet. Mit diesem Projekt sollten Aktivitäten im Bereich IT-Sicherheitsbewusstsein und Schulung zu IT-Sicherheitsfragen an der Hochschule initiiert und insbesondere eine Security Awareness Kampagne durchgeführt werden. Neben der Anwendung des erworbenen Wissens im Bereich IT-Sicherheitsmanagement in der Praxis waren bei der Bearbeitung des Themas weitere Kompetenzen wie beispielsweise Kreativität, Teamfähigkeit oder Kommunikation gefragt. Die Studierenden entwickelten eigenständig Ideen, etablierten ein Projektmanagement, bearbeiteten das Thema in Projektteams und realisierten eine Security Awareness Kampagne an der Hochschule mit einer abschließenden Evaluation. Das Projekt wird als Beispiel aktiven Lernens untersucht, der Aufwand für Studierende und Lehrende sowie die Projektergebnisse werden analysiert und bewertet.

Keywords: aktives Lernen, Didaktik, Hochschulausbildung, Informationssicherheitsmanagement, IT-Sicherheit, IT-Sicherheitsbewusstsein Kompetenzen, projektorientiertes Lernen, problembasiertes Lernen, Security Awareness

1 Einführung

Ständige Weiterentwicklungen der Informations- und Kommunikationstechnologien und der darauf basierenden Anwendungen verändern Gesellschaft, Wirtschaft, Wissenschaft und Ausbildung. Die zunehmende Vernetzung, die Integration der Netze, die Ubiquität der Informationsnutzung, das enorme Wachstum von Datenmengen und eine Zunahme der Komplexität bestimmen die Entwicklung. Dabei werden die Grenzen der bisherigen Informationsverarbeitung überschritten, wenn beispielsweise Smartgeräte im Haushalt zum Einsatz kommen oder autonome Fahrzeuge unterwegs sind. Andererseits werden jeden Tag neue Sicherheitsvorfälle und Bedrohungen bekannt, deren Ursachen in einer unzureichenden Informationssicherheit liegen. Nutzerdaten von Millionen von Nutzern wurden ausgespäht und missbräuchlich genutzt. Als Beispiel seien die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang 2014 publizierten Fälle des Identitätsdiebstahls von 16 bzw. 18 Millionen E-Mail-Adressen und Passwörtern genannt (vgl. [BS14], S. 29). Die wirtschaftlichen Folgen dieser Sicherheitsvorfälle sind ebenfalls gravierend, in Deutschland liegt der Schadensumfang durch Verbrechen unter Ausnutzung von Informations- und Kommunikationstechnik in der Größenordnung von

[1] Hochschule Zittau/Görlitz, Fakultät Elektrotechnik/Informatik, Theodor-Körner-Allee 16, 02763 Zittau, m.spangenberg@hszg.de

1,6 % des Bruttoinlandprodukts ([CS14]). Mit dem Stuxnet-Virus wurde die Verletzlichkeit von industriellen Steuerungssystemen verdeutlicht. Zunehmend sind diese Systeme ähnlichen Bedrohungen wie die traditionelle IT-Landschaft ausgesetzt (vgl. [BS13], S. 32-36). Die Nutzung der sozialen Netzwerke sowie aller Anwendungen, die auf der Nutzung des Internets basieren, bergen Gefahren für die Nutzer. Inwieweit ist beispielsweise Tracking im Netz mit unseren Persönlichkeitsrechten vereinbar? Damit werden neben technischen Fragen der Informationssicherheit zunehmend rechtliche, organisatorische, wirtschaftliche, finanzielle, aber auch ethische Fragen aufgeworfen, die in der modernen Hochschulausbildung adressiert werden sollten (vgl. [AC13], S. 35).

2 Herausforderungen der Informatikausbildung

Das Spannungsfeld der Beurteilung der Informatik bewegt sich zwischen der Einordnung als Hilfswissenschaft mit den daraus resultierenden „Bindestrich-Informatikern“ oder als Universalwissenschaft. Unbestritten ist in jedem Fall die Durchdringung aller Gebiete unseres Lebens durch Techniken und Methoden der Informatik mit vielen Anwendungsmöglichkeiten.

Als Schlagworte seien Big Data, Industrie 4.0, Cloud, Bring Your Own Device (BYOD) und das Internet der Dinge genannt. Die ungeheure Dynamik der Entwicklung der Informatik führt zu einem rasch verfallenden aktuellen Wissen in der Informatik. Das ist besonders für die Informatikausbildung relevant, da diese nicht von ein paar Schlagworten geprägt sein sollte, sondern Grundlagenwissen und Kompetenzen sollten derart vermittelt werden, dass die Studierenden für ihr zukünftiges Berufsleben dazu befähigt werden, sich neues Wissen eigenständig anzueignen und adäquat anzuwenden.

Bei den zu vermittelnden Inhalten ist es mittlerweile selbstverständlich, dass Informationssicherheit bzw. IT-Sicherheit in unterschiedlichen Facetten zum Fächerkanon der Informatikausbildung gehört (vgl. [AC13], S. 37). Neben konkreten Empfehlungen zur inhaltlichen Ausgestaltung der Ausbildung im Bereich der Informatik und IT-Sicherheit orientiert die Gesellschaft für Informatik (GI) für die Bachelor- und Masterausbildung im Fach Informatik zunehmend auf geforderte Kompetenzen (vgl. [GI05], S. 8ff.; [GI06], S. 4ff.). Der Fokus liegt nicht mehr auf Inhalten, sondern auf den Kompetenzen, die von einem Absolventen eines Informatikstudienganges erwartet werden.

Die genannte Problematik der großen Dynamik wird in den Bereichen IT-Sicherheit sowie IT-Sicherheitsmanagement besonders sichtbar. Täglich gibt es neue Angriffe auf Informationssysteme und IT-Infrastrukturen. IT-Sicherheit wird von der technologischen Entwicklung aber auch von der Kreativität und kriminellen Energie der Angreifer getrieben. Es kann in der Ausbildung nicht darum gehen, heute aktuelle Angriffsmethoden und Gegenmaßnahmen zu vermitteln, sondern es geht um prinzipielle Herangehensweisen und Methoden, die an aktuellen Fallbeispielen erworben und trainiert werden. Als Fallbeispiel soll ein Projekt im Modul „IT-Sicherheitsmanagement“ im Masterstudiengang Informatik der Hochschule Zittau/Görlitz dienen.

3 Modul IT-Sicherheitsmanagement

Das Modul wird im 1.Semester des Masterstudienganges Informatik angeboten und umfasst 4 Semesterwochenstunden (SWS) mit 2 SWS Vorlesung und 2 SWS Übung bzw. Seminar. Als Lehr- und Lernformen sind Vorlesung mit Präsentationen und Demonstration praktischer Beispiele, die selbstständige Erarbeitung von Stoffkomplexen, praktische Arbeit mit Risikomanagement- bzw. Sicherheitstools, Fallstudien, die eigenständige und Teamarbeit während der Projektbearbeitung, die Gestaltung von Workshops und eine exemplarische Vertiefung bestimmter Themen mittels Lösung einer komplexen Projektaufgabe mit möglichst starkem Praxisbezug vorgesehen. Neben Fachkompetenzen wie beispielsweise zu Methoden des Risikomanagement, der Methodik des IT-Grundschutzes des BSI, juristischen und wirtschaftlichen Grundkompetenzen, der Kenntnis und Anwendung von fachspezifischen Standards sollen die folgenden fachunabhängigen Kompetenzen erreicht werden ([Mo16]):

- Problemlösefähigkeit
- Planungs- und Entscheidungstechniken, Umsetzungskompetenz
- Kommunikationsfähigkeit
- Teamfähigkeit, Eigeninitiative
- Kreativität
- Leistungsbereitschaft
- Übernahme von Verantwortung

Wie bereits ausgeführt geht es um die Vorbereitung auf das berufliche Tätigkeitsfeld in der Zukunft. Hier ergibt sich die Frage, inwieweit mit traditionellen inhaltsbezogenen und lehrendenzentrierten Lehrformen die geforderten Ziele und Kompetenzentwicklung erreicht werden können oder ob aktive Lehr- und Lernformen besser geeignet sind. Gerade die Vermittlung nicht fachspezifischer Kompetenzziele, aber auch fachspezifischer Kompetenzen im Bereich des IT-Sicherheitsmanagements lassen eine weniger inhaltsorientierte und mehr projektorientierte Lehre sinnvoll erscheinen (vgl. [AC13], S. 24). Das schließt die Vermittlung von Grundlagen und aktuellen Inhalten ein, diese werden sozusagen als Mittel zum Zweck benutzt. Darauf aufbauend sollen Methoden und eigene Erfahrungen für die Zukunft entwickelt werden. Eine didaktische Zielstellung der Hochschulausbildung besteht in der Vermittlung eines möglichst anschaulichen und nachvollziehbaren Blicks auf das spätere Berufsfeld (vgl. [Wj05], S. 15). Die European Union Agency for Network and Information Security (ENISA) empfiehlt in [EN14] speziell für die Ausbildung auf dem Gebiet der Netzwerk- und Informationssicherheit konkrete Praxisbezüge und Kooperationen mit der Wirtschaft und Behörden.

4 Aktives Lernen

Der Begriff des „aktiven Lernens“ ist nicht präzise definiert. Die folgenden Merkmale werden aus pragmatischer Sicht als charakteristisch für das aktive Lernen angesehen:

- Die Studierenden sind über das reine Zuhören hinaus beteiligt.
- Die Entwicklung studentischer Fähigkeiten und Fertigkeiten ist wichtiger als die Informationsweitergabe.
- Die Studierenden werden zu höheren kognitiven Leistungen angeregt (Analyse, Synthese, Evaluation).
- Die Studierenden werden aktiviert (lesen, schreiben, diskutieren, beschreiben, …).
- Es wird größerer Wert darauf gelegt, dass die Studierenden ihre eigenen Konzepte, Einstellungen und Werte erkunden, so dass anstelle von Dozentenzentrierung eine Studierendenzentrierung erfolgt.

Nach [Rm12, S. 18 ff.] werden unterschiedliche Konzepte des aktiven Lernens wie beispielsweise handlungsorientiertes, problemorientiertes oder projektorientiertes Lernen unterschieden.

Bei dem untersuchten Fallbeispiel kommen traditionelle Lehre in Form von Vorlesung und Übung und projektorientiertes Lernen zum Einsatz. Die zu lösende Aufgabe stammt unmittelbar aus dem Berufsfeld, es erfolgt eine eigenständige Arbeit durch die Projektgruppe und es wird Wissen aus verschiedenen Bereichen verknüpft. Elemente des problemorientierten Lernens sind ebenfalls vertreten, indem unter Begleitung durch den Dozenten eine eigenständige Wissensaneignung während des Lernprozesses erfolgt. Der Wissenserwerb wird somit nach Mandl und Krause (vgl. [MK01], S. 4ff.) als aktiver, konstruktiver, situativer und sozialer Prozess realisiert.

5 Projekt IT-Security Awareness-Kampagne

Im Rahmen des zu untersuchenden Projektes „Entwicklung von IT-Sicherheitsbewusstsein an der Hochschule Zittau/Görlitz“ im Modul „IT-Sicherheitsmanagement“ sollte von den Studierenden eine Security Awareness Kampagne für die Hochschule organisiert werden. Die Awareness Kampagne war Bestandteil der Entwicklung eines Informationssicherheitsmanagementsystems (ISMS) basierend auf ISO 27001 und IT-Grundschutz (BSI) an der Hochschule. Die Ziele der Awareness Kampagne bestanden in der Sensibilisierung der Hochschulangehörigen in IT-Sicherheitsfragen und der Schaffung einer Basis für Schulungsprojekte.

Das hier dargestellte Projekt sollte sowohl matrikelübergreifend gestaltet werden als auch eine große praktische Relevanz zur Verstärkung der Elemente der aktiven Lehre aufweisen. Das Lernen sollte in einer komplexen und realitätsnahen Situation erfolgen.

In Abbildung 1 ist die Einbettung des Projektes in den Ablauf des gesamten Semesters dargestellt. Es ist ersichtlich, dass zu Beginn des Semesters traditionelle Lehrformen zur grundlegenden Wissensvermittlung und zum Kennenlernen entsprechender Methoden gewählt wurden.

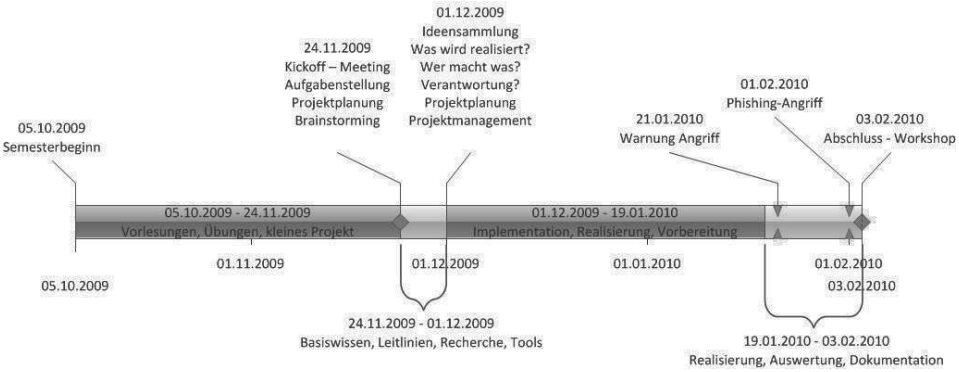

Abb. 1: Ablauf Projekt – Einordnung in das Semester

Gerade bei der Einführung von ISMS in Unternehmen klaffen Anspruch und Realität oft weit auseinander. Die Durchsetzbarkeit ist schwierig, sei es weil Ressourcen fehlen oder die Akzeptanz nicht vorhanden ist oder die Kommunikation ganz einfach schlecht oder unzureichend ist und es an IT-Sicherheitsbewusstsein mangelt. Diese Situation bereits während des Studiums kennenzulernen und Lösungsmöglichkeiten für die Praxis zu entwickeln, ist für Studierende eine große Chance, wesentliche Kompetenzen für die berufliche Arbeit zu entwickeln.

Die detaillierten Projektziele waren wie folgt formuliert:

- Lösung einer konkreten Aufgabenstellung aus dem Fachgebiet/zukünftigem Berufsfeld für ein Unternehmen (Hochschule)
- Kenntnisse aus dem Fachgebiet anwenden und weiterentwickeln
- eigenständige Bearbeitung durch Projektgruppe
- Verknüpfung von Wissen aus verschiedenen Bereichen
- Entwicklung von Eigeninitiative und Kreativität
- Auswahl geeigneter Werkzeuge, Methoden und Hilfsmittel
- Einsatz geeigneter Medien
- Projektmanagement
- Kommunikation und Teamfähigkeit

Diese Ziele stehen für projektorientiertes bzw. projektbasiertes Lernen.

Die Ideensammlung beim Kickoff-Meeting reichte vom einheitlichen Logo über die Gestaltung eines Webauftrittes, Workshops zu Sicherheitsthemen, einem Quiz, einem Video bis zu einem fingierten Phishingangriff. Aufgrund des großen Engagements der Studierenden konnten alle Ideen realisiert werden. Die Arbeit erfolgte in Gruppen mit jeweils 2 bis 4 Studierenden je nach Teilaufgabenstellung. Da alle Aktivtäten und Komponenten der Kampagne miteinander verzahnt sein sollten, waren regelmäßige Abstimmungen im gesamten Team notwendig. Dazu fand pro Woche ein Treffen des gesamten Teams zur Darstellung des Arbeitsstandes, zur Klärung und Abstimmung offener Fragen statt. Neben den Treffen wurde über ein Wiki und per E-Mail kommuniziert.

Die Kampagne umfasste die folgenden Elemente: Logo, Plakate, Flyer, Workshops mit Mitarbeitern und Studierenden inkl. Evaluation, „Beobachtungen“ zum Sicherheitsbewusstsein, Quiz, Phishingangriff, Video, Webseite, hochschulweiter Workshop. In Abbildung 2 ist ein Plakat als beispielhaftes Ergebnis dargestellt.

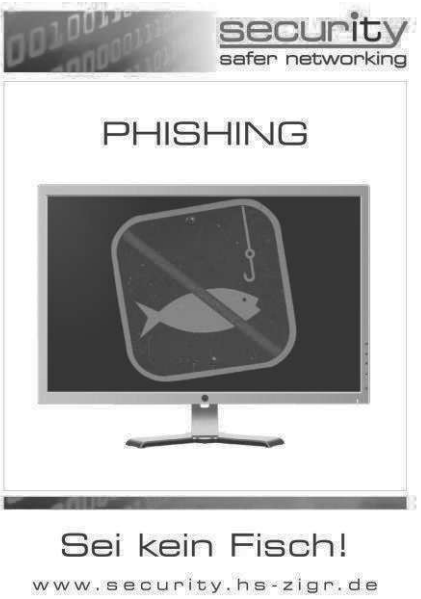

Abb.2: Beispiel eines Plakates der Kampagne

6 Elemente der Kampagne unter dem Aspekt aktiven Lernens

Alle Elemente der Kampagne waren Ergebnis des Brainstormings und stellten damit eigene Ideen der Studierenden dar. Die Bearbeitung erfolgte nach Interessenlage und persönlichen Erfahrungen, die teilweise auch aus anderen Fachgebieten stammten. Wissen wurde aktiv, selbstgesteuert und konstruktiv erworben und angewendet. Dabei

konnte auf die Inhalte der Lehrveranstaltung zurückgegriffen werden, aber auch eigene Recherchen waren erforderlich.

Bei Workshops zur Passwortsicherheit mit Mitarbeitern und Studierenden unterschiedlicher Fakultäten waren insbesondere die Kommunikation mit Nichtinformatikern und eine Ausrichtung der Inhalte auf das jeweilige Auditorium gefragt. Es wurde eine Evaluation der Ergebnisse durch Befragung der Teilnehmer durchgeführt. Mit der eingesetzten Methodik der Befragung und Auswertung erfolgte die Zusammenführung fächerübergreifender Erfahrungen. Beim Logo, den Plakaten und den Flyern mussten einerseits inhaltliche Fragen und andererseits ein ansprechendes Design beachtet werden. Der hochschulweite Phishingangriff erforderte Kenntnisse der Programmierung, zum Netzwerk, zu Anwendungen, zur IT-Sicherheit, zum Datenschutz und war eine Herausforderung in der Organisation. Auch beim Video spielten adäquate Inhalte der IT-Sicherheit, aber auch eine spannende Story eine Rolle. Es mussten Schauspieler akquiriert werden und die Videoproduktion einschließlich der technischen Voraussetzungen war zu organisieren. Die Vorbereitung des abschließenden hochschulweiten Workshops erforderte eine perfekte Organisation über Einladung, Anmeldung, Raumorganisation und Öffentlichkeitsarbeit und die ansprechende Präsentation der Ergebnisse. Damit wird deutlich, dass jedes Element der Kampagne unmittelbar aktives Lernen war und sowohl die geforderten Fachkompetenzen als auch die fachunabhängigen Kompetenzen in ihrer Entwicklung gefördert hat.

Die Rolle der Lehrenden hat trotz der unmittelbaren Studierendenzentrierung nicht an Bedeutung verloren. Ganz wichtig war die Beratung in Fachfragen und zur Organisation. Es bestand die Notwendigkeit, Abstimmungen mit den Verantwortlichen der Hochschule (Hochschulleitung, IT-Sicherheitsmanagementteam, Hochschulrechenzentrum, Dezernaten, Fakultäten) vorzunehmen. Gegenüber dem Auftraggeber war die Gesamtverantwortung für das Projekt zu übernehmen und als Ansprechpartner für alle Beteiligten zu fungieren.

7 Erfahrungen

Die Laufzeit des Projektes umfasste ca. zwei Monate, 19 Studierende waren beteiligt. Innerhalb dieses Zeitraums wurden ca. 20 Zeitstunden des Unterrichts für das Projekt aufgewendet. Der zusätzliche Aufwand pro Studierendem belief sich laut Befragung der Studierenden zwischen 30 und 200 Stunden. Das Video beanspruchte dabei die meiste Zeit. Allein die Bearbeitungszeit steht für ein weit überdurchschnittliches Engagement der Studierenden. Es ist gelungen, die Studierenden zu motivieren und zu aktivieren. Das Projekt soll nun aus unterschiedlichen Sichten eingeschätzt werden.

Sicht der Studierenden

Die studentische Arbeit kann mit den Stichwörtern: Begeisterung, Initiative, Motivation, Selbstverwirklichung, Organisation, Kooperation, Kommunikation auch mit Nichtinfor-

matikern, Kreativität, Übernahme von Verantwortung, Verlässlichkeit beschrieben werden. Das Projekt verursachte zumindest partiell einen sehr hohen Workload, der aber von den Studierenden nicht beklagt wurde. Allerdings wurden während der Bearbeitungszeit teilweise Abstriche bei anderen Modulen gemacht. Die praktische Aufgabenstellung und das unmittelbare Feedback wie beispielsweise die Reaktionen auf den Phishingangriff beflügelten die Studierenden. Unterschiede zwischen Theorie und Praxis mussten ebenfalls realisiert werden.

Sicht der Lehrenden

Die Projektbegleitung stellte aufgrund der Einbindung des Projektes in den Hochschulalltag eine neue Herausforderung dar. Es handelte sich nicht um ein fiktives Fallbeispiel, bei dem das Ergebnis für die Lehrende zu Projektbeginn feststeht, sondern um die Integration des Projektes in die Praxis mit allen Problemen der Organisation und der Abstimmung mit Verantwortlichen der Hochschule.

Sehr beeindruckend war das Erleben des herausragenden studentischen Engagements, das teilweise beim Generieren immer neuer Ideen gedrosselt werden musste. Das unmittelbare Feedback der Studierenden hinsichtlich der praktischen Relevanz der Inhalte, die in der Lehrveranstaltung vermittelt wurden, ist positiv hervorzuheben. Insgesamt war der Zeitaufwand für die Betreuung des Projektes sehr groß, da neben der Betreuung der Studierenden in einem neuen Projektumfeld die Kampagne an der Hochschule als Ansprechpartner begleitet werden musste.

Die erreichten Ergebnisse und Befragungen der Studierenden zeigen, dass diese Form der Projektarbeit und des aktiven Lernens sehr gut geeignet ist, die geforderten fachspezifischen und fachunabhängigen Kompetenzen zu erreichen. Der Wissenserwerb erfolgt sehr intensiv und nachhaltig.

Sicht des „Auftraggebers“ Hochschule

Sowohl hinsichtlich der unmittelbaren Wirkung als auch der Nachhaltigkeit hat die Security Awareness Kampagne alle Ziele erreicht. Mitarbeiter und Studierende wurden für IT-Sicherheitsprobleme sensibilisiert und motiviert, sich mit der Problematik auseinanderzusetzen. Gerade die Erfahrung mit dem Phishingangriff hat zu kritischen Reflexionen der eigenen Handlungsweise angeregt. Die Studierenden erstellten viele unmittelbar nachnutzbare Materialien, die als Basis für weitere Entwicklungen im Bereich Security Awareness genutzt werden konnten.

8 Fazit

Die Studierenden des Projektteams konnten beim Projektstart auf dem Gebiet der IT-Sicherheit auf eine fundierte Ausbildung im Rahmen ihres Bachelor- und Masterstudiums aufbauen. Sie waren aber bis dato keine Spezialisten in Awareness Kampagnen, im Management oder in der Kommunikation von IT-Sicherheitskonzepten. Trotzdem ist es gelungen, eine sehr komplexe Projektaufgabe aus dem Bereich Security Awareness zu

lösen und an der Hochschule mit ca. 4000 Studierenden und 400 Mitarbeitern wirksam werden zu lassen. Sehr positiv ist die Möglichkeit des bewussten Einbringens persönlicher Erfahrungen aus anderen Fachgebieten und die Integration persönlicher Interessen der Studierenden in die Projektarbeit zu bewerten. Darin werden wesentliche Gründe für die starke Motivation, die Effektivität und Effizienz der Projektbearbeitung gesehen. Zusammenfassend ist einzuschätzen, dass diese Form der Lehre und Projektbearbeitung sehr gut geeignet ist, die geforderten Lernziele zu erreichen und Kompetenzen zu entwickeln. Sehr motivierend haben sich die unmittelbare Anwendung der Projektergebnisse in der Praxis und das Feedback für die Studierenden ausgewirkt. Für zukünftige Projekte wird die Verknüpfung des traditionellen Wissenserwerbs mit realen praktischen Erfahrungen als wesentlich angesehen, wobei als praktisches Zielobjekt auch eine Hochschule geeignet ist.

Derartige Projektarbeit macht sowohl Studierenden als auch Lehrenden Spaß. Der Nachteil ist der immense zeitliche Aufwand. Wenn alle Module des Curriculums in dem Maße aktive Lehre einsetzen würden, würde das weit über das verfügbare zeitliche Volumen der Studierenden hinausgehen. Die Argumentation, dass der Lehrende für einen angepassten Umfang die Verantwortung trägt, ist nur bedingt zielführend, da ein solches Projekt gerade von der Aktivität und Initiative der Bearbeiter lebt, so dass eine strikte Begrenzung kontraproduktiv wäre.

Für Lehrende an Fachhochschulen mit 18 SWS ++ wäre eine komplette Umstellung auf aktive Lehr- und Lernformen in dieser Intensität in allen Modulen unter Beibehaltung der gegenwärtigen Studien- und Prüfungsordnungen nicht machbar. Die Durchführung von fächerübergreifenden Projekten stellt einen möglichen Lösungsansatz dar. Im Fallbeispiel konnte gezeigt werden, dass durch einen „dosierten“ Einsatz der aktiven Lehre geforderte Kompetenzen bei den Studierenden besser erreicht werden können als allein durch traditionelle Lehrformen.

Literaturverzeichnis

[AC13] ACM Computer Science Curricula 2013, December 2013, https://www.acm.org/education/CS2013-final-report.pdf, 20.3.2016

[BS14] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/-Publikationen/Lageberichte/Lagebericht2014.pdf, 20.3.2016

[BS13] Bundesamt für Sicherheit in der Informationstechnik (BSI): ICS Security Kompendium 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2, 20.3.2016

[CS14] Center for Strategic and International Studies: Net Losses: Estimating the Global Cost of Cybercrime, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, 20.3.2016

[GI05] GI, Gesellschaft für Informatik e.V.: Empfehlungen für Bachelor- und Masterpro-

gramme im Studienfach Informatik an Hochschulen, http://www.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung_BaMa2005.pdf, 20.3.2016

[GI06] GI, Gesellschaft für Informatik e.V.: IT-Sicherheit in der Ausbildung, 2006 verabschiedet, https://www.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung-IT-Sicherheit-in-der-Ausbildung-2006.pdf, 20.3.2016

[EN14] ENISA: Public Private Partnerships in Network and Information Security Education, Case Studies, October 2014, https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education, 20.3.2016

[MK01] Mandl, Heinz; Krause, Ulrike-Marie: Lernkompetenz für die Wissensgesellschaft, Forschungsbericht 145, LMU, 2001, https://epub.ub.uni-muenchen.de/253/1/FB_145.pdf, 20.3.2016

[Mo16] Modulkatalog der Hochschule Zittau/Görlitz, IT-Sicherheitsmanagement, https://web.hszg.de/Modulkatalog/, 20.3.2016

[Rm12] Rummler, Monika: Innovative Lehrformen: Projektarbeit in der Hochschule, Beltz Verlag, Weinheim und Basel, 2012

[Wj05] Wildt, Johannes: From Teaching to Learning, Tagung EWTF, Berlin, 17.11.2005