Lehrveranstaltungsbeschreibung

1. Angaben zum Programm

1.1 Hochschuleinrichtung	Babes-Bolyai Universität, Cluj-Napoca
1.2 Fakultät	Mathematik und Informatik
1.3 Department	Informatik
1.4 Fachgebiet	Informatik
1.5 Studienform	Master
1.6 Studiengang / Qualifikation	Fortgeschrittene Informationssysteme: Modellierung, Entwurf, Entwicklung

2. Angaben zum Studienfach

2.1 LVBezeichnung (de) (en) (ro)	Sicherheit der Informationssysteme						
2.2 Lehrverantwortlicher – Vorlesung							
2.3 Lehrverantwortlicher – Seminar							
2.4 Studienjahr	2	2.5 Semester	3	2.6. Prüfungsform	Prüfung	2.7 Art der LV	Verpflichtend
2.8 Modulnummer		MMG8157					

3. Geschätzter Workload in Stunden

3.1 SWS	3	von denen: 3.2 Vorlesung	2	3.3 Seminar/Übung	1 Sem		
3.4 Gesamte Stundenanzahl im Lehrplan	42	von denen: 3.5 Vorlesung	28	3.6 Seminar/Übung	14		

Verteilung der Studienzeit:	Std.
Studium nach Handbücher, Kursbuch, Bibliographie und Mitschriften	35
Zusätzliche Vorbereitung in der Bibliothek, auf elektronischen Fachplattformen und durch Feldforschung	45
Vorbereitung von Seminaren/Übungen, Präsentationen, Referate, Portfolios und Essays	47
Tutorien	15
Prüfungen	16
Andere Tätigkeiten:	-
3.7 Gesamtstundenanzahl Selbststudium	158
3.8 Gesamtstundenanzahl / Semester	200
3.9 Leistungspunkte	8

4. Voraussetzungen (falls zutreffend)

4.1 curricular	• Rechnernetze, Softwareentwicklung, Kryptographie
4.2 kompetenzbezogen	•

5. Bedingungen (falls zutreffend)

5.1 zur Durchführung der Vorlesung	•
5.2 zur Durchführung des Seminars / der Übung	•

6. Spezifische erworbene Kompetenzen

Berufliche Kompetenzen	C1.1 Kenntnis der theoretischen und praktischen Begriffe, Konzepte und Prinzipien im Zusammenhang mit dem allgemeinen Bereich der Informationssicherheit. Identifizierung und Verstehen der Sicherheitsprobleme, die im Zusammenhang mit bestimmten Sprachen auftreten können. C1.2Evaluierung bestehender Softwareprojekte und Identifizierung von Sicherheitsmängeln in Bezug auf Architektur, Programmiermodus oder Testverfahren. Möglichkeit, eine Codeüberprüfung durchzuführen, um Fehler zu beseitigen, die sich auf die Sicherheitsstufe von Softwareanwendungen auswirken. C1.4 Entwicklung von Softwaremodulen oder Dienstprogrammen zur Gewährleistung eines hohen Sicherheitsniveaus. Vorschlag von Szenarien und Möglichkeiten, bestehende Projekte zu testen, um deren Qualität aus Sicht der Sicherheit zu gewährleisten. C2.1 Kenntnis der grundlegenden Prinzipien und Konzepte, die zum Entwerfen, Entwickeln und Verwalten einer sicheren Codierung erforderlich sind. Kenntnis der üblichen Software und Sicherheitswerkzeuge. Kenntnisse von Betriebssystemarchitekturen und Plattformen, die zur Entwicklung von Sicherheitslösungen benötigt werden. C2.4Identifizierung und Verwendung geeigneter Kriterien und Methoden zur Bewertung von Sicherheitsanwendungen auf verschiedenen Abstraktionsebenen. Fähigkeit, die Qualität von IT-Anwendungen aus Sicherheitsgründen zu bewerten und zu dokumentieren. C6.1 Die Architekturen von Computersystemen und ihre Kommunikationsmuster durch Netzwerke verstehen. Fähigkeit, robuste Kommunikationskanäle unter dem Gesichtspunkt der Sicherheit der übertragenen Informationen zu entwerfen.
Transversale Kompetenzen	CT1. Anwendung und Förderung von defensiven, sicheren und effizienten Design- und Programmierkenntnissen. Verbesserung der beruflichen Fähigkeiten durch Nutzung der neu erworbenen Perspektiven, der Sicherheit von Softwaresystemen.

7. Ziele (entsprechend der erworbenen Kompetenzen)

7.1 Allgemeine Ziele der Lehrveranstaltung	Die Studenten lernen, wie man die Systemsicherheit verwaltet, indem sie die grundlegenden Elemente der Sicherheit von Informationssystemen und verwandten Prozessen lernen
7.2 Spezifische Ziele der Lehrveranstaltung	Die Studierenden erlernen Kenntnisse aus den folgenden Bereichen: • Zugangskontrolle • Netzwerk- und Kommunikationssicherheit • Information Securitz Governance und Risikomanagement
	• Sicherheit der Softwareentwicklung • Kryptographie • Sicherheitsarchitekturen • Betriebssicherheit • Notfallwiederherstellungsplanung • Gesetzliche Regelung

8. Lehrinhalte

8.1 Vorlesung	Lehrmethoden	Bemerkung
1. Zugriffsrichtlinien: Kontrollarten, Identifizierungs- und Authentifizierungsverfahren, Autorisierungsmechanismen	Darstellung, Erklärung, Beispiele, Besprechung	
2. Sicherheit von Computernetzen und Kommunikationsnetzen: Sicherheitsarchitekturen, Sicherung von Komponenten, Sicherung von Kommunikationskanälen	Darstellung, Erklärung, Beispiele, Besprechung	
3 & 4. Information Security Governance und Risikomanagement: organisatorische Abläufe, Sicherheitskonzepte in Organisationen, Integritäts- und Vertraulichkeitskonzepte, Implementierung von Sicherheitsrichtlinien, Life-Cycle-Management, Verständnis und Anwendung von Risikomanagementkonzepten, Personalsicherheitsmanagement	Darstellung, Erklärung, Beispiele, Besprechung	
5 & 6. Sicherheit der Softwareentwicklung: Sicherheitskonzepte im Lebenszyklus eines Softwareprodukts verstehen und integrieren, Steuerungsvariablen verstehen, die Effektivität von Sicherungsmechanismen analysieren	Darstellung, Erklärung, Beispiele, Besprechung	

7 & 8 und 9. Cryptography. Anwendungs- und Nutzungsszenarien, Verständnis des kryptographischen Lebenszyklus (Grenzen, kryptographische Governance), Verständnis der grundlegenden Konzepte der Kryptographie, Verständnis des Schlüsselverwaltungsprozesses, digitale Signaturen, Authentifizierungsverfahren.	Darstellung, Erklärung, Beispiele, Besprechung	
10. Sicherheitsarchitekturen. Schwachstellen und Bedrohungen verstehen, Abwehrmaßnahmen	Darstellung, Erklärung, Beispiele, Besprechung	
11. Sicherheit von Operationen. Disaster Recovery Planung.	Darstellung, Erklärung, Beispiele, Besprechung	
12 & 13 & 14. Rechtsrahmen. Fallstudien. Schlussfolgerungen.	Darstellung, Erklärung, Beispiele, Besprechung	
Literatur M. Down, J. McDonald, J. Schuh, „The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities", AddisonWesley, 2007 M. Howard, D. LeBlanc, J. Viega, „24 Deadly Sins of Software Security. Programming Flows and How to Fix Them", McGraw Hill, 2010		
M. Howard, D. LeBlanc, „Writing Secure Code for Windows Vista", Microsoft Press, 2007 G. McGraw, „Software Security:Building Security In", AddisonWesley, 2006 R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems", AddisonWesley, 2 nd edition, 2014 „Common Weaknesses Enumeration (WCE)", online: http://cwe.mitre.org/data/index.html		
8.2 Übung / Labor	Lehrmethoden	Bemerkung
1. Zugriffsrichtlinien: Angriffe verstehen und ihnen entgegenwirken	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	2 Stunden Übung jede 2. Woche
2. Netzwerksicherheit: Angriffe	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	
3. Sicherheitsfunktionen verwalten	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	Präsentation Eigenarbeit
4. Analyse der Wirksamkeit von Sicherheitsmaßnahmen	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	Präsentation Eigenarbeit
5. Kryptographische Angriffe	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	Präsentation Eigenarbeit
6. Sicherheitslücken von Sicherheitsarchitekturen	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	Präsentation Eigenarbeit

7. Analysen und Fallstudien.	Darstellung, Erklärung, Beispiele, Besprechung, Dialog	Präsentation Eigenarbeit

Literatur:

M. Down, J. McDonald, J. Schuh, „The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities", AddisonWesley, 2007

M. Howard, D. LeBlanc, J. Viega, „24 Deadly Sins of Software Security. Programming Flows and How to Fix Them", McGraw Hill, 2010

M. Howard, D. LeBlanc, „Writing Secure Code for Windows Vista", Microsoft Press, 2007

G. McGraw, „Software Security:Building Security In", AddisonWesley, 2006

R. Seacord, „CERT C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems", AddisonWesley, 2 nd edition, 2014

„Common Weaknesses Enumeration (WCE)", online: http://cwe.mitre.org/data/index.html

9. Verbindung der Inhalte mit den Erwartungen der Wissensgemeinschaft, der Berufsverbände und der für den Fachbereich repräsentativen Arbeitgeber

Diese Lehrveranstaltung ist eingebunden in den Lehrplänen ähnlicher Studienrichtungen.

10. Prüfungsform

Veranstaltungsart	10.1 Evaluationskriterien	10.2 Evaluationsmethoden	10.3 Anteil an der Gesamtnote
10.4 Vorlesung	Die Fertigkeit, erworbene Kenntnisse in realistischen Szenarien anzuwenden	Schriftliche Prüfung	75%
10.5 Seminar / Übung	Die Qualität der mündlichen Präsentation	Mündliche Prüfung	25%
10.6 Minimale Leistungsstandards			
Die Gesamtnote muss mindestens 5 (auf einer Skala von 1 bis 10) betragen			

Ausgefüllt am: Vorlesungsverantwortlicher Seminarverantwortlicher

Genehmigt im Department am: Departmentdirektor

Prof. Dr. Andreica Anca