MODULARES INNOVATIVES
NETZWERK FÜR DURCHLÄSSIGKEIT

ZERTIFIKATSKURSBESCHREIBUNG

1. VERSION UND GÜLTIGKEIT

Zertifikatskursbeschreibung gültig ab: 09. Februar 2017
Erstellt von: Zentrum für Weiterbildung und Wissensmanagement (OTH mind)
Verantwortlich: Zentrum für Weiterbildung und Wissensmanagement (OTH mind)
Wissenschaftliche Leitung: Prof. Dr. Clarissa Rudolph, Wissenschaftliche Leiterin „OTH mind“
Prof. Dr. Christoph Skornia, Fakultät Informatik und Mathematik

2. ANGABEN ZUR QUALIFKATION

Bezeichnung der Qualifikation

Datensicherheit

Name der Einrichtung, die die Qualifikation verliehen hat

Ostbayerische Technische Hochschule Regensburg,
93025 Regensburg; Bundesrepublik Deutschland

Name der Einrichtung, die die Weiterbildung durchgeführt hat

Zentrum für Weiterbildung und Wissensmanagement (ZWW) der Ostbayerischen Technischen Hochschule Regensburg (Organisation und Zertifizierung)

3. ANGABEN ZU STRUKTUR UND UMFANG DER AUSBILDUNG

Umfang

Insgesamt ca. 250 Unterrichtseinheiten Aufwand, davon mindestens 70 Unterrichtseinheiten Kontakt-/Präsenzzeit.

Mit dem Zertifikat werden 10 Credits, Leistungspunkte nach dem European Credit Transfer and Accumulation System (ECTS) vergeben.

Struktur

Die modularisierte Ausbildung (insgesamt acht Teilmodule) strukturiert sich wie folgt:
1. Authentifizierung
2. Identity Management
3. Datenschutz
4. Signaturverfahren
5. Sichere Softwareentwicklung
6. Ausgewählte Themen der Systemsicherheit
7. Verschlüsselung
8. Grundlagen des Penetration Testing

Prüfungsleistung: schriftliche Prüfung 150 Minuten

Inhalte der Teilmodule

Vorbemerkung

- Sämtliche Teilmodule enthalten Inhalte zu folgenden Themen:
  (1) Schutzziele der IT-Sicherheit
  (2) Sicherheitsmanagement
  (3) Risiko- und Sicherheitsbewusstsein
  (4) Analysen von konkrete Anwendungsszenarien der Informationssicherheit

Teilmodul I: Authentifizierung

Inhalte

- 1-Faktor, 2-Faktor Authentifizierungsverfahren
- Biometrische Authentifizierung
- Starke Authentifizierung mit kryptographischen Verfahren, Zero-Knowledge Protokolle
- Code Signing
- Sichere E-Mail: S/MIME, DE-Mail
- Chipkarten, RFID-Systeme

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden haben fundierte Kenntnisse zum Thema Authentifizierung erworben und beherrschen die Methoden und Werkzeuge, um moderne Authentifizierungsverfahren in verschiedenen Sicherheitsniveaus einzubinden.
- Sie können das Potential sowie die Vor- und Nachteile verschiedener Authentifizierungsverfahren im Kontext einer Anwendung evaluieren.
- Die Studierenden haben Kenntnisse der Funktionsweise und der Sicherheitsleistung fortgeschrittener Authentifizierungswerkzeuge, wie Chipkarten und RFID-Systeme erworben.

Literatur

- C. Eckert, IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg, 9. Auflage, 2014
- J. Buchmann: Einführung in die Kryptographie, Springer Spektrum, 2016

Teilmodul II: Identity Management

Inhalte

- Identity Provider, ServiceProvider, Single-Sign-On, gängige Protokolle, Policies
- Machine-to-machine Kommunikation und ID-Management, Webservices, DNSSec
- Public Key Infrastrukturen, Artefakte, Protokolle und zugehörige Dienste, LDAP, OCSP
- X.509-Zertifikate, Lifecycle
- eID-Funktion des Personalausweises

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden haben fundierte Kenntnisse zum Thema Identity Management erworben.
- Sie beherrschen die Methoden und Werkzeuge, um ID-Management Technologien in Anwendungen einzubinden.
- Die Studierenden verstehen die Grundlagen, Protokolle und Dienste von Public-Key Infrastrukturen, die Funktionsweise verschiedener ID-Management-Systeme und können sie in verschiedenen Szenarien einsetzen.

Literatur

- C. Eckert, IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg, 9. Auflage, 2014

Teilmodul III: Datenschutz

Inhalte

- Für die Informatik relevante, rechtliche Grundlagen des Datenschutzes
- Bedrohungen des Datenschutzes
- Privacy by Design, Privacy by Default, Best Practices
- Begriffe, Rechte und Maßnahmen: Datenerhebung, Speicherung, Verarbeitung, Kontrolle, Weitergabe, Löschung, Sperrung, Zweckbindung, Datensparsamkeit
- Verfahrensverzeichnis, Vorab-Kontrolle, Datenschutzbeauftragte/r, Auftragsdatenverarbeitung
- Neue Begriffe und Regelungen der EU-Datenschutzgrundverordnung: Rechenschaftspflicht ("Accountability"), Verzeichnis von Verarbeitungstätigkeiten, Sicherheit der Verarbeitung, Meldepflichten bei Verstößen, Datenschutz-Folgenabschätzung, Autragsverarbeiter, Bußgelder
- Datenschutzmanagement
- Anforderungen und Techniken zur sicheren Pseudonymisierung und Anonymisierung
- Anforderungen für den rechtskonformen und sicheren Einsatz von Cloud Diensten

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden beherrschen die Grundlagen des Datenschutzes in der Informationstechnologie und können datenschutzkonforme IT-Systeme entwerfen, betreiben und evaluieren.
- Die Studierenden haben Kenntnisse zum Datenschutzmanagement und zur rechtskonformen Auslagerung von IT-Diensten erworben und beherrschen die rechtlichen und technischen Anforderungen für den datenschutzkonformen Einsatz von Cloud-Diensten.

Literatur

- G. Borges, J. Schwenk: Daten- und Identitätsschutz in Cloud-Computing, E-Government und E-Commerce, Springer-Verlag Berlin-Heidelberg, 2012
- D. Loomans, M. Matz, M. Wiedemann: Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems. Springer-Vieweg, 2014
- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung). Amtsblatt der Europäische Union, 27.04.2016

Teilmodul IV: Signaturverfahren

Inhalte

- Kryptographische Hashfunktionen: Konstruktion, Eigenschaften, Anwendungen
- Integrität und Authentizität von Netzwerkdaten: Message Authentication Codes, HMAC
- Elektronische Signaturen: kryptographische und technische Grundlagen
- Qualifizierte elektronische Signaturen, Zeitstempel, Siegel
- Anforderungen an die Archivierung elektronisch signierter Dokumente, relevante Vertrauensdienste

Lernziele / Lernergebnisse / Kompetenzen

Die Studierenden verfügen über fundierte Kenntnisse zu den mathematischen, technischen und rechtlichen Grundlagen und Methoden von Signaturverfahren und Vertrauensdiensten und können diese in der Praxis evaluieren und einsetzen.

Literatur

- C. Eckert, IT-Sicherheit: Konzepte - Verfahren - Protokolle, De Gruyter Oldenbourg, 9. Auflage, 2014
- V. Gruhn et al: Elektronische Signaturen in modernen Geschäftsprozessen, Vieweg, 2007
- J. Buchmann: Einführung in die Kryptographie, Springer Spektrum, 2016

Teilmodul V: Sichere Softwareentwicklung

Inhalte

- Sicherheitsbezogene Anforderungsanalyse für die Softwareentwicklung
- Implementierung ausgewählter Sicherheitsfunktionalitäten aus den Bereichen Authentifizierung und Verschlüsselung
- Analyse von Softwareschwachstellen mittels statischer und dynamischer Analyse
- Strategien zur Vermeidung häufiger Sicherheitsprobleme in Software
- Verfahrensmodelle für sicheres Softwaredesign

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden kennen die wichtigsten Sicherheitsprobleme aktueller Software und deren Ursachen sowie Strategien zu deren Vermeidung.
- Sie können ausgewählte Sicherheitsfunktionalitäten implementieren.
- Darüber hinaus sind Sie in der Lage sicherheitsorientiertes Softwaredesign in Entwicklungsprojekten umzusetzen.

Literatur

- Müller, Klaus-Rainer. IT-Sicherheit mit System: Sicherheitspyramide-Sicherheits-, Kontinuitäts-und Risikomanagement-Normen und Practices-SOA und Softwareentwicklung. Springer-Verlag, 2007
- Viega, John, and Matt Messier. Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Input Validation & More. " O'Reilly Media, Inc.", 2003
- Viega, John, and Gary McGraw. "Building Secure Software: How to Avoid Security Problems the Right Way (paperback)." (2011)
- Krutz, Ronald L., and Alexander J. Fry. The CSSLP Prep Guide: Mastering the Certified Secure Software Lifecycle Professional. Wiley Publishing, 2009
- Howard, Michael, and Steve Lipner. The security development lifecycle. Vol. 8. Redmond: Microsoft Press, 2006
- Howard, Michael, and David LeBlanc. Writing secure code. Pearson Education, 2003

Teilmodul VI: Ausgewählte Themen der Systemsicherheit

Inhalte

- Angriffsoberfläche und Angriffsvektoren
- Sicherheitsanalyse von Informationssystemen
- Lokale Gefahrenquellen
- Gefahren aus dem Netzwerk
- Schutzziele und Sicherheitsmodelle
- Technische Maßnahmen der lokalen Systemsicherheit
- Technische Maßnahmen der Netzwerksicherheit

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden verstehen Verfahren zur Sicherheitsanalyse von Informationssystemen und können diese in der Praxis einsetzen.
- Sie sind in der Lage Schwachstellen zu identifizieren, zu bewerten und Maßnahmen zu deren Behebung vorzuschlagen.
- Sie können ihr Vorgehen dabei auf Basis gängiger Sicherheitsmodelle selbstständig planen und umsetzen.

Literatur

- Eckert, Claudia. IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter, 2013
- Hofmann, Jürgen. "IT-Sicherheitsmanagement." Masterkurs IT-Management. Vieweg+ Teubner, 2010. 287-334
- BSI, IT. "Sicherheitsmanagement und IT-Grundschutz-BSI-Standards zur IT-Sicherheit." (2005)

Teilmodul VII: Verschlüsselung

Inhalte

- Historische Verschlüsselungsverfahren
- Aktuelle symmetrische und asymmetrische Verschlüsselungsverfahren
- Block- und Stromchiffren
- Schlüsselaustauschverfahren
- Public-Key Verschlüsselung
- Public-Key Infrastruktur

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden beherrschen die konzeptionellen Grundlagen der Verschlüsselung.
- Sie sind in der Lage ausgewählte Algorithmen korrekt einzusetzen sowie übergeordnete Verschlüsselungsverfahren auf Ihre Eignung für ein konkretes Anwendungsszenario zu beurteilen.

Literatur

- Ertel, Wolfgang. Angewandte Kryptographie. Carl Hanser Verlag GmbH Co KG, 2012
- Eckert, Claudia. IT-Sicherheit: Konzepte-Verfahren-Protokolle. Walter de Gruyter, 2013
- Buchmann, Johannes. Einführung in die Kryptographie. Vol. 3. Springer, 2008

Teilmodul VIII: Grundlagen des Penetration Testing

Inhalte

- Einsatz von Penetration Testing zur Erhöhung der IT-Sicherheit
- Phasenmodell im Penetration Testing
- Kill-Chain-Methodologie
- Schwachstellen
- Einsatz von Werkzeugen im Penetration Testing am Beispiel von Metasploit und Kali Linux

Lernziele / Lernergebnisse / Kompetenzen

- Die Studierenden verstehen den systematischen Aufbau von Penetrationstests und können diesen in der Praxis anwenden.
- Sie wissen, wie verfügbare Werkzeuge dazu zur Erhöhung der Sicherheit eingesetzt werden.

Literatur

- Beggs, Robert W. Mastering Kali Linux for Advanced Penetration Testing. Packt Publishing Ltd, 2014
- Messier, Ric. "Penetration testing basics." (2016)
- Weidman, Georgia. Penetration testing: A hands-on introduction to hacking. No Starch Press, 2014

Übersicht zum Zertifikatskurs „Datensicherheit“

Zuständige Fakultät	Fakultät Informatik und Mathematik
Spezielle Studienziele	Fähigkeit zur Einschätzung von Sicherheitsanforderungen in komplexen Szenarien. Kompetenz zur Auswahl und Implementierung geeigneter Technologien zur Erkennung von Schwachstellen und deren Behebung.
Spezielle Qualifikationsvoraussetzungen	Voraussetzung für die Zulassung ist ein einschlägiger erster Studienabschluss. Als einschlägig gelten Informatik-, Informationstechnologie- und Ingenieursstudiengänge sowie naturwissenschaftliche Studiengänge deutscher Hochschulen. Berufliche Praxis im IT-Bereich wünschenswert.
Spezielle Studienorganisation	Berufsbegleitend, in Blockveranstaltung
Regelstudiendauer	Ein Studiensemester

Übersicht über Kursmodule, Leistungsnachweise und Credits

1	2	3	4	5	6	7	8	9
Modul Nr.	**Kursmodulbezeichnung**	**UE*)**	**Credits*)**	**Art der Lehrver-anstaltung**	**Prüfungen**			**Ergänzende Regelungen**
					Mündlich Schriftlich Dauer in Min.	**Studien-begleitende Leistungsnachweise**	**Fremdsprachige Prüfungen**	
1	**Datensicherheit**	**250**	**10**					
1.1	Authentifizierung	(37,5)	1,5	SU	Schriftliche Prüfung (150 Minuten)			
1.2	Identity Management	(25)	1	SU				
1.3	Datenschutz	(37,5)	1,5	SU				
1.4	Signaturverfahren	(25)	1	SU				
1.5	Sichere Softwareentwicklung	(37,5)	1,5	SU				
1.6	Ausgewählte Themen der Systemsicherheit	(37,5)	1,5	SU				
1.7	Verschlüsselung	(25)	1	SU				
1.8	Grundlagen des Penetration Testing	(25)	1	SU				

*) Angaben in Klammern geben den jeweiligen Anteil eines Teilmoduls am Gesamtmodul an.
Ein Credit entspricht im Durchschnitt einer Arbeitsbelastung für Präsenz und Selbststudium von 25 Unterrichtseinheiten.

Abkürzungen

m.E.	Bewertung mit/ohne Erfolg	StA	Studienarbeit	SU	Seminaristischer Unterricht ggf. mit Übungen
TN	Teilnahmenachweis	UE	Unterrichtseinheit		