SQ MAGAZIN

ASQF®
Das Expertennetzwerk

Ausgabe 54 | März 2020

KI & SOFTWARE TESTING

Sonderdruck für sogeti Part of Capgemini

FORTBILDUNGEN IN IT-SICHERHEIT

WELCHE ZERTIFIZIERUNG PASST ZU MIR?

Im Zuge eines wachsenden Bewusstseins über die Bedeutung von IT-Sicherheit rückt auch die einschlägige Ausbildung der eigenen Mitarbeiter in den Fokus von Unternehmen und öffentlichen Einrichtungen. Neue Studiengänge, Online-Kurse und Seminarangebote schießen wie Pilze aus dem Boden.

Anhand von fünf ausgewählten Personen-Zertifizierungsschemata möchten wir erläutern, welche Themenkomplexe in IT-Sicherheitsausbildungen vermittelt werden. Darüber hinaus geben wir einen Überblick über verschiedene Ausbildungsschwerpunkte, welche Zielgruppen im Fokus stehen und welches Vorwissen für das jeweilige Schema empfehlenswert ist. Damit bieten wir eine Entscheidungshilfe für IT-Manager, Personalabteilungen und Mitarbeiter bei der Auswahl einer Fortbildung in IT-Sicherheit, die den eigenen Bedarf am besten trifft.

BERUFSBILDER IN DER IT-SICHERHEIT

Der ‚Hacker' oder Penetration-Tester ist meistens die erste Rolle, die einem beim Thema Security einfällt. Daneben gibt es viele weitere Anwendungsgebiete wie IT-Sicherheitsmanagement, sichere Software-Entwicklung, Datenschutz oder IT-Forensik. Die Hauptthemenbereiche für Fortbildungen liegen in den genannten Bereichen, daneben gibt es Auditorenausbildungen und spezielle Fortbildungen für Systemadministratoren.

Der Artikel konzentriert sich auf fünf Seminarangebote unterschiedlicher Anbieter, die für Testmanager, Tester, Anforderungs-Experten und Software- oder System-Entwickler interessant sind. Auswahlkriterien waren die internationale Verfügbarkeit und die Transparenz der Ausbildungs- und Prüfungsinhalte.

BEWERTUNGSKRITERIEN

Die betrachteten Ausbildungen werden in sechs Inhaltskategorien verglichen (Abb. 1): Die Kategorie Sicherer Entwicklungsprozess bewertet, ob Lebenszyklus-Aktivitäten wie z.B. die der ISO/IEC 27034, die sichere Systementwicklung unterstützen, geschult werden. Requirements Engineering & Threat Modeling sowie Sichere Software-Entwicklung betrachten, ob spezifische Vorgehensweisen zur Ermittlung von Security-Requirements und zum Entwurf der Systemarchitektur und Implementierung des Quellcodes besprochen werden. Penetration-Testing und Arbeiten mit konkreten Werkzeugen schätzen ein, wie gut sich das jeweilige Schema für eine Hands-On-Ausbildung als Sicherheitstester eignet. IT-Sicherheitsmanagement-Prozesse evaluiert die Relevanz der Inhalte für Personen, die IT-Sicherheitsprozesse im Unternehmen berücksichtigen müssen.

Darüber hinaus werden Angaben über benötigte Vorkenntnisse, Schwierigkeit, typische Kursdauern, Prüfungsart und typische Kosten gemacht. Alle Angaben geben die Meinungen und Recherche-Ergebnisse der Autoren wieder und erfolgen ohne Gewähr.

A4Q SECURITY ESSENTIALS

Die Schulung führt allgemein in Aspekte der Cyber Security ein. Auch wenn die Teilnehmer keine Vorkenntnisse benötigen, ist ein grundlegendes Verständnis für IT durchaus hilfreich. Es werden sowohl IT-Einsteiger angesprochen, die über die verbreiteten Awareness-Schulungen hinaus Interesse an Security haben, als auch Mitarbeiter in IT-Projekten, in denen IT-Sicherheit eine Rolle spielt. Weiterhin eignet sich die Schulung als Grundlage für eine spätere Spezialisierung zum Sicherheitsexperten.

Der Fokus der Schulung liegt auf der theoretischen Einführung von Begriffen und grundlegenden Prozessen. Thematisiert werden an den beiden Schulungstagen zudem die wichtigsten Angriffsszenarien sowie die Rolle der Security im Kontext des Softwarelebenszyklus.

A4Q bietet einen ausführlichen Lehrplan [1] zum freien Download. Trainingsanbieter können fertige Schulungsunterlagen und eine Musterprüfung gegen eine Lizenzgebühr in Schulungen verwenden, haben jedoch auch die Freiheit, Inhalte z.B. durch praktische Anteile zu vertiefen. Die Schulung schließt mit einer einstündigen Multiple Choice Prüfung mit 40 Fragen ab.

ISTQB® CERTIFIED TESTER ADVANCED LEVEL – SICHERHEITSTESTER (ISTQB® CT-AL-SEC)

Das ISTQB® bietet seit etwa drei Jahren eine Zertifizierung als Sicherheitstester auf dem Niveau „Advanced Level" an [2], [3]. Seit diesem Jahr ist bei einigen Trainingsanbietern nun auch eine deutsche Schulung verfügbar. Trainingsanbieter verwenden vom zuständigen nationalen Board akkreditierte, selbst entwickelte Schulungsunterlagen. Das ISTQB® bietet den Lehrplan sowie eine Musterprüfung (bisher nur in Englisch) zum freien Download.

Die Inhalte des Kurses orientieren sich stark am Certified Tester Schema, und greifen Aspekte aus ande-

ren ISTQB®-Schulungen auf, etwa den Testprozess aus dem Foundation Level (das Voraussetzung für diese Zertifizierung ist) oder den Risikomanagement-Prozess des Advanced Level Testmanager. Begrifflichkeiten und grundlegende Prozesse werden in der Schulung erläutert, können an den drei Schulungstagen jedoch nicht in aller Tiefe behandelt werden, so dass Grundkenntnisse in IT-Sicherheit sowie mehrjährige Erfahrung in der Software-Entwicklung, mit IT-Systemen und Netzwerken unbedingt zu empfehlen sind. Die zweistündige Multiple Choice Prüfung beinhaltet 45 Fragen.

CERTIFIED ETHICAL HACKER (CEH)

Der CEH [5] ist ein international gut etabliertes Schema zur Ausbildung von Penetration Testern mit Zertifizierung durch den EC-Council. Voraussetzung ist entweder eine Zulassungsprüfung durch den EC-Council oder die Teilnahme an einem Kurs. Das Schema wird regelmäßig aktualisiert und liegt derzeit in der Version 10 vor. Angeboten werden sowohl Präsenzkurse über akkreditierte Anbieter als auch Online-Kurse und Labore durch den EC-Council selbst. Der CEH versteht sich als Grundkurs im Penetration Test, allerdings sind gute technische Vorkenntnisse bzgl. Netzwerken und Betriebssystemen sehr empfehlenswert. Eine gute Übersicht der Kurs- und Prüfungsinhalte findet sich auf der Webseite des EC-Council. Zum CEH gibt es umfangreiche Sekundärliteratur, die aber sorgfältig ausgewählt werden muss – nicht alles ist empfehlenswert. Die Prüfung ist eine Multiple Choice Prüfung mit 125 Fragen, die in vier Stunden beantwortet werden müssen.

OFFENSIVE SECURITY CERTIFIED PROFESSIONAL (OSCP)

Der OSCP bietet eine praktische Ausbildung zum Penetration Tester. Die Zertifizierung wird durch die Offensive Security LLC angeboten. Sie besteht u.a. aus dem „Penetration Testing with Kali“ (PWK) Kurs, der im Selbststudium durchgearbeitet wird. Das Curriculum [7] ist frei einsehbar und das Selbststudium wird durch Videos unterstützt, die wertvolle Zusatzinformationen über das Skript hinaus bieten. Zudem ist viel praktisches Üben in virtuellen Laboren (Paketgrößen 30, 60 oder 90 Tage Zugang) notwendig. Hierbei muss man Aufgaben aus dem Skript lösen und „Capture the Flag“-ähnliche (CTF) Herausforderungen meistern. Das Skript ist durch Verständnis- und Praxisfragen abgerundet, deren Lösung bis zu fünf Bonuspunkte für die Prüfung geben. Die Prüfung selbst ist eine 24 Stunden Hacking Challenge gefolgt von 24 Stunden für das Verfassen eines aussagekräftigen Testberichts. Die Bewertungskriterien sind sehr streng, aber auch sehr genau beschrieben [8]. Der Kurs vermittelt viel praktisches Wissen und die Lernumgebung mit Laboren und Foren bietet einen guten Startpunkt für die Karriere als Penetration Tester. Gute Vorkenntnisse über Betriebssysteme und Netzwerke, sowie ein sicherer Umgang mit Konsolen sind als Voraussetzung sehr zu empfehlen.

SCHEMA	SICHERER ENTWICKLUNGS-PROZESS	REQUIREMENTS ENGINEERING & THREAT MODELING	SICHERE SOFTWARE-ENTWICKLUNG	PENETRATION-TESTING	IT-SICHERHEITS-MANAGEMENT-PROZESSE	ARBEITEN MIT KONKRETEN WERKZEUGEN	VORKENNTNISSE	LEVEL / ANSPRUCH INSGESAMT	"MINDEST-KURSDAUER (PFLICHT VS. OPTIONAL)"	ART DER PRÜFUNG (ANZAHL)	KOSTEN (NETTO) INKLUSIVE PRÜFUNG
A4Q Security Essentials	++	++	+	0/+	+	0	Keine	+	2 Tage Präsenz (optional)	Multiple Choice über 1 Stunde	ca. 1.200,- bis 1.500,-EUR
ISTQB CTAL-SEC	++	+	+	+	++	0	CTFL erforderlich, 2 Jahre Berufserfahrung im Softwaretest, Grundkenntnisse in Netzwerktechnik und IT-Sicherheit empfohlen	++	3 Tage (optional)	Multiple Choice über 2 Stunden	ca. 1.800,- bis 2.100,- EUR
EC-Council CEH	0	0	0	++	+	++	Gute technische Kenntnisse in Netzwerktechnik und Betriebssystemen	++	5 Tage Präsenz oder Abo für E-Learning mit virtueller Laborumgebung	Multiple Choice über 4 Stunden	E-Learning ca. 3.000,- USD Präsenz ca. 3.700,-EUR
Offensive Security OSCP	0	0	0	+++	+	+++	Sehr gute technische Kenntnisse in Netzwerktechnik und Betriebssystemen	+++	30 bis 90 Tage, virtuelle Laborumgebung	Praktische Prüfung über 24 Stunden (Praxis) + 24 Stunden Berichterstelleung	800,- bis 1.150,- USD [30/60/90 Tage Lab + PWK]
(ISC)² CISSP	+++	++	++	+	+++	+	5 Jahre Vollzeit Berufserfahrung in IT-Sicherheit, Unbescholtenheit	+++	5 bis 7 Tage Präsenz oder Online-Kurs (ca. 6 Monate Zugang)	Adaptiv oder Multiple Choice	ca. 4.000,- bis 5.000,- EUR Präsenz, Online ab ca. 1.500,-EUR

Abbildung 1: Legende: 0 = nicht thematisiert, + = bespricht Grundlagen,
++ = Grundlagen und Vertiefung in verschiedenen Kontexten, +++ = vermittelt Expertenwissen auf hohem Niveau

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL ((ISC)2 CISSP)

Ein Chief Information Security Officer ohne die im CISSP geforderten Kenntnisse ist wie ein Osterhase ohne Ohren. Der CISSP [4] richtet sich an diejenigen, die IT-Sicherheitsprozesse definieren, verwalten, auditieren oder verantworten müssen. Das Ausbildungsschema stammt von (ISC)2, einer nicht-profitorientierten Mitgliederorganisation mit Schwerpunkt Cyber-Sicherheit. Es vermittelt und prüft Kenntnisse aus acht Bereichen: Risikomanagement, Asset Sicherheit, Sichere Architektur und Engineering, Netzwerk- und Kommunikationssicherheit, Identitäts- und Zugangsmanagement, Assessment und Testen, Operations und sichere Entwicklung. Dabei wird Vollzeit-Berufserfahrung von mindestens fünf Jahren in mindestens zwei dieser Bereiche gefordert. Technische Kenntnisse und Fertigkeiten werden vorausgesetzt und abgeprüft. Zum CISSP gibt es einen umfangreichen Body of Knowledge, viel Sekundärliteratur, Präsenz- und Onlinekurse, sowie Kurse für reines Selbststudium. Besonders sind die zwei unterschiedlichen Examensformen: Eine adaptive Online-Prüfung über drei Stunden, mit bis zu 150 Fragen oder eine klassische sechsstündige Multiple Choice Prüfung mit 250 Fragen.

FAZIT

Die Mehrzahl der Ausbildungen richtet sich an Personen mit Vorkenntnissen. Die große Ausnahme stellt hier das A4Q Security Essentials Schema dar. Wer eine praktische Ausbildung speziell im Penetration Test sucht, ist mit dem CEH und vor allem dem OSCP gut beraten. Für Allrounder ist der ISTQB® CT-AL-SEC und für die mit ganz hohen Ansprüchen oder hoher Verantwortung der CISSP eine gute Wahl. ■

AUSGEWÄHLTE QUELLEN

[1] LP A4Q Security Essentials Syllabus, 2019, URL: https://www.alliance4qualification.info/a4q-security-essentials

[2] ISTQB CT AL-SEC Syllabus, 2016, URL: https://www.istqb.org/downloads/syllabi/advanced-level-security-tester-syllabus.html

[3] Simon et al.: Basiswissen Sicherheitstests, dpunkt.verlag, 2019.

[4] The Ultimate Guide to the CISSP, (ISC)2, 2018.

[5] EC-Council Certified Ethical URL: https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

[6] Offensive Security OSCP Course description. URL: https://www.offensive-security.com/pwk-oscp/

[7] OSCP Curriculum. URL: https://www.offensive-security.com/documentation/penetration-testing-with-kali.pdf

[8] OSCP Bewertungskriterien:] https://support.offensive-security.com/oscp-exam-guide/

Dipl.-Math. Christian Alexander Graf berät mittelständische Unternehmen zur Qualitätssicherung. Er unterrichtet IT-Security an der DHBW in Mannheim und hat an den Lehrplänen zu A4Q Security Essentials und ISTQB® CT-AL-SEC mitgearbeitet. Er ist Mit-Autor von „Basiswissen Sicherheitstests“.

Dipl.-Inform. Markus Niehammer ist Senior Consultant und Trainer, u.a. für IT-Sicherheit, bei der Sogeti Deutschland GmbH. Neben der Durchführung von Kundenschulungen ist er zuständig für Schulungsentwicklung sowie für die Durchführung von Audits zur Testprozessoptimierung nach TPI NEXT®.

M. Sc. Christoph Ponikwar berät Kunden in Fragen der Informationssicherheit, koordiniert und führt Penetration Tests durch. Darüber hinaus gibt er Schulungen im Bereich Penetration Testing und Web Application Security. Er hält aktuell Zertifikate für OSWP, OSCP, OSCE und ISO 27k 2013 Foundation.

Der Artikel erschien im SQ-Magazin #54 MÄRZ 2020 **„KI & SOFTWARE TESTING“**

www.sq-magazin.de