Einleitung

»The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.«
Gene Spafford

»Und um genau in solchen Zweifelsfällen maximale Transparenz zu bekommen, bedarf es der Sicherheitstests.«
Die Autoren

Was ist heute der mit Abstand wichtigste Aspekt einer IT-Strategie? Eine verbesserte User Experience? Eine bessere funktionale Qualität? Die Nutzung von Cloud? Die Einführung neuer Vorgehensweisen wie »Agile« oder »DevOps«?

Es ist die IT-Sicherheit!

Der World-Quality-Report 2018/2019 [CapGemini et al. 18] hebt deutlich hervor, dass die IT-Sicherheit heute das entscheidende Qualitätsmerkmal schlechthin ist und über eine entsprechende IT-Strategie gefördert werden muss. Gute Gründe dafür sind:

- Der eigene Schutz und der Schutz der Kunden sowie die damit verbundene Fähigkeit, am Markt nachhaltig bestehen zu können.
- Die Außenwahrnehmung, um als verantwortungsbewusster und professioneller Anbieter angesehen zu werden und darüber Wettbewerbsvorteile darstellen zu können.
- Die Notwendigkeit, gesetzliche Vorgaben zu erfüllen.

Unabhängig von den konkreten Gründen zeigt sich jeweils schnell, dass die Sicherheit kein reines Technikthema ist: Sicher kennt jeder die Hacker-Sessions auf Konferenzen und Ausstellungen, in denen meist junge Hacker eindrucksvoll demonstrieren, wie technische Schwachstellen in IT-Systemen leichtgewichtig und live ausgehebelt werden können. Aber ebenso sollte heute klar sein, dass die beste Technik kaum

hilft, wenn sie nicht in die entsprechenden Prozesse eingewoben ist, die von Organisationen mit geschulten Menschen genutzt wird. Sicherheit ist ein extrem vielschichtiges Qualitätsmerkmal, dessen Gesamtstatus durch das schwächste Glied der Kette definiert ist, das häufig wiederum beim Menschen selbst liegt. Das auch heute immer noch weltweit meistgenutzte Passwort als Zeichenfolge »123456« belegt dies eindrucksvoll (vgl. z. B. [HPI 18]).

Eine bisher wenig im Rampenlicht stehende Teildisziplin ist hier das Sicherheitstesten, also das systematische Prüfen, inwieweit die Sicherheit eines Systems angemessen ist und durch entsprechende Konzepte nachhaltig garantiert werden kann. Oder andersherum das Aufzeigen, wo eben die schwächsten Glieder in einer gesamten Organisation liegen und wie diese abgesichert werden können.

Dieses Buch ist genau diesem Thema gewidmet. Als inhaltlicher Leitfaden dient hierbei der Syllabus »Sicherheitstester« des German Testing Board (GTB), der seinerseits die Lokalisierung des Syllabus »Security Tester« des International Software Testing Qualifications Board (ISTQB®) darstellt. Dass eine Lokalisierung mehr als eine reine Übersetzung ist, zeigt bereits die Schwierigkeit des Begriffs *Security*: Während im englischsprachigen Raum eine klare Abtrennung zur *Safety*, also dem Schutz der physischen Unversehrtheit, existiert, subsumiert der deutsche Begriff Sicherheit umgangssprachlich meist beide Facetten. In diesem Buch möchten die Autoren trotzdem den Begriff des Sicherheitstesters alias Security Tester etablieren, auch um sich nicht zu weit vom De-facto-ISTQB®-Standard zu entfernen.

Der Vorteil dieser inhaltlichen Nähe ist dann auch die Möglichkeit, sich mit diesem Buch aktiv auf die entsprechenden Prüfungen zum »ISTQB® Certified Tester – Advanced Level Specialist – Security Tester« vorzubereiten. Der Nachteil ist, dass es kaum Möglichkeiten gibt, bestimmte Aspekte wegzulassen, neue Aspekte hinzuzufügen oder ggf. in einem ganz anderen Kontext zu erläutern: Die Struktur des Buches ist eng am Syllabus angelegt, die durch klar definierte Rollen der Autoren beleuchtet und letztlich angereichert wurde:

- Die wissenschaftliche Seite, vertreten durch Prof. Dr. Jürgen Mottok, Professor für sichere und zuverlässige Systeme an der Ostbayerischen Technischen Hochschule Regenburg, zeigt auf, was heute als Stand der Wissenschaft grundsätzlich überhaupt möglich ist (und was nicht).
- Die forschende Anwendungsseite, vertreten durch Dr. Jürgen Großmann und Martin Schneider des Fraunhofer-Instituts FOKUS, bringt die Praktikabilität wissenschaftlicher Techniken als Stand der Technik ein.

- Die Anwendungsseite, vertreten durch Dr. Frank Simon von der Zurich Versicherungsgruppe Deutschland, steuert den Stand der Praxis und die typischen Herausforderungen existierender Systeme für die Gegenwart und die Zukunft bei.
- Die pädagogisch-didaktische Seite, vertreten durch Christian Graf als langjährigen Trainer unterschiedlicher Schulungen, trägt Best Practices im Bereich der Vermittlung nicht trivialer Inhalte wie Sicherheitstesten bei.

Trotz dieser vielschichtigen Expertise und gerade wegen des speziellen Themas kann dieses Buch nur einen Impuls geben, sich mit dem Thema Sicherheitstesten intensiv zu beschäftigen. Es wäre fahrlässig zu behaupten, nach der Lektüre ausgewiesener Sicherheitstester zu sein. Nicht ohne Grund verlangen die GTB/ISTQB®-Statuten für den Sicherheitstester, dass als Vorbedingung einer entsprechenden Prüfung mindestens zwei Jahre Praxiserfahrung im Bereich des Testens vorgewiesen werden müssen. Und selbst dann sorgt die extrem hohe Dynamik im Bereich der Sicherheit dafür, dass einmal erlerntes Wissen jederzeit obsolet werden kann, ggf. modifiziert werden muss oder durch vollständig neue Aspekte erweitert werden sollte. Dieses Buch will und kann hier nur einen initialen Anstoß für eine hochspannende Reise in viele einzelne tiefe Bereiche des Sicherheitstestens geben.

Konkret nähert sich dieses Buch dem Thema Sicherheitstesten über neun Kapitel:

- Kapitel 1 beginnt mit der grundlegenden Notwendigkeit für das Sicherheitstesten, den Sicherheitsrisiken. Außerdem wird hier das Konzept der Informationssicherheitsrichtlinien vorgestellt, das sich in der Praxis diesen Sicherheitsrisiken entgegenstellt. Das Sicherheitsaudit, dem der Sicherheitstest zuarbeiten kann, analysiert letztlich das nach Bereinigung der Wirkung der Richtlinien verbliebene Sicherheitsrisiko.
- Kapitel 2 wendet sich dann konkret dem Sicherheitstest zu: Neben einem Überblick über typische Sicherheitslücken werden Zweck und Ziele von Sicherheitstests an Beispielen erläutert und deren notwendige Verknüpfung mit Unternehmenszielen aufgezeigt. Außerdem werden hier erste Ideen zu Vorgehensweisen von Sicherheitstests sowie deren Erfolgsmessung aufgezeigt.
- Kapitel 3 fokussiert dann genau diese Vorgehensweisen über die Beschreibung konkreter Sicherheitstestprozesse. Hierbei wird die Nähe zum klassischen ISTQB®-Testen und zum Testprozess begründet und auf die jeweiligen Folgeschritte Planung, Entwurf, Ausführung

und Bewertung für den Sicherheitstest wird ausführlich eingegangen.

- Kapitel 4 projiziert den Sicherheitstest und den zugrunde liegenden Prozess dann auf den Softwareentwicklungsprozess. Die dortigen Phasen Anforderungsermittlung, Entwurf, Implementierung, Test und Betrieb werden hier um wichtige Aspekte des Sicherheitstestens angereichert.
- Kapitel 5 beschäftigt sich mit den Kernthemen des Sicherheitstestens, der Überprüfung klassischer Sicherheitstechniken: Wie können IT-Systeme bezüglich der Sicherheit getestet werden, wie können Authentifizierungs-, Autorisierungs- und Verschlüsselungsmethoden geprüft werden, wie sehen effektive Infrastrukturen wie Firewalls und Netzwerkzonen aus? Kontrastiert wird dies durch das Testen mittels aufdeckender Technologien wie Angriffserkennungen, Malware-Scans und Datenmaskierungen sowie durch die Erläuterung der Wichtigkeit präventiver Arbeit in Form von Schulungen.
- Kapitel 6 untersucht die menschlichen Faktoren beim IT-Sicherheitstest: Warum und wie denken und arbeiten Angreifer? Wie funktioniert Social Engineering und welche Rolle spielt das allgemeine Sicherheitsbewusstsein von Mitarbeitern für eine möglichst hohe IT-Gesamtsicherheit?
- Kapitel 7 beschreibt, wie Sicherheitstests ausgewertet und die Ergebnisse in Abschlussberichten aufbereitet sein sollten und welche besonderen Anforderungen an die Sicherheitstestergebnisse bezüglich der Berichterstattung gestellt werden.
- Kapitel 8 zeigt einige typische Beispiele von Sicherheitstestwerkzeugen und beschreibt praxiserprobte Methoden zur Werkzeugauswahl.
- Kapitel 9 beschließt dieses Buch mit einer Einführung in für den Sicherheitstester besonders relevante Standards und Branchentrends. Es gibt darüber hinaus eine Übersicht, über welche Informationskanäle welche Arten von Informationen ein Sicherheitstester erlangen kann und sollte.

Nach dem Lesen und Durcharbeiten dieser Kapitel sollte es möglich sein, sowohl eine Prüfung zum Certified Sicherheitstester erfolgreich abzulegen als auch nur einen guten Überblick über den Themenbereich Sicherheitstester insgesamt zu bekommen. Das umfangreiche Quellenverzeichnis sowie der Index erlauben zudem auch das punktuelle Einarbeiten und Nachschlagen, wenn es um den aktuellen Stand der Technik im Bereich des Sicherheitstestens für bestimmte Themenblöcke geht.