Vorwort

»Mit dem Wissen wächst der Zweifel.«

Johann Wolfgang von Goethe, Maximen und Reflexionen

Bereits im Herbst 2015 waren mit dem Start des Beta-Reviews des ISTQB® Security-Tester-Lehrplans die Weichen gestellt: »ISTQB goes Security.« Im Sommer 2016 wurde dann der Syllabus in der finalen Version veröffentlicht. Im German Testing Board (GTB), dem deutschen Repräsentanten des ISTQB®, war bereits nach der Bekanntgabe der Kursankündigung schnell klar, dass dies ein höchst logischer Schritt zur bedarfsgerechten Erweiterung des gesamten Schulungsportfolios war. Als dann der finale Syllabus mit 86 Seiten erschien, kamen die ersten **Zweifel**: Was für eine umfangreiche Themensammlung! Wie aufwendig wird eine Lokalisierung für den deutschen Markt sein?

Und doch: Das German Testing Board hat sehr bald eine eigene Security-Arbeitsgruppe gegründet, um initial erst einmal die entsprechenden Experten zusammenzubringen. Sie sollten den Inhalt verstehen, in einen deutschen Lehrplan überführen, für spätere Zertifizierungen die entsprechenden Fragen erstellen und ggf. sogar ein begleitendes Buch verfassen. Als dann die ersten Einladungen verschickt waren, kamen die nächsten **Zweifel**: Jeder Security-Experte ertrinkt seit Jahren in Arbeit, kann hervorragende Tagessätze abrufen und hat darüber hinaus noch fortwährend die Aufgabe, sein Wissen kontinuierlich irgendwie aktuell zu halten. Und dann kommt noch die Einladung, sich innerhalb eines »Testing-Vereins« ehrenamtlich zu engagieren? An Abenden und Wochenenden? Für Ruhm und Ehre?

Und doch: Es hat sich eine schlagkräftige Gruppe gefunden, die sich der Übersetzung angenommen hat. Schnell wurde klar, dass das mehr als eine einfache Übersetzung ist und die Lokalisierung im Vordergrund steht: Schon über die Frage, wie denn »Security-Tester« übersetzt werden kann, lässt sich trefflich streiten. Ebenso wie über die Vielzahl nationaler/europäischer Normen und Vorgaben, die gerade für den Sicherheitstester in Deutschland relevant werden würden. Erneut kamen **Zweifel** auf, ob das »Cross-Site-Scripting« tatsächlich mit »webseitenübergreifenden Skripten« übersetzt werden sollte? Ob das »Salting« tatsächlich mit »Salzen« übersetzt werden kann? Ob »Social Engineering« tatsächlich dasselbe ist wie »soziale Manipulation«?

Und doch: Im Oktober 2018 konnte nach einem umfangreichen Beta-Review mit vielen späteren Trainingsanbietern der finale, übersetzte und lokalisierte Syllabus zum »Sicherheitstester« veröffentlicht werden. Er lässt sich seitdem kostenlos über die Internetseite des German Testing Board herunterladen. Doch mit 104 Seiten Umfang wuchsen wiederum die **Zweifel** daran, ob dieser Kurs, dessen Thema allgegenwärtig in der Presse präsent ist, mit seinem enorm breiten Themenspektrum von den Interessenten akzeptiert wird? Einem Spektrum, das von Risikomanagement über Testprozesse und Sicherheitsprozesse bis hin zu spezifischen Sicherheitstesttechniken, entsprechenden Werkzeugen und regulatorischen Vorgaben reicht?

Und doch: Bereits Mitte 2018 fanden sich fünf Security-Begeisterte, die genau diese Herausforderung annahmen: Das extrem umfangreiche Sicherheitstester-Material so weit in einem entsprechenden Buch aufzubereiten, dass sowohl der Prüfungsinteressierte sich hiernach vorbereiten kann als auch der nur Themeninteressierte in diesem Werk ein gutes Kompendium rund um dieses Thema findet. Viele Beispiele sollten es sein, mit einer hohen Praxisrelevanz. Je konkreter die ersten Seiten wurden, desto mehr **Zweifel** kamen abermals auf: Wie viel Wissen kann beim Leser vorausgesetzt werden? Ist der ISTQB®-Testprozess bereits bekannt? Darf angenommen werden, dass der Leser C oder Java beherrscht? Dass dem Interessierten die Institution BSI und das IT-Grundschutz-Kompendium wenigstens grob bekannt sind? Wie viele tausend Seiten würde das Buch benötigen?

Und doch: Nach unzähligen Telefonkonferenzen, Wochenendmeetings, E-Mail-Schlachten und Sharepoint-Versionsabenteuern ist es im Januar 2019 so weit: Über 400 Seiten geballtes Wissen rund um das Sicherheitstesten stehen bereit, angereichert mit unzähligen Beispielen, fachlichen Exkursen, Referenzen und Erläuterungen. Komplexen Themengebieten wird man nicht dadurch gerecht, dass man sie kleinredet, sondern ihnen angemessen begegnet. Erneut kamen **Zweifel**, ist der Leser nach der Lektüre nun ausgewiesener Sicherheitstester? Kann er die heute immer schnelllebigeren IT-Systeme wirkungsvoll absichern? Wohlwissend, dass die Hacker vermutlich schon einen Schritt weiter sind?

Und doch: Mit dem Wissen in diesem Buch wird hoffentlich auch Ihr Zweifel wachsen: 100 %ige Sicherheit? Vollständiges Beseitigen aller Schwachstellen? Keine Risiken mehr? **Zweifel!** Aber die werden nicht dadurch ausgeräumt, dass man etwas nicht weiß, sondern dadurch, dass man lernt und fortwährend besser wird.

Viel Spaß beim Sicherheitstesten wünschen die fünf Autoren!

Danksagung

Ein Buch zu schreiben bedeutet für nicht hauptberuflich tätige Autoren wie uns, einen großen Teil der Freizeit zu opfern.

An allererster Stelle möchten wir uns daher bei unseren Partnern und Familien für ihr Verständnis und ihre wundervolle Unterstützung und Ausdauer bedanken. Ohne diese wäre dieses Buch nicht möglich gewesen, denn unsere Freizeit ist eigentlich die Zeit mit ihnen.

Unser Dank gilt ebenfalls dem German Testing Board (GTB), das durch die Gründung der AG Security auch die Autorengruppe selbst zusammengebracht und bei ihrer Arbeit unterstützt hat. Unser Dank gilt ganz besonders den weiteren Mitgliedern der AG Security und den Reviewern des deutschen Sicherheitstester-Lehrplans.

Beim dpunkt.verlag bedanken wir uns herzlich für die umfangreiche Unterstützung in allen organisatorischen und technischen Fragen rund um das Buch und insbesondere, dass der Verlag uns die Gelegenheit gab, dieses Buch überhaupt zu schreiben.

An Professor Dr. Andreas Spillner sei an dieser Stelle ein herzliches Dankeschön gerichtet und ein großes Lob für seine hilfreichen Anmerkungen und Verbesserungsvorschläge bei der Entstehung des Buches.

Frank Simon, Jürgen Großmann, Christian Alexander Graf, Jürgen Mottok, Martin A. Schneider

P.S.: Zu guter Letzt bedanken sich Christian Alexander Graf, Jürgen Mottok, Martin Schneider und Jürgen Großmann ausdrücklich bei Frank Simon für die hervorragende Projektleitung, die vielen Reviews und die professionelle Organisation und Moderation von Telkos und Autorentreffen. Ohne dich, Frank, wäre dieses Buch wahrscheinlich auch 2020 noch nicht fertig.

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.