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.