

---

# Inhaltsverzeichnis

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Einleitung</b>   | <b>1</b>  |
| 1.1      | Ziele dieses Buches .....                                     | 1         |
| 1.2      | Inhalte dieses Buches .....                                   | 7         |
| 1.3      | ISSECO und die CPSSE-Zertifizierung .....                     | 10        |
| <b>2</b> | <b>Die Sicht des Kunden</b>                                   | <b>13</b> |
| 2.1      | Ben und sein Projektteam .....                                | 13        |
| 2.2      | Verschiedene Interessengruppen – verschiedene Interessen .... | 14        |
| 2.3      | Warum erwarten Kunden sichere Software? .....                 | 17        |
| 2.4      | Was genau erwarten Kunden eigentlich? .....                   | 19        |
| 2.5      | Werte, Bedrohungen und Risiken .....                          | 23        |
| 2.6      | Von Erwartungen zu technischen Anforderungen .....            | 25        |
| 2.7      | Helfen Sie dem Kunden, dann helfen Sie sich selbst! .....     | 26        |
| 2.8      | Ben spricht noch einmal mit dem Kunden .....                  | 28        |
| <b>3</b> | <b>Die Sicht des Angreifers</b>                               | <b>29</b> |
| 3.1      | Jewgeni .....   | 29        |
| 3.2      | Was sind Hacker? .....  | 30        |
| 3.3      | Wie geht ein Hacker vor? .....                                | 36        |
| 3.4      | Jewgeni hat eine Idee .....                                   | 43        |
| <b>4</b> | <b>Methodologien für sichere Software</b>                     | <b>45</b> |
| 4.1      | Bens Entwicklungsmethodik .....                               | 45        |
| 4.2      | Sichere Software im Überblick .....                           | 46        |
| 4.3      | Softwareentwicklungsmethoden .....                            | 47        |
| 4.4      | Maßnahmen zur Verbesserung der Sicherheit .....               | 50        |
| 4.5      | Existierende Modelle .....                                    | 54        |
| 4.6      | Ben denkt über Sicherheit nach .....                          | 67        |

---

|          |   |            |
|----------|---|------------|
| <b>5</b> | <b>Sicherheitsanforderungen</b>                               | <b>69</b>  |
| 5.1      | Bens Sicherheitsanforderungen .....                           | 69         |
| 5.2      | Was sind Anforderungen? .....                                 | 69         |
| 5.3      | Wie identifiziert man Sicherheitsanforderungen? .....         | 75         |
| 5.4      | Wichtige Sicherheitsanforderungen .....                       | 78         |
| 5.5      | Bens neue Anforderungsliste .....                             | 85         |
| <b>6</b> | <b>Bedrohungsmodellierung</b>                                 | <b>87</b>  |
| 6.1      | Bens Bedrohungsmodellierung .....                             | 87         |
| 6.2      | Der Nutzen einer Bedrohungsmodellierung .....                 | 87         |
| 6.3      | Die Phasen der Bedrohungsmodellierung .....                   | 89         |
| 6.4      | Bens zweiter Versuch .....                                    | 111        |
| <b>7</b> | <b>Sicherer Softwareentwurf</b>                               | <b>113</b> |
| 7.1      | Bens Softwareentwurf für Sicherheit .....                     | 113        |
| 7.2      | Sicherer Softwareentwurf und sichere Softwarearchitekturen .. | 114        |
| 7.3      | Secure Design Patterns .....                                  | 116        |
| 7.4      | Secure Design Principles .....                                | 127        |
| 7.5      | Review der Sicherheitsarchitektur .....                       | 132        |
| 7.6      | Ben war auf einer Konferenz .....                             | 133        |
| <b>8</b> | <b>Sicheres Programmieren</b>                                 | <b>135</b> |
| 8.1      | Bens Tricks zum sicheren Programmieren .....                  | 135        |
| 8.2      | Es gibt keine Tricks .....                                    | 136        |
| 8.3      | Welche Schwachstellen sind am kritischsten? .....             | 136        |
| 8.4      | Wiederkehrende Muster von Schwachstellen .....                | 142        |
| 8.5      | Techniken für sicheres Programmieren .....                    | 144        |
| 8.6      | Die wichtigsten Schwachstellen und Gegenmaßnahmen .....       | 149        |
| 8.7      | Werkzeuge zur sicheren Programmierung .....                   | 152        |
| 8.8      | Klaus' Empfehlungen für die sichere Programmierung .....      | 153        |

|           |   |            |
|-----------|---|------------|
| <b>9</b>  | <b>Software auf Sicherheit testen</b>       | <b>155</b> |
| 9.1       | Bens Sicherheitstest                        | 155        |
| 9.2       | Sicherheit und Softwaretests                | 156        |
| 9.3       | Hacking-Techniken als Sicherheitstests      | 160        |
| 9.4       | Sicherheitsspezifische Testmuster           | 164        |
| 9.5       | Sicherheitskritische Testbereiche           | 167        |
| 9.6       | Codereview                                  | 169        |
| 9.7       | Sicherheitstestberichte schreiben           | 170        |
| 9.8       | Der Sicherheitstest vom QMB                 | 171        |
| <b>10</b> | <b>Sichere Auslieferung und Einrichtung</b> | <b>173</b> |
| 10.1      | Bens Installationsanleitung                 | 173        |
| 10.2      | Sicherheit im IT-Betrieb                    | 174        |
| 10.3      | Phasen der Softwareeinrichtung              | 179        |
| 10.4      | Pauls Korrekturen der Installation          | 187        |
| <b>11</b> | <b>Umgang mit Schwachstellen</b>            | <b>189</b> |
| 11.1      | Bens Security Response                      | 189        |
| 11.2      | Sicherheit im normalen Supportprozess       | 190        |
| 11.3      | Offenlegungsstrategien für Schwachstellen   | 194        |
| 11.4      | Erfolgreich über Schwachstellen reden       | 196        |
| 11.5      | Standards für Schwachstellenbeschreibungen  | 199        |
| 11.6      | Entwicklung einer Security Response Policy  | 204        |
| 11.7      | Ben und die IT-Presse                       | 205        |
| <b>12</b> | <b>Metriken für Sicherheit</b>              | <b>207</b> |
| 12.1      | Bens Messgrößen                             | 207        |
| 12.2      | Warum überhaupt Metriken für Sicherheit?    | 207        |
| 12.3      | Softwaremetriken                            | 209        |
| 12.4      | Arten von Metriken                          | 211        |
| 12.5      | Qualitätskriterien für Metriken             | 212        |
| 12.6      | Existierende Metriken für Sicherheit        | 214        |
| 12.7      | Entwicklung von Metriken für Sicherheit     | 217        |

|   |            |
|---|------------|
| <b>13 Codeschutz</b>  | <b>221</b> |
| 13.1 Ben und seine eigene IT-Sicherheit .....               | 221        |
| 13.2 Gründe, den Code zu schützen .....                     | 221        |
| 13.3 Technische Risiken während der Entwicklungsphase ..... | 223        |
| 13.4 Grundsätzliche Schutzmechanismen .....                 | 225        |
| 13.5 Besondere Anforderungen durch Export und Politik ..... | 227        |
| 13.6 Technische Lösungen für den Schutz von Code .....      | 229        |
| 13.7 Lizenzschutz .....                                     | 234        |
| 13.8 Was hätte Ben unternehmen können? .....                | 239        |
| <b>14 Testfragen</b>  | <b>241</b> |
| <b>Abkürzungen</b>  | <b>259</b> |
| <b>Glossar</b>  | <b>261</b> |
| <b>Literatur</b>  | <b>273</b> |
| <b>Index</b>  | <b>281</b> |