

---

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	1
<b>2</b>	<b>Allgemeines</b> .....	5
2.1	Allgemeine Herausforderungen in Bezug auf die IT-Sicherheit. ....	5
2.2	IT-sicherheitsspezifische Herausforderungen bei der Beschaffung .....	9
<b>3</b>	<b>Allgemeines zum Beschaffungsprozess</b> .....	11
3.1	Beschaffung für interne Infrastruktur. ....	12
3.2	Komponentenbeschaffung in der Produktion. ....	14
3.3	Beschaffung für Handelsbetriebe. ....	16
3.4	Beschaffung von Standardsoftware versus Individualsoftware .....	16
3.5	Beschaffung von quelloffener Software. ....	18
3.5.1	Freie versus Open Source Software. ....	18
3.5.2	IT-Sicherheit. ....	19
<b>4</b>	<b>Maßnahmen einer IT-sicheren Beschaffung</b> .....	21
4.1	Risikoanalyse, Schutzbedarfsfeststellung, IT-Sicherheitsanforderungen .....	22
4.1.1	Schutzbedarfsfeststellung. ....	24
4.2	Ausarbeitung der IT-Sicherheitsanforderungen. ....	25
4.3	Weitere Maßnahmen .....	26
4.3.1	Feststellung und Bewertung von Produktzertifizierungen .....	26
4.3.2	SLA für Leistungsfähigkeit und Ordnungsmäßigkeit des Anbieters .....	27

4.3.3	Incident-Management und Reporting . . . . .	27
4.3.4	Überprüfung und Bewertung von Referenzen und Erfahrungsberichten . . . . .	28
4.3.5	Überprüfung und Bewertung von IT-Sicherheitstests . . . . .	28
4.3.6	Geschäftskontinuität. . . . .	29
4.3.7	Ansprechpartner beim Anbieter bzw. Hersteller . . . . .	30
4.3.8	Bewertung von IT-Sicherheitsdokumentationen und „Hardening“ . . . . .	30
4.4	Juristische Aspekte . . . . .	30
4.4.1	Vertragsänderung oder -auflösung . . . . .	30
4.4.2	Gewährleistung . . . . .	31
4.4.3	Beispiel von allgemeinen Haftungsbedingungen für Software . . . . .	32
4.5	Herkunft IT-sicherheitskritischer Komponenten . . . . .	33
4.5.1	In-Design Schwachstellen . . . . .	35
4.6	Beschaffungsrelevante Informationssysteme für IT-Sicherheit. . . . .	35
4.7	Vorgehensmodelle zur Softwarebeschaffung . . . . .	39
4.8	IT-Sicherheitsgütezeichen . . . . .	40
4.9	Berücksichtigung von branchenspezifischen Vorgaben . . . . .	41
4.10	Kleinteilige Hardware und Software . . . . .	42
4.11	Herstellerseitige Maßnahmen . . . . .	43
4.11.1	Unternehmenszertifizierungen . . . . .	43
4.11.2	Sicherer Entwicklungsprozess – Secure by Design Ansatz . . . . .	43
4.11.3	Berücksichtigung von anerkannten Standards, Richtlinien und Gesetze . . . . .	44
4.11.4	Sicherheitsbezogener Support und Kommunikation . . . . .	45
4.11.5	Sicherheitsdokument und produktbezogene Sicherheitsmaßnahmen . . . . .	45
4.11.6	Produktzertifizierungen und Produkttests . . . . .	45
4.11.7	Bug Bounty Programme. . . . .	45
4.11.8	Open Source (FOSS, FLOSS) . . . . .	46
4.11.9	Transparenzberichte . . . . .	46
4.11.10	Code Signing . . . . .	46
4.11.11	Fortbildung und Zertifizierungen von Mitarbeiter . . . . .	46
4.11.12	Sichere Auslieferungskonfiguration. . . . .	47
4.11.13	Branchenspezifische Vorgaben. . . . .	47

---

<b>5 Beschaffung von Hard- und Software mithilfe einer Beschaffungsplattform</b>	49
5.1 Die Beschaffungsplattform	49
5.2 Beschaffungstexte: IT-Sicherheitsanforderungstexte	50
<b>6 Abschließende Bemerkungen</b>	53
<b>Literatur</b>	55

Beschaffung unter Berücksichtigung der IT-Sicherheit  
Wichtigkeit, Herausforderungen und Maßnahmen

Piller, E.

2017, XIII, 58 S. 4 Abb., Softcover

ISBN: 978-3-658-18598-5