1 Einführung 1
1.1 Warum brauchen wir Cybersecurity für Kraftfahrzeuge? 1
1.2 Warum braucht Cybersecurity ein strukturiertes Engineering? 5
1.3 Wie sieht das Gebäude eines Cybersecurity Engineering-Prozesses aus? 6

2 Übergeordnetes (projektunabhängiges) Management der Cybersecurity 11
2.1 Cybersecurity als Element der Unternehmenskultur 11
2.2 Informationssicherheitsmanagementsystem 12

3 Kontinuierliche Weiterentwicklung der Cyberabwehrfähigkeit 15
3.1 Kontinuierliche Überwachung der Cybersecurity von IT-Systemen 15
3.2 Behandlung von Sicherheitsvorfällen 16
3.3 Schwachstellenanalyse 17
3.4 Schwachstellenbehandlung 17

4 Projektbezogenes Management der Cybersecurity 19
4.1 Planung auf die Cybersecurity bezogener Maßnahmen 19
4.2 Wiederverwendbarkeit von Komponenten 21
4.3 Nachweisführung und sachverständige Beurteilung 22
4.3.1 Unabhängigkeit der Konformitätsbewertung 22
4.3.2 Entwicklungsbegleitender Ansatz der Konformitätsbewertung 23
4.4 Management der Cybersecurity in einer verteilten Entwicklung 25

Bibliografische Informationen
https://d-nb.info/1285699025

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

5 Risikoorientierte Bestimmung der gebotenen Schutzmaßnahmen ... 27
5.1 Identifikation von Schadensszenarien ... 27
5.2 Schadensschwere der Schadensszenarien ... 28
5.3 Identifikation von Bedrohungsszenarien ... 29
5.4 Identifikation von Angriffspfaden ... 31
5.5 Ermittlung der Erfolgswahrscheinlichkeit eines Angriffs ... 33
5.6 Ermittlung des Risikos ... 34
5.7 Entscheidung zur Risikobehandlung ... 35

6 Entwurf angriffssicherer Systeme ... 37
6.1 Systemdefinition als Ausgangspunkt der Entwicklung ... 37
6.2 Cybersecurity: Ziele und Konzept ... 38
6.3 Ableitung und Verfeinerung technischer Cybersecurity-Anforderungen ... 39
6.4 Cybersecurity-Anforderungen an Hardware und Software ... 42

7 Eigenschaftsabsicherung angriffssicherer Systeme ... 43
7.1 Nachweis der Angriffssicherheit durch Fuzz-Testing ... 43
7.2 Nachweis der Angriffssicherheit durch Schwachstellentests ... 45
7.3 Nachweis der Angriffssicherheit durch Eindringungstests ... 46

8 Der Entwicklung nachgelagerte Lebenszyklusphasen ... 49
8.1 Schutz vor unberechtigtem Zugriff in der Produktion ... 49
8.2 Schutz vor unberechtigtem Zugriff in Betrieb und Instandhaltung ... 50
8.2.1 Feldbeobachtung ... 50
8.2.2 Reaktion of Cyber-Sicherheitsvorfälle ... 51
8.2.3 Software-Updates zur Behebung von Sicherheitslücken ... 52
8.3 Schutz vor unberechtigtem Zugriff bei Stilllegung ... 52

9 Zukünftige Herausforderungen ... 53
9.1 Co-Engineering von Funktionaler Sicherheit und Cybersecurity ... 53
9.2 Absicherung von „Softwareupdates over the air“ (SOTA) ... 54

Literatur ... 57