

Inhalt

1	Einführung	1
1.1	Motivation	1
1.2	Einordnung und Abgrenzung	4
2	Grundlagen zur API-Sicherheit	7
2.1	Begriffsbestimmung	7
2.1.1	Safety (Funktionssicherheit)	8
2.1.2	Security (Informationssicherheit)	9
2.1.3	Compliance (Einhaltung von Gesetzen, Regeln und Normen)	9
2.2	Stakeholder	9
2.2.1	API-Consumer	10
2.2.2	API-Provider	11
2.2.3	API-Broker / API-Manager	11
2.2.4	API-User	11
2.3	Angriffsvektoren	11
2.4	Zusammenfassung	13
3	Empirische Betrachtung des Forschungsgegenstands	15
3.1	Generische Empfehlungen	15
3.1.1	Firmenspezifische Aussagen zur API-Sicherheit	16
3.1.2	Branchenspezifische Ansätze zur API-Sicherheit	17
3.1.3	Empfehlungen unabhängiger Organisationen	19
3.2	Existierende empirische Analysen	21
3.2.1	Allgemeine Analysen – impliziter Themenbezug	21
3.2.2	Explizite Umfrage zum Thema API-Security	21
3.2.3	Spezialanalyse eingesetzter Sicherheitsmechanismen	24
3.3	Eigene Umfrage zur API-Sicherheit	26
3.3.1	Ziele und Konzeption der Umfrage	26
3.3.2	Detailergebnisse der Umfrage	28
3.3.3	Gewonnene Erkenntnisse	33
3.4	Zusammenfassung	34

4	API-Management.....	37
4.1	Aufgaben & Prozessbeteiligte.....	38
4.2	API-Lifecycle-Management.....	38
4.2.1	Provide API.....	39
4.2.2	Consume API.....	41
4.3	API-Gateway	41
4.4	API-Katalog.....	42
4.5	Zusammenfassung	43
5	Konstruktive Qualitätssicherung von APIs.....	45
5.1	Security Requirements.....	45
5.2	Security Design.....	46
5.2.1	Security Principles.....	46
5.2.2	Security Design Pattern	48
5.2.3	Bedrohungsmodellierung.....	49
5.2.4	Risikobewertung.....	52
5.2.5	Maßnahmen und Controls	54
5.3	Security Implementation	55
5.4	Authentifizierung und Autorisierung mit DLT	59
5.4.1	Funktionsweise der Blockchain	62
5.4.2	Verfügbare Frameworks	67
5.4.3	DLT-basierte Secure Web-APIs	68
5.5	Zusammenfassung	72
6	Analytische Qualitätssicherung von APIs.....	75
6.1	Testszenarien.....	75
6.1.1	Spoofing identity (Vortäuschen von Identitäten).....	76
6.1.2	Tampering with data (Datenmanipulation).....	77
6.1.3	Repudiation (Zurückweisen von korrekten Verbindungen).....	77
6.1.4	Information disclosure (Informationsabfluss)	78
6.1.5	Denial of service (Blockieren des Dienstes).....	79
6.1.6	Elevation of privilege (illegale Rechteerweiterung)	80
6.2	Testansätze	80

6.2.1	Authentifizierung und Autorisierung.....	80
6.2.2	Verschlüsselung.....	81
6.2.3	Rate Limitation.....	82
6.2.4	Denial of Service.....	82
6.2.5	Injection Test und Parameter Tempering /Fuzzing	83
6.3	Zusammenfassung.....	83
7	Betriebliche Qualitätssicherung	85
7.1	Bestandteile des Sicherheits-Managements von Web-APIs	86
7.1.1	Sicherheitsorganisation und Rollen	86
7.1.2	Sicherheitsziele	87
7.1.3	Sicherheitsstrategie	87
7.1.4	(Sicherheits-)Leitlinie	88
7.2	Sicherheitsmaßnahmen	88
7.2.1	Organisatorisch.....	89
7.2.2	Betrieblich	90
7.2.3	Technisch.....	90
7.3	Maßnahmenkatalog eines Secure Web-API-Managements.....	90
7.3.1	Organisatorische Sicherheitsmaßnahmen	91
7.3.2	Betriebliche Sicherheitsmaßnahmen	93
7.3.3	Technische Sicherheitsmaßnahmen.....	99
7.4	Zusammenfassung.....	105
8	Weiterführende Themenbereiche	107
8.1	Holistisches Secure Web-API-Management	107
8.2	Prototyp DLT – Secure Web-APIs.....	108
8.2.1	Anwendungsfall	108
8.2.2	Funktionsweise.....	108
8.2.3	Testbeispiel.....	110
8.3	Risiko- und Reifegradmodell für den Web-API Einsatz.....	111
8.4	Wechselwirkungen zu „Künstlicher Intelligenz“	111
9	Fazit zur Monografie	113
10	Literaturverzeichnis.....	115

11	Anhang	123
11.1	Weitere IAM Projekte mit DLT.....	123
11.2	Threat Modeling Report (Ausschnitt).....	128
11.3	Katalog betrieblicher Maßnahmen.....	131