Theorie der Cybersecurity

Modelle, Prinzipien und mathematische Grundlagen

Lucien Sina

Theorie der Cybersecurity

Modelle, Prinzipien und mathematische Grundlagen

Lucien Sina

26.7.2026

Inhaltsverzeichnis

1 Vorwort **1**

2 Einleitung **4**

I Das Sicherheitsmodell **8**

3 Was ist Cybersecurity **9**
3.1 Motivation: Sicherheit als Zustand? 9
3.2 Systemsicherhiet 13
3.3 Sicherheitsziele und deren Konflikte . . . 15
3.4 Dynamisches Gleichgewicht 17

4 Adversariale Systeme **19**
4.1 Das Konzept 19
4.2 Akteursmodelle 28
4.3 Zielkonflikte zwischen Akteuren 31
4.4 Ökonomie der Sicherheit 33
4.5 Sicherheit als Spiel 35

5 Modelle und Systemgrenzen **39**
5.1 Information als Ressource 39
5.2 Informationsflussmodelle 43
5.3 Systemgrenzen und Schnittstellen 46
5.4 Vertrauensgrenzen 49
5.5 Daten und Code 53

6 Schutzziele **57**
6.1 Die CIA-Triade 57
6.2 Authentizität 62
6.3 Nichtabstreitbarkeit 63
6.4 Privacy als Erweiterung 65
6.5 Sicherheit vs. Usability 68
6.6 Zielkonflikte in realen Systemen 71

7 Bedrohungsmodelle **75**
7.1 Was ist ein Bedrohungsmodell? 75
7.2 Annahmen über Angreifer 79
7.3 Annahmen über Verteidiger 83
7.4 Angriffsflächen als Konsequenz 86
7.5 Fehlerhafte Bedrohungsmodelle 91

8 Strategische Modelle **94**
8.1 Cybersecurity als Strategie 94
8.2 Grundbegriffe der Spieltheorie 97
8.2.1 Spiel 98
8.2.2 Spieler 99
8.2.3 Strategien 99
8.2.4 Auszahlungen (Nutzen und Kosten) 100
8.2.5 Spielrunden 101

8.3 Angreifer und Verteidiger 102
8.3.1 Strategien des Angreifers 103
8.3.2 Strategien des Verteidigers 104
8.3.3 Informationsasymmetrien 105
8.4 Nash-Gleichgewicht 107
8.4.1 Idee des Gleichgewichts 107
8.4.2 Warum perfekte Sicherheit selten existiert 109
8.4.3 Verteidigerasymmetrie 110
8.5 Dynamische Spiele 112
8.5.1 Anpassung von Strategien 113
8.5.2 Evolution von Angriff und Verteidigung 114
8.5.3 Sicherheit als permanenter Prozess 115

9 Informationstheorie 119
9.1 Informationssicherheit 119
9.2 Information und Unsicherheit 124
9.3 Informationsgehalt und Entropie 129
9.4 Redundanz als Chance und Risiko 135
9.5 Information und Adversarialität 141
9.6 Wahrscheinlichkeiten 147
9.7 Informationsgewinn des Angreifers 153
9.8 Informationsverlust des Verteidigers . . . 159
9.9 Informationstheoretische Grenzen der Sicherheit 166

II Mechanismen der Sicherheitsdurchset-

zung **174**

10 Zugriffskontrolle und Autorisierung **175**
10.1 Prinzipien der Zugriffskontrolle 175
10.2 ACLs und Capabilities 179
10.3 Least Privilege 183
10.4 Delegation und Rollenmodelle 187
10.5 Strategieausschluss 191
10.6 Grenzen von Zugriffskontrolle 194

11 Isolation und Systemgrenzen **197**
11.1 Isolation als Sicherheitsprinzip 197
11.2 Handlungseinschränkungen 201
11.2.1 Isolation als Einschränkung von Handlungsmöglichkeiten 202
11.2.2 Handlungsmöglichkeiten und Strategien 202
11.2.3 Systemgrenzen als spieltheoretische Barrieren 203
11.2.4 Architektur als Gestaltung des Spiels 204
11.3 Grenzen von Isolation 205

12 Identität, Authentizität und Vertrauen **209**
12.1 Was ist Identität im digitalen Raum? . . . 209
12.2 Authentifizierung vs. Autorisierung 213
12.3 Vertrauen als Systemannahme 216
12.4 Spoofing als Identitätsbruch 220
12.5 Phishing als Vertrauensangriff 223

III Implementierung von Sicherheitsmechanismen 227

13 Sichere Software und Programmiermodelle 228
13.1 Software als Realisierung von Sicherheitsmodellen 228
13.2 Implementierungssicherheit ist entscheidend 232
13.2.1 Abstraktion vs. Implementierung . 232
13.2.2 Fehlannahmen zwischen Design und Code 234
13.3 I. Modellgrenzen in Software 236
13.3.1 Daten und Code: Die zentrale Sicherheitsgrenze 236
13.3.2 Eingabeverarbeitung und Injection-Modelle 239
13.4 II. Laufzeit- und Systemverhalten 242
13.4.1 Speichersicherheit und Kontrollfluss 243
13.4.2 Fehlerklassen in sicherer Software . 248
13.5 III. Design- und Architekturfehler 253
13.5.1 Sichere Programmiermodelle . . . 254
13.5.2 Schnittstellen und API-Sicherheit . 262
13.5.3 Software als Angriffsfläche 266

IV Kryptographie als mathematische Sicherheitsbasis 270

14 Grundlagen der kryptographischen Sicherheit 271
14.1 Was ist Kryptografie? 272

14.2 Ausgangsproblem 275
14.3 Lösung: Ver- und Entschlüsselung 277
14.4 Kryptosysteme 279
14.4.1 Das mathematische Modell eines Kryptosystems 280
14.4.2 Chiffrier- und Dechiffrierfunktionen 281
14.4.3 Warum muss die Chiffrierfunktion injektiv sein? 281
14.4.4 Kryptosysteme im Modell der Cybersecurity 283
14.5 Kommunikation in Kryptosystemen . . . 284
14.6 Sicherheit durch Unwissenheit vs. Rechenaufwand 288
14.7 Perfect Secrecy (Shannon-Idee) 293
14.8 Computational Security 298
14.9 Reduktionen als Sicherheitsbeweise 302
14.10Angriffsmodelle in der Kryptographie . . . 307

15 Asymmetrische Kryptographie und Zahlentheorie 312
15.1 Idee öffentlicher und privater Schlüssel . . 313
15.2 Zahlentheoretische Grundlagen 317
15.3 Das RSA-Verfahren 321
15.4 Konzept und Funktion von RSA funktioniert325
15.4.1 Beweise 330
15.5 Auffinden großer Primzahlen 357
15.6 Grenzen und Annahmen der Sicherheit . . 363

16 Neue Rechenmodelle der Kryptographie 368
16.1 Warum Sicherheit vom Rechenmodell abhängt 369
16.2 Grenzen klassischer Sicherheitsannahmen 371
16.3 Quantencomputer 375
16.4 Wie ändern Quantencomputer die Kryptographie? 379
16.5 Der Shor-Algorithmus 384
16.6 Der Grover-Algorithmus 388
16.7 Quantenkryptographie 392
16.8 Post-Quantum-Kryptographie 396

17 Hashfunktionen und Integrität 409
17.1 Hashfunktionen als Kompressionsabbildung 410
17.2 Kollisionsresistenz 413
17.3 Anwendungen: Integrität und Signaturen . 417
17.4 Sicherheitsmodelle für Hashfunktionen . . 421
17.5 Struktur statt Algorithmus 425

18 Digitale Signaturen 429
18.1 Signaturen als Nachweis der Authentizität 430
18.2 Message Authentication Codes 433
18.3 Public Key Infrastructures 437
18.4 Vertrauen in Dritte 440
18.5 Skalierung von Vertrauen 443

19 Erweiterte kryptographische Konstrukte 447
19.1 Zero-Knowledge 448
19.2 Commitment Schemes 452
19.3 Protokollbasierte Sicherheit 456

19.4 Zusammensetzung von Sicherheit 459

V Information Hiding und verdeckte Kommunikation 464

20 Information Hiding als Sicherheitsprinzip 465
20.1 Verbergen als Sicherheitsmechanismus . . 466
20.2 Steganographie 470
20.3 Watermarking 476
20.4 Covert Channels 480
20.5 Nebenkanäle (Side Channels) 486

VI Angriffe als Verletzung von Modellen 491

21 Allgemeine Angriffsprinzipien 492
21.1 Angriff als Modellverletzung 494
21.2 Klassifikation von Angriffen 499
21.3 Wirtschaftlichkeit von Angriffen 504
21.4 Automatisierung von Angriffen 509

22 Technische Angriffe (konzeptionell erklärt) 515
22.1 Abhören von Kommunikation (Sniffing) . 516
22.2 Identitätsfälschung (Spoofing) 520
22.3 Injection-Angriffe (Code/Data Trennung) 524
22.4 Speicherfehler und Kontrollfluss (Buffer Overflow) 529
22.5 Social Engineering (Phishing) 533

23 Kryptographische Angriffe **539**
23.1 Brute Force als universeller Angriff 540
23.2 Strukturangriffe (Kryptoanalyse) 544
23.3 Angriff auf mathematische Sicherheit . . . 549
23.4 Angriffe auf Implementierungen 554
23.5 Side-Channel-Angriffe 559

VII Verteidigung und Systemdesign **565**

24 Sicherheitsarchitekturen **566**
24.1 Defense in Depth 567
24.2 Least Privilege 571
24.3 Zero Trust 576
24.4 Redundanz und Fehlertoleranz 582
24.5 Design für Unsicherheit 588

25 Organisation und menschliche Faktoren **595**
25.1 Sicherheitsprozesse 596
25.2 Der Mensch als Teil des Systems 601
25.3 Fehler, Täuschung und Verhalten 607
25.4 Sicherheitskultur 613
25.5 Compliance vs. reale Sicherheit 619

26 Fallstudien und Szenarien **626**
26.1 Reale Sicherheitsvorfälle 627
26.2 Fiktive Angriffsszenarien 632
26.3 Analyse im Modellrahmen 638
26.4 Lehren aus Systemversagen 644

VIII Ausblick **651**

27 Zukunft der Cybersecurity **652**
27.1 KI und autonome Angriffe 653
27.2 Fortschritt und Paradigmenwechsel 658
27.3 Komplexität moderner Systeme 665
27.4 Sicherheit als permanenter Prozess 672

28 KI-Sicherheit **678**
28.1 KI als Sicherheitsproblem 678
28.2 KI als Akteur in adversarialen Systemen . 684
28.3 Zielfunktionen und Optimierungsprobleme 690
28.4 Zielkonflikte und Alignment 696
28.5 Informationsasymmetrien zwischen Mensch und KI 702
28.6 Autonomie und strategisches Verhalten . . 708
28.7 Manipulation von KI-Systemen 712
28.8 Verifikation, Kontrolle und Begrenzung . . 718
28.9 Sicherheit zukünftiger KI-Systeme 724

IX Übungen und Lösungen **731**

29 Aufgaben **732**
29.1 Das Sicherheitsmodell 732
29.2 Mechanismen der Sicherheitsdurchsetzung 737
29.3 Implementierung von Sicherheitsmechanismen 742
29.4 Kryptographie 749
29.5 Information Hiding 759

29.6 Angriffe 761
29.7 Verteidigung und Systemdesign 767
29.8 Die Zukunft 772

30 Abschließende Worte **778**
30.1 Zusammenfassung 778
30.2 Private und unternehmerische Sicherheit . 784
30.3 Die Kernbotschaft dieses Buches 788
30.4 Buchempfehlungen 791
30.5 Dank 794

Kapitel 1

Vorwort

Cybersecurity gehört heute zu den zentralen Herausforderungen der Informatik. Nahezu alle Bereiche unseres gesellschaftlichen, wirtschaftlichen und privaten Lebens basieren auf digitalen Informationssystemen. Kommunikation, Finanzwesen, Industrie, Verwaltung, Wissenschaft und Medizin sind auf ihre Verfügbarkeit, Vertrauenswürdigkeit und Sicherheit angewiesen. Gleichzeitig entstehen durch neue Technologien nicht nur leistungsfähigere Möglichkeiten zur Verarbeitung von Informationen, sondern auch neue Angriffsmöglichkeiten. Sicherheitsannahmen verändern sich kontinuierlich. Dennoch besitzen viele grundlegende Prinzipien der Cybersecurity eine bemerkenswerte Beständigkeit: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Vertrauen bleiben zentrale Schutzziele unabhängig davon, welche konkreten Technologien eingesetzt werden. Dieses Buch verfolgt daher

einen bewusst modellorientierten Ansatz. Cybersecurity wird nicht primär als Sammlung einzelner Werkzeuge oder Verfahren betrachtet, sondern als wissenschaftliche Disziplin, die auf Modellen, mathematischen Grundlagen und algorithmischen Prinzipien beruht. Ausgangspunkt ist die Frage, was Sicherheit innerhalb adversarialer Systeme bedeutet. Unterschiedliche Akteure verfolgen eigene Ziele, besitzen unterschiedliche Fähigkeiten und beeinflussen sich gegenseitig. Aus dieser Perspektive entstehen die grundlegenden Konzepte des Buches: Sicherheitsziele, Bedrohungsmodelle, Informationsflüsse, Vertrauensgrenzen und Sicherheitsmechanismen. Darauf aufbauend werden Zugriffskontrolle, Isolation, Authentifizierung, sichere Softwareentwicklung und kryptographische Verfahren als unterschiedliche Antworten auf gemeinsame Sicherheitsprobleme betrachtet. Besonderer Wert liegt dabei auf der Verbindung von systemtheoretischen, mathematischen und algorithmischen Sichtweisen. Kryptographie wird nicht nur als Anwendung fertiger Verfahren behandelt, sondern aus ihren mathematischen Grundlagen heraus entwickelt. Das Buch richtet sich insbesondere an Studierende der Informatik, Cybersicherheit, Mathematik und verwandter Fachrichtungen sowie an interessierte Praktiker, die Cybersecurity nicht nur anwenden, sondern in ihren theoretischen Grundlagen verstehen möchten. Grundlegende Kenntnisse der Informatik und Mathematik werden vorausgesetzt; die für das Verständnis wesentlichen Konzepte werden jedoch systematisch eingeführt. Definitionen, Prinzipien, mathematische Herleitungen,

Beispiele, Fallstudien und Aufgaben mit ausführlichen Musterlösungen unterstützen dabei ein aktives Verständnis der behandelten Inhalte. Ziel ist nicht nur die Vermittlung aktueller Verfahren, sondern die Entwicklung eines dauerhaften Verständnisses, das auch dann Bestand hat, wenn sich Technologien, Programmiersprachen oder Angriffsmethoden verändern. Der Titel *Theorie der Cybersecurity* wurde bewusst gewählt. Dieses Buch versteht Cybersecurity als eine zusammenhängende Theorie sicherer Informationssysteme, die Modellbildung, Mathematik, Algorithmik, Kryptographie, Systemdesign und organisatorische Aspekte miteinander verbindet. Wer diese grundlegenden Zusammenhänge versteht, besitzt nicht nur Kenntnisse über heutige Sicherheitsmechanismen, sondern auch eine Grundlage, um zukünftige Entwicklungen systematisch einordnen und bewerten zu können.

Ich wünsche Ihnen Freude beim Lesen, Neugier beim Hinterfragen der Modelle und Erfolg beim Entdecken der theoretischen Grundlagen einer Disziplin, deren Bedeutung in den kommenden Jahrzehnten weiter zunehmen wird.

Kapitel 2

Einleitung

Cybersecurity wird in der Praxis häufig als eine Sammlung technischer Maßnahmen verstanden: Firewalls, Verschlüsselung, Authentifizierungsverfahren, Sicherheitsupdates oder Anti-Malware-Software. Diese Sichtweise ist verständlich, aber zu eng. Sie reduziert Sicherheit auf Werkzeuge und konkrete Technologien, die sich im Laufe der Zeit verändern und ersetzen lassen. Dieses Buch verfolgt einen anderen Ansatz.

Cybersecurity ist die Kontrolle über Informationszugriff in einem adversarialen Systemmodell.

Diese Definition ist bewusst abstrakt gewählt. Sie verschiebt den Fokus weg von einzelnen Technologien hin zu einem grundlegenden Modell: Systeme, in denen mehrere Akteure mit unterschiedlichen und teilweise widersprüchlichen Zielen auf dieselbe Informationsbasis zugreifen, interagieren und miteinander konkurrieren. Sicherheit

entsteht in diesem Modell nicht durch ein einzelnes Werkzeug, sondern durch die Struktur des Systems selbst: durch die Art, wie Informationen fließen, wie Zugriffe geregelt werden, wie Vertrauen modelliert wird und wie gut ein System auf gezielte Störungen vorbereitet ist. Das zentrale Merkmal eines solchen Systems ist seine **Adversarialität**. Das bedeutet, dass mindestens ein Akteur existiert, der aktiv versucht, die Sicherheitsziele des Systems zu unterlaufen. Gleichzeitig existieren Verteidiger, deren Aufgabe es ist, diese Ziele unter realen Randbedingungen durchzusetzen. Hinzu kommen weitere Beteiligte wie Nutzer, Betreiber oder regulatorische Instanzen, die eigene Optimierungsziele verfolgen, etwa Benutzerfreundlichkeit, Kostenreduktion oder rechtliche Konformität. Cybersecurity ist daher kein statischer Zustand, sondern ein **dynamisches Gleichgewicht konkurrierender Interessen**. Aus dieser Perspektive ergeben sich vier fundamentale Ebenen, die dieses Buch strukturieren:

- **Prinzipien der Cybersecurity:** Abstrakte, zeitlose Grundlagen wie Sicherheitsziele, Bedrohungsmodelle, Informationsflüsse und Vertrauensgrenzen.
- **Mechanismen und Methoden:** Konkrete technische und konzeptionelle Verfahren zur Durchsetzung von Sicherheit, etwa Zugriffskontrolle, Isolation und kryptographische Verfahren.
- **Mathematische Fundierung:** Die formalen Grundlagen sicherheitskritischer Verfahren, insbe-

sondere der Kryptographie, einschließlich zahlentheoretischer Strukturen wie bei RSA.

- **Anwendungen und Narrative:** Reale und fiktive Angriffs- und Abwehrszenarien, die zeigen, wie die abstrakten Modelle in konkreten Systemen verletzt oder durchgesetzt werden.

Darüber hinaus behandelt das Buch zwei Erweiterungen, die in modernen Sicherheitsmodellen eine zentrale Rolle spielen:

- **Information Hiding:** Die Kontrolle nicht nur über den Zugriff auf Informationen, sondern auch über deren Sichtbarkeit und Wahrnehmbarkeit. Dazu gehören Steganographie, Side Channels und verdeckte Kommunikationskanäle.
- **Quantenkryptographie und neue Rechenmodelle:** Eine Erweiterung der klassischen kryptographischen Annahmen durch physikalisch motivierte Modelle, die insbesondere die Grundlagen der Sicherheit in zukünftigen Systemen betreffen.

Die Struktur des Buches ist so aufgebaut, dass diese Ebenen nicht isoliert behandelt werden, sondern aufeinander aufbauen. Die grundlegenden Prinzipien bilden das Fundament. Darauf aufbauend werden Mechanismen entwickelt, die diese Prinzipien umsetzen. Die mathematischen Kapitel liefern die formale Absicherung zentraler Verfahren der Kryptographie. Schließlich werden

diese Konzepte in realen und narrativen Szenarien sichtbar gemacht. Das Ziel dieses Buches ist es nicht, eine vollständige Sammlung aktueller Sicherheitstechnologien bereitzustellen. Stattdessen soll ein dauerhaft gültiges Verständnis entstehen, das unabhängig von konkreten Produkten, Implementierungen oder technischen Trends funktioniert. Der Einstieg erfolgt daher bewusst auf einer abstrakten Ebene.

Teil I

Das Sicherheitsmodell

Kapitel 3

Was ist Cybersecurity

3.1 Motivation: Sicherheit als Zustand?

Cybersecurity wird im Alltag häufig als ein erreichbarer Zustand verstanden: ein System ist *sicher*, wenn bestimmte Schutzmaßnahmen implementiert wurden, und *unsicher*, wenn diese fehlen. Diese Sichtweise ist intuitiv, aber unvollständig. In realen Systemen ist Sicherheit kein stabiler Endpunkt, sondern eine Eigenschaft, die sich kontinuierlich unter wechselnden Bedingungen verändert. Systeme entwickeln sich weiter, Bedrohungen passen sich an, und auch die Nutzungskontexte verändern sich dynamisch. Sicherheit ist daher kein Zustand, sondern ein fortlaufender Prozess in einem Umfeld konkurrierender Interessen. Aus dieser Perspektive betrachtet, existiert kein absolut sicheres System im praktischen Sinne. Stattdessen

bewegen sich Systeme in einem Spannungsfeld aus Schutzmaßnahmen, Ressourcenbeschränkungen, Fehlannahmen und aktivem Gegenverhalten. Jede Sicherheitsmaßnahme verschiebt dieses Gleichgewicht, beseitigt es jedoch nicht endgültig. Ein zentrales Missverständnis vieler traditionellen Betrachtungen ist die Vorstellung, dass Sicherheit ausschließlich durch das Hinzufügen technischer Kontrollen erreicht werden könne. Tatsächlich entstehen Sicherheitsniveaus jedoch erst durch das Zusammenspiel von Systemstruktur, Implementierung, Nutzung und adversarialem Verhalten. Damit wird Cybersecurity zu einer Eigenschaft von **interagierenden Systemen**, nicht von isolierten Komponenten. Im Zentrum dieser Betrachtung steht ein grundlegendes Modell:

Prinzip 1 (Leitprinzip 1). Cybersecurity ist die Kontrolle über Informationszugriffe innerhalb eines adversarialen Systems.

Dieses Modell enthält drei wesentliche Elemente:

- **Information** als zentrale Ressource, deren Zugriff, Sichtbarkeit und Integrität gesteuert werden muss.
- **Systeme** als Strukturen, die Informationsflüsse ermöglichen, begrenzen oder transformieren.
- **Akteure** als rationale oder teilweise rationale Entitäten, die mit unterschiedlichen Zielen auf diese Informationen zugreifen.

Das Adversariale im Modell bedeutet, dass mindestens ein Akteur existiert, der aktiv versucht, die Sicherheits-

ziele des Systems zu unterlaufen. Gleichzeitig existieren Verteidiger, deren Aufgabe es ist, diese Ziele unter realen Randbedingungen durchzusetzen. Beide Seiten agieren dabei nicht statisch, sondern reagieren aufeinander und optimieren ihre Strategien innerhalb gegebener Beschränkungen. Wichtig ist dabei, dass auch Verteidiger als rationale Akteure betrachtet werden müssen. Sie optimieren nicht nur Sicherheit im abstrakten Sinn, sondern bewegen sich innerhalb von Zielkonflikten wie Kosten, Komplexität, Benutzerfreundlichkeit und Systemleistung. Ebenso sind weitere Akteure wie Nutzer, Betreiber oder regulatorische Instanzen Teil dieses Systems und beeinflussen dessen Sicherheitszustand indirekt. Damit wird Cybersecurity nicht als binäres Merkmal („sicher“ oder „unsicher“) verstanden, sondern als dynamisches Gleichgewicht konkurrierender Optimierungsprozesse. Im weiteren Verlauf des Buches wird dieses Grundmodell schrittweise erweitert. Zunächst werden die grundlegenden Prinzipien eingeführt, auf denen Sicherheitsmodelle basieren. Darauf aufbauend werden Mechanismen betrachtet, mit denen diese Prinzipien in realen Systemen umgesetzt werden. Anschließend folgt eine mathematische Fundierung zentraler kryptographischer Verfahren, bevor diese Konzepte in praktischen Angriffen und Abwehrstrategien sichtbar gemacht werden. Die Struktur des Buches folgt dabei vier zentralen Ebenen:

- **Prinzipien der Cybersecurity:** Zeitlose Grundlagen wie Sicherheitsziele, Bedrohungsmodelle und Informationsflüsse.

- **Mechanismen und Methoden:** Technische und konzeptionelle Verfahren zur Durchsetzung von Sicherheit, insbesondere Zugriffskontrolle, Isolation und Kryptographie.
- **Mathematische Fundierung:** Formale Grundlagen sicherheitskritischer Verfahren, insbesondere der Kryptographie und Zahlentheorie.
- **Anwendungen und Narrative:** Reale und fiktive Szenarien, in denen Sicherheitsmodelle verletzt oder durchgesetzt werden.

Ergänzend dazu behandelt das Buch zwei erweiternde Perspektiven, die für moderne Sicherheitssysteme zunehmend relevant sind:

- **Information Hiding:** Verfahren zur Kontrolle nicht nur des Zugriffs auf Informationen, sondern auch ihrer Sichtbarkeit und indirekten Übertragungswege.
- **Quantenkryptographie:** Erweiterungen klassischer kryptographischer Annahmen durch physikalisch motivierte Rechen- und Kommunikationsmodelle.

Ziel dieses Buches ist es, kein rein technisches Nachschlagewerk zu sein, sondern ein strukturiertes Verständnis von Cybersecurity als System- und Modellproblem zu vermitteln. Dieses Verständnis soll unabhängig von

konkreten Technologien gültig bleiben und auf zukünftige Entwicklungen übertragbar sein.

3.2 Systemsicherhiet

Sicherheit wird häufig als Eigenschaft einzelner Komponenten verstanden: eine Software ist sicher, ein Protokoll ist sicher oder ein Gerät ist sicher. Diese Sichtweise ist jedoch nur eingeschränkt tragfähig. In realen Umgebungen entsteht Sicherheit nicht durch isolierte Eigenschaften einzelner Teile, sondern durch das Zusammenspiel eines gesamten Systems. Ein System im Sinne der Informationssicherheit umfasst nicht nur Software und Hardware, sondern auch Benutzer, Kommunikationskanäle, organisatorische Prozesse und externe Schnittstellen. Sicherheit ist daher keine Eigenschaft eines einzelnen Elements, sondern eine Eigenschaft der **Interaktion zwischen diesen Elementen**. Formal betrachtet entsteht Sicherheit erst dann, wenn eine Menge von Sicherheitszielen unter allen relevanten Systemzuständen und Interaktionen eingehalten wird. Diese Zustände sind jedoch nicht statisch. Systeme verändern sich durch Updates, Nutzerverhalten, neue Anforderungen und externe Einflüsse. Dadurch ist Sicherheit stets kontextabhängig und zeitlich variabel. Ein zentrales Problem besteht darin, dass die lokale Sicherheit eines Teilsystems nicht notwendigerweise zur globalen Sicherheit des Gesamtsystems führt. Ein sicher konfigurierter Dienst kann beispielsweise in Kombination mit anderen Diensten neue Angriffsflächen

erzeugen. Ebenso kann eine sichere Komponente durch fehlerhafte Integration in ein unsicheres Gesamtsystem kompromittiert werden. Damit wird deutlich, dass Sicherheit nicht modular im Sinne einer einfachen Komposition verstanden werden kann. Stattdessen handelt es sich um eine systemische Eigenschaft, die aus der Struktur der Verbindungen, Abhängigkeiten und Informationsflüsse entsteht. Ein wichtiger Aspekt ist die Abhängigkeit von Annahmen. Jede Sicherheitsgarantie basiert auf expliziten oder impliziten Voraussetzungen über das Verhalten anderer Systemteile, über die Integrität der Umgebung und über das Verhalten potentieller Angreifer. Sobald diese Annahmen verletzt werden, kann eine zuvor gültige Sicherheitseigenschaft ihre Gültigkeit verlieren. Daher ist Sicherheit keine absolute Eigenschaft, sondern eine **relationale Eigenschaft eines Systems unter definierten Annahmen**. Sie hängt sowohl von der Systemarchitektur als auch von der Korrektheit der zugrunde liegenden Modelle ab. Im weiteren Verlauf wird dieses Verständnis erweitert, indem Sicherheitsziele formalisiert und ihre inhärenten Konflikte untersucht werden. Darauf aufbauend wird gezeigt, warum Sicherheit stets in einem dynamischen Gleichgewicht zwischen konkurrierenden Anforderungen und Akteuren entsteht.

3.3 Sicherheitsziele und deren Konflikte

Sicherheitsziele beschreiben die Eigenschaften, die ein System erfüllen soll, um als sicher zu gelten. In der klassischen Betrachtung werden diese Ziele häufig als feste Anforderungen formuliert. In realen Systemen zeigen sich jedoch grundlegende Spannungen zwischen diesen Zielen, sodass sie nicht gleichzeitig in maximaler Ausprägung erfüllt werden können. Die bekanntesten grundlegenden Sicherheitsziele lassen sich in der sogenannten CIA-Triade zusammenfassen:

- **Vertraulichkeit (Confidentiality):** Informationen sollen nur autorisierten Akteuren zugänglich sein.
- **Integrität (Integrity):** Informationen sollen nicht unbemerkt verändert werden können.
- **Verfügbarkeit (Availability):** Systeme und Informationen sollen bei Bedarf zugänglich sein.

Diese drei Ziele bilden jedoch keine unabhängigen Dimensionen. Vielmehr stehen sie in einem systematischen Spannungsverhältnis. Maßnahmen zur Erhöhung eines Ziels können andere Ziele beeinträchtigen. Beispielsweise kann eine starke Erhöhung der Vertraulichkeit durch strikte Zugriffsbeschränkungen die Verfügbarkeit reduzieren. Umgekehrt kann eine hohe Verfügbarkeit durch redundante und offene Zugriffsstrukturen die Angriffsfläche

vergrößern und damit die Vertraulichkeit und Integrität gefährden. Neben der CIA-Triade existieren weitere Sicherheitsziele, die insbesondere in modernen Systemen an Bedeutung gewinnen:

- **Authentizität:** Die Echtheit von Informationen und Kommunikationspartnern muss gewährleistet sein.
- **Nichtabstreitbarkeit (Non-Repudiation):** Eine Handlung oder Kommunikation kann später nicht plausibel bestritten werden.
- **Privatsphäre:** Kontrolle darüber, welche Informationen über ein Subjekt gesammelt, verarbeitet oder weitergegeben werden.

Auch diese erweiterten Ziele stehen in Wechselwirkung mit den grundlegenden Zielen. Beispielsweise kann eine stärkere Anonymisierung die Rückverfolgbarkeit reduzieren und damit die Nichtabstreitbarkeit beeinträchtigen. Ebenso können Mechanismen zur Verbesserung der Authentizität zusätzliche Datenverarbeitung erfordern, was wiederum Datenschutzaspekte beeinflusst. Ein zentrales Merkmal von Sicherheitszielen ist daher ihre **Unvereinbarkeit in maximaler Form**. Sicherheit ist kein Optimierungsproblem mit einer eindeutigen globalen Lösung, sondern ein Mehrzielproblem mit inhärenten Zielkonflikten. Diese Zielkonflikte sind nicht nur theoretischer Natur, sondern ergeben sich unmittelbar aus der Struktur realer Systeme. Ressourcenbeschränkungen,

Benutzerfreundlichkeit, technische Komplexität und organisatorische Anforderungen verstärken diese Spannungen zusätzlich. Im weiteren Verlauf wird daher betrachtet, wie Sicherheit nicht als statische Optimierung dieser Ziele verstanden werden kann, sondern als ein dynamisches Gleichgewicht, in dem diese Ziele kontinuierlich gegeneinander abgewogen werden müssen.

3.4 Dynamisches Gleichgewicht

Sicherheit in realen Systemen ist kein statischer Zustand, sondern ein fortlaufender Prozess. Systeme verändern sich, Bedrohungen entwickeln sich weiter, und auch die Anforderungen der Nutzer und Betreiber unterliegen kontinuierlichen Anpassungen. Dadurch entsteht ein permanentes Wechselspiel zwischen Schutzmaßnahmen und Angriffsmöglichkeiten. Dieses Wechselspiel lässt sich nicht als einmalige Optimierungsaufgabe verstehen, sondern als ein dynamisches Gleichgewicht. Jede Veränderung auf der einen Seite des Systems erzeugt Reaktionen auf der anderen Seite. Wird beispielsweise eine Sicherheitsmaßnahme verbessert, kann dies Angreifer dazu veranlassen, neue Strategien zu entwickeln oder alternative Schwachstellen auszunutzen. Umgekehrt zwingt ein erfolgreicher Angriff häufig zu einer Anpassung der Verteidigungsstrategien. Dieses Prinzip gilt sowohl auf technischer als auch auf organisatorischer Ebene. Neue Software-Patches, geänderte Sicherheitsrichtlinien oder verbesserte kryptographische Verfahren verschieben das Gleichgewicht, beseitigen je-

doch nicht die zugrunde liegende Dynamik. Sicherheit ist daher immer ein Zustand temporärer Stabilität innerhalb eines sich ständig verändernden Systems. Ein weiterer wichtiger Aspekt dieses Gleichgewichts ist die Rolle konkurrierender Ziele. Sicherheitsmaßnahmen werden nicht isoliert betrachtet, sondern müssen stets mit Anforderungen wie Effizienz, Benutzerfreundlichkeit, Skalierbarkeit und Kosten in Einklang gebracht werden. Diese konkurrierenden Anforderungen führen dazu, dass Sicherheit nie maximal, sondern nur angemessen im jeweiligen Kontext realisiert werden kann. Damit wird deutlich, dass Cybersecurity nicht als Ziel mit endgültiger Lösung verstanden werden kann, sondern als kontinuierlicher Anpassungsprozess zwischen mehreren rational handelnden Akteuren und sich verändernden Systembedingungen.

Kapitel 4

Adversariale Systeme

4.1 Das Konzept

Im vorherigen Kapitel wurde Cybersecurity als Eigenschaft von Systemen beschrieben, die sich aus der Kontrolle von Informationszugriffen unter sich ständig verändernden Bedingungen ergibt. Dabei wurde insbesondere deutlich, dass Sicherheit kein statischer Zustand ist, sondern als dynamisches Gleichgewicht zwischen konkurrierenden Anforderungen und sich gegenseitig beeinflussenden Akteuren verstanden werden muss. Diese Perspektive führt zu einer grundlegenden Einsicht: Reale Informationssysteme bestehen nicht aus ausschließlich kooperierenden Komponenten. Stattdessen existieren unterschiedliche Akteure, deren Ziele nicht nur voneinander abweichen, sondern sich teilweise direkt widersprechen können. Während einige Akteure den Schutz, die Integrität und die

Verfügbarkeit von Informationen sicherstellen wollen, verfolgen andere Akteure das Ziel, genau diese Eigenschaften zu verletzen, zu umgehen oder gezielt auszunutzen. Damit unterscheidet sich Cybersecurity fundamental von klassischen Teilgebieten der Informatik, in denen häufig angenommen wird, dass alle Komponenten eines Systems entsprechend ihrer Spezifikation korrekt und kooperativ arbeiten. In der Sicherheitsbetrachtung genügt diese Annahme nicht. Vielmehr muss zusätzlich berücksichtigt werden, dass einzelne Akteure bewusst gegen die intendierte Funktionsweise eines Systems handeln können. Aus diesem Grund reicht es nicht aus, Systeme ausschließlich hinsichtlich ihrer korrekten Funktionalität zu analysieren. Entscheidend ist vielmehr, wie sich Systeme unter Bedingungen verhalten, in denen einzelne Akteure aktiv versuchen, ihre Sicherheitsziele zu verletzen. Diese Perspektive führt zum Begriff des adversarialen Systems. Der Begriff *adversarial* leitet sich vom englischen Wort *adversary* (Gegner) ab und beschreibt Systeme, in denen Konkurrenz, Täuschung, Manipulation oder gezielte Gegenmaßnahmen integrale Bestandteile des Systemverhaltens sind. Die grundlegende Idee lässt sich in einer formalen Definition zusammenfassen.

Definition 1 (Adversariales System)**.** *Ein adversariales System ist ein System, in dem mehrere Akteure auf gemeinsame Ressourcen einwirken, unterschiedliche oder gegensätzliche Ziele verfolgen und mindestens ein Akteur aktiv versucht, die Sicherheitsziele eines anderen Akteurs zu beeinträchtigen, zu umgehen oder zu verletzen.*

Diese Definition ist bewusst abstrakt und technologieunabhängig formuliert. Sie gilt unabhängig davon, ob es sich um einzelne Rechner, verteilte Systeme, Unternehmensnetzwerke, Cloud-Infrastrukturen oder kryptographische Protokolle handelt. Entscheidend ist nicht die konkrete technische Realisierung, sondern die strukturelle Eigenschaft, dass mehrere Akteure mit unterschiedlichen Interessen innerhalb desselben Systems agieren. Aus dieser Definition ergeben sich mehrere zentrale Konsequenzen, die für das weitere Verständnis von Cybersecurity grundlegend sind. Erstens kann Sicherheit niemals isoliert betrachtet werden. Die Bewertung der Sicherheit eines Systems hängt stets davon ab, welche Akteure berücksichtigt werden, welche Ressourcen geschützt werden sollen und welche Fähigkeiten diesen Akteuren zugeschrieben werden. Sicherheit ist somit immer relativ zu einem bestimmten Modell der beteiligten Akteure. Zweitens besitzt Sicherheit keinen absoluten Charakter. Aussagen über Sicherheit sind grundsätzlich an ein zugrunde liegendes Bedrohungsmodell gebunden. Wird dieses Modell verändert – beispielsweise durch stärkere Angreifer, zusätzliche Angriffsvektoren oder neue Systemannahmen – kann sich die Bewertung der Sicherheit eines Systems vollständig ändern, ohne dass sich das System selbst verändert hat. Drittens entsteht Sicherheit nicht ausschließlich durch technische Mechanismen. Ebenso relevant sind organisatorische, wirtschaftliche und menschliche Faktoren. Auch diese beeinflussen das Verhalten der Akteure innerhalb des adversarialen Systems und damit die tatsächliche

Sicherheit eines Systems im praktischen Betrieb. Das adversariale Systemmodell bildet damit den konzeptionellen Ausgangspunkt des gesamten weiteren Buches. Es erlaubt, sehr unterschiedliche Sicherheitsprobleme innerhalb eines einheitlichen Rahmens zu beschreiben und zu analysieren. Kryptographische Verfahren, Zugriffskontrollmechanismen, Sicherheitsarchitekturen oder auch Angriffe lassen sich alle als unterschiedliche Erscheinungsformen derselben Grundstruktur verstehen: der Interaktion mehrerer Akteure innerhalb eines gemeinsamen Systems unter konfligierenden Zielen.

Leitprinzip der Cybersecurity

Die Einführung des adversarialen Systemmodells erlaubt es, Cybersecurity nicht mehr als Sammlung isolierter technischer Verfahren zu betrachten, sondern als einheitliches konzeptionelles Problem. Aus diesem Modell ergibt sich ein grundlegendes Leitprinzip, das im weiteren Verlauf des gesamten Buches als Referenzpunkt dient.

Prinzip 2 (Zentraler Modellansatz der Cybersecurity). Cybersecurity wird in diesem Buch als Kontrolle über Informationszugriffe innerhalb eines adversarialen Systems verstanden.

Dieses Leitprinzip fasst die zentrale Idee des Buches in einer kompakten Form zusammen. Es betont zwei wesentliche Aspekte: Zum einen steht nicht die Technik im Vordergrund, sondern der Zugriff auf Informationen. Zum anderen wird Sicherheit stets innerhalb eines adver-

sarialen Kontextes betrachtet, in dem mehrere Akteure mit unterschiedlichen Zielen interagieren. Alle späteren Kapitel lassen sich auf dieses Leitprinzip zurückführen. Kryptographische Verfahren regulieren den Zugriff auf Informationen unter adversarialen Bedingungen. Zugriffskontrollmechanismen beschränken die Handlungsoptionen einzelner Akteure. Sicherheitsarchitekturen strukturieren den Informationsfluss innerhalb des Systems. Selbst Angriffe lassen sich als Versuche interpretieren, diese Kontrolle über Informationszugriffe zu unterlaufen. Um dieses Modell präzise anwenden zu können, ist eine gemeinsame Sprache erforderlich. Daher werden im Folgenden die grundlegenden Begriffe definiert, die im gesamten Buch verwendet werden.

Modellvokabular

Die folgenden Definitionen bilden das formale Grundvokabular dieses Buches. Sie sind bewusst allgemein gehalten, um eine einheitliche Beschreibung unterschiedlicher Sicherheitssysteme zu ermöglichen.

Grundobjekte des Modells

Definition 2 (System)**.** *Ein System ist eine Menge miteinander interagierender Komponenten, die gemeinsam Informationen verarbeiten, speichern oder übertragen.*

Definition 3 (Akteur)**.** *Ein Akteur ist eine Entität, die innerhalb eines Systems handelt und dabei bestimmte Ziele*

verfolgt. Akteure können Menschen, Software, Hardware oder organisatorische Einheiten sein.

Definition 4 (Ressource)**.** *Eine Ressource ist ein Objekt innerhalb eines Systems, das geschützt, genutzt oder verwaltet werden soll. Typische Beispiele sind Informationen, Rechenleistung, Kommunikationskanäle oder kryptographische Schlüssel.*

Sicherheitsbezogene Begriffe

Definition 5 (Sicherheitsziel)**.** *Ein Sicherheitsziel ist eine gewünschte Eigenschaft eines Systems oder einer Ressource. Typische Beispiele sind Vertraulichkeit, Integrität und Verfügbarkeit.*

Definition 6 (Angriffsfläche)**.** *Die Angriffsfläche eines Systems ist die Gesamtheit aller Schnittstellen und Eigenschaften eines Systems, über die Sicherheitsziele verletzt oder beeinträchtigt werden können.*

Definition 7 (Vertrauensgrenze)**.** *Eine Vertrauensgrenze ist eine konzeptionelle Grenze zwischen Bereichen eines Systems, für die unterschiedliche Annahmen über die Vertrauenswürdigkeit der beteiligten Akteure gelten. Der Übergang über eine solche Grenze erfordert geeignete Sicherheitsmechanismen.*

Modellannahmen und Mechanismen

Definition 8 (Bedrohungsmodell)**.** *Ein Bedrohungsmodell umfasst sämtliche Annahmen über die Fähigkeiten,*

Ziele und Handlungsmöglichkeiten potentieller Angreifer sowie die Struktur der zu schützenden Ressourcen.

Definition 9 (Sicherheitsmechanismus)**.** *Ein Sicherheitsmechanismus ist ein Verfahren oder eine technische beziehungsweise organisatorische Maßnahme, die darauf abzielt, Sicherheitsziele innerhalb eines adversarialen Systems durchzusetzen oder zu unterstützen.*

Diese Begriffe bilden gemeinsam die formale Sprache des adversarialen Systemmodells. Sie ermöglichen es, sehr unterschiedliche Sicherheitsprobleme in einer einheitlichen Struktur zu beschreiben und miteinander zu vergleichen.

Das adversariale Systemmodell als universeller Betrachtungsrahmen

Das im bisherigen Kapitel entwickelte Modell ist nicht nur eine abstrakte Definition, sondern ein allgemeiner Rahmen zur Beschreibung nahezu aller sicherheitsrelevanten Aspekte moderner Informationssysteme. In den folgenden Kapiteln wird sich zeigen, dass sich eine Vielzahl scheinbar unterschiedlicher Konzepte auf dieses Modell zurückführen lässt. So lässt sich **Kryptographie** als Mechanismus zur Kontrolle des Informationszugriffs innerhalb eines adversarialen Systems interpretieren. Der zentrale Zweck kryptographischer Verfahren besteht darin, Informationen so zu transformieren, dass sie nur für bestimmte Akteure zugänglich oder nutzbar sind, selbst wenn andere Akteure Zugriff auf das zugrunde liegende

System besitzen. **Zugriffskontrollmechanismen** wie Berechtigungssysteme, Rollenmodelle oder Authentifizierungsverfahren lassen sich ebenfalls innerhalb dieses Rahmens verstehen. Sie beschränken die Handlungsmöglichkeiten einzelner Akteure innerhalb des Systems und definieren damit, welche Operationen innerhalb bestimmter Vertrauensgrenzen zulässig sind. **Sichere Software** stellt die korrekte Umsetzung von Sicherheitsmodellen in ausführbaren Systemen dar. Fehler in der Implementierung können dabei als unbeabsichtigte Erweiterungen der Angriffsfläche interpretiert werden, die es adversarialen Akteuren ermöglichen, die intendierten Sicherheitsziele zu umgehen. Auch das Konzept des **Information Hiding** fügt sich nahtlos in dieses Modell ein. Während Kryptographie primär den Inhalt von Informationen schützt, adressiert Information Hiding zusätzlich deren Sichtbarkeit. Ziel ist es, die Existenz oder Struktur bestimmter Informationen vor adversarialen Akteuren zu verbergen oder zu verschleiern. Schließlich lassen sich auch **Sicherheitsarchitekturen** und organisatorische Maßnahmen als Strukturierung von Vertrauensgrenzen innerhalb eines adversarialen Systems verstehen. Sie definieren, welche Akteure welchen Bereichen des Systems vertrauen dürfen und wie Informationen zwischen diesen Bereichen kontrolliert ausgetauscht werden. **Angriffe** erscheinen in diesem Modell nicht als isolierte technische Ereignisse, sondern als gezielte Versuche, die im Systemmodell angenommenen Sicherheitsgrenzen, Ziele oder Mechanismen zu verletzen. Ein Angriff ist damit stets eine Modellverlet-

zung innerhalb eines adversarialen Systems. Damit wird deutlich, dass das adversariale Systemmodell einen einheitlichen interpretativen Rahmen für sämtliche im weiteren Verlauf behandelten Themen bildet. Unterschiedliche Technologien und Verfahren unterscheiden sich nicht in ihrer grundlegenden Zielstruktur, sondern lediglich in der Art und Weise, wie sie Informationszugriffe innerhalb eines adversarialen Systems kontrollieren. Diese einheitliche Sichtweise erlaubt es, Cybersecurity nicht als Sammlung voneinander unabhängiger Themenbereiche zu behandeln, sondern als zusammenhängendes System von Prinzipien, Mechanismen und Modellen. Im nächsten Schritt muss dieses abstrakte Modell um eine entscheidende Dimension erweitert werden: die explizite Modellierung der beteiligten Akteure. Denn bisher wurde lediglich beschrieben, *dass* unterschiedliche Akteure existieren und miteinander interagieren. Um Sicherheitsprobleme systematisch analysieren zu können, muss nun präzisiert werden, *welche Arten von Akteuren* existieren, welche Ziele sie verfolgen und wie sie innerhalb des adversarialen Systems handeln. Im folgenden Abschnitt werden daher **Akteursmodelle** eingeführt. Dabei wird insbesondere zwischen verschiedenen Rollen unterschieden, darunter Angreifer als rationale Optimierer, Verteidiger als rationale Risikomanager sowie weitere Stakeholder wie Nutzer, Betreiber und regulatorische Instanzen. Darauf aufbauend werden Zielkonflikte zwischen diesen Akteuren analysiert und gezeigt, dass Sicherheit im Kern stets aus der Interaktion konkurrierender Interessen entsteht. Abschließend wird Sicherheit als

ökonomisches und interaktives Gleichgewicht zwischen diesen Akteuren betrachtet.

4.2 Akteursmodelle

Das adversariale Systemmodell beschreibt Cybersecurity als Interaktion mehrerer Akteure mit teilweise konfligierenden Zielen. Um diese Interaktionen systematisch analysieren zu können, reicht es jedoch nicht aus, Akteure lediglich als abstrakte Entitäten zu betrachten. Vielmehr ist es notwendig, ihre typischen Handlungslogiken, Zielstrukturen und Entscheidungsprinzipien zu modellieren. Ein **Akteursmodell** beschreibt daher nicht die konkreten Eigenschaften einzelner realer Akteure, sondern eine abstrahierte Rolle innerhalb eines adversarialen Systems. Diese Rollen sind idealisierte Beschreibungen typischer Verhaltensmuster, die es ermöglichen, Sicherheitsprobleme systematisch zu analysieren. Im Folgenden werden drei zentrale Akteursmodelle eingeführt, die im weiteren Verlauf des Buches immer wieder verwendet werden.

Angreifer als rationaler Optimierer

Ein Angreifer wird im Modell als ein Akteur verstanden, der versucht, innerhalb eines adversarialen Systems seinen erwarteten Nutzen zu maximieren. Dieser Nutzen kann beispielsweise in Form von Informationsgewinn, finanziellen Vorteilen, Kontrolle über Systeme oder Störung von Diensten interpretiert werden. Dabei ist entschei-

dend, dass Angreifer nicht notwendigerweise „böse“ oder irrational handeln. Vielmehr wird angenommen, dass sie innerhalb ihrer gegebenen Möglichkeiten effizient handeln und dabei versuchen, mit minimalem Aufwand maximalen Nutzen zu erzielen. Dieses Modell führt zu einer wichtigen Konsequenz: Angriffe entstehen nicht zufällig, sondern dort, wo der erwartete Nutzen einer erfolgreichen Attacke die dafür erforderlichen Kosten übersteigt.

Verteidiger als rationaler Risikomanager

Der Verteidiger verfolgt eine strukturell andere Zielsetzung. Während Angreifer versuchen, Nutzen zu maximieren, zielt der Verteidiger darauf ab, das Gesamtrisiko innerhalb eines Systems zu minimieren. Risikomanagement bedeutet in diesem Kontext, dass nicht alle Angriffe vollständig verhindert werden können oder müssen. Stattdessen werden Sicherheitsmaßnahmen so gewählt, dass ein akzeptables Gleichgewicht zwischen Aufwand, Kosten und verbleibendem Risiko entsteht. Damit ist Sicherheit im adversarialen Systemmodell niemals absolut, sondern stets das Ergebnis einer Optimierung unter Ressourcenbeschränkungen.

Stakeholder: Nutzer, Betreiber und Regulatoren

Neben Angreifern und Verteidigern existiert in realen Systemen eine Vielzahl weiterer Akteure, die indirekt Einfluss auf die Sicherheit nehmen. Diese werden hier

unter dem Begriff **Stakeholder** zusammengefasst. Dazu gehören insbesondere Nutzer, die ein System verwenden, Betreiber, die für den Betrieb verantwortlich sind, sowie regulatorische Instanzen, die rechtliche und organisatorische Rahmenbedingungen festlegen. Im Gegensatz zu Angreifern und klassischen Verteidigern verfolgen Stakeholder häufig keine rein sicherheitsbezogenen Ziele. Stattdessen stehen Aspekte wie Benutzerfreundlichkeit, Kosten, Leistungsfähigkeit oder rechtliche Konformität im Vordergrund. Gerade diese Vielfalt an Zielen führt dazu, dass Sicherheitsentscheidungen in realen Systemen fast immer Kompromisse darstellen.

Zusammenfassung 10. *Akteure werden im adversarialen Systemmodell nicht als isolierte Einheiten betrachtet, sondern als Rollen mit spezifischen Optimierungszielen und Beschränkungen. Sicherheit entsteht somit nicht aus dem Verhalten eines einzelnen Akteurs, sondern aus dem Zusammenspiel dieser unterschiedlichen Rollen innerhalb eines gemeinsamen Systems.*

Im nächsten Schritt wird untersucht, wie diese unterschiedlichen Zielsetzungen zu systematischen Spannungen führen. Insbesondere stellt sich die Frage, warum Sicherheitsentscheidungen häufig Konflikte zwischen verschiedenen Akteuren erzeugen und wie diese Konflikte im Modell beschrieben werden können.

4.3 Zielkonflikte zwischen Akteuren

Im adversarialen Systemmodell wurde Sicherheit als Ergebnis der Interaktion unterschiedlicher Akteure beschrieben, die jeweils eigene Ziele verfolgen. Sobald mehrere Akteure auf dieselben Ressourcen oder Systeme einwirken, entsteht jedoch eine grundlegende strukturelle Eigenschaft: Zielkonflikte sind nicht die Ausnahme, sondern die Regel. Ein **Zielkonflikt** liegt vor, wenn die Optimierung des Ziels eines Akteurs die Zielerreichung eines anderen Akteurs verschlechtert. Im Kontext der Cybersecurity bedeutet dies insbesondere, dass Maßnahmen zur Erhöhung der Sicherheit häufig mit anderen Systemzielen in Spannung stehen. Diese Konflikte entstehen nicht zufällig, sondern sind eine direkte Konsequenz der gemeinsamen Nutzung von Ressourcen innerhalb eines adversarialen Systems. Jede Sicherheitsmaßnahme verändert die Bedingungen, unter denen andere Akteure handeln können. Ein zentrales Beispiel ist der Konflikt zwischen Sicherheit und Benutzerfreundlichkeit. Maßnahmen wie starke Authentifizierungsverfahren erhöhen die Sicherheit eines Systems, können jedoch gleichzeitig die Zugänglichkeit für legitime Nutzer erschweren. Ähnlich kann eine strikte Zugriffskontrolle die Flexibilität eines Systems reduzieren, obwohl sie dessen Angriffsfläche verkleinert. Ein weiterer grundlegender Konflikt besteht zwischen Sicherheit und Effizienz. Sicherheitsmechanismen benötigen in der Regel zusätzliche Ressourcen, sei es in Form von Rechenzeit, Speicher oder organisatorischem Aufwand. Diese Ressour-

cen stehen dann für andere Aufgaben nicht mehr zur Verfügung. Im adversarialen Kontext tritt ein zusätzlicher, besonders wichtiger Konflikt hinzu: der Konflikt zwischen Angreifern und Verteidigern. Jede Verbesserung der Verteidigung verändert die Kostenstruktur möglicher Angriffe. Gleichzeitig passen sich Angreifer an diese Veränderungen an, indem sie neue Angriffswege suchen oder bestehende Schwachstellen gezielter ausnutzen. Damit entsteht eine dynamische Wechselwirkung zwischen den Akteuren. Sicherheitsmaßnahmen sind nicht nur statische Schutzmechanismen, sondern beeinflussen aktiv das Verhalten adversarialer Akteure. Umgekehrt reagieren diese Akteure auf neue Sicherheitsmaßnahmen mit Anpassungen ihrer Strategien. Diese wechselseitige Beeinflussung führt dazu, dass Sicherheit niemals isoliert optimiert werden kann. Jede Entscheidung über eine Sicherheitsmaßnahme verändert das Gesamtsystem und damit auch die Zielerreichung aller beteiligten Akteure. Aus diesem Grund ist es im adversarialen Systemmodell nicht sinnvoll, Sicherheit als absolutes Optimum zu betrachten. Stattdessen handelt es sich stets um eine Kompromisslösung zwischen konkurrierenden Zielen. Diese Einsicht bildet die Grundlage für die nächste Betrachtungsebene: die ökonomische Struktur von Sicherheitsentscheidungen. Denn viele dieser Zielkonflikte lassen sich präziser verstehen, wenn Sicherheit als Frage von Kosten, Nutzen und Risiko betrachtet wird.

4.4 Ökonomie der Sicherheit

Die im vorherigen Abschnitt beschriebenen Zielkonflikte lassen sich auf einer tieferen Ebene als ökonomisches Problem verstehen. Im adversarialen Systemmodell ist Sicherheit nicht nur eine technische Eigenschaft, sondern das Ergebnis von Entscheidungen unter begrenzten Ressourcen. Jede Sicherheitsmaßnahme verursacht **Kosten**. Diese Kosten können unterschiedliche Formen annehmen, beispielsweise finanzielle Aufwände, zusätzliche Rechenzeit, erhöhte Systemkomplexität oder Einschränkungen der Benutzerfreundlichkeit. Gleichzeitig reduziert eine Sicherheitsmaßnahme das **Risiko**, dass ein Angreifer erfolgreich ist oder ein Sicherheitsziel verletzt wird. Um diese Beziehung präziser zu erfassen, reicht eine reine Betrachtung von Kosten und Risiko jedoch nicht aus. Zusätzlich muss die **Schadenswirkung** eines erfolgreichen Angriffs berücksichtigt werden. Die Schadenswirkung beschreibt den tatsächlichen Verlust oder die Konsequenzen, die eintreten, wenn ein Sicherheitsziel verletzt wird. Dieser Schaden kann beispielsweise den Verlust sensibler Daten, finanzielle Schäden, Reputationsverlust oder die Beeinträchtigung kritischer Dienste umfassen. Damit ergibt sich eine dreidimensionale Struktur sicherheitsrelevanter Entscheidungen: **Kosten** bezeichnen den Aufwand zur Implementierung und Aufrechterhaltung von Sicherheitsmaßnahmen, **Risiko** die Wahrscheinlichkeit eines erfolgreichen Angriffs unter gegebenen Bedingungen und **Schadenswirkung** die Konsequenzen im Falle eines

erfolgreichen Angriffs. Das Zusammenspiel dieser drei Größen bestimmt, welche Sicherheitsmaßnahmen in einem adversarialen System als sinnvoll angesehen werden können. Eine Maßnahme ist nicht allein deshalb gerechtfertigt, weil sie das Risiko reduziert, sondern nur dann, wenn das Verhältnis zwischen Kosten, Risikoreduktion und Schadensvermeidung angemessen ist. Insbesondere ist es möglich, dass sehr teure Sicherheitsmaßnahmen nicht sinnvoll sind, wenn der potenzielle Schaden gering ist. Umgekehrt können selbst aufwändige Schutzmaßnahmen notwendig sein, wenn die Schadenswirkung eines erfolgreichen Angriffs extrem hoch ist, etwa bei kritischer Infrastruktur oder sensiblen Datenbeständen. Im adversarialen Systemmodell bedeutet dies, dass Sicherheit stets eine Optimierungsaufgabe unter Unsicherheit darstellt. Akteure müssen Entscheidungen treffen, ohne den zukünftigen Verlauf aller möglichen Angriffe exakt vorhersehen zu können. Sehr wichtig ist auch die asymmetrische Struktur zwischen Angreifern und Verteidigern. Während Angreifer oft nur einmal erfolgreich sein müssen, um Schaden zu verursachen, müssen Verteidiger alle relevanten Angriffsvektoren berücksichtigen. Diese Asymmetrie verstärkt die Bedeutung einer sorgfältigen Abwägung zwischen Kosten, Risiko und Schadenswirkung erheblich. Wir sehen damit, dass Sicherheitsentscheidungen niemals rein technisch getroffen werden können. Sie sind immer auch ökonomische Entscheidungen über den Einsatz begrenzter Ressourcen in einem adversarialen Umfeld. Diese ökonomische Perspektive führt unmittelbar zur nächsten Be-

trachtungsebene: Sicherheit als Interaktion strategischer Akteure. Dort wird untersucht, wie sich diese Kosten-Nutzen-Strukturen auf das Verhalten von Angreifern und Verteidigern auswirken und warum Sicherheit letztlich als dynamisches Wechselspiel verstanden werden muss.

4.5 Sicherheit als Spiel

Die bisherigen Betrachtungen haben gezeigt, dass Sicherheit im adversarialen Systemmodell aus dem Zusammenspiel mehrerer Akteure mit unterschiedlichen Zielen entsteht. Diese Interaktionen lassen sich besonders präzise verstehen, wenn sie als strategische Entscheidungen innerhalb eines Spiels interpretiert werden. Im Folgenden wird diese Intuition durch eine formale, jedoch bewusst einfache Modellierung ergänzt.

Definition 11 (Adversariales Sicherheitsspiel)**.** *Ein adversariales Sicherheitsspiel ist ein Tupel* $G = (A, S, U)$ *mit* $A = \{A_1, \ldots, A_n\}$ *als Menge von Akteuren (Spielern),* S_i *als Menge der Strategien jedes Akteurs* A_i *und* $U_i : S_1 \times \cdots \times S_n \to \mathbb{R}$ *als Nutzenfunktion jedes Akteurs. Ein Sicherheitszustand ergibt sich aus der Interaktion der gewählten Strategien* $s_i \in S_i$ *aller Akteure.*

Im einfachsten Sinne kann ein adversariales System somit als ein Spiel verstanden werden, in dem der Ausgang nicht allein durch ein einzelnes Systemverhalten bestimmt wird, sondern durch das Zusammenspiel aller gewählten Strategien. Jeder Akteur verfügt über eine Menge

möglicher Handlungsstrategien. Ein Angreifer wählt beispielsweise eine konkrete Angriffsmethode, während ein Verteidiger eine Sicherheitsarchitektur, Zugriffskontrolle oder kryptographische Maßnahme implementiert. Der tatsächliche Zustand des Systems ergibt sich aus der Kombination dieser Entscheidungen. Ein zentrales Merkmal dieses Modells ist die **strategische Abhängigkeit**: Die Wirksamkeit einer Verteidigungsstrategie hängt von der gewählten Angriffsstrategie ab, und umgekehrt hängt die Wahl eines Angriffs von der erwarteten Verteidigung ab. Damit unterscheidet sich das adversariale System grundlegend von klassischen Optimierungsproblemen. Es existiert kein isoliertes global optimales Sicherheitsdesign, da jede Strategie nur relativ zu den Strategien anderer Akteure bewertet werden kann. Diese wechselseitige Abhängigkeit führt zu einem dynamischen Anpassungsprozess. Neue Sicherheitsmechanismen verändern die Nutzenstruktur adversarialer Akteure und verschieben damit deren optimale Strategien. Umgekehrt reagieren Angreifer auf diese Veränderungen durch Anpassung ihrer Vorgehensweisen. Im erweiterten Sinne umfasst dieses Spiel nicht nur Angreifer und Verteidiger, sondern auch weitere Akteure wie Nutzer, Betreiber oder Regulatoren. Diese beeinflussen das System indirekt, etwa durch Kostenstrukturen, rechtliche Rahmenbedingungen oder technische Anforderungen. Ein zentrales Konzept der Spieltheorie ist das **Gleichgewicht**. Für Cybersecurity ist insbesondere das folgende intuitive Verständnis relevant:

Definition 12 (Sicherheitsgleichgewicht (informell))**.**

Ein Sicherheitsgleichgewicht liegt vor, wenn kein Akteur durch einseitige Änderung seiner Strategie seinen Nutzen verbessern kann, solange die Strategien der anderen Akteure unverändert bleiben.

In einem solchen Zustand ist das System nicht „absolut sicher“, sondern stabil unter den gegebenen Annahmen über die Strategien der beteiligten Akteure. Änderungen treten erst dann auf, wenn sich die Fähigkeiten, Ziele oder Ressourcen eines Akteurs verändern. Ein wichtiges Ergebnis dieser Betrachtung ist daher, dass Sicherheit niemals als statischer Endzustand verstanden werden kann. Selbst wenn ein System zu einem Zeitpunkt in einem Gleichgewichtszustand ist, kann dieses Gleichgewicht durch neue Angriffe, neue Technologien oder veränderte Rahmenbedingungen verschoben werden. Aus dieser Perspektive wird Sicherheit zu einem fortlaufenden Prozess strategischer Anpassung innerhalb eines adversarialen Spiels. Sicherheitsmechanismen sind dabei nicht nur Schutzmaßnahmen, sondern auch Einflussfaktoren auf die Nutzenstruktur der Akteure. Spieltheoretische Konzepte erlauben es, diese Intuition weiter zu präzisieren, etwa durch die Analyse von Gleichgewichten, dominanten Strategien oder optimalen Reaktionen. Für das weitere Verständnis dieses Buches genügt jedoch zunächst die qualitative Einsicht, dass Sicherheit immer aus interdependenten Entscheidungen mehrerer Akteure entsteht. Im nächsten Kapitel wird der Fokus von den Akteuren auf die Struktur dessen verlagert, was sie kontrollieren und angreifen: Information. Dabei wird untersucht, was