1 How to Eliminate the Prevailing Ignorance and Complacency Around Cybersecurity 1
Stefanie Frey
1.1 The Challenges of the Twenty First Century 2
1.2 Current Situation 3
1.2.1 We Have Not Had a Cyber 9/11 5
1.2.2 Complexity 7
1.3 Conclusion 8
References 9

Teil I Beispiele aus der Praxis

2 Angriff aus der Dunkelheit: Cyberattacke auf das Lukaskrankenhaus Neuss 13
Ulla Dahmen und Nicolas Krämer
Literatur 20

3 Audrey and Reto Gfeller People Like You and Me 23
Audrey and Reto Gfeller
3.1 The Storyline 23
3.2 Emails Received After the Alleged Purchase 25
3.3 Continuation of Events After Returning from Vacation 26
3.4 The End 28
3.5 List of All Bought Items 28

Teil II Staaten und Behörden
States and Authorities

4 Vorworte 37
Arne Schönbohm und Udo Helmbrecht
4.1 Integrierte Wertschöpfungskette der Cyber-Sicherheit 38
4.2 Cyber Security Is a Shared Responsibility 39
References 41

digitalisiert durch:
IDS Luzern

5 ENISA's Contribution to National Cyber Security Strategies 43
Dimitra Liveri, Anna Sarri and Eleni Darra
5.1 *Introduction* 44
5.2 A Resilient National Strategy 45
5.2.1 Member State's Objectives 47
5.2.2 Objective 3: Organize Cybersecurity Exercises 47
5.2.3 Objective 4: Establish Baseline Security Measures 48
5.2.4 Objective 5: Establish Incident Reporting Mechanisms 48
5.2.5 Objective 6: Raise User Awareness 49
5.2.6 Objective 7: Strengthen Training and Educational Programs 49
5.2.7 Objective 8: Establishment of Incident Response Capability 50
5.2.8 Objective 9: Address Cyber Crime 51
5.2.9 Objective 10: Engage in International Cooperation 51
5.2.10 Objective 11: Establish a Public-Private Partnership 52
5.2.11 Objective 13: Institutionalize Cooperation Between Public Agencies 53
5.3 Governance Structures in the EU 54
5.3.1 Centralized Approach 55
5.3.2 Decentralized Approach 56
5.3.3 Co-regulation with the Private Sector 57
5.4 Challenges 59
5.5 ENISA's Contribution to NCSS 60
5.6 The Next Steps for NCSS 60
5.7 Conclusions 63
References 63

6 Die Allianz für Cyber-Sicherheit: Netzwerke schützen Netzwerke 65
Stefan Wunderlich
6.1 Warum eine Allianz für Cyber-Sicherheit? 65
6.2 Die Allianz für Cyber-Sicherheit 66
6.3 Struktur der Allianz für Cyber-Sicherheit 67
6.3.1 Die Teilnehmer 67
6.3.2 Partner 67
6.3.3 Multiplikatoren 68
6.4 Die Angebote der Allianz für Cyber-Sicherheit 69
6.4.1 Informationspool 70
6.4.2 Erfahrungsaustausch 71
6.4.3 Praxis 72
6.5 Fazit und Ausblick 72
Literatur 72

7 **Polizei – Klotz am Bein oder Partner in der Krise?** 73
Dirk Kunze
Literatur 80

8 **Comprehensive Cyber Security Approach: The Finnish Model** 83
Aapo Cederberg
8.1 Introduction 84
8.2 The Cyberworld from the Finnish Perspective 85
8.2.1 Cyber as a Game Changer 86
8.2.2 National and International Politics 87
8.3 The Structure of the Strategy and Main Principles 88
8.3.1 Cyber Security Strategy: Guiding Vision 89
8.4 Basic Principles of Cyber Security Management 90
8.5 Situational Awareness 91
8.6 Legal Basis 93
8.7 Education and Awareness of All Societal Actors 94
8.8 Fighting Against Cybercrime 95
8.9 Cyber Defence 96
8.10 Private-Public Partnership (PPP) 97
8.11 Critical Infrastructure Protection (CIP) 98
8.12 International Cooperation 99
8.13 The Cyber Security Strategy Process 100
8.14 Conclusions 102

9 **The "Petnica Group": A Case of Public-Private Partnership for Cyber Security in the Republic of Serbia** 107
Irina Rizmal
9.1 Introduction 107
9.2 History: The "Petnica Group" 108
9.3 Legislative Framework and PPP 110
9.4 Continued Efforts: Serbia's "Cyber Security Nexus" 111
9.5 Lessons Learnt 114
References 115

10 **Nationale Cyber-Strategie: Einbezug der lokalen Ebene in einem föderalen Staat** 117
André Duvillard und Melanie Friedli
10.1 Nationale Cyber-Strategie: 2012–2017 117
10.2 Der Sicherheitsverbund Schweiz (SVS) 118
10.3 Umsetzung der Nationalen Cyber-Strategie mit den Kantonen 2012–2017 118
10.4 Nationales Krisenmanagement bei Krisen mit Cyberausprägung 119

10.5 Übung POPULA 122
10.6 Lessons learned 123
10.7 Nationale Cyber-Strategie II: 2018–2022 123

11 ...limitem esse delendam – Grenzen sind zu überwinden 125
Mark A. Saxer
11.1 „Cui bono"? (Wem nützt das?) 126
11.2 Labor omnia vincit ... – Statuten, Prozesse, Vertrag 127
11.3 „Rheingold": Tit for Tat oder „Quid pro Quo" 130
11.4 Übung „Loge" [3] (DHS2015 „iRat") 132
11.5 „Claimant Notification B" (Oder: Die Problembeschreibung) 134
11.6 „Cyber Europe 2016" (MELANI und SCE beübt) 135
11.7 „...limitem esse delendam" – Grenzen sind zu überwinden 136
Literatur 138

12 E-Voting in der Schweiz – Herausforderungen und Schutzprinzipen 139
Christian Folini und Denis Morel
12.1 Einführung 140
12.2 Elektronische Stimmabgabe in der Schweiz 140
12.2.1 Allgemeine Besonderheiten des politischen Systems 140
12.2.2 E-Voting in der Schweiz 141
12.3 Prinzipielle Herausforderungen beim E-Voting 142
12.4 Bedrohungen 143
12.5 Rechtliche und regulatorische Grundlagen und Richtlinien 144
12.5.1 Regulation in der Schweiz 144
12.5.2 Individuelle Verifizierbarkeit 145
12.5.3 Universelle Verifizierbarkeit 146
12.5.4 BSI Common Criteria 146
12.5.5 Zertifizierungen 146
12.6 Schutzprinzipien 147
12.7 Zusammenfassung 149
Literatur 149

Teil III Cyber Defence

13 NATO: Ein transatlantischer Blick auf die Cybersicherheit 153
Dieter Warnecke und Sorin Ducaru
13.1 Cyber-Sicherheit geht uns alle an 154
13.2 Cyber Defense Best Practice: The NATO Experience 156
13.2.1 Meeting Challenges in Cyberspace: NATO's Cyber Defense Evolution 156

13.2.2 Best Practices and Lessons Learned ... 158
13.2.3 NATO as a Platform for Developing and Promoting and Best Practice ... 162
13.2.4 The Way Ahead ... 167
References ... 167

14 Cyber Defence – eine zwingende Notwendigkeit! ... 169
Walter J. Unger
14.1 Verteidigung – ein militärischer Begriff ... 169
14.2 Sicherheitspolitisches Umfeld und Technologiewandel ... 171
14.3 Technologiewandel: Digitalisierung, Automatisierung und Vernetzung ... 171
14.4 Strategische Bedeutung der Sicherheit ... 173
14.5 Die aktuelle Bedrohung – erkennbare Trends [5] ... 174
14.6 Folgerungen aus dem Bedrohungsbild [16] und Herausforderungen ... 177
14.7 Die Österreichische Strategie für Cyber-Sicherheit (ÖSCS) [24] ... 181
14.8 Cyber-Sicherheit – sicher Leben im Cyber-Raum ... 184
14.9 Grundsätze der Sicherheit und Verteidigung im Cyber-Raum ... 185
14.10 Cyber-Verteidigung ... 187
14.11 Ausblick ... 189
Literatur ... 190

15 Erfahrungselemente erfolgreicher Strategie-Entwicklung und -Umsetzung im Umgang mit existenziellen Risiken im Cyber-Raum ... 193
Gérald Vernez und Adolf J. Dörig
15.1 Komplexität beherrschen – Gleiches verstehen, analysieren und behandeln ... 194
15.2 Finden und verknüpfen – Systeme, Prozesse und Technologien verstehen, entwickeln und führen ... 196
15.3 Strategieschöpfungsprozess – alte Planungsvorgehensweise an neue dynamische Realitäten anpassen ... 198
15.4 Architektur – die Meta-Ebene der Organisation und Prozesse ... 200
Literatur ... 202

Teil IV IT-Industrie (Anwender, Dienstleister und Hersteller)
IT Industry (Users, Service Providers and Producers)

16 Vorworte ... 205
Heinz Karrer und Holger Mühlbauer
16.1 Mit Sicherheit zum wirtschaftlichen Erfolg im Cyber-Raum ... 206
16.2 IT Security made in Germany ... 208

17 Was Unternehmen von Staaten lernen können: Cyberstrategieentwicklung 211
Stefanie Frey
17.1 Cyberbedrohungslage 212
17.2 Bedrohungen der Zukunft 213
17.2.1 Einige Beispiele 213
17.3 Staaten: Cyberstrategieentwicklung 216
17.3.1 Internationale Gremien und Kooperationen 217
17.4 Grundsätze der Strategieentwicklung 218
17.4.1 Cyberstrategieentwicklung für Unternehmen 219
17.4.2 Maßnahmenentwicklung 222
17.5 Szenariobasierte Übungen als erster Schritt der Cyberstrategieentwicklung 223
17.5.1 Ziel und Ablauf des War Game 225
17.5.2 Resultate des War Game 226
17.6 Zusammenfassung 226
Literatur 227

18 Cyberangriffe: Teil des Alltags? 229
Teresa Ritter und Marc Bachmann
18.1 Methode 230
18.2 Ergebnisse der Wirtschaftsschutzstudie 2017 231
18.2.1 Mittelständische Unternehmen – ein besonders beliebtes Angriffsziel 231
18.2.2 Über Umwege zum Ziel 232
18.2.3 Rund 55 Milliarden Euro Schaden pro Jahr 233
18.2.4 Täterkreis: Mitarbeiter 234
18.2.5 IT-Sicherheitssysteme spielen bei der Aufdeckung kaum eine Rolle 235
18.2.6 Jeder dritte Betroffene schaltet staatliche Stellen ein 235
18.2.7 Angst vor Imageschäden 236
18.2.8 Wie Schutz heute aussieht 236
18.3 Ausblick in die Zukunft 237
Literatur 238

19 Private and Public Partnership: An Unavoidable Issue 239
Christian Aghroum
19.1 Introduction 239
19.2 Putting It into Perspective 240
19.2.1 Defining PPPs 240
19.2.2 An Evolution of Realities 240

19.2.3 The Decline of the State and the Advent of Capitalism 241
19.2.4 Sharing the Territory of Data 242
19.3 The Revision of the Relationship Between State and Private Partners ... 243
19.3.1 The Public Sector Is Lagging Behind 243
19.3.2 Practice Leads to a Revision of Standards 243
19.3.3 Legal Requests Are Good Examples of This Evolution 244
19.3.4 The Weight of International Actors 244
19.4 Persistent Constraints 245
19.4.1 Lack of Legality 246
19.4.2 Mutual Ignorance 246
19.5 The Best Conditions for Founding a PPP 246
19.5.1 Judicial Framework 247
19.5.2 Governance Involvement 247
19.5.3 Involving All Actors 248
19.5.4 An Ongoing Challenge 248
19.5.5 Enlarging the Circle of Actors 249
19.5.6 Shared Standards 249
19.6 Conclusion 250
References 251

20 Best Practices in Cybersecurity from Intergovernmental Discussions and a Private Sector Proposal 253
Richard Hill
20.1 The Eleven Norms of Paragraph 13 of the UN GGE 2015 Report 253
20.2 Additional Recommendations 257
References 259

21 Woher nehmen, wenn nicht stehlen – oder wo haben Sie Ihren CISO her? 261
Michael Bartsch
21.1 Der CISO Dein Freund und Helfer 261
21.2 Wie wird man eigentlich CISO? 262
21.3 Jetzt hat man einen CISO und was nun? 264
21.4 Positionierung des CISO im Unternehmen 265
21.5 Warum es trotz CISO zum Cyberangriff kommt 266
21.6 Der CISO als Krisenmanager 267
21.7 Der CISO als „Enabler" im Unternehmen 268
21.8 Fazit 269
Literatur 269

22 Einbindung Datenschutz und Betriebsrat beim Aufbau eines SIEM 271
Matthias Drodt, Ludger Pagel und Thomas Biedorf
22.1 Cyberangriffe bekommen ein immer breiteres Spektrum und werden für Unternehmen zunehmend kritischer 272
22.2 Entscheidend zur Angriffserkennung ist die Zeitdauer der Datenspeicherung 278
22.3 Kernpunkte sind enge Zweckbindung und stark eingeschränkter Kreis der Zugriffsberechtigten 280
22.4 Für den Weg durch die Instanzen ist eine zeitnahe Einbindung nötig 282
Literatur 284

23 Divide et Impera: Sicherheit durch Separation 285
Dirk Loss und Magnus Harlander
23.1 Sicherheitsprobleme durch Komplexität 285
23.2 Mehr Beherrschbarkeit durch Separation 286
23.3 MILS als Vorgehensweise zur Konzeption einer angemessenen Separierung 287
23.4 Mechanismen für die Separation innerhalb von IT-Systemen 291
23.5 Anwendungsbeispiel Datendiode 294
23.6 Separation innerhalb einzelner Programme 295
23.6.1 Privilege Separation 295
23.6.2 Module 296
23.7 Zusammenfassung 296
Literatur 297

24 Die Komplexität der IT-Security meistern 299
Ramon Mörl
24.1 Sind wir zu dumm für IT-Sicherheit? 300
24.1.1 Fachkräftemangel und Fehlendes Know-how in der IT-Sicherheit 300
24.1.2 Vertrauensketten sind mehrdimensional 302
24.1.3 Geeignete Sekundärindikatoren bei der Entscheidungsfindung 305
24.1.4 Anforderungen an IT-Sicherheit in der Beschaffung 307
24.1.5 Schwellenwerte/Minimalanforderung 309
24.1.6 Informationsaustauschplattform 310
24.1.7 Bewertung von IT-Sicherheitslösungen – mangels Metrik 310
24.1.8 Relevante Strukturen in der Herstellung von IT-Sicherheit 312
24.1.9 Herstellung von Schutzverfahren – make or buy 314
24.1.10 IT-Security– eine unsichtbare Investition? 316

24.1.11 Verfügbarkeit und Integrität – gegenläufige Ziele 317
24.1.12 Medienkompetenz und Wertewandel 318
24.1.13 Fazit zum Status der KMU 320
24.2 IT-Sicherheitsarchitektur, was ist das, wem nutzt das, wie geht das – ein nicht ganz fiktives Beispiel 321
24.2.1 Schutzräume für Services und Daten 322
24.2.2 Ordnung im Dschungel des Möglichen 322
24.2.3 Kosteneffizienz mit durchdachter Architektur 323
24.2.4 Unmöglichkeit einer gültigen Rechtssicherheit 324
24.2.5 Sicherheit der Anwendung hängt an der Sicherheit des Systems 324
24.2.6 Angriff auf den Deutschen Bundestag 325
24.2.7 Erwartungshaltung für mobile Sicherheit 326
24.2.8 Bewertung des erreichten Schutzes 327
24.3 Was läuft falsch in der Cyber-Sicherheit? 327
24.3.1 Beispielhafte Schwachstellen in einem Sicherheitsprodukt im zeitlichen Verlauf: 331
24.3.2 Unterstützung organisatorischer Verfahren durch technische Aspekte 333
24.3.3 Geeignete Maßnahmen 334
Quellenverzeichnis 335

25 Progressing Towards a Prescriptive Approach on Cyber Security – Adopting Best Practices and Leverage Technical Innovation 339
Jörg Eschweiler
25.1 Motivation 339
25.2 Relevance of Threat Intelligence 340
25.3 From Security Operations to Cyber Defense: Changing Roles and Approach 342
25.4 Prescriptive Security: Using the Haystack to Find the Needle 344
25.5 Simplification in Cyber Security by Emerging Technologies? 346
References 347

26 Increasing the Efficiency of Security Analysts 349
Alain Gut and Andreas Wespi
26.1 Introduction 349
26.2 Security Monitoring and Analytics 350
26.2.1 Principles 351
26.2.2 Security 360° 352
26.3 Security in the Cognitive Computing Era 354

26.4 Watson for Cyber Security . . . 356
26.4.1 Architecture . . . 356
26.4.2 Security Threat Investigation . . . 357
26.4.3 Operational Efficiency . . . 358
26.5 Future Cognitive Security Enhancements . . . 360
26.6 Conclusion . . . 361
References . . . 361

27 Intelligence and Cyber Threat Management . . . 363
Martin Dion
27.1 Introduction . . . 363
27.2 Part 1: Intelligence and the Cyber Domain . . . 364
27.2.1 Intelligence: Its Traditional Use and Value . . . 364
27.2.2 Cyber Intelligence: How Does It Differ? . . . 367
27.2.3 The Intelligence Cycle . . . 368
27.2.4 The OODA Loop . . . 369
27.2.5 Cyber Intelligence: The Three Pillars and Product Family . . . 370
27.2.6 Bringing It All Together . . . 371
27.3 Part 2: Building the Cyber Intelligence Management System (CIMS) . . . 373
27.3.1 Program Management Versus Management System . . . 374
27.3.2 Understanding the Management System Components . . . 376
27.3.3 Initiating the Cyber Intelligence Management System Program . . . 377
27.3.4 Building the Cyber Intelligence Management System . . . 378
27.3.5 Production Measurement and Continual Improvement . . . 388
27.4 Conclusion . . . 389
References . . . 391

28 Die digitale Transformation . . . 393
Michael Kranawetter
28.1 Compliance als Nutzbringer für den Geschäftserfolg . . . 393
28.2 Entwicklungen der digitalen Transformation . . . 396
28.2.1 Technologien, Trends und Ziele . . . 396
28.2.2 Digitalisierung von Geschäftsprozessen . . . 397
28.2.3 Digitaler und mobiler Workspace . . . 398
28.2.4 Veränderte Arbeitstechniken . . . 398
28.2.5 Internet der Dinge . . . 399
28.3 Herausforderungen der digitalen Transformation . . . 400
28.3.1 Kooperation durch übergreifende Workflows . . . 400
28.3.2 Mobilität, Flexibilität, Sicherheit . . . 400
28.3.3 Schnelle und automatisierte Kommunikation . . . 401
28.3.4 Die Welt der Maschinen . . . 401

28.4 Strategische Aspekte der digitalen Transformation ... 402
28.4.1 Technologische Entwicklungen ... 402
28.4.2 Cloud als Basistechnologie ... 403
28.5 Compliance und die digitale Transformation ... 403
28.5.1 Compliance – eine Einführung ... 403
28.5.2 IT-Compliance und Corporate Compliance – Grenzen verschwimmen ... 404
28.5.3 IT-Compliance – eine Frage der Sicherheit? ... 405
28.6 Compliance und Cloud: Risiko oder Chance? ... 408
28.6.1 Compliance als Strategie für Cloud-Anbieter ... 408
28.6.2 Wie unterstützt die Cloud die Umsetzung von Compliance? ... 409
28.6.3 Compliance as a Service? Leichter als gedacht! ... 410
28.7 Resümee: Compliance wird digitaler und standardisierter ... 411
28.8 Compliance und Geschäftserfolg verbinden – Ein Modell ... 412
28.8.1 Compliance als strategischer Ansatz ... 412
28.8.2 Compliance aus Governance-Sicht ... 412
28.8.3 GRC – Governance, Risk Management und Compliance ... 413
28.9 Mit Compliance zum Geschäftserfolg ... 414
28.9.1 Nutzenpotenziale resultieren aus gemeinsamen Zielen ... 414
28.9.2 Kernbereiche regulatorischer und geschäftlicher Anforderungen ... 417
28.10 Anwendung des Compliance-Modells: Vom Verständnis- zum Anwendungsmodell ... 421
28.10.1 Verfeinerung des Modells ... 421
28.10.2 Analyse als Basis für unternehmerisches Handeln ... 422
28.10.3 Handlungsfelder zur Verbesserung des Geschäftserfolges ... 422
28.11 Beitrag der Cloud zu Compliance und Geschäftserfolg ... 432
28.11.1 Cloud-Service-Modelle im Vergleich ... 432
28.11.2 Steuerung des Anbieter-Kunden-Verhältnisses ... 434
28.12 Die Cloud als Win-win-Strategie ... 438
28.13 Epilog ... 438

29 Moderne digitale Kooperationen und Verbundkonzepte mit sensiblen Daten ... 441
Jörg Kebbedies
29.1 Grenzen Digitaler Strukturen ... 441
29.2 Strategie Digitaler Prozessformen ... 443
29.3 Digitaler Kooperationsraum ... 444
29.3.1 A. Konzept vertrauenswürdiger Kooperation ... 446
29.3.2 B. Konzept vertraulicher Kooperation ... 447
29.4 Schutz der E-Akten ... 449
29.5 Ausblick ... 451
Literatur ... 452

30 Mehr Cyber-Sicherheit geht uns alle an ... 453
Wolfgang Schwabl
30.1 Die Cyber-Herausforderung ... 453
30.2 Cyber-Sicherheit bei A1 ... 455
30.3 Cyber-Sicherheit für Konsumenten ... 460
30.3.1 Wie kann Digitalisierung zu mehr Cyber-Sicherheit führen? ... 461
30.4 Abschliessende Worte ... 462
Literatur ... 462

31 Cyber-Sicherheits-Check ... 463
Tobias Glemser
31.1 Einleitung ... 464
31.2 Entstehungsgeschichte ... 464
31.3 Üblicher Ablauf ... 464
31.4 Methodik ... 465
31.4.1 Verteidigungslinien ... 465
31.4.2 Die Phasen des Cyber-Sicherheits-Checks ... 466
31.4.3 Ergebnis ... 468
31.5 Praxis und Fazit ... 470

32 IT-Sicherheit in Industrienetzen – IoT und IIoT ... 471
Sascha Herzog
32.1 Wie gehen Angreifer und auch unsere Analysten (als erlaubte Angreifer) vor? ... 472
32.2 Mögliche Schutzmaßnahmen ... 476

33 Cyber Governance: Knowing and Doing What's Important for making Smart Cities resilient ... 477
Lars Minth
33.1 Daring to Give Advice? ... 477
33.2 Setting the Foundation ... 479
33.3 Let's Start ... 479
33.3.1 Definitions: Including Serval Embeddings ... 480
33.3.2 Framework for the Governance of Cyber Security ... 482
33.3.3 Circle of CYBER GOVERNANCE ... 484
33.3.4 Circle of CYBER Management ... 487
33.3.5 Circle of CYBER Architecture ... 488
33.3.6 Circle of Operational Security Countermeasures ... 489
33.3.7 Bringing Together the Distinct CYBER Fragments ... 489
33.3.8 Bringing Together: Second Try ... 490
33.3.9 The Other Ingredients ... 492
References ... 492

34 How Blockchain Will Change Cybersecurity Practices 493
Claudio Di Salvo
34.1 A New Approach to Cybersecurity Is Required 494
34.2 The Economics of Cybersecurity Favors the Attackers 494
34.2.1 Misaligned Incentives 495
34.2.2 Information Asymmetries 495
34.2.3 Externalities 496
34.3 The Cybersecurity Problem in the Cloud 497
34.4 What Should a Business Do Then? 499
34.5 Blockchain Can Reengineer Cybersecurity 500
34.5.1 What Is a Blockchain? 501
34.6 Rethinking Cloud Security with a Zero Trust Security Model 502
34.6.1 The BeyondCorp Story from Google 502
34.6.2 Software Defined Perimeter 506
34.7 Putting All Together: A New-Gen Cybersecurity Model with Zero Trust, SDP, and the Blockchain 507
References 510

35 Worst Case Cyberkrise: Es ist keine Frage ob, sondern wann 511
Axel Allerkamp

36 Being More Effective Through Information Sharing and Cooperation 517
Michael Weatherseed
36.1 What Should Be Shared? 518
36.1.1 Challenges to Sharing Information: Choose What You Share 518
36.1.2 Support from the Top 518
36.1.3 Choose with Whom You Share 519
36.2 What Are the Options? 519
36.2.1 CISO Associations 519
36.2.2 Exhibitions 519
36.2.3 Conferences 520
36.2.4 "Business Meetings" 520
36.2.5 "Think-Tank Meetings" 521
36.3 Conclusion 521

Teil V Forschung und Lehre
Research and Education

37 Cybersecurity Capacity Building: A Swiss Approach 525
Laura Crespo, Bastien Wanner and Solange Ghernaouti
37.1 Introduction 526
37.2 Context, Approaches, and Definitions 527
37.3 The Swiss Approach to Cybersecurity Capacity Building 531
37.4 Recommendations 534
References 536

38 Research and Education as Key Success Factors for Developing a Cybersecurity Culture 539
Solange Ghernaouti and Bastien Wanner
38.1 Needs and Context 539
38.2 Some Stakes and Recommendations for Developing a Cybersecurity Culture 541
38.3 An Innovative Master Programme 543
38.4 Lessons Learned from the European Research Project E-Crime 543
38.5 Constraints and Challenges Encountered in Researching Cybersecurity and the Fight Against Cybercrime 544
38.6 Conclusion 549
References 551

39 Eine vertrauenswürdige Zusammenarbeit mit Hilfe der Blockchain-Technologie 553
Norbert Pohlmann
39.1 Einleitung 553
39.2 Elemente, Prinzipien und Struktur der Blockchain-Technologie 555
39.3 Anwendungsformen und Anwendungen der Blockchain 562
39.4 Blockchain-as-a-Service 567
39.5 Sicherheit und Vertrauenswürdigkeit von Blockchains 568
39.6 Zusammenfassung 569
Literatur 569

40 Cybersecurity for Everyone 571
Jan van den Berg
40.1 Introduction 571
40.2 Limitations of Existing Information Security Approaches 573
40.2.1 Computers, the Internet, and Information Security 573
40.2.2 Information Security Developments in the Twenty-First Century 574
40.2.3 Summarizing the Current Limitations of Information Security 575
40.3 Conceptualizing Cyberspace 575
40.4 4 Cybersecurity Challenges 577
40.5 Reflections 580
40.6 Conclusions 581
References 582

41 Learning from the Past: Designing Secure Network Protocols 585
Tobias Fiebig, Franziska Lichtblau, Florian Streibelt, Thorben Krüger, Pieter Lexis, Randy Bush and Anja Feldmann
41.1 Introduction 586
41.2 RFCs: Engineering-Driven Standardization 587
41.3 Threat Modeling 587
41.3.1 Weak Attacker: Good Enough 588
41.3.2 Weak Attacker: Perfect Security 588
41.3.3 Strong Attacker: Perfect Security 588
41.3.4 Strong Attacker: Good Enough 588
41.4 Protocol Design in the Early Internet 589
41.4.1 Example Protocols 590
41.4.2 Discussion 591
41.5 Protocol Design Facing Emerging Threats 592
41.5.1 Example Protocols 593
41.5.2 Discussion 595
41.6 Complex Security Solutions in Protocol Design 596
41.6.1 Example Protocols 597
41.6.2 Discussion 599
41.7 A New Simplicity in Protocol Design 600
41.7.1 Example Protocols 601
41.7.2 Discussion 604
41.8 Lessons Learned 605
41.8.1 The Early Internet 605
41.8.2 Emerging Threats 606
41.8.3 Complex Security 606
41.8.4 A New Simplicity 606
41.9 Summary 607
References 608

42 National Cybersecurity Legislation: Is There a Magic Formula? 615
Eneken Tikk
42.1 The Notion of "Cyber" in National Legislative Process 615
42.2 Trends and Developments in National Cyber Legislation 617
42.3 Regulating Information Society in Estonia 618
42.4 Best Practices in Regional and International Instruments 621
42.5 Information Society and Cybersecurity Regulation in Estonia 628
42.6 Conclusion 628
References 629

Sachwortverzeichnis 635