Thomas Schulz (Hrsg.)

CYBER-SICHERHEIT

FÜR VERNETZTE ANWENDUNGEN IN DER INDUSTRIE 4.0

Ein Fachbuch von

elektro technik | INDUSTRY OF THINGS | Security Insider

VOGEL COMMUNICATIONS GROUP

Thomas Schulz (Hrsg.)

Cybersicherheit

Thomas Schulz (Hrsg.)

Cybersicherheit

für vernetzte Anwendungen in der Industrie 4.0

VOGEL COMMUNICATIONS GROUP

Der Herausgeber:
Dipl.-Ing. Thomas Schulz, Channel Manager Central and Eastern Europe – GE Digital

Die Autoren:
Dipl.-Ing. Heiko Adamczyk, Leiter Innovation and Competence Center – KORAMIS GmbH
Dr. rer. nat. Kemal Akman, Executive Director Advisory Services – KPMG Deutschland Wirtschaftsprüfungsgesellschaft AG
Prof. Dr. rer. nat. Frederik Armknecht, Inhaber Lehrstuhl Praktische Informatik – Universität Mannheim
Johannes Beckers, LL.B., M.Sc., Spezialist Kompetenzstelle Cyber – AXA Versicherungs AG
Daniel Conta, B.Sc., IT Consultant und Programmleiter Medgentis – Medplus-Kompetenz
Dipl.-Math. David Fuhr, Head of Research – HiSolutions AG
Dr. Dipl.-Phys. Christoph Glowatz, Chief Information Security Officer – Hochschule Düsseldorf
Christian A. Gorke, M.Sc., Wissenschaftlicher Mitarbeiter – Universität Mannheim
Dr.-Ing. Christian Haas, Gruppenleiter sichere vernetzte Systeme – Fraunhofer ISOB
Dipl.-Inf. Mark Hartmann, Product Manager Device & Application Control and Artificial Intelligence – DriveLock SE
Peter Haufs-Brusberg, M.Sc., Chief Information Security Officer – Deutsche Bank Luxembourg SA
Dipl.-Ing. Jens Hempel, Advanced Specialist – TÜV Rheinland Industrie Service GmbH
Prof. Dr. Nils Herda, Professor für Wirtschaftsinformatik – Hochschule Albstadt-Sigmaringen
Prof. Dr.-Ing. Hans-Joachim Hof, Professor für IT-Sicherheit – Technische Hochschule Ingolstadt
Dr.-Ing. Lutz Jänicke, Product & Solution Security Officer – Phoenix Contact GmbH & Co. KG
Dipl.-Inf. Michael Jochem, Director Business Chief Digital Office Industrial Technology – Robert Bosch GmbH
Dipl.-Ing. (FH) Dirk Kalinowski, Senior Produktmanager Kompetenzstelle Cyber – AXA Versicherungs AG
Dr.-Ing. Tobias Kleinert, Teamleiter Fachstelle Automatisierungstechnik – BASF Schwarzheide GmbH
Michael Krammel, Geschäftsführer – KORAMIS GmbH
Erwin Kruschitz, M.Sc., Vorstand – anapur AG
Dipl.-Ing. Thomas Leifeld, Wissenschaftlicher Mitarbeiter – Technische Universität Kaiserslautern
Dipl.-Ing. Helmut Leopold, PhD, Head of Center for Digital Safety & Security – AIT Austrian Institute of Technology GmbH
Dipl.-Inf. (FH) Jens Mehrfeld, M.Comp.Sc., Referent Cybersicherheit in Industrieanlagen – Bundesamt für Sicherheit in der Informationstechnik
Sebastian Neef, B.Sc., Inhaber – IT Solutions Neef
Prof. Dipl.-El.-Ing. ETH Armand Portmann, Dozent und Kursleiter – Hochschule Luzern (HSLU)
Dipl.-Inf. (FH) Peter Rehäußer, Executive Director Advisory Cybersecurity – Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft
Prof. Dr. Stefan Ruf, Professor Informationsmanagement – Hochschule Albstadt-Sigmaringen
Prof. Dr.-Ing., Dipl.-Math. Holger Schmidt, Professor für Informatik, insb. IT-Sicherheit – Hochschule Düsseldorf
Dipl.-Ing. Thomas Schulz, Channel Manager Central and Eastern Europe – GE Digital
Dr. rer. pol. Frank Stummer, Business Development Director – Rhebo GmbH
Paul Trompisch, MPP, Referent – Verein Industrie 4.0 Österreich, die Plattform für intelligente Produktion

Raphael Vallazza, Geschäftsführer – Endian Spa
Prof. Dr.-Ing. Oliver Weissmann, Geschäftsführer – xiv-consult GmbH

Resonanzen von Verbänden:
Henning Banthien, Secretary General – Plattform Industrie 4.0
Hans-Wilhelm Dünn, Präsident – Cyber-Sicherheitsrat Deutschland e.V.
Steffen Zimmermann, Leiter Competence Center Industrial Security – VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.
Lukas Linke, Senior Manager Cybersecurity – ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
Lukas Klingholz, Referent Big Data & Künstliche Intelligenz – Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.

Weitere Informationen:
www.vogel-fachbuch.de
http://twitter.com/vogelfachbuch
www.facebook.com/vogelfachbuch

ISBN 978-3-8343-3424-4
1. Auflage. 2020

Inhaltsverzeichnis

Grußwort 19
(Henning Banthien / Plattform Industrie 4.0)

Vorwort des Herausgebers 21
(Thomas Schulz)

Resonanzen der Verbände

I Zentrale Enabler einer erfolgreichen digitalen Transformation 29
(Hans-Wilhelm Dünn / Cyber-Sicherheitsrat Deutschland e.V.)

II Modulares Bausteinsystem der Security 31
(Steffen Zimmermann / VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.)

III Etablierung einer Sicherheitskultur 33
(Lukas Linke / ZVEI Zentralverband Elektrotechnik- und Elektronikindustrie e.V.)

IV Wirtschaftsschutz in der digitalen Welt 35
(Lukas Klingholz / Bitkom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.)

A Cybersicherheit als Voraussetzung für erfolgreiche Digitalisierung

A.1 Bedrohungen durch die Digitalisierung der Industrie 39
(Jens Mehrfeld)
A.1.1 Einleitung 39
A.1.2 Cybersicherheit in bestehenden Industrieanlagen 40
A.1.2.1 Vorgehen der Angreifer bei gezielten Angriffen 40
A.1.2.2 Auswirkungen von Angriffen auf Produktionssysteme 42
A.1.2.2.1 Steuerungskontrolle 42
A.1.2.2.2 Anzeige 43
A.1.2.2.3 Safety 43
A.1.2.2.4 Daten 43
A.1.3 Veränderungen durch Industrie 4.0 44
A.1.3.1 Wertschöpfungsnetzwerke 45
A.1.3.1.1 Verbindungen zu Kunden 46
A.1.3.1.2 Cloud-Services 47
A.1.3.1.3 Fernzugriffe 48
A.1.3.1.4 Auftragsfertigung 49

A.1.3.1.5 Benutzer- und Berechtigungsverwaltung 49
A.1.3.2 Blick in Unternehmen 50
A.1.3.2.1 Schwachstellen 51
A.1.3.2.2 Dynamische Konfiguration 52
A.1.3.2.3 Entwicklung 53
A.1.3.2.4 Updates und Änderung der Funktionen 54

A.2 Cybersicherheit als Grundlage für die Digitalisierung der Industrie 57
(Helmut Leopold; Paul Trompisch)
A.2.1 Cybersicherheit – ein inhärenter Bestandteil der Digitalisierung 57
A.2.1.1 Umfassende Digitalisierung und Vernetzung 57
A.2.1.2 Veränderung der Geschäftsmodelle und Disruptive Effekte 57
A.2.2 Bedrohungslage 58
A.2.2.1 Grundlegende Technologieabhängigkeit 58
A.2.2.2 Cyberspace – der neue Aktionsraum der internationalen Kriminalität 58
A.2.2.3 Vielfältige Cyber-Security-Angriffsmethoden 59
A.2.2.4 Neue Trends: Cybercrime as a Service 60
A.2.3 Herausforderungen für Unternehmen 60
A.2.3.1 IT-Systeme sind grundsätzlich fehleranfällig 60
A.2.3.2 Die steigende Komplexität verstärkt die Verletzlichkeit unserer IT-Systeme 61
A.2.3.2.1 Externe, aber auch interne Gefahren 61
A.2.3.2.2 Legacy-Systeme 62
A.2.3.3 Digitalisierung und Cybersicherheit brauchen eine neue Kultur des Miteinanders 63
A.2.3.4 Standardisierung 64
A.2.3.5 Cybersicherheit muss neu verstanden werden 65
A.2.4 Herausforderung für die Wirtschaft 65
A.2.4.1 Fachkräftemangel 65
A.2.4.2 Breites Problembewusstsein und internationale Governance fehlen 67
A.2.4.3 Europäische Markttreiber mit Vorbildwirkung 67
A.2.5 Cybersicherheit verlangt neue Schutz- und Verteidigungsstrategien und neue Formen der Kooperation 68

B Regelkonformität mit Normen und Richtlinien

B.1 Normenreihe ISO/IEC 27 000: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme 73
(Prof. Dr. Oliver Weissmann)
B.1.1 Hintergrund 73
B.1.2 Gliederung, Inhalte und Abschnitte 76
B.1.2.1 Kontext der Organisation 76
B.1.2.2 Leadership / Organisationsleitung 77
B.1.2.3 Planung 78
B.1.2.4 Unterstützung 79
B.1.2.5 Betrieb 80

B.1.2.6 Performance-Bewertung ... 80
B.1.2.7 Kontinuierliche Verbesserung ... 81
B.1.3 Möglicher Anwendungsbereich und Kontext ... 81
B.1.4 Umsetzungen mit hohem Anwendernutzen ... 83

B.2 Normenreihe IEC 62 443: Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme ... 87
(David Fuhr)
B.2.1 Hintergrund ... 87
B.2.2 Aufbau ... 87
B.2.2.1 Anwendungsbereiche ... 89
B.2.2.1.1 Betreiber ... 89
B.2.2.1.2 Dienstleister ... 89
B.2.2.1.3 Integrator ... 89
B.2.2.1.4 Hersteller ... 89
B.2.2.1.5 Zertifizierungen ... 90
B.2.2.2 Umsetzungen ... 90
B.2.2.2.1 Grundkonzepte ... 90
B.2.2.2.2 IEC 62 443-2-1 ... 91
B.2.2.2.3 IEC 62 443-2-4 ... 92
B.2.2.2.4 IEC 62 443-3-3 ... 92
B.2.2.2.5 IEC 62 443-4-1 und IEC 62 443-4-2 ... 93
B.2.2.3 Der Weg durch die IEC 62 443 ... 93

B.3 Richtlinienreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung ... 97
(Heiko Adamczyk; Michael Krammel)
B.3.1 Hintergrund und Anwendungsbereich ... 97
B.3.2 Aufbau und inhaltliche Gliederung ... 98
B.3.3 Umsetzungen mit hohem Anwendernutzen ... 100

B.4 NAMUR-Arbeitsblatt NA 163: IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen ... 109
(Thomas Leifeld; Erwin Kruschitz)
B.4.1 Einführung ... 109
B.4.2 Allgemeine Beschreibung der Vorgehensweise ... 110
B.4.3 Identifikation des betrachteten Systems ... 111
B.4.4 Definition der Schutzziele ... 111
B.4.5 Verfahren zur detaillierten Risikoanalyse ... 112
B.4.6 Betrachtung möglicher Auswirkungen ... 113
B.4.7 Einteilung des betrachteten Systems in Zonen und Übergänge ... 113
B.4.8 Detaillierte Risikobetrachtung ... 114
B.4.9 Anwendung des Verfahrens ... 114

C Fabrik als Anwendungsdomäne / Industrial Control Systems

C.1 Einführung und Grundlagen Cybersicherheit für Industrielle Steuerungssysteme (ICS) 119
(Dr.-Ing. Christian Haas; Thomas Schulz)
C.1.1 Die Fabrik als Anwendungsdomäne 119
C.1.1.1 Der Unterschied zwischen Information Technology (IT) und Operational Technology (OT) 119
C.1.1.2 Bedrohungen der Digitalisierung in der Industrie 121
C.1.1.3 Grundbegriffe der Cybersicherheit in der Industrie 123
C.1.2 Systemsicherheit für industrielle Steuerungssysteme 124
C.1.2.1 Sicherheitsmaßnahmen 126
C.1.2.1.1 Relevante Standards 126
C.1.2.1.2 Organisatorische Maßnahmen 127
C.1.2.1.3 Technische Maßnahmen 128
C.1.2.2 Grundkonzepte technischer Maßnahmen 129
C.1.2.2.1 Trennung von Unternehmensnetz und Produktion (Demilitarized Zone – DMZ) 130
C.1.2.2.2 Segmentierung in Anlagen-Subnetze 130
C.1.2.2.3 Netzwerkzugangskontrolle (Network Access Control – NAC) 131
C.1.2.2.4 Überwachungstechniken (Deep Packet Inspection – DPI) .. 132

C.2 Grundlegende Sicherheitsbedrohungen und Lösungsmöglichkeiten im ICS-Umfeld: Probleme – Lösung – Beispiele 135
(Dr. rer. nat. Kemal Akman; Peter Rehäußer)
C.2.1 Einleitung 135
C.2.2 Schwachstellen und veränderte Bedrohungslage 135
C.2.2.1 Angriffe auf industrielle Kontrollsysteme 136
C.2.2.2 Advanced Persistent Threats 139
C.2.3 Standards und Richtlinien als Grundlage für erste Orientierungen 140
C.2.4 Strategien zum Schutz 141
C.2.4.1 Netzwerksicherheit 141
C.2.4.2 Netzwerkarchitektur 141
C.2.4.3 Übersicht einiger relevanter Netzwerkprotokolle unter Sicherheitsaspekten 144
C.2.4.3.1 OLEPC, Modbus, ICCP, DNP3 144
C.2.4.3.2 Spezialisierte Feldbusprotokolle 147
C.2.4.4 Angriffserkennung und Anomalieerkennung 148
C.2.4.5 Sicherheit der Maschinen und Anlagen 149
C.2.4.5.1 SPS / PLC 149
C.2.4.5.2 HMI 149
C.2.4.5.3 IEDs 149
C.2.4.5.4 RTUs 150
C.2.4.5.5 Anzeigesysteme 150
C.2.4.5.6 Weitere Komponenten 150
C.2.5 Bedrohungsszenarien der Maschinen und Anlagen 151

C.2.6 Sicherheitsmaßnahmen für Maschinen und Anlagen ... 151
C.2.7 Sicherheit im und durch den Prozess ... 152
C.2.7.1 Security by Design ... 152
C.2.7.2 Erkennung und Management von Schwachstellen ... 153
C.2.7.3 Patch Management ... 154
C.2.7.4 Konfigurationsmanagement ... 154
C.2.7.5 Netzwerksegmentierung ... 154
C.2.7.6 Detect ... 155
C.2.7.7 Respond & Recover ... 156
C.2.7.8 Lifecycle Management ... 156

C.3 Monitoring der Kommunikation im ICS – Transparenz und Anomalieerkennung ... 159
(Dr. rer. pol. Frank Stummer)
C.3.1 Einleitung: Einbindung des Monitoring in die Gesamtsicherheitsstrategie ... 159
C.3.2 Spezifika im industriellen Umfeld ... 160
C.3.2.1 Aktion vs. Rückwirkungsfreiheit und Safety ... 161
C.3.2.2 Verallgemeinerungen vs. Domänenbesonderheiten ... 161
C.3.2.3 Organisatorische Einbindung ... 162
C.3.3 Typen von Anomalien ... 163
C.3.3.1 Angriffe ... 163
C.3.3.2 Fehlkonfigurationen ... 165
C.3.3.3 Netzwerküberwachung ... 167
C.3.4 Kommunikationsmonitoring als Datenquelle für SIEM und Co. ... 168
C.3.4.1 Datentypen und Nutzungsmöglichkeiten ... 168
C.3.4.2 Normierung und Vollständigkeit ... 169

C.4 Cyber Security im Lebenszyklus von automatisierten Sicherheitseinrichtungen ... 171
(Dr.-Ing. Tobias Kleinert; Thomas Leifeld)
C.4.1 Automatisierte Sicherheitseinrichtungen ... 171
C.4.1.1 Zweck und Funktion ... 171
C.4.1.2 Functional Safety Management und SIS-Lebenszyklus ... 172
C.4.2 Cyberrisiko für automatisierte Sicherheitseinrichtungen ... 173
C.4.2.1 Betrachtungsgegenstand und funktionale Trennung der Automatisierung ... 173
C.4.2.2 Bedrohung durch Cyberangriffe ... 175
C.4.2.3 Grundsätzliches zur Cybersicherheit von SIS ... 176
C.4.3 SIS-Cyber-Security-Management ... 177
C.4.3.1 Grundkonzept und Kernelemente ... 177
C.4.3.2 SIS-Cyber-Sicherheitskonzept ... 178
C.4.3.3 SIS-Cyber-Risikoanalyse ... 178
C.4.3.4 SIS-Cyber-Risikohandhabung ... 179
C.4.3.5 SIS-Cyber-Sicherungsmaßnahmen ... 180
C.4.3.6 Organisation, Auditierung und kontinuierliche Verbesserung ... 181
C.4.3.7 Einbindung in den SIS-Lebenszyklus ... 181
C.4.3.8 Praktische Anwendbarkeit der Methoden ... 182

D Mobile und intelligente Komponenten / Smart Devices

D.1 Cybersicherheit für mobile und intelligente Komponenten – Einführung und Grundlagen ... 185
(Prof. Dr.-Ing. Hans-Joachim Hof)
D.1.1 Einleitung ... 185
D.1.2 Cybersicherheit in Industrie-4.0-Anwendungen ... 185
D.1.3 Allgemeine Bedrohungen der Sicherheitsziele in Industrie-4.0-Anwendungen 189
D.1.4 Spezifische Bedrohungen für mobile und intelligente Komponenten in Industrie-4.0-Anwendungen ... 192
D.1.4.1 Bedrohungen durch unsichere lokale Schnittstellen ... 192
D.1.4.2 Bedrohungen durch unsichere Wartungs- und Administrationszugänge ... 193
D.1.4.3 Bedrohungen durch unsichere Zugangskontrolle ... 194
D.1.4.4 Bedrohungen durch unsichere Datenspeicherung ... 195
D.1.4.5 Bedrohungen durch unsichere Netzwerkkommunikation ... 195
D.1.4.6 Bedrohungen des Device-Managements ... 196
D.1.5 Sicherheitsmaßnahmen ... 196
D.1.5.1 Schutz vor Manipulation von Software und Firmware ... 196
D.1.5.2 Schutz kryptographischen Materials ... 199
D.1.5.3 Schutz der Kommunikation ... 200
D.1.5.4 Sichere Identitäten ... 201

D.2 Cyber Security für Industrie-4.0-Komponenten ... 207
(Michael Jochem / Dr.-Ing. Lutz Jänicke)
D.2.1 Gesichert in die digitale und vernetzte Produktion einsteigen ... 207
D.2.2 Kommunikations- und Vertrauensbeziehungen ... 207
D.2.2.1 Sicherheit im Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) ... 208
D.2.2.2 Sicherheit in der Verwaltungsschale der Industrie-4.0-Komponente ... 210
D.2.3 Sichere Kommunikation als Kernthema ... 212
D.2.3.1 Kommunikationsbeziehungen ... 213
D.2.3.2 Kommunikationsstrukturen ... 214

D.3 Wirksamer Schutz von Smart Devices mit Künstlicher Intelligenz (KI) ... 219
(Mark Hartmann)
D.3.1 Einleitung ... 219
D.3.2 Verbesserung der Cyberabwehr durch Künstliche Intelligenz ... 219
D.3.3 Künstliche Intelligenz zum Schutz von Smart Devices ... 219
D.3.3.1 Künstliche Intelligenz (KI) ... 220
D.3.3.2 Machine Learning (ML) ... 221
D.3.3.2.1 Klassifizierung und Supervised Learning ... 221
D.3.3.2.2 Clustering und Non-supervised Learning ... 222
D.3.3.3 Deep Learning (DL) ... 223
D.3.3.4 Ersatz regelbasierter Schutzsysteme durch ML-Modelle ... 224
D.3.3.5 Erkennen von Anomalien ... 225

D.3.3.6 Berücksichtigung der gesetzlichen Anforderungen zum Datenschutz beim Einsatz von ML ... 225
D.3.3.6.1 Einwilligung der betroffenen Person ... 225
D.3.3.6.2 Zweckbindung ... 226
D.3.3.6.3 Automatisierte Entscheidung ... 226
D.3.3.6.4 Verarbeitung von Daten in einem anderen Land ... 226
D.3.3.6.5 Weitere rechtliche Aspekte ... 227
D.3.4 Schlussfolgerungen und Ausblick ... 227
D.3.4.1 Wo gibt es heute schon effektive Lösungen? ... 227
D.3.4.2 Was ist Stand heute noch nicht vollständig gelöst? ... 227
D.3.4.3 Wie könnte die zukünftige Entwicklung aussehen? ... 228

D.4 Eine Analyse von Angriffen auf Smart Devices und der richtige Umgang mit Sicherheitslücken ... 229
(Sebastian Neef)
D.4.1 Einleitung ... 229
D.4.2 Praktische Angriffe auf Smart Devices an ausgewählten Beispielen ... 229
D.4.2.1 Smarte Bluetooth(Tür-)-Schlösser ... 230
D.4.2.1.1 Funktionsweise ... 230
D.4.2.1.2 Angriffe ... 231
D.4.2.2 Smarte Glühbirnen ... 232
D.4.2.2.1 Funktionsweise ... 233
D.4.2.2.2 Angriffe ... 233
D.4.2.3 Human Machine Interfaces ... 236
D.4.2.3.1 Funktionsweise ... 236
D.4.2.3.2 Angriffe ... 236
D.4.2.4 Gemeinsamkeiten und Erkenntnisse ... 238
D.4.3 Der richtige Umgang mit Sicherheitslücken ... 239
D.4.3.1 Perspektive eines Hackers ... 239
D.4.3.2 Perspektive eines Herstellers ... 240

E Plattformen mit gehosteten Anwendungen / Cloud Computing

E.1 Einführung und Grundlagen der Cloud-Sicherheit ... 245
(Christian A. Gorke; Prof. Dr. rer. nat. Frederik Armknecht)
E.1.1 Cloud Computing ... 245
E.1.1.1 Vor- und Nachteile ... 245
E.1.1.2 Technologie ... 246
E.1.1.3 Servicemodelle ... 247
E.1.1.4 Cloud-Modelle ... 248
E.1.2 Interoperabilität und Datenaustausch ... 249
E.1.2.1 OSI-Modell und TCP/IP-Modell ... 249
E.1.2.1.1 Das OSI-Modell ... 250
E.1.2.1.2 Das TCP/IP-Modell ... 250
E.1.2.2 Datentransport via HTTP ... 253
E.1.2.3 Schnittstellen und Datendarstellung ... 254

E.1.2.3.1 Standardisierte Datenformate ... 254
E.1.2.3.2 Schnittstellen ... 255
E.1.3 Bedrohungsszenarien ... 257
E.1.3.1 Die CIA-Sicherheitsziele ... 258
E.1.3.2 Die wichtigsten Sicherheitsrisiken ... 258
E.1.3.3 Seitenkanalangriffe ... 260
E.1.4 Datenschutz und Compliance ... 261
E.1.4.1 Geschichte und Entwicklung des Datenschutzes ... 261
E.1.4.2 Der Wert von Privatsphäre und Daten ... 263
E.1.4.3 Grundprinzipien des Datenschutzes ... 265
E.1.4.4 Bundesdatenschutzgesetz (BDSG) ... 265
E.1.4.5 Datenschutz-Grundverordnung (DSGVO) ... 266
E.1.4.5.1 Praktische Schritte zur DSGVO-Compliance ... 266
E.1.4.6 Standards für Sicherheit und Datenschutz in der Cloud ... 267
E.1.4.7 Cloud-Auditierung ... 268
E.1.5 Sicherheitsmaßnahmen und Implementierungen ... 270
E.1.5.1 Data in Transit ... 270
E.1.5.2 Data at Rest ... 271
E.1.5.3 Implementierungen bei Cloud-Anbietern ... 272
E.1.5.4 Ausblick: Verfügbarkeit und Anonymität in der Cloud ... 272

E.2 Bedrohungsszenarien und Lösungsansätze für Industrie-4.0-Plattformen ... 275
(Raphael Vallazza)
E.2.1 Plattformen als Voraussetzung für Industrie 4.0 ... 275
E.2.2 Funktionen und Aufgaben einer IoT-Plattform ... 276
E.2.3 Risiken und Bedrohungsszenarien ... 277
E.2.3.1 Datenschutz ... 278
E.2.3.2 Hacking-Angriffe ... 279
E.2.3.3 Organisation ... 279
E.2.3.4 Risikofaktor Mensch ... 280
E.2.4 Ganzheitliches Sicherheitskonzept – Security by Design ... 280
E.2.4.1 Maschinen, Geräte und Anwender sicher vernetzen ... 282
E.2.4.2 Netzwerksegmentierung und Verschlüsselung ... 284
E.2.4.3 Mandantenfähigkeit, Berechtigungsmanagement, Protokollierung ... 285
E.2.4.4 OpenSource und Skalierbarkeit ... 287
E.2.4.5 Usability für mehr Sicherheit ... 288

E.3 Cybersicherheit am Beispiel einer Entwicklungsplattform für industrielle IoT-Anwendungen ... 291
(Thomas Schulz)
E.3.1 Die Schlüssel zur Plattform-Sicherheit ... 291
E.3.2 Hohe Sicherheitsstandards von Plattformen ... 292
E.3.2.1 Sicherheitsnormen ... 292
E.3.2.1.1 ISO/IEC 27 001 ... 293
E.3.2.1.2 ISO/IEC 27 017 ... 293
E.3.2.1.3 ISO 27 018 ... 293
E.3.2.1.4 ISO 9001 ... 293
E.3.2.1.5 AICPA SOC 2 ... 293

E.3.2.1.6 CSA CCM v3.0.1 ... 294
E.3.2.2 Defense in Depth ... 294
E.3.2.2.1 Schutz der Daten ... 294
E.3.2.2.2 Security by Design ... 295
E.3.2.2.3 Schutz von Plattform, Netzwerk und Infrastruktur ... 295
E.3.2.2.4 Governance und Compliance ... 296
E.3.2.2.5 Schutz der Edge ... 296
E.3.2.2.6 Identitäts- und Zugriffsmanagement ... 296
E.3.2.2.7 Schlüsselmanagement und Verschlüsselung ... 296
E.3.2.2.8 Kontinuierliche Bewertung ... 297
E.3.3 Sichere Entwicklungsumgebung von Anwendungen ... 297
E.3.3.1 Sicherheitsreview-Richtlinien ... 298
E.3.3.1.1 Phase I: Third Party Risk Management (TPRM) ... 298
E.3.3.1.2 Phase II: Technical Security Assessment ... 299
E.3.3.1.3 Phase III: Secure by Design ... 299
E.3.3.1.4 Phase IV: Penetration Testing ... 301
E.3.3.1.5 Continuous Risk Management (eGRC) ... 302
E.3.3.2 Secure Development Lifecycle (SDL) ... 302
E.3.3.2.1 Sicherheitsschulungen für Entwickler ... 303
E.3.3.2.2 Design- und Architektur-Review ... 304
E.3.3.2.3 Security User Stories / Sicherheitsanforderungen ... 304
E.3.3.2.4 Bedrohungsmodellierung ... 305
E.3.3.2.5 Automatische statische Anwendungssicherheitstests (SAST) 306
E.3.3.2.6 Automatische dynamische Anwendungssicherheitstests (DAST) ... 307
E.3.3.2.7 Vulnerability Assessment für Open-Source-Software (OSS) 307
E.3.3.2.8 Penetrationstest ... 308
E.3.4 Kontinuierliche Überwachung und Reaktion im Betrieb ... 308
E.3.4.1 Bedrohungsanalyse ... 309
E.3.4.2 Monitoring ... 310
E.3.4.3 Inspektion ... 311
E.3.4.4 Detektion ... 311
E.3.4.5 Incident Response ... 312

F Unternehmensorganisation

F.1 Unternehmensorganisation und Informationssicherheit – Einführung und Grundlagen ... 315
(Dr. Dipl.-Phys. Christoph Glowatz; Peter Haufs-Brusberg; Prof. Dr.-Ing. Holger Schmidt)
F.1.1 Einleitung ... 315
F.1.2 Der Faktor Mensch in der Informationssicherheit ... 316
F.1.2.1 Beispiele für Social-Engineering-Angriffe ... 317
F.1.2.2 Social-Engineering-Angriffsarten ... 318
F.1.2.3 Sicherheitsmaßnahmen zur Verbesserung von Security Awareness ... 319
F.1.3 Organisation der Informationssicherheit ... 320
F.1.3.1 Informationssicherheitsorganisation ... 321

F.1.3.2 Rollen und Verantwortlichkeiten ... 322
F.1.3.3 Aufgaben, Kompetenzen, Verantwortlichkeiten und Prozesse ... 323
F.1.3.4 Organisatorische und technische Maßnahmen ... 324
F.1.3.5 Fortbildung, Training und Schulung ... 325
F.1.4 Prozesse in der Informationssicherheit ... 325
F.1.4.1 Das Asset Management in der Informationssicherheit ... 326
F.1.4.1.1 Gefahren eines mangelhaften (Information) Asset Managements ... 327
F.1.4.1.2 Das Asset Management in Standards und Frameworks ... 327
F.1.4.1.3 Das (Information) Asset Management in der Praxis ... 328
F.1.4.2 Das Incident Management in der Informationssicherheit ... 329
F.1.4.2.1 Gefahren eines mangelhaften Information Security Incident Managements ... 329
F.1.4.2.2 Das Incident Management in Standards und Frameworks ... 330
F.1.4.2.3 Das Security Incident Management in der Praxis ... 330
F.1.4.3 Das Problem Management in der Informationssicherheit ... 331
F.1.4.3.1 Gefahren eines mangelhaften Problem Managements ... 331
F.1.4.3.2 Das Problem Management in Standards und Frameworks ... 332
F.1.4.3.3 Das Problem Management in der Praxis ... 332
F.1.4.4 Das Change Management in der Informationssicherheit ... 332
F.1.4.4.1 Gefahren eines mangelhaften Change Managements ... 333
F.1.4.4.2 Das Change Management in Standards und Frameworks ... 333
F.1.4.4.3 Das Change Management in der Praxis ... 333

F.2 Informationssicherheits-Managementsystem (ISMS) zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit ... 335
(Prof. Dipl.-El.-Ing. Armand Portmann)
F.2.1 Managementsysteme ... 335
F.2.1.1 Informationssicherheits-Managementsystem nach ISO/IEC 27 001 ... 337
F.2.1.2 Zertifizierung des Informationssicherheits-Managementsystems ... 342
F.2.1.3 Integrierte Managementsysteme ... 343

F.3 Aufbau eines Identitäts- und Berechtigungsmanagements ... 345
(Daniel Conta)
F.3.1 Einleitung ... 345
F.3.2 Identitätsmanagement ... 345
F.3.2.1 Identitätsarten ... 345
F.3.2.2 Identifizierung von Identitäten ... 346
F.3.3 Zugriffskontrolle ... 347
F.3.3.1 Authentifizierung ... 347
F.3.3.2 Autorisierung ... 347
F.3.4 Berechtigungssteuerung ... 348
F.3.4.1 Rollen ... 348
F.3.4.2 Berechtigungen ... 348
F.3.4.3 Ressourcen ... 350

F.3.4.4 Lebenszyklusphasen ... 351
F.3.5 Role Based Access Control ... 352
F.3.6 Authentifikationsprozesse ... 353
F.3.6.1 Verteilung der Verantwortlichkeiten ... 353
F.3.6.2 Genehmigungsprozess ... 356
F.3.6.3 Benutzerverwaltung ... 358
F.3.6.4 Rollenverwaltung ... 358
F.3.6.5 Ressourcenverwaltung ... 359
F.3.6.6 Zugriffsverwaltung ... 360
F.3.6.7 Berechtigungsverwaltung ... 360
F.3.6.8 Validierung ... 361
F.3.7 Schrittweiser Aufbau eines Identity Access Managements ... 361
F.3.7.1 Schritt 1: Analyse der IT-Landschaft ... 361
F.3.7.2 Schritt 2: Festlegen von Anforderungen und Ziele ... 362
F.3.7.3 Schritt 3: Definition der Identitätsarten und -träger ... 364
F.3.7.4 Schritt 4: Bildung eines Rollenmodells ... 364
F.3.7.5 Schritt 5: Ressourcen überführen und konsolidieren ... 365
F.3.7.6 Schritt 6: Benutzer und Rollen zuordnen ... 366
F.3.7.7 Schritt 7: Einführung der Teilprozesse ... 367
F.3.7.8 Schritt 8: Schaffung von Kontrollmöglichkeiten ... 367
F.3.7.9 Schritt 9: Inbetriebnahme ... 368
F.3.7.10 Schritt 10: Kontinuierliche Verbesserung ... 369

G Risikomanagement

G.1 Risikomanagement – Einführung und Grundlagen ... 373
(Prof. Dr. Stefan Ruf; Prof. Dr. Nils Herda)
G.1.1 Einleitung ... 373
G.1.2 Grundlegende Begriffe und Definitionen des Risikomanagements ... 374
G.1.3 Unternehmerisches Risikomanagement ... 376
G.1.4 Normatives Risikomanagement im Kontext der Cyberrisiken ... 377
G.1.5 Strategisches Risikomanagement im Kontext der Cyberrisiken ... 378
G.1.6 Operatives Risikomanagement von Cyberrisiken ... 379

G.2 Integration der operativen Cybertechnologien in das Risikomanagement des Unternehmens ... 383
(Jens Hempel)
G.2.1 Beschreibung des Geltungsbereichs ... 383
G.2.1.1 Risikomanagement vs. OT-Cyberrisiko ... 383
G.2.1.2 Wo steht OT mit Bezug auf Cyberrisiken? ... 384
G.2.2 Lebenszyklus ... 386
G.2.2.1 Cyberrisiken im Vorfeld der OT-Nutzung ... 388
G.2.2.2 Souveränes Risikomanagement im OT-Betrieb ... 390
G.2.2.3 Wie bleibt das Rad am Rollen? ... 391
G.2.3 Tragende Säulen – mehr als Tools ... 392
G.2.3.1 Personen im Zentrum ... 392

G.2.3.2 Gemeinsames Vokabular ... 392
G.2.3.3 Vom GRC zum IRM ... 393
G.2.3.4 Standards im Praxisumfeld ... 394
G.2.3.5 Effizientes Risikomanagement ... 395
G.2.4 Ausblick ... 396

G.3 Cyberversicherungen als Element eines ganzheitlichen Risikomanagements ... 397
(Johannes Beckers; Dirk Kalinowski)
G.3.1 Einführung: Sinn und Zweck einer Cyberversicherung ... 397
G.3.1.1 Schadenbeispiele ... 397
G.3.1.2 Versicherungsmanagement – Einordnung in das Portfolio ... 398
G.3.1.3 Lösung: Cyberversicherung ... 399
G.3.2 Cyberversicherung ... 399
G.3.2.1 Inhalt und Aufbau einer Cyberversicherung ... 400
G.3.2.1.1 Drittschadendeckung ... 400
G.3.2.1.2 Eigenschadendeckung ... 400
G.3.2.2 Marktüberblick ... 401
G.3.2.3 Auswahlkriterien ... 402
G.3.2.4 Nutzenbewertung ... 404
G.3.3 Der Weg zum Abschluss einer Cyberversicherung ... 405
G.3.3.1 Technisch-organisatorische Voraussetzungen ... 405
G.3.3.2 Obliegenheiten ... 407
G.3.4 Ausblick ... 408
G.3.4.1 Künftige Entwicklung der Cyberversicherung ... 408
G.3.4.2 Silent Cover ... 408
G.3.4.3 Kumulbetrachtung ... 409

Resümee

Schlusswort des Herausgebers ... 411
(Thomas Schulz)

Management-Statement

Die Bedrohungslage für industrielle Steuerungssysteme wird sich weiter zuspitzen – wirtschaftliche und trotzdem sichere Lösungen zur Gefahrenabwehr sind aber vorhanden ... 415
(WAGO)

Abkürzungen ... 419

Lebensläufe ... 425

Quellenverzeichnis ... 432

Stichwortverzeichnis ... 469

Grußwort

Es ist in aller Munde: Wie andere Gesellschaftsbereiche revolutioniert Digitalisierung auch die Industrie rasend schnell. Das bietet vor allem für den Innovations- und Wirtschaftsstandort Deutschland enorme Potenziale, sei es Effizienz- und Qualitätssteigerung oder vollkommen neue, datenbasierte Geschäftsmodelle. Gleichzeitig gehen aber mit der Digitalisierung auch Herausforderungen in puncto Sicherheit einher. Wie sollen sensible Kundendaten sicher verwahrt und kritische Infrastrukturen vor dem Zugriff Unbefugter geschützt werden?

Insbesondere kleine und mittlere Unternehmen fühlen sich von Sicherheitsfragen überfordert. Cybersicherheit wird als trocken, teuer und aufwendig wahrgenommen. Dabei wird der Wert von durchdachten Sicherheitskonzepten für die Industrie 4.0 im Buch eindeutig herausgestellt: Cybersicherheit ist nicht nur sinnvoll, sondern absolute Grundvoraussetzung für erfolgreiche Digitalisierung. Standardisierte Sicherheitsarchitekturen werden zum «Enabler» für Industrie 4.0. Erst das Vertrauen in IT-Sicherheit ermöglicht datenbasierte Geschäftsmodelle und neue Partnerschaften. Die Autoren machen klar, dass Security als Qualitätsmerkmal in allen relevanten technischen Aktionsfeldern verankert werden muss – egal ob Smart Devices, Cloud Computing oder Industrial Control Systems.

Das Buch erklärt nicht nur die Bedeutung von IT-Sicherheit, sondern bietet auch die nötige Unterstützung. Durch eine umfangreiche Analyse des Themas fügen sich Beiträge der Experten und Praktiker zu einem Leitfaden für industrielle Anwender.

Damit Sicherheit umfassend und dauerhaft eintritt, bedarf es «Security by design». Eine vorausschauende Sicherheitskultur muss sich im Bewusstsein der Verantwortlichen sowie im Portfolio der Unternehmen widerspiegeln. Genauso wichtig ist jedoch die internationale Zusammenarbeit, denn die Bedrohungslage kennt keine Grenzen und Nationalitäten. Nur eine globale, standardisierte und vertrauenswürdige Sicherheitsinfrastruktur über gesamte Wertschöpfungsnetzwerke und industrieller Lebenszyklen ermöglicht es, die Potenziale der Industrie 4.0 voll auszuschöpfen. Hier geht das Buch auch auf die Rolle der Plattform Industrie 4.0 und ihrer Arbeitsgruppe «Sicherheit vernetzter Systeme» ein, die globale Key Player zusammenbringt, um Lösungsansätze, Handlungsempfehlungen und konkrete Anwendungsbeispiele für eine sichere, vernetzte Industrie zu entwickeln.

In diesem Sinne des Austausches und Know-how-Transfers bieten die folgenden Seiten viel Wissenswertes rund um das Thema Cybersicherheit – egal ob für Privatpersonen, Großkonzern oder Mittelstand.

Viel Spaß beim Lesen und Lernen!

Henning Banthien, Secretary General der Plattform Industrie 4.0

Vorwort des Herausgebers

Mehr als sechs Millionen Cyberangriffe finden jeden Tag weltweit statt. Anzunehmen ist, dass sich die Anzahl und Intensität hochspezialisierter Cyberangriffe in Zukunft weiter steigern werden. Die steigende Anzahl von «Smart Factories» mit neuen digitalen Technologien und vernetzten Objekten, wie sie Industrie 4.0 mit sich bringt, wird die Anfälligkeit für Cyberangriffe dynamisieren und die Angriffsfläche weiter erhöhen. Eine ständig steigende Angriffskomplexität und Angriffsqualität heben die Gefährdungslage zusätzlich auf ein neues Niveau.

Die Auswirkungen von Cyberattacken im Bereich der Industrie sind gravierend und können ernste Folgen haben: illegaler Wissens- und Technologietransfer durch Datendiebstahl und technische Spionage (streng vertrauliche Informationen zur Produktherstellung werden ausspioniert), Wirtschaftssabotage (sensible Produktionsdaten werden manipuliert oder das gesamte Wertschöpfungsnetzwerk wird komplett zum Stillstand gebracht) und nicht zuletzt leidet das Gesamtimage eines Unternehmens nach außen bei Geschäftspartnern und Kunden erheblich. Angesichts solcher Szenarien stellt sich immer drängender die Frage: Wie können wir die Digitalisierung so gestalten, dass die zu erwartenden Vorteile nicht durch den nächsten Cyberangriff zunichte gemacht werden?

Jedes industrielle Unternehmen ist dafür selbst verantwortlich, seine Unternehmensdaten und den laufenden Betrieb der Wertschöpfung sicher vor Cyberangriffen zu machen. Dies im Sinne des Unternehmenserfolges strategisch und nachhaltig umzusetzen ist Chefsache. Großunternehmen haben dabei im Laufe der letzten Jahrzehnte gegen Cyber-Sicherheitsvorfälle durch entsprechende Maßnahmen ein sehr hohes Absicherungsniveau erreicht. Doch wo ein international operierendes Großunternehmen erhebliche Summen investieren kann, um sich vor dubiosen Machenschaften Cyberkrimineller zu schützen, muss sich ein mittelständisches Unternehmen mit weitaus geringeren Mitteln helfen.

Eigenes Wissen ist dabei immer noch die beste Verteidigung. Mit dem vorliegenden Buch möchte ich als Herausgeber einen Beitrag dazu leisten, dass mittelständische Unternehmen einen leichteren Zugang zu dem Thema Cybersicherheit für vernetzte industrielle Anwendungen erlangen. Mit diesem Werk adressiere ich bewusst auch neue digitale Entwicklungen, wie sie Industrie 4.0 und die Digitalisierung mit sich bringen, und spreche den fachinteressierten Leser an, der sich grundlegend in die Thematik einarbeiten möchte und dafür praxisbezogene, allgemein verständliche Informationen benötigt.

Das Thema wird umfassend und in vielen Facetten beleuchtet und analysiert. Dabei liegt das Hauptaugenmerk der Beiträge nicht nur auf dem möglichen Gefahrenpotenzial, sondern auch in konkreten Handlungsanweisungen und Schutzmaßnahmen. Somit wird dem interessierten Leser ein praxisbezogener Leitfaden an die Hand gegeben, mit dessen Hilfe er das Konzept Cybersicherheit für vernetzte industrielle Anwendungen verstehen und umsetzen kann.

Dazu erarbeiteten wir mehrere sich ergänzende und ineinandergreifende Themenblöcke, die aus Expertensicht in ihrer Gesamtheit für die Entwicklung von Cybersicherheit bei Industrie 4.0 von zentraler Bedeutung sind. Durch einen abwechslungsreichen Mix wurde darauf geachtet, dass Einblicke aus Großkonzernen, Mittelstand, Start-ups sowie Meinungen von Forschungs- und Bildungseinrichtungen vermittelt werden. Das Werk besitzt eine sinnlogische Reihenfolge, aber einzelne Kapitel können auch unabhängig voneinander gelesen werden.

Der Mittelteil dieses Buches orientiert sich an den drei für die Praxis von Cybersicherheit für vernetzte industrielle Anwendungen besonders relevanten technischen Aktionsfeldern: die Informationstechnik auf den lokalen Servern und in den Datenzentren (IT – Information Technology), die industriellen Steuerungs- und Leitsysteme (OT – Operational Technology) und die in

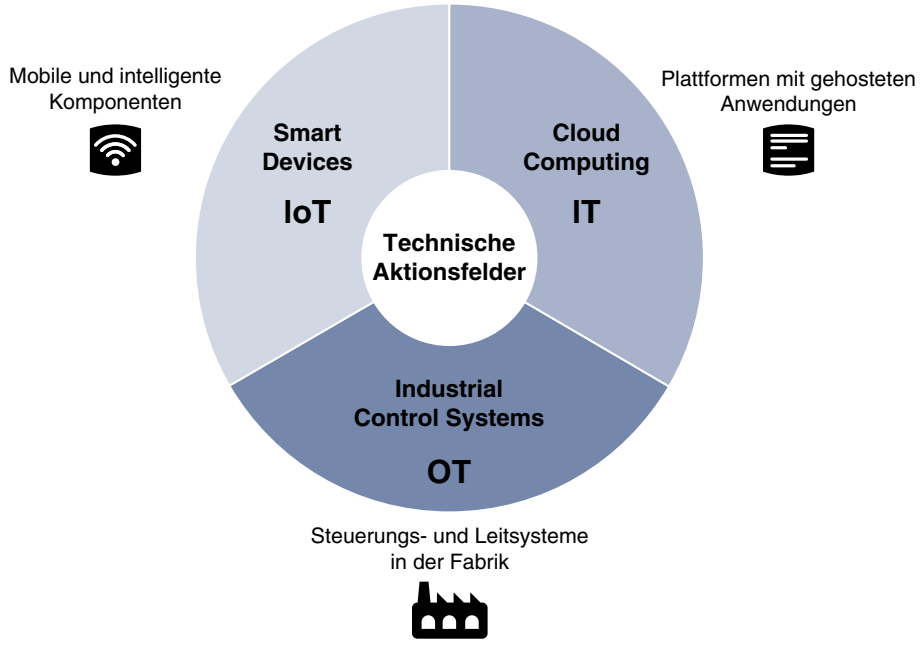

Bild 1 *Technische Aktionsfelder der Cybersicherheit bei Industrie 4.0*

industriellen Anwendungen verwendeten Komponenten des Internets der Dinge (IoT – Internet of Things).

Bild 1 fasst diese drei technischen Komponenten der Cybersicherheit zusammen. Die Sicherheitsarchitektur dieser drei technischen Systeme und Komponenten muss grundlegend neu gedacht werden. Dabei muss die Sicherheit durch «Security by Design» und «Security by Default» von vornherein gewährleistet sein.

Im Teil C «Fabrik als Anwendungsdomäne / Industrial Control Systems» wird der Unterschied zwischen Information Technology und Operational Technology herausgearbeitet. Cyberangriffe auf industrielle Anlagen und kritische Infrastrukturen können ernste Folgen haben und lassen sich nicht einfach durch übliche Sicherheitsmaßnahmen wie bei Anwendungen in der Büro- und IT-Umgebung vermeiden. Es werden typische Schwachstellen und das daraus resultierende grundlegende Bedrohungspotenzial für industrielle Steuerungssysteme, ergänzt durch Praxisbeispiele aus dem Monitoring von verschiedenen ICS, vorgestellt. Es erfolgt eine detaillierte Betrachtung technischer und organisatorischer Maßnahmen mit einzelnen Aspekten der Sicherheitskonzepte für ICS-Systeme. Insbesondere werden Besonderheiten automatisierter Sicherheitseinrichtungen (SIS) aus Sicht der Manipulierbarkeit bzw. Kompromittierbarkeit durch Cyberangriffe dargestellt und wesentliche Elemente eines dedizierten SIS-Cyber-Security-Managements beschrieben und Aspekte der praktischen Umsetzung erörtert.

Im Teil D «Mobile und intelligente Komponenten / Smart Devices» geben wir eine Einführung und einen Überblick über Cyber Security für Industrie-4.0-Komponenten als wichtigen Bestandteil vieler Industrie-4.0-Anwendungen. Diese Komponenten zeichnen sich dadurch aus, dass sie sich mit anderen Komponenten vernetzen und über Systemgrenzen hinweg kommunizieren, um so im Zusammenspiel mit Backend-Diensten die Industrie-4.0-Anwendungen zu realisieren. Die Teilnehmer in einem Industrie-4.0-System müssen sich in zunehmendem Maße auf die Korrekt-

heit, Vollständigkeit und Unverfälschtheit ihrer Daten, Systeme und Prozesse verlassen können. Insbesondere sind lokale Schnittstellen, Wartungs- und Administratorzugänge, die Datenspeicherung und die Netzwerkkommunikation zu schützen. Grundlegende Sicherheitsmaßnahmen umfassen den Schutz der ausgeführten Firmware und Software, den Schutz von kryptographischem Material, sichere Kommunikationsverbindungen sowie sichere Identitäten durch Identitätszertifikate. Mögliche Angriffe auf solche Geräte werden in praktischer Hinsicht analysiert und diskutiert.

Im Teil E «Plattformen mit gehosteten Anwendungen / Cloud Computing» befassen wir uns mit den wichtigsten Sicherheitsrisiken und Bedrohungsszenarien virtualisierter IT-Ressourcen wie Rechenkapazität, Datenspeicher, IoT-Plattformen und Software durch einen Service Provider über das Internet. Grundprinzipien des Datenschutzes und Prinzipien für die Sicherheit industrieller IoT-Plattformen werden beschrieben. Eine IoT-Plattform ist eine wiederverwendbare Basis an Technologien, Diensten und Realisierungen von Prozessen, auf denen aufbauend weitere Technologien, Dienste, Realisierungen von Prozessen und Anwendungen entwickelt werden können. Sicherheitsmechanismen, die bereits bei der Konzipierung der Plattform integriert sind, und Sicherheitsstrategien im Prozess der Anwendungsentwicklung spielen neben dem kontinuierlichen Monitoring mit intelligenter Detektion und schneller Reaktion auf Systemanomalien eine wesentliche Rolle.

In der Gesamtheit bedarf die offene, vernetzte Wertschöpfung der Industrie 4.0 einer durchgängigen, geschlossenen Lösung der Cybersicherheit zur Bewältigung der Gefahren durch neue digitale Technologien im industriellen Umfeld. Cybersicherheit ist dabei keine Innovationsbremse, sondern vielmehr ein wichtiger Garant für zukünftigen unternehmerischen Erfolg. Neben den drei technischen Aktionsfeldern beschreiben wir wichtige Einflussfaktoren, deren Kenntnisse für die Cybersicherheit vernetzter Industrie-4.0-Anwendungen in Unternehmen unterstützend oder zwingend notwendig sind (Bild 2).

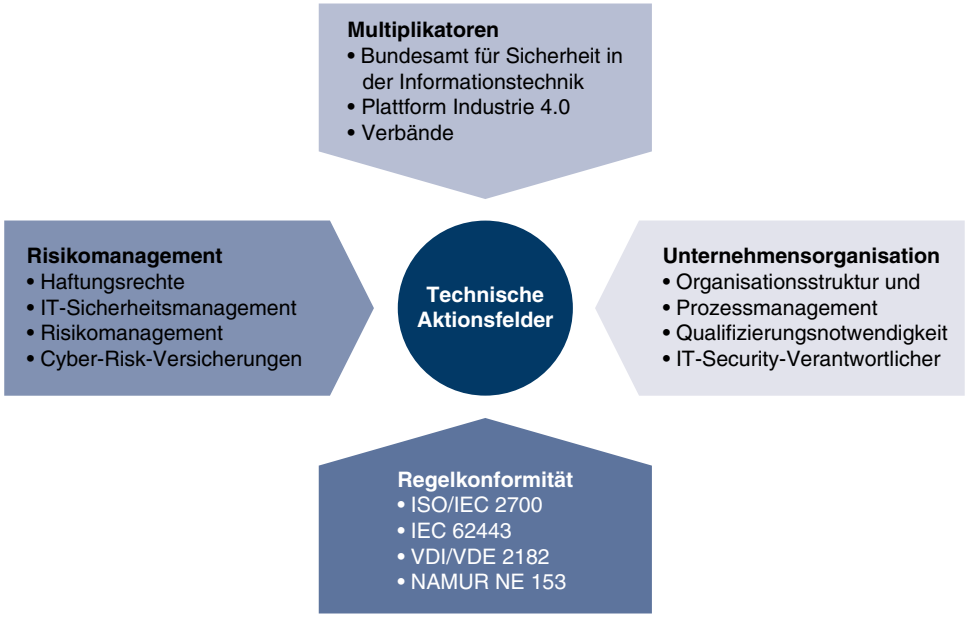

Bild 2 *Einflussfaktoren auf die technischen Aktionsfelder der Cybersicherheit*

Welche Multiplikatoren unterstützen die Industrie bei der Verbreitung und Akzeptanz von Cybersicherheit? Zum einen gilt das Bundesamt für Sicherheit in der Informationstechnik (BSI) als zentraler Ansprechpartner für den Ausbau der Beratung für die Wirtschaft zum Thema Informationssicherheit in der Digitalisierung. Weiterhin befassen sich mit dem Thema Cybersicherheit für vernetzte Anwendungen in der Industrie 4.0 der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), der Verband Deutscher Maschinen- und Anlagenbau e.V. (VDMA), der Zentralverband Elektrotechnik- und Elektronikindustrie e.V. (ZVEI), der Cyber-Sicherheitsrat Deutschland e.V. sowie die deutsche und die österreichische Plattform Industrie 4.0; sie haben dazu eigene Arbeitsgruppen gebildet, um ihren Mitgliedern aktive Unterstützung bei der Umsetzung dieser Thematik zu gewähren. Eine Vielzahl von Publikationen, größtenteils frei verfügbar im Internet, sind daraus hervorgegangen.

Im Teil A «Cybersicherheit als Voraussetzung für erfolgreiche Digitalisierung» gehen wir der Frage nach, welche Bedrohungen sich generell durch die Digitalisierung der Industrie ergeben. Das Vorgehen der Angreifer bei gezielten Angriffen wird beschrieben sowie die Auswirkungen von Angriffen auf Produktionssysteme und welche Veränderungen Industrie 4.0 mit sich bringen wird. Cybersicherheit wird als ein inhärenter Bestandteil der Digitalisierung definiert. Die steigende Komplexität verstärkt zunehmend die Verletzlichkeit der installierten Systeme. Neben vielfältigen bekannten Angriffsmethoden wird auch «Cyber Crime as a Service» als neuer Trend erläutert. Es wird die Schlussfolgerung gezogen, dass Digitalisierung und Cybersicherheit einer neuen Kultur des Miteinanders mit erweiterten Formen der Kooperation sowie neue Schutz- und Verteidigungsstrategien bedürfen.

Im Teil B «Regelkonformität mit Normen und Richtlinien» werden ausgesuchte, wichtige Standards vorgestellt. Die Normenreihe ISO/IEC 27000: IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme (ISMS) gibt die Möglichkeit, eine unternehmensweite Strategie im Hinblick auf Informationssicherheit zu etablieren. Mögliche Anwendungsbereiche und der Anwendernutzen von Umsetzungen werden aufgezeigt. Die Normenreihe IEC 62443: Industrielle Kommunikationsnetzte – IT-Sicherheit für Netze und Systeme hat sich zwischenzeitlich mit ihrem Umfang und ihrer Komplexität als der Security-Standard für die Automatisierungstechnik etabliert. Anwendungsbereiche und Umsetzungen werden erläutert. Die Richtlinienreihe VDI/VDE 2182: Informationssicherheit in der industriellen Automatisierung stellt ein allgemeines Vorgehensmodell zur Berücksichtigung von Security bei der Herstellung, Integration und Betrieb von industriellen Automatisierungskomponenten bzw. -anlagen vor. Die Anwendung des Vorgehensmodells wird aus Sicht des Herstellers, Integrators bzw. Maschinenbauers und Betreibers beschrieben. Das NAMUR-Arbeitsblatt NA 163: IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen beschreibt ein Verfahren, mit dem die IT-Sicherheit von Prozessleittechnik-Sicherheitssystemen schnell und einfach analysiert werden kann.

Im Teil F «Unternehmensorganisation» definieren wir die Sicherheit als eine feste Säule der Grundsätze der Unternehmensführung. Technik allein bringt noch keine Sicherheit. Deshalb gehen wir der Frage nach, wie nun die Etablierung und das Management von Informationssicherheit und Cyber-Security-Grundsätzen im Unternehmen erfolgen kann. Ein großer Teil aller Cyberbedrohungen kann schon mit gut koordinierten technisch-organisatorischen Methoden abgewehrt werden. Ein Informationssicherheits-Managementsystem (ISMS) dient dabei der Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit in einer Unternehmung. Dazu müssen die Risiken, die die Informationssicherheit bedrohen, identifiziert, bewertet und ihnen mit geeigneten Maßnahmen entgegengewirkt werden. Ein wichtiger Punkt ist dazu ein Identitäts- und Berechtigungsmanagement. Es regelt den unkontrollierten Informationsfluss und den generellen Zugang zu Informationen.

Im Teil G «Risikomanagement» befürworten wir, Risiken durch umfassende Analysen frühzeitig aufzudecken, um sich rechtzeitig auf mögliche Schadensfälle vorzubereiten. Durch systematische Risikomanagementprozesse sowie die Bereitstellung geeigneter Ressourcen für die Cyberabwehr können die Gefahren von Cyberangriffen und mögliche Verwundbarkeiten systematisch reduziert werden. Im Folgenden wird die Integration der operativen Cybertechnologien in das Risikomanagement des Unternehmens dargelegt. Ziel dabei ist es, die sich ergebenen Anforderungen effizient in existierende Risiko-Management-Systeme (RMS) einpassen zu können. Praktische Handlungsanweisungen zur Umsetzung des Risikomanagements für vernetzte industrielle Anwendungen werden vermittelt und die Auswirkungen des Risikomanagements auf den operativen Betrieb aus dem Blickwinkel der Betreiberverantwortung betrachtet. Cyberversicherungen können ebenso als ein Element eines ganzheitlichen Risikomanagements dienen. Sinn und Zweck einer Cyberversicherung für Produktionsbetriebe werden betrachtet.

Mein ganz besonderer Dank gilt Niels Bernau, der durch motivierenden Zuspruch, fachliche Diskussionen und konstruktive Anregungen in hohem Maße zum Gelingen der Arbeit beitrug. Dank sagen möchte ich dem gesamten Team der Vogel Communications Group für ihre freundliche Art und tatkräftige Unterstützung sowie die zahlreichen guten Ideen.

Thomas Schulz

D.1 Cybersicherheit für mobile und intelligente Komponenten – Einführung und Grundlagen

D.1.1 Einleitung

Industrie-4.0-Anwendungen versprechen mehr Flexibilität in der Produktion und eine stärkere Individualisierung der erzeugten Produkte. Ein wichtiger Bestandteil vieler Industrie-4.0-Anwendungen sind mobile und intelligente Komponenten. Diese Komponenten zeichnen sich dadurch aus, dass sie sich mit anderen Komponenten vernetzen und im Zusammenspiel mit Backend-Diensten die Industrie-4.0-Anwendungen realisieren. Oftmals kommunizieren die betrachteten mobilen und intelligenten Komponenten über Systemgrenzen hinweg, öffnen also vormals geschlossene Systeme nach außen (siehe z.B. [1]). Sie bewegen sich dabei in einem meist jahrzehntealten Umfeld mit Systemen, die niemals für eine Öffnung vorgesehen waren und nur allmählich erneuert werden, wobei die relevanten Innovationszyklen im Bereich von Jahrzehnten liegen können.

Als wesentliche Bestandteile einer Industrie-4.0-Anwendung und durch den hohen Grad der Vernetzung auch über Systemgrenzen hinweg haben mobile und intelligente Komponenten ein erhöhtes Risiko für Angriffe aus dem Cyberraum. Es ist zu beobachten, dass beim Entwurf von mobilen und intelligenten Komponenten aus Kostengründen bevorzugt herkömmliche IT-Komponenten eingesetzt werden, wodurch die Anfälligkeit für in der Office IT gängige Angriffe steigt. Durch die in typischen Industrieautomatisierungsnetzen oft nicht ausreichenden oder gar fehlenden Schutzmechanismen ist die Notwendigkeit der besonderen Sorgfalt bei der Betrachtung der Cybersicherheit von mobilen und intelligenten Komponenten gegeben.

D.1.2 Cybersicherheit in Industrie-4.0-Anwendungen

Die Cybersicherheit betrachtet alle Seiten der Informationssicherheit und Kommunikationssicherheit, wobei der in der IT-Sicherheit übliche Blick auf einzelne Systeme erweitert wird auf die Betrachtung des gesamten Cyberraums. Der Cyberraum umfasst dabei sämtliche mit öffentlichen Netzen wie dem Internet verbundene Systeme und deren Interaktion – sowohl extern als auch intern. Gerade in Industrie-4.0-Szenarien mit einer hohen Vernetzung der Komponenten untereinander ist eine Erweiterung des Fokus von IT-Sicherheit auf Cybersicherheit notwendig und nützlich.

Die Erfahrungen mit der Absicherung von komplexen Systemen haben gezeigt, dass diese nie vollständig und umfassend gegen Angriffe geschützt werden können, denn in der Cybersicherheit existiert ein Ungleichgewicht zwischen dem Aufwand des Angreifers und dem Aufwand des Verteidigers, dem Betreiber einer Industrie-4.0-Anwendung. Während ein Angreifer lediglich eine ausnutzbare Sicherheitslücke in einem Industrie-4.0-System identifizieren muss, um erfolgreich zu sein, muss der Verteidiger alle Sicherheitslücken schließen, um erfolgreich zu sein – ein sehr mühseliges Unterfangen, das selten von Erfolg gekrönt ist. Das Ungleichgewicht zwischen Angreifer und Verteidiger ist der Grund, warum es im letzten Jahrzehnt einen Paradigmenwechsel vom Ansatz «*Perimeterschutz*» hin zum Ansatz «*Defense in Depth*» gab.

Bild D.1.1 zeigt ein Beispiel für Perimeterschutz. Beim *Perimeterschutz* basiert die Sicherheit eines Systems darauf, dass der Perimeter, also die Systemgrenze, möglichst undurchlässig gestaltet wird und dort starke Sicherheitsmechanismen zum Einsatz kommen. Innerhalb des Perimeters wurden jedoch häufig Sicherheitsmechanismen vernachlässigt. Der Angreifer musste also für einen erfolgreichen Angriff lediglich den Perimeter überwinden. Mit stark vernetzten -Industrie-4.0-Systemen wird dieser Ansatz mehr und mehr wirkungslos, weswegen «Defense in Depth» eingesetzt wird.

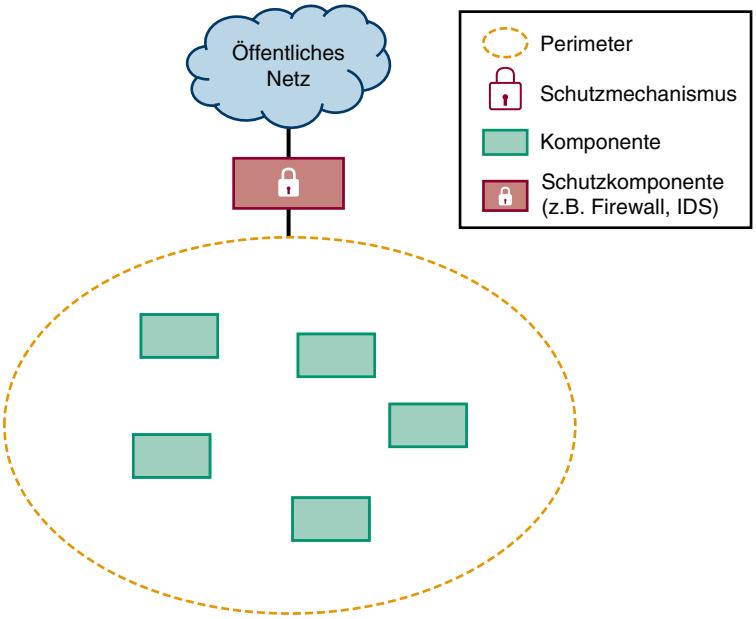

Bild D.1.1 *Perimeterschutz*

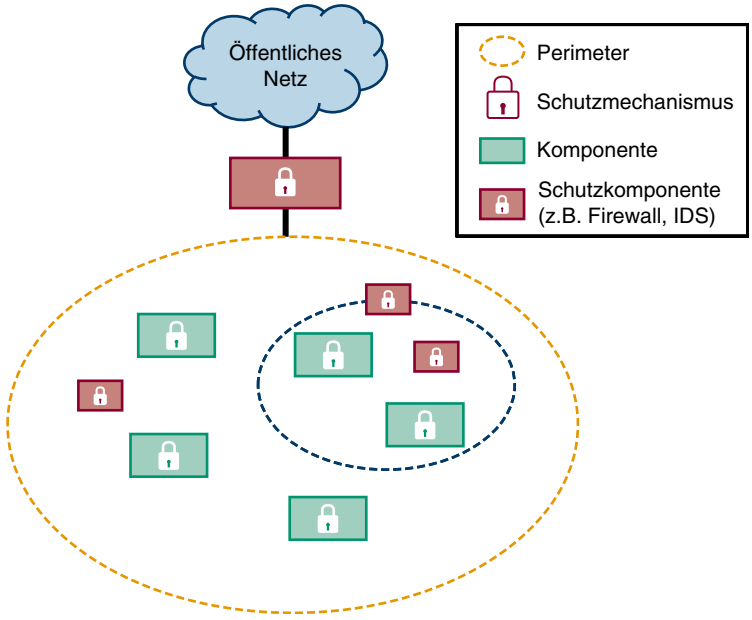

Bild D.1.2 *Defense in Depth*

Bild D.1.2 zeigt ein Beispiel für Defense in Depth. Die Schutzwirkung von «*Defense in Depth*» beruht auf vielen verschiedenen Sicherheitsmechanismen sowohl innerhalb des eigenen Systems als auch an den Systemgrenzen. Konzeptionell können auch innerhalb des eigenen Systems

Perimeter existieren, die Bereiche mit erhöhtem Schutzbedarf vom Rest des eigenen Systems trennen. Die in Defense in Depth verwendeten Sicherheitsmechanismen sind idealerweise so angeordnet, dass ein Angreifer sie nacheinander überwinden muss, um erfolgreich zu sein. Der Angreifer muss also eine größere Anzahl an Sicherheitslücken finden und ausnutzen und hat damit einen größeren Aufwand. Dem «Defense in Depth»-Ansatz liegt auch das Sicherheitsprinzip «Assume a state of compromise» zugrunde, das aussagt, dass man im Betrieb eines Systems immer davon ausgehen muss, dass zumindest ein Teil des Systems von einem Angreifer infiltriert ist. Deswegen setzt Defense in Depth Methoden zur Erkennung und Nachverfolgung von laufenden Angriffen ein, z.B. Intrusion-Detection-Systeme (IDS). In Bild D.1.2 sind die IDS als Schutzkomponenten dargestellt, die sich nicht auf einem Perimeter befinden (graues Rechteck mit Schloss ohne Verbindung zu einer gestrichelten Linie). Durch die Notwendigkeit zur sequenziellen Überwindung der implementierten Sicherheitsmechanismen steigt für den Angreifer die Gefahr einer Entdeckung, so dass die angewendeten Angriffserkennungsmethoden effektiv arbeiten.

Sowohl «Defense in Depth» als auch das Prinzip «Assume a state of compromise» rücken Schutzmaßnahmen für mobile und intelligente Komponenten in den Blickpunkt der Industrie-4.0-Sicherheit. Wenn Systeme zumindest zum Teil infiltriert sind, dann stellen mobile und intelligente Komponenten ein interessantes Einfallstor in Industrie-4.0-Anwendungen dar, zumal in bisherigen Systemen die IT-Sicherheit von mobilen und intelligenten Komponenten eher selten betrachtet wurde.

Ebenso wie bei vielen anderen Systemen stehen auch bei Industrie-4.0-Systemen die VIVA-Kriterien als Sicherheitsziele im Mittelpunkt der Betrachtungen: **V**ertraulichkeit, **I**ntegrität, **V**erfügbarkeit und **A**uthentizität.

Vertraulichkeit ist wie folgt definiert:

DEFINITION

Ein System oder eine Komponente eines Systems gewährleistet **Vertraulichkeit** (engl.: *confidentiality*), wenn kein unautorisierter Informationsgewinn möglich ist.

Der Begriff «unautorisiert» in dieser Definition bedeutet, dass keine Erlaubnis vorliegt. Die Unterscheidung von autorisiertem und nicht autorisiertem Zugriff auf Informationen ist notwendig, um sowohl Sender und Empfänger von Informationen die Wahrnehmung dieser Informationen zu ermöglichen und zusätzliche, berechtigte Aufgabenbereiche zu berücksichtigen, z.B. einen Systemadministrator. Der Begriff «Informationsgewinn» in der Definition bezeichnet durch den Angreifer gewonnenes zusätzliches Wissen über Informationen in dem betrachteten System oder in der betrachteten Systemkomponente. Es ist dabei zu beachten, dass dieser Informationsgewinn sowohl die geschützten Informationen betreffen kann als auch Metadaten über diese Informationen.

Das Sicherheitsziel Integrität hat einen Schutz vor Manipulationen zum Inhalt:

DEFINITION

Ein System gewährleistet **Integrität** von Daten (engl.: *integrity*), wenn es einer Entität nicht möglich ist, die zu schützende Daten unautorisiert und unbemerkt zu manipulieren.

Der Begriff «unautorisiert» ist genauso definiert wie in der Definition von Vertraulichkeit. Ebenso wie bei der Definition des Sicherheitsziels Vertraulichkeit wird auch für das Sicherheitsziel Integrität berücksichtigt, dass es berechtigten Entitäten möglich sein soll, Daten zu manipulieren. Die Definition von Integrität fordert nicht, dass Manipulationen verhindert werden sollen, sondern lediglich, dass die Daten nicht unbemerkt geändert werden können. Dies ist dadurch motiviert, dass es in vielen Fällen gar nicht möglich ist, eine Manipulation zu verhindern. So kann z.B. in der drahtlosen Kommunikation nicht ausgeschlossen werden, dass ein Angreifer die Funkkommunikation durch zeitgleiches Senden stört und damit die Kommunikation manipuliert. Dies ist durch die Eigenschaft des Funkmediums bedingt. Jedoch können solche Manipulationen erkannt werden. Die oben genannte Definition ist für die allermeisten Anwendungsfälle ausreichend. In wenigen Fällen ist starke Integrität notwendig.

DEFINITION

Ein System gewährleistet **starke Integrität** von Daten oder Systemen (engl.: *integrity*), wenn es einer Entität nicht möglich ist, die zu schützenden Daten / das zu schützende System unautorisiert zu manipulieren.

Diese Definition sagt aus, dass eine nachträgliche Manipulation von Daten nicht möglich ist. Anwendung findet das Sicherheitsziel starke Integrität dann, wenn es Gründe gibt, dass Daten über die gesamte Lebenszeit hinweg nachvollziehbar sein müssen oder wenn auch eine erkannte Manipulation von Daten größeren Schaden nach sich ziehen kann.

Das Sicherheitsziel Verfügbarkeit thematisiert die Erreichbarkeit und Reaktionsfähigkeit eines Systems. Von allen Sicherheitszielen ist Verfügbarkeit oft am schwersten zu realisieren. Gerade in Industrie-4.0-Systemen existieren jedoch Systembausteine, die hohe Anforderungen an die Verfügbarkeit haben (z.B. Echtzeitanforderungen). Aktuelle Distributed-Denial-of-Service-Angriffe wie z.B. Mirai [2] gefährden die Verfügbarkeit aller mit dem Internet verbundenen Systeme.

Verfügbarkeit ist wie folgt definiert:

DEFINITION

Ein System gewährleistet **Verfügbarkeit** (engl.: *availability*), wenn authentifizierte und autorisierte Entitäten in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden können.

Der Begriff «autorisiert» ist analog zum Begriff «unautorisiert» in den Definitionen von Vertraulichkeit und Identität festgelegt. Der Begriff «authentifiziert» bezieht sich hier darauf, dass die Echtheit einer behaupteten digitalen Identität bereits sichergestellt ist. Wie auch schon bei Integrität wurde hier eine schwache Form des Sicherheitsziels definiert, da nur für authentifizierte Entitäten die Erreichbarkeit und Reaktionsfähigkeit sichergestellt werden müssen. Auch hier ist diese Definition der Praxis geschuldet, in der es sehr schwer – sogar nahezu unmöglich – ist, anonyme Benutzer von Angreifern zu unterscheiden. Wenn aber nur authentifizierte Benutzer von Angreifern sicher unterschieden werden können, dann macht es auch nur Sinn, Vertraulichkeit über diesen Weg zu definieren. Übrigens umfasst die hier vorgestellte Definition von Vertraulichkeit nicht nur die Verhinderung der Dienstnutzung, sondern stellt schon eine Beeinträchtigung als zu verhindernder Angriff dar. In diesem Sinne wäre also eine weitere, schwächere Definition

von Verfügbarkeit möglich. Hier besteht jedoch das Problem, ein noch akzeptables Niveau der Dienstbereitstellung zu definieren.

Schließlich berücksichtigt das Sicherheitsziel Authentizität die Echtheit von digitalen Identitäten, also den Absender oder Besitzer von Daten.

DEFINITION

Unter der **Authentizität** (engl.: *authenticity*) eines Objekts bzw. Subjekts versteht man die Echtheit und Glaubwürdigkeit des Objekts bzw. Subjekts, die anhand einer eindeutigen digitalen Identität und charakteristischer Eigenschaften überprüfbar ist.

Das Sicherheitsziel Authentizität wird durch die Vorgänge Authentisierung (Echtheit nachweisen) und Authentifizierung (Echtheit überprüfen) realisiert. Der Besitzer einer digitalen Identität authentisiert sich also an einem Dienst, der entsprechende Dienst authentifiziert den Besitzer. Es soll an dieser Stelle darauf hingewiesen werden, dass selbst in der Fachpresse die Begriffe Authentifizierung und Authentisierung oft nicht korrekt verwendet werden, oft sogar als synonym angesehen werden.

D.1.3 Allgemeine Bedrohungen der Sicherheitsziele in Industrie-4.0-Anwendungen

Angriffe bedrohen die im letzten Abschnitt beschriebenen Sicherheitsziele von Industrie-4.0-Anwendungen.

Angriffe auf die Vertraulichkeit von mobilen und intelligenten Komponenten in Industrie-4.0-Systemen umfassen insbesondere das Abhören von Kommunikationsverbindungen und das Auslesen von Speichermedien, wenn ein Zugriff auf die mobile und intelligente Komponente möglich ist. Das Abhören von Kommunikationsverbindungen kann sowohl als passiver Angriff oder als aktiver Angriff realisiert werden.

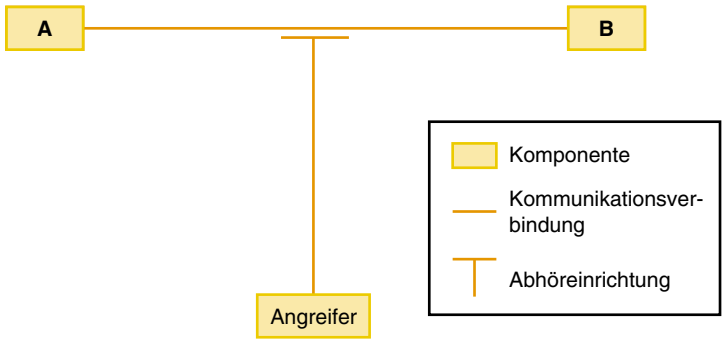

Bild D.1.3 *Abhören einer Kommunikationsverbindung*

Bild D.1.3 zeigt einen passiven Angriff: Die Komponenten A und B kommunizieren miteinander, der Angreifer hört diese Kommunikationsverbindung mittels einer Abhöreinrichtung ab.

Handelt es sich bei der Verbindung zwischen A und B um eine Funkstrecke, so ist – zumindest bei unverschlüsselten Verbindungen – lediglich ein Gerät zum Abhören notwendig, das den verwendeten Funkstandard implementiert. Passive Angriffe auf Kommunikationsverbindungen sind sehr schwierig zu erkennen, da ein Angreifer nicht aktiv in das Netzwerk eingreift, sondern passiv bleibt.

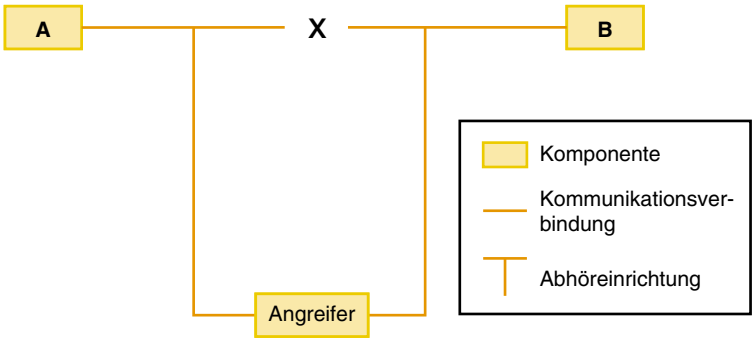

Bild D.1.4 *Man-in-the-Middle-Angriff auf eine Kommunikationsverbindung*

Bild D.1.4 zeigt einen aktiven Angriff zum Abhören auf eine Kommunikationsverbindung: einen so genannten **Man-in-the-Middle-Angriff**. Bei diesem Angriff unterbricht der Angreifer die Kommunikationsverbindung zwischen A und B und leitet diese Kommunikationsverbindung über sich selbst um. Dadurch kann der Angreifer den Datenstrom mitlesen und auch manipulieren. Angriffe auf die Vertraulichkeit können einerseits der Industriespionage dienen und andererseits der Erlangung von Zugriffsdaten auf andere Systeme. Der Angriff auf die Vertraulichkeit kann also sowohl das eigentliche Ziel des Angreifers sein als auch eine Vorstufe zum eigentlichen Angriff.

Angriffe auf die Integrität in Industrie-4.0-Anwendungen dienen meist zur Manipulation von Industrie-4.0-Anwendungen. Beispielsweise können einzelne mobile und intelligente Komponenten manipuliert werden. Sind diese Komponenten in Steuer- oder Regelkreisläufe eingebunden, so kann eine einzelne angegriffene Komponente dazu führen, dass die gesamte Industrie-4.0-Anwendung sich nicht mehr regelkonform verhält. Der Angriff kann z.B. wie oben erwähnt mit einem Man-in-the-Middle-Angriff durchgeführt werden. Ebenfalls ist es möglich, auf verwendeten Datenträgern (z.B. SD-Karten) gespeicherte Daten zu manipulieren.

Angriffe auf die Verfügbarkeit dienen oft der Sabotage von Industrie-4.0-Anwendungen. Die Angriffe können sich sowohl gegen Komponenten der Industrie-4.0-Anwendung richten als auch gegen die Netzwerkanbindung, über die die Komponenten der Anwendung kommunizieren. Man spricht in diesem Fall von einem **Denial-of-Service-Angriff**. Ein Denial-of-Service-Angriff (DoS-Angriff) ist ein Angriff, der es zum Ziel hat, durch den Verbrauch oder die Blockade von System- oder Netzwerk-Ressourcen die Reaktionsfähigkeit eines Systems einzuschränken. Ein Spezialfall von Denial-of-Service-Angriffen sind **Distributed-Denial-of-Service-Angriffe** (DDoS-Angriffe). Bei einem DDoS-Angriff erfolgt der Ressourcenverbrauch nicht durch ein einziges entferntes System, sondern durch eine Großzahl von Systemen. Die erschwert ganz erheblich die Abmilderung von Angriffen, da eine einfache Filterung der entfernten Angreifer nach Netzwerkadressen aufgrund der großen Anzahl von Angreifern nicht mehr möglich ist.

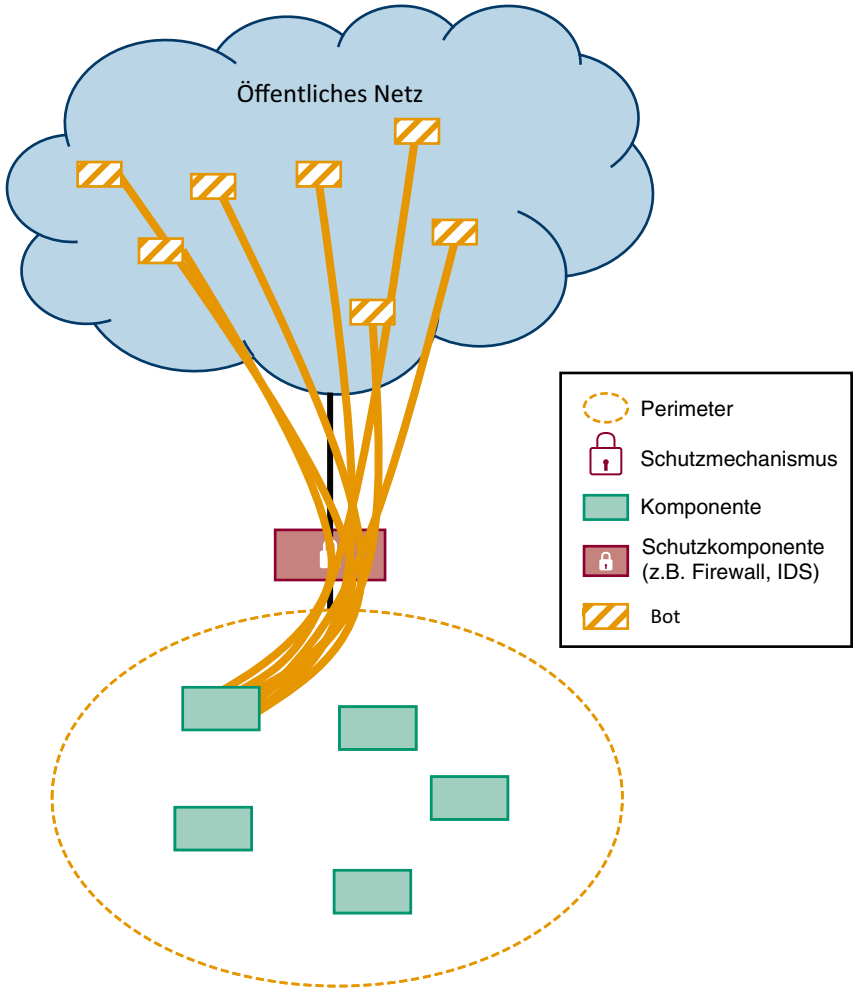

Bild D.1.5 *Distributed-Denial-of-Service-Angriff*

Mobile und intelligente Komponenten können auf zweierlei Arten durch Distributed-Denial-of-Service-Angriffe in Mitleidenschaft gezogen werden. Einerseits kann ein Angreifer Sicherheitslücken in der Implementierung einer mobilen und intelligenten Komponente nutzen, um die Komponente zu übernehmen und einem sogenannten **Botnetz** hinzuzufügen. Ein Botnetz ist eine Sammlung von gehackten IT-Systemen (sogenannte Bots), die durch einen Botnetzbetreiber, den eigentlichen Angreifer, gesteuert werden. Botnetze finden häufig Einsatz bei Distributed-Denial-of-Service-Angriffen, um die Angriffslast durch viele verschiedene Systeme zu erzeugen. Bild D.1.5 zeigt einen beispielhaften Angriff, bei dem mehrere Bots eine einzelne Komponente der Industrie-4.0-Anwendung angreifen. In der Abbildung ist der koordinierende Angreifer nicht dargestellt.

Ein aktuelles Botnetz, das Mirai-Botnetz [2], griff z.B. Internet-der-Dinge-Geräte an, indem es Default-Passwörter durchprobierte. Bei Erfolg übernahm Mirai die Kontrolle über das Gerät. Betroffen waren vor allem Überwachungskameras, Router und VoIP-Telefone. In Summe konnte das Mirai-Botnetz eine Angriffsbandbreite von mehr als einem Terrabit pro Sekunde erreichen

und hat damit das Potenzial, die Netzwerk-Anbindung der allermeisten Industrie-4.0-Anwendungen überlasten zu können. Im Jahr 2016 demonstrierte Mirai seine Schlagkraft, indem es die Managed DNS Services der Firma Dyn erfolgreich angriff. Im Internet ist das DNS-System für die Übersetzung von DNS-Namen (z.B. www.thi.de) in IP-Adressen (z.B. 194.94.240.176) zuständig. Genau diese Namensauflösung lagern viele Firmen über Managed DNS Services an externe Firmen aus, wobei Dyn als einer der Marktführer gilt. Der erfolgreiche Angriff auf Dyn führte zu Beeinträchtigungen auch großer Webseiten, z.B. Airbnb, Amazon.com und somit zu einem Schaden in Millionenhöhe.

Schließlich können **Angriffe auf die Authentizität** eine Sabotage von Industrie-4.0-Anwendungen ermöglichen. Die Authentifizierung ist ein ganz grundlegender Dienst, auf dem jede weitere Rechtevergabe innerhalb eines Systems basiert. Neben der Authentifizierung kann auch die Authentizität von ausgetauschten Nachrichten angegriffen werden – mit denselben Auswirkungen.

D.1.4 Spezifische Bedrohungen für mobile und intelligente Komponenten in Industrie-4.0-Anwendungen

Nachdem oben allgemeine Angriffe auf Industrie-4.0-Anwendungen betrachtet wurden, widmet sich dieser Abschnitt spezifischen Bedrohungen für mobile und intelligente Komponenten. Die Bedrohungen betreffen die folgenden Bereiche:

- unsichere lokale Schnittstellen,
- unsichere Wartungs- und Administrationszugänge,
- unsichere Zugangskontrolle,
- unsichere Datenspeicherung,
- unsichere Netzwerkkommunikation.

Die einzelnen Bedrohungsbereiche werden im Folgenden beschrieben.

D.1.4.1 Bedrohungen durch unsichere lokale Schnittstellen

Lokale Schnittstellen zeichnen sich dadurch aus, dass sie nur über physikalischen Zugriff auf die mobile und intelligente Komponente oder in der unmittelbaren Umgebung der Komponente zugreifbar sind. Lokale Schnittstellen umfassen unter anderem

- serielle Schnittstellen,
- USB-Ports,
- JTAG-Schnittstelle,
- Nahbereichsfunktechniken, z.B. Bluetooth, Zigbee usw.

Oft wird beim Design von mobilen und intelligenten Geräte davon ausgegangen, dass ein Angreifer keinen physikalischen Zugriff auf eine Komponente hat. Es ist genau zu evaluieren, ob diese Annahme für eine konkrete Industrie-4.0-Anwendung auch wirklich hält. Selbst Komponenten, die auf einem geschützten Firmengelände eingesetzt werden, müssen vor physikalischem Zugriff geschützt werden, da heutzutage beim Design von Industrie-4.0-Anwendungen auch von Innentätern ausgegangen werden muss.

Angriffe auf die lokalen Schnittstellen nutzen meist eine fehlende oder schwache Authentifizierung an lokalen Schnittstellen aus, beispielsweise eine Standard-PIN 0000 bei einer Bluetooth-Schnittstelle. Oft verfügen mobile und intelligente Systeme über weitreichende Interaktionsmöglichkeiten über eine lokale Schnittstelle. Das Ziel des Angreifers ist es, über die lokale Schnittstelle einen Administrationszugang zum System zu erlangen, z.B. um die Komponente zu übernehmen, wie oben beim Botnet Mirai beschrieben. Dies ist oft möglich, weil die Industrie-4.0-Anwendung davon ausgeht, dass lokaler Zugang zu einer mobilen und intelligenten Komponente nur autorisiertem Personal möglich ist. Deswegen ist die Nutzung von privilegierten Command Line Interfaces oft nur lokal an der Komponente möglich. Eine weitere Angriffsmöglichkeit ist das Zurücksetzen der mobilen und intelligenten Komponente mit der Hoffnung, dass ein unsicherer Zustand eingenommen wird, der für Angriffe ausnutzbar ist. Bei vielen mobilen und intelligenten Komponenten ist es über physikalischen Zugriff auf die Komponente möglich, einen Reset oder eine Zurücksetzung der Komponente auf Werkseinstellungen auszulösen.

Schließlich kann durch physikalischen Zugriff oft auf Hardware-Debugging-Schnittstellen (z.B. JTAG) oder Hardware-Konfigurationsschalter (Jumper oder DIP-Schalter) zugegriffen werden. Auch für diese Zugangsmöglichkeiten zum System wird oft angenommen, dass sie nur von autorisierten Personen vorgenommen werden können.

D.1.4.2 Bedrohungen durch unsichere Wartungs- und Administrationszugänge

Viele Industrie-4.0-Anwendungen bieten heute ein Web-Interface – oftmals verfügen auch die mobilen und intelligenten Komponenten über ein eigenes Web-Interface, z.B. zur Konfiguration und Wartung. Verfügen Komponenten über ein Web-Interface, so sind prinzipiell alle Angriffe, die auf Web-Anwendungen anwendbar sind, auch auf den mobilen und intelligenten Komponenten durchführbar. Für eine Liste der zehn häufigsten Bedrohungen von Web-Anwendungen sei auf das OWASP Top 10 Web Application Security Risks Project hingewiesen [3]. Allerdings unterscheidet sich die Häufigkeit von Angriffsarten bei Industrie-4.0-Komponenten oftmals von Angriffen auf Web-Anwendungen. Bedingt durch die meist einfache Implementierung von Web Interfaces von mobilen und intelligenten Komponenten kommen dort oft keine Datenbanken zum Einsatz, so dass beispielsweise SQL-Injection-Schwachstellen seltener sind als in klassischen Web-Anwendungen. Allerdings werden bei Web-Interfaces von mobilen und intelligenten Komponenten oft CGI-Skripte eingesetzt, so dass Command Injection weitaus häufiger vorkommt als bei normalen Web-Anwendungen. Beim Angriff Command Injection gelingt es einem Angreifer, durch geschickte Wahl der Benutzereingabe (z.B. im Authentifizierungsdialog) einen Linux-Befehl auf der Kommandozeile zur Auswahl zu bringen.

Weitaus häufiger als bei normalen Web-Anwendungen werden bei Web Interfaces von mobilen und intelligenten Komponenten Default-Passwörter für den Zugang eingesetzt, also fest voreingestellte Passwörter. Diese Passwörter sind meist relativ schnell der Allgemeinheit bekannt. Einer der erfolgreichsten Botnetze der letzten Jahre, das Mirai-Botnetz, nutzte eine Liste von bekannten Default -Passwörtern für Default-Benutzeraccounts, um Hunderttausende von Internet-der-Dinge-Geräten zu übernehmen und mit diesen die bis zu diesem Zeitpunkt unerreichte Angriffsbandbreite für Denial-of-Service-Angriffe zu erreichen. Da Web-Interfaces von mobilen und intelligenten Komponenten oft über passwortbasierte Authentifizierung verfügen, sind sie auch für alle Schwachstellen von passwortbasierter Authentifizierung empfänglich. Dies bezieht sich auch auf die zugelassene Verwendung von schwachen Passwörtern, die mit Durchprobieren schnell erraten werden können.

Eine besondere Form der Wartungs- und Administrationszugänge ist die Funktionalität von Software- und Firmware-Update. Da Software in der Praxis nicht ohne Fehler entwickelt werden kann (siehe z.B. [4, 5]), sehen viele mobile und intelligente Komponenten von Industrie-4.0-Anwendungen eine Möglichkeit zum Software- bzw. Firmware-Update vor. Diese Update-Funktionalität kann meist aus der Ferne genutzt werden. Für einen Angreifer stellt die Update-Funktionalität einen interessanten Angriffsvektor dar. Dabei versucht der Angreifer, der Update-Funktionalität eigenen Angriffscode unterzuschieben, so dass dieser auf der mobilen und intelligenten Komponente installiert und ausgeführt wird. Besonders bedroht sind Update-Funktionen, die keinerlei kryptographische Sicherung von Updates vornehmen, also keine Signierung von Code verwenden.

Aber selbst bei der Verwendung von Code-Signaturen durch die Update-Funktionalität ist immer noch ein so genannter Downgrading-Angriff möglich. Bei diesem Angriff spielt ein Angreifer eine veraltete Softwareversion mit bekannten Sicherheitslücken in die mobile und intelligente Komponente ein. Das Update verfügt über eine gültige Signatur, da es sich ja um ein gültiges Update aus der Vergangenheit handelt. Anschließend nutzt der Angreifer die bekannten Sicherheitsschwachstellen der alten Software / Firmware aus.

D.1.4.3 Bedrohungen durch unsichere Zugangskontrolle

Angriffe auf Komponenten können auf die **Zugangskontrolle der Industrie-4.0-Anwendung** zielen, an deren Realisierung eine mobile und intelligente Komponente beteiligt ist. Typische Schwachstellen umfassen:

- implizites Vertrauen zwischen Komponenten,
- Enrollment,
- Außerbetriebsetzung,
- Widerruf von Zugangsberechtigungen.

Eine typische Schwachstelle in diesem Kontext ist implizites Vertrauen zwischen Komponenten. Implizites Vertrauen wird während des Designs der Industrie-4.0-Anwendung definiert. Probleme entstehen dadurch, dass durch das implizite Vertrauen die Angriffsoberfläche einer mobilen und intelligenten Komponente auf weitere Komponenten und die Kommunikation mit diesen erweitert wird. Verfügt die vertraute Komponente über eine ausnutzbare Schwachstelle, so ist auch die vertrauende Komponente von einem Angriff betroffen.

Eine weitere Schwachstelle ist oft das Enrollment von Komponenten.

DEFINITION

Mit **Enrollment** wird die Aufnahme von intelligenten und mobilen Anwendungen in die Industrie-4.0-Anwendung bezeichnet.

Die Aufnahme umfasst auch eine Konfiguration der Sicherheit. Ist das Enrollment nicht sicher gestaltet, so kann die Komponente durch einen Angreifer unsicher konfiguriert werden oder für den Schutz der Kommunikation genutzte geheime Schlüssel werden bekannt. Das Enrollment ist meist anwendungsspezifisch, so dass eine Anpassung für die jeweilige Industrie-4.0-Anwendung notwendig ist.

Auch der komplementäre Prozess zum Enrollment, die Außerbetriebsetzung einer mobilen und intelligenten Komponente, stellt oft eine Sicherheitsschwachstelle dar. Bei der Außerbetriebsstellung muss sichergestellt werden, dass die Industrie-4.0-Anwendung die außer Betrieb gestellte mobile und intelligente Komponente nicht mehr akzeptiert. Weiterhin sollten alle geheimen Daten sicher von der mobilen und intelligenten Komponente gelöscht werden.

Schließlich müssen auch Mechanismen vorgesehen werden, die es ermöglichen, bei verloren gegangenen Zugangsrechten die verwendeten Credentials (Schlüssel, Passwörter usw.) zu sperren und einen Zugang für einen legitimen Akteur wiederherzustellen.

D.1.4.4 Bedrohungen durch unsichere Datenspeicherung

Eine mobile und intelligente Komponente speichert üblicherweise sowohl vertrauliche Daten einer Industrie-4.0-Anwendung selbst als auch vertrauliche Daten wie Schlüssel, die zum Schutz der Kommunikationsbeziehungen verwendet werden. Diese Daten müssen sowohl im volatilen Speicher als auch auf persistenten Speichermedien dem Sicherheitsniveau der Industrie-4.0-Anwendung angemessen geschützt werden. Liegen diese Informationen unverschlüsselt im Speicher vor, so kann ein Angreifer nach einem erfolgreichen Angriff darauf zugreifen. Viele heutige Industrie-4.0-Anwendungen machen es erforderlich, dass eine mobile und intelligente Komponente Schlüssel für Dienste im Backend speichert. Der Diebstahl des Schlüssels führt dazu, dass ein Angreifer die Identität der bestohlenen Komponente übernehmen kann. Neben den im RAM gespeicherten Daten ist es notwendig, persistent gespeicherte Daten (z.B. Daten auf einer SD-Karte oder Daten im Flash-Speicher) auf mobilen und intelligenten Komponenten zu verschlüsseln und gegen Änderungen zu schützen. Ein besonderes Augenmerk liegt hier auch wieder auf für die IT-Sicherheit relevanten Daten wie Schlüsseln oder Passwörtern sowie auf sensitiven Informationen der Industrie-4.0-Anwendung. Durch physikalischen Zugriff kann ein Angreifer z.B. versuchen, die Firmware der mobilen und intelligenten Komponenten zu extrahieren. Dies ist z.B. möglich, wenn die mobile und intelligente Komponente eine Standard-SD-Karte als Speichermedium verwendet, wie dies oft bei Internet-der-Dinge-Geräten realisiert ist. Durch Analyse der extrahierten Firmware kann ein Angreifer Wissen über weitere Angriffsmöglichkeiten, z.B. Schwachstellen in der Firmware, erlangen. Ebenso kann er implizite Vertrauensbeziehungen erkennen und die durch diese mobile und intelligente Komponente genutzten Backend-Dienste identifizieren. Verfügt das Backend der Industrie-4.0-Anwendung nicht über geeignete Authentifizierungsverfahren, so kann ein Angreifer alleine durch das Wissen der genutzten Backend-Dienste die Identität der mobilen und intelligenten Komponenten übernehmen.

D.1.4.5 Bedrohungen durch unsichere Netzwerkkommunikation

Weitere Schwachstellen stellen die Netzwerkkommunikation und die im Netzwerk angebotenen Dienste dar. Unverschlüsselter Datenverkehr mit anderen mobilen und intelligenten Komponenten oder mit Backend Servern ermöglicht eine Offenlegung von sensitiven Informationen und ist deswegen unbedingt zu vermeiden. Netzwerkdienste können den Zugang zu einem Command Line Interface für Benutzer oder Administratoren über das Netzwerk anbieten. Hier ist insbesondere darauf zu achten, dass in diesem Fall unbedingt eine verschlüsselte Kommunikation verwendet werden und der Zugriff auf das Command Line Interface authentifiziert erfolgen muss.

Kommt passwortbasierte Authentifizierung zum Einsatz, so kann ein Angreifer durch Durchprobieren versuchen, verwendete Passwörter zu identifizieren.

Das Netzwerk in einer Industrie-4.0-Anwendung kann generell immer durch Denial-of-Service-Angriffe oder Distributed-Denial-of-Service-Angriffe in Mitleidenschaft gezogen werden. Entsprechende Angriffe sind auch auf einzelne mobile und intelligente Komponenten möglich. Ein Angreifer kann durch gezieltes Ausschalten von mobilen und intelligenten Komponenten versuchen, in einer Industrie-4.0-Anwendung einen Fehler zu erzeugen, der die ganze Anwendung lahmlegt.

Eine weitere Schwachstelle stellen unnötig aktivierte Dienste mit Netzwerkkommunikation dar – insbesondere, wenn diese ursprünglich dem Debugging dienten und in einer Produktivversion einer mobilen und intelligenten Komponente eigentlich deaktiviert sein sollte. Aus der IT bekannt ist der UPnP-Dienst (*Universal Plug and Play*). UPnP dient zur automatischen Konfiguration von Geräten und zur automatischen Nutzung von Diensten. Im Industrie-4.0-Kontext sollten UPnP und ähnliche Dienste unbedingt deaktiviert werden, da diese einfach von Angreifern ausgenutzt werden können.

D.1.4.6 Bedrohungen des Device-Managements

Eine weitere Angriffsoberfläche ist das Device-Management in einer Industrie-4.0-Anwendung. Übliche Funktionen sind z.B. eine Überprüfung des Gerätezustands von mobilen und intelligenten Komponente aus der Ferne (*health check*) und die Überprüfung des Vorhandenseins einer Komponente (*heartbeat*). Beide Funktionen sind anfällig für Angriffe; so kann ein Angreifer z.B. die für die Präsenzprüfung verwendeten regelmäßigen Heartbeat-Nachrichten unterdrücken, um der Industrie-4.0-Anwendung vorzutäuschen, dass ein Gerät nicht mehr vorhanden ist. Je nach Programmierung der Industrie-4.0-Anwendung kann er damit einen Denial-of-Service-Angriff durchführen oder auftretende Fehlzustände für weitere Angriffe nutzen.

D.1.5 Sicherheitsmaßnahmen

Die oben genannten Bedrohungen für mobile und intelligente Komponenten können durch den Einsatz verschiedener grundlegender Sicherheitsmechanismen auf den Komponenten verhindert oder zumindest abgeschwächt werden.

D.1.5.1 Schutz vor Manipulation von Software und Firmware

Ein grundlegender Schutzmechanismus für mobile und intelligente Komponenten ist der Schutz der ausgeführten Software und Firmware vor bösartiger Manipulation. Zum Schutz vor Manipulation kommt ein Verfahren zum Einsatz, das **Secure Boot** genannt wird. Secure Boot stellt sicher, dass nach dem Systemstart bis zum abgeschlossenen Start des Betriebssystems nur vertrauenswürdige Software ausgeführt wird, wobei vertrauenswürdige Software hier als Software definiert ist, die vom Hersteller der Komponente herausgegeben wurde. Um die Herkunft der Software zu überprüfen, wird **Code Signing** eingesetzt. Code Signing ist ein Prozess, in dessen Rahmen für eine oder mehrere Binärdateien eine digitale Signatur erstellt wird. Mittels der digitalen Signatur ist es möglich, während des Secure-Boot-Vorgangs die Authentizität und Integrität der Binärdatei zu überprüfen. Binärdateien werden für ein Software- oder Firmware-Update signiert übertragen und werden auch lokal signiert gespeichert.

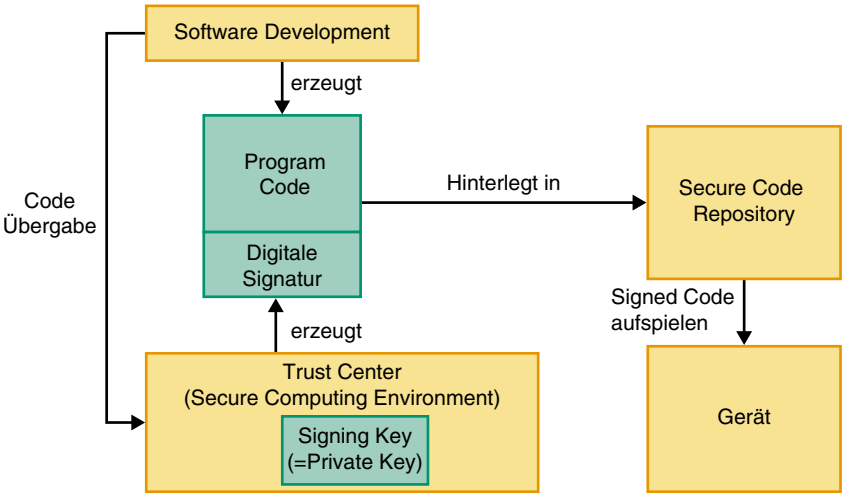

Bild D.1.6 *Prozess Code Signing*

Bild D.1.6 zeigt einen Überblick über die notwendigen Prozesse beim Einsatz von Code Signing in der Software-Entwicklung. Die organisatorischen Herausforderungen umfassen unter anderem den Betrieb eines Trust Centers, das die sichere Code-Übergabe zwischen den verschiedenen Instanzen organisiert, Freigabeprozesse steuert und mit sachkundigem Personal unterstützt. Im Trust Center müssen die für die Erzeugung der digitalen Signaturen verwendeten Signing Keys verwaltet werden einschließlich der Definition und Implementierung eines Lebenszyklus für Signing Keys und eventuell Aufbau einer Schlüsselhierarchie. Schließlich stellt auch die revisionssichere Vorhaltung von Code in einem Secure Code Repository eine große Herausforderung dar, gerade für Systeme mit langer Lebenszeit, wie sie üblicherweise in Industrie-4.0-Anwendungen eingesetzt werden.

Auf Seite der mobilen und intelligenten Komponente ist es notwendig, den oder die Schlüssel zur Überprüfung von Code-Signaturen authentisch und integer zu speichern, so dass es einem Angreifer nicht möglich ist, diese Schlüssel durch eigene Schlüssel zu ersetzen. Die Code-Signaturen werden beim Start der mobilen und intelligenten Komponente überprüft. Der Code, der diese Überprüfung vornimmt, ist meist im ROM hinterlegt und wird **BootROM** genannt. Dieser Code wird selbst nicht überprüft und alles Vertrauen in die Komponente basiert auf der Integrität und Fehlerfreiheit dieses Codes, weswegen er auch oft **Root of Trust** genannt wird. Bei der Entwicklung eines BootROMs sollten sicherheitsunterstützende Prozesse, z.B. [4; 5], eingesetzt werden. Ist die Überprüfung der Code-Signatur erfolgreich, so übergibt das BootROM die Programmausführung an den überprüften Code. Bei komplexeren Komponenten wird oft ein mehrstufiges Secure-Boot-Verfahren verwendet. Dabei startet das BootROM eine erste Bootstufe, die die Signatur einer weiteren Bootstufe überprüft und diese startet und so weiter. Dadurch sind einzelne Bootstufen voneinander unabhängig austauschbar, was unter anderem Software- und Firmware-Updates deutlich vereinfacht.

Bild D.1.7 zeigt einen Secure-Boot-Vorgang mit zwei Boot-Stufen: ***L**ow **L**evel **B**ootloader* (LLB) und Betriebssystem (OS). Das BootROM überprüft die Signatur des LLB-Codes. Ist diese Signatur korrekt, so übergibt das BootROM die Ausführung an den LLB. Der LLB setzt die Ausführung fort und prüft nach eigener Initialisierung die Signatur des OS. Ist diese korrekt, so übergibt der LLB die Ausführung an das OS, das den Secure Boot Vorgang abschließt. Bei der Realisierung von Secure

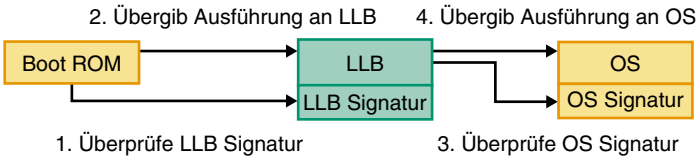

Bild D.1.7 *Secure Boot mit zwei Bootstufen*

Boot auf mobilen und intelligenten Komponenten von Industrie-4.0-Anwendungen müssen eventuell vorgegebene maximale Zeiten für den Systemstart sowie Begrenzung der zur Verfügung stehenden Ressourcen (RAM, Flash) berücksichtigt werden. Der Aufwand für die Überprüfung einer Bootstufe setzt sich zusammen aus der Errechnung eines Hash-Wertes der Software mittels einer Hash-Funktion (z.B. SHA-1) und der Überprüfung der Signatur, z.B. mittels RSA oder ECC. In [6] werden beispielhafte Werte für Ressourcen-Verbrauch und Dauer von verschiedenen kryptographischen Operationen auf einem 400 MHz ARM MPCore vorgestellt. Die Werte sind in Tabelle D.1.1 dargestellt.

Tabelle D.1.1 *Ressourcen-Bedarf und Dauer von kryptographischen Operationen auf einem 400 MHz ARM MPCore*

Algorithmus	Flash	RAM	Durchsatz bzw. Laufzeit
SHA-1 (Hash-Funktion)	898 Byte	352 Byte	3026 KB/s
RSA 1024 Signaturüberprüfung	1410 Byte	1136 Byte	2 ms
ECC 160 (ECDSA Signaturüberprüfung)	4244 Byte	1108 Byte	66 ms
AES-128 Verschlüsselung im Modus CBC	1410 Byte	236 Byte	661 KB/s

Beim Schutz vor Manipulation von Software und Firmware muss ein besonderes Augenmerk auf der Software- bzw. Firmware-Update-Funktion liegen. Insbesondere gilt es, hier einen Downgrading-Angriff zu verhindern, also einen Angriff, bei dem ältere Versionen der Software bzw. Firmware eingespielt werden, von denen die Schwachstellen bekannt sind. Um solche Angriffe zu verhindern bieten sich zwei Verfahren an: ein Online-Verfahren und ein Offline-Verfahren.

Beim **Online-Verfahren zur Vermeidung von Downgrading-Angriffen** wird davon ausgegangen, dass die mobile und intelligente Komponente eine sichere Verbindung (siehe Abschnitt D.1.5.3) zu einem Update-Server aufbauen kann. Beim jedem Software-Update wird die aktuelle Version vom Update-Server erfragt und andere Versionen werden nicht akzeptiert.

Beim **Offline-Verfahren zur Vermeidung von Downgrading-Angriffen** wird die aktuelle Softwareversion in einem sicheren Bereich auf der mobilen und intelligenten Komponente gespeichert, idealerweise in einem Trusted Platform Module oder einem Hardware Security Module. Gegen diese gespeicherte Versionsnummer vergleicht die Software-Update-Funktion jede einzuspielende Software. Die Versionsnummer sollte dabei im signierten Code enthalten sein. Gegenüber dem Online-Verfahren hat das Offline-Verfahren den Nachteil, dass nicht sichergestellt ist, dass nur die aktuellste Version der Software / Firmware eingespielt wird, sondern nur sichergestellt, dass eine Version eingespielt wird, die aktueller ist als die aktuelle Version. Jedoch kann gerade bei mobilen und intelligenten Komponenten nicht immer davon ausgegangen werden, dass der Update-Server erreichbar ist, weswegen auch das Offline-Verfahren seine Berechtigung hat.

D.1.5.2 Schutz kryptographischen Materials

Mobile und intelligente Komponenten von Industrie 4.0 benötigen kryptographisches Material wie z.B. Schlüssel, um sicher kommunizieren zu können oder um einen externen Datenträger (z.B. SD-Karte) zu verschlüsseln. Da eine mobile und intelligente Komponente üblicherweise nicht von einem Benutzer bedient wird, ist eine automatisierte sichere Speicherung bei gleichzeitiger Nutzbarkeit der kryptographischen Schlüssel notwendig. Um diese Funktionalität sinnvoll zu realisieren, bietet sich eine Hardware-Unterstützung an.

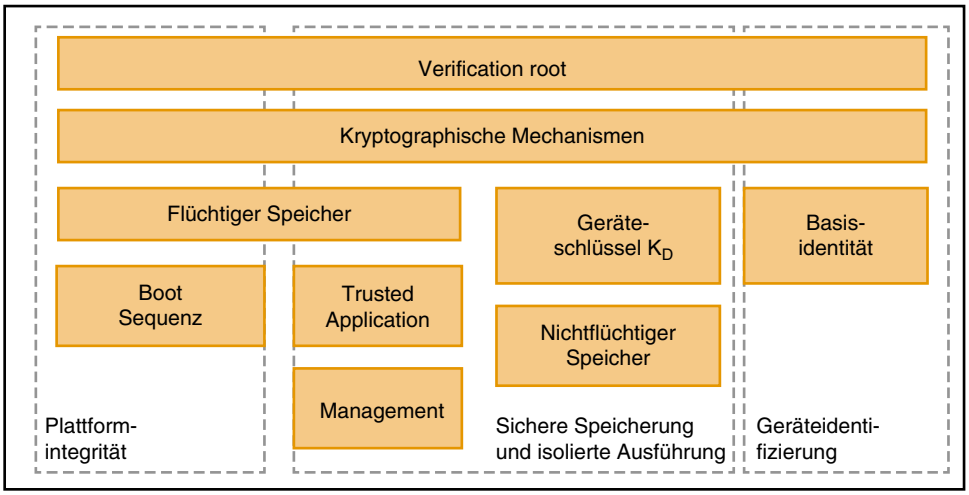

Bild D.1.8 *Beispiel Aufbau einer Hardware-Unterstützung für eine mobile und intelligente Komponente*

Bild D.1.8 zeigt ein Beispiel für den Aufbau einer Hardware-Unterstützung. In Hardware sind verschiedene kryptographische Mechanismen, z.B. Verschlüsselung, Hash-Funktionen und Signaturprüfung, implementiert, die von der mobilen und intelligenten Komponente genutzt werden können. Die Implementierung in Hardware bringt Performance-Vorteile und schont die Ressourcen auf der mobilen und intelligenten Komponente. Ebenfalls ist dort die Verification Root implementiert. Im Verification Root ist z.B. die Verifikationsroutine des BootROMs für Secure Boot integriert (siehe Abschnitt D.1.5.1). Die Hardware stellt eine gesicherte Identität zur Verfügung (siehe Abschnitt D.1.5.4). Im nichtflüchtigen Speicher der Hardware können Informationen zum Versionsstand der Plattform für Angreifer unveränderbar gespeichert werden ebenso wie Schlüssel, die zur Verschlüsselung von externen Speichermedien (z.B. SD-Karte) eingesetzt werden. Viele moderne Prozessorarchitekturen unterstützen das Konzept einer Hardware-Unterstützung von Security-Mechanismen, z.B. ARM TrustZone, TI M-Shield, Intel SGX, Smart Cards, kryptographische Coprozessoren und ***T**rusted **P**latform **M**odules* (TPM). Je nach Bedarf und Randbedingungen der jeweiligen Industrie-4.0-Anwendung muss eine geeignete Hardwarelösung für die mobilen und intelligenten Komponenten ausgewählt werden.

Die erwähnte Hardware-Unterstützung wird dann genutzt, um Security-Funktionalitäten auf den mobilen und intelligenten Komponenten zu implementieren. Ein Beispiel sind **Key Stores**. In Key Stores können kryptographische Schlüssel sicher abgespeichert werden. Dabei wird in Hardware meist nur ein einziger Schlüssel gespeichert, der dazu verwendet wird, andere Schlüssel zu verschlüsseln. Mit diesen wiederum werden dann z.B. einzelne Schlüssel des Key Stores verschlüsselt. Hierdurch entsteht eine Hierarchie von Schlüsseln.

D.1.5.3 Schutz der Kommunikation

Industrie-4.0-Anwendungen erbringen ihren Dienst meist durch eine komplexe Kommunikation zwischen mobilen und intelligenten Komponenten und Backend Services der Anwendung. Auch heute noch kommen viele Protokolle zum Einsatz, die keinerlei Sicherheitsmaßnahmen zur Verfügung stellen. Es ist dann notwendig, durch den Einsatz eines Sicherheitsprotokolls die Verbindung abzusichern. Im Umfeld Industrie 4.0 kommt oft SSL / TLS oder (seltener) IPSec zum Einsatz.

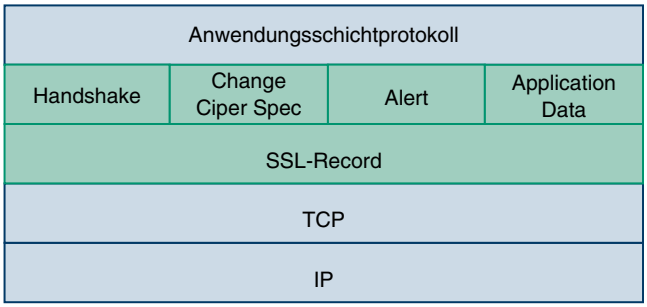

Bild D.1.9 *Aufbau SSL / TLS*

Transport Layer Security (TLS) oder veraltet Secure Socket Layer (SSL) ist ein Protokoll zur Realisierung von Ende-zu-Ende-Sicherheit. TLS gewährleistet Integrität und Vertraulichkeit von Daten und ermöglicht eine zertifikatsbasierte Authentifizierung. Bild D.1.9 zeigt einen Überblick zur Protokollstruktur und zum Einsatz von TLS. Der Handshake dient dabei der Authentifizierung, Aushandlung der kryptographischen Verfahren und dem eigentlichen Schlüsselaustausch. Mittels ChangeCipherSpec wird der richtige Record für die Kommunikation ausgewählt. Alert ermöglicht die Übermittlung von Fehlermeldungen und Application Data dient dazu, geschützte Daten aus dem Anwendungsprotokoll zu übermitteln.

TLS unterstützt die Aushandlung von kryptographischen Protokollen, die für den Schutz von Nachrichten verwendet werden. Dadurch realisiert TLS Crypto Agility.

DEFINITION

Crypto Agility ist ein Verfahren, um kryptographische Verfahren dynamisch austauschen zu können.

Gerade in Industrie-4.0-Anwendungen ist die Möglichkeit zum Austausch von kryptographischen Verfahren sehr wichtig, da diese Systeme oft eine lange Lebenszeit haben. Aktuell stellt z.B. der Quantencomputer eine große Unsicherheit für Industrie-4.0-Anwendungen dar. Für den Quantencomputer sind Algorithmen bekannt, die gängige kryptographische Verfahren brechen können. Bisher besteht diese Gefahr jedoch nur theoretisch, da noch kein Quantencomputer existiert, auf dem diese Algorithmen ausgeführt werden könnten. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt jedoch die Entwicklungen beim Quantencomputer genau im Blick zu halten bei Anwendungen, die über das Jahr 2024 hinaus betrieben werden sollen [7]. Crypto Agility ist eine Möglichkeit, schon heute auf die zukünftigen Herausforderungen durch einen zukünftigen Quantencomputer reagieren zu können. Für die Konfiguration von TLS sei auf die

Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik für Cipher Suites zum Einsatz mit TLS verwiesen [8].

Beim Einsatz von TLS in Industrie-4.0-Anwendungen ist auf die Randbedingungen zu achten. TLS erfordert einen aufwendigen Handshake zwischen den Kommunikationspartnern, so dass der Aufbau einer Verbindung eine gewisse Zeit dauern kann.

Neben den Standardverfahren TLS und IPSec zur Kommunikation gibt es eine Reihe von auf Industrie 4.0 spezialisierten Protokollen, die unter anderem sichere Kommunikation realisieren, z.B. [10]. Auf eine ausführliche Darstellung wird hier aus Platzgründen verzichtet.

D.1.5.4 Sichere Identitäten

Ein grundlegendes Problem in Systemen mit vielen dezentralen Komponenten oder mit vielen verschiedenen Akteuren stellt die Frage dar, wie sichere Identitäten zur Verfügung gestellt werden können. Sichere Identitäten von mobilen und intelligenten Komponenten dienen z.B. dazu, im Backend mit Sicherheit zu wissen, mit welchem Gerät aktuell kommuniziert wird. Für Industrie-4.0-Anwendungen eignen sich besonders digitale Zertifikate als sichere Identitäten. Genauer gesagt, kommen so genannte Identitätszertifikate zum Einsatz.

DEFINITION

Ein **Identitätszertifikat** ist eine Zuordnung einer Identität sowie optional einer Menge von Attributen und Metadaten zu einem Public Key. Die Zuordnung wird von einer Zertifizierungsstelle (*Certificate Authority*) durch eine digitale Signatur über den Zertifikatinhalt bestätigt.

Üblicherweise besteht eine Identität aus einem Bezeichner. Dieser Bezeichner kann für Server z.B. ein Hostname sein (z.B. industrie40.thi.de), in der E-Mail-Kommunikation kommt die E-Mail Adresse als Identität zum Einsatz (z.B. hof@thi.de). Die Identität kann durch Attribute ergänzt werden. Im Beispiel der E-Mail-Adresse hof@thi.de könnte ein Attribut «Funktion» den Wert «Professor» haben. Metadaten beschreiben die Randbedingungen des Zertifikats. Übliche Metadaten sind z.B. Beginn und Ende der Gültigkeit des Zertifikats. Über den dadurch definierten Gültigkeitszeitraum kann die Auswirkung eines Diebstahls einer sicheren Identität begrenzt werden. Identität und Metadaten werden einem Public Key durch das Zertifikat einem Public Key zugeordnet. Der zugehörige Private Key ist nur dem Besitzer des Zertifikats bekannt.

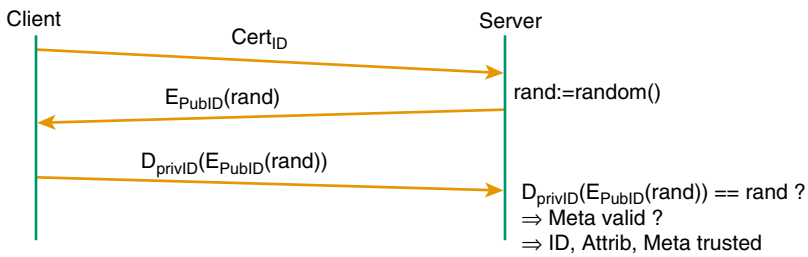

Bild D.1.10 *Überprüfung eines Zertifikats*

Zur Überprüfung eines Identitätszertifikats geht ein Server nun vor wie in Bild D.1.10 beschrieben. Der Server erhält ein Identitätszertifikat ($Cert_{ID}$) von einem Client (einer mobilen und intelligenten Komponente). Der Server ermittelt eine Zufallszahl rand. Er verschlüsselt die Zufallszahl mit dem Public Key aus dem Zertifikat $Cert_{ID}$ und sendet die verschlüsselte Zufallszahl E_{PublD} (rand) an den Client. Zur Entschlüsselung der Zufallszahl ist die Kenntnis des zum Public Key gehörenden Private Keys notwendig. Lediglich der legitime Client verfügt über diese Information, da Private Keys geheim gehalten werden müssen. Der Client entschlüsselt mit dem Private Key die Zufallszahl und sendet das Ergebnis der Entschlüsselung D_{privID} (E_{publD} (rand)) wieder an den Server. Der Server überprüft, ob die vom Client gesendete Zufallszahl der vom Server gesendeten Zufallszahl entspricht. Falls dies der Fall ist, hat der Client erfolgreich nachgewiesen, dass er den Private Key zum Public Key im Zertifikat $Cert_{ID}$ kennt. Nun überprüft der Server, ob die Metadaten des Zertifikats anzeigen, dass das Zertifikat gültig ist. So wird z.B. überprüft, ob das aktuelle Datum und die aktuelle Uhrzeit innerhalb der Gültigkeitsdauer des Zertifikats liegen. Wurden die Metadaten erfolgreich validiert, wird anschließend die Signatur des digitalen Zertifikats überprüft. Die Signatur wurde von einer Zertifizierungsstelle erzeugt. Zur Überprüfung der Signatur ist es notwendig, den Public Key der Zertifizierungsstelle zu kennen. Der Server verfügt nur über Zertifizierungsstellen, denen er vertraut. Ist die Überprüfung der Signatur erfolgreich, so gilt als sicher, dass der Client die im Zertifikat angegebene Identität hat.

Ein gängiges Zertifikatsformat ist X.509 (auch bekannt als Standard ISO/IEC 9594-8). X.509 beschreibt Identität als String, bestehend aus Zuweisungen von Werten zu vorgegebenen Schlüsseln. Die Schlüssel sind CN (gebräuchlicher Name), O (Organisation), C (Land), ST (Bundesland) und L (Ort). Beispielsweise ist in X.509 der Bezeichner «CN=hof@thi.de, O=Technische Hochschule Ingolstadt, C= Deutschland, ST=Bayern, L=Ingolstadt» eine gültige Identität. X.509 kann flexibel um eigene Metadaten und Attribute erweitert werden. Der Erweiterungsmechanismus ermöglicht es auch festzulegen, welche Erweiterungen auf jeden Fall bekannt sein müssen, falls ein Zertifikat verwendet werden soll.

In Bild D.1.11 ist das X.509-Zertifikat des Webservers der Technischen Hochschule Ingolstadt zu sehen. Eingesetzt wird X.509 in der Version 3. Zur Signaturerzeugung kommen die Hash-Funktion SHA256 und der Signaturalgorithmus RSA zum Einsatz. Die Signatur ist am Ende des Zertifikats zu sehen und erstreckt sich über den gesamten Inhalt des Zertifikats. Der gebräuchliche Name (*Common Name*) des Webservers ist www.thi.de. Der Public Key hat eine Länge von 2048 Bit und wird für das Verfahren RSA verwendet. Es sind mehrere Erweiterungen enthalten, z.B. die Angabe, dass das Zertifikat zur Authentifizierung eines Servers über TLS verwendet werden soll (*X509v3 Extended Key Usage*). Darüber hinaus wird eine URL angegeben, an der eine ***C**ertificate **R**evocation **L**ist* (CRL) der Zertifizierungsstelle heruntergeladen werden kann (*X509v3 CRL Distribution Points*).

Zum Umgang mit dem Diebstahl von Zertifikaten mit zugehörigem Private Key gibt es zwei Sicherheitsmechanismen: begrenzte Gültigkeitsdauer und Certificate Revocation Lists. Die Gültigkeitsdauer eines Zertifikats gibt an, in welchem Zeitraum ein Zertifikat verwendet werden darf. Vor und nach diesem Zeitraum ist das Zertifikat ungültig und kann nicht verwendet werden. Nach dem Diebstahl eines Zertifikats und Private Keys kann ein Missbrauch der gestohlenen Informationen nur während der Gültigkeitsdauer erfolgen. Eine geringe Gültigkeitsdauer verringert also das Angriffsfenster. Allerdings ist in diesem Fall eine regelmäßige Erneuerung von Zertifikaten notwendig. Das in Bild D.1.11 dargestellte Zertifikat ist gültig vom 12. April 2017 10:00:25 Uhr bis zum 9. Juli 2020, 10:00:25. Um die Zeitspanne, in der ein gestohlenes Zertifikat eingesetzt werden kann, noch kleiner zu gestalten, kann von einer Zertifizierungsstelle eine Liste mit zurückgerufenen Zertifikaten gepflegt werden, eine so genannte Zertifikatswiderrufsliste (*Certificate Revocation List*). Alle Zertifikate auf dieser Liste werden als ungültig erklärt und können nicht mehr verwendet werden. Bei der Überprüfung von Zertifikaten sind die Überprüfer angehalten, die zugehörigen Zertifikatswiderrufslisten vor der Verwendung eines Zertifikats zu berücksichtigen.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            1d:0d:78:48:d7:35:c1:36:c1:df:93:5f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=DE, O=Verein zur Foerderung eines Deutschen Forschungsnetzes e. V., OU=DFN-PKI, CN=DFN-Verein Global Issuing CA
        Validity
            Not Before: Apr 12 10:00:25 2017 GMT
            Not After : Jul  9 10:00:25 2020 GMT
        Subject: C=DE, ST=Bayern, L=Ingolstadt, O=Technische Hochschule Ingolstadt, OU=Rechenzentrum, CN=www.thi.de
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:a1:00:ef:df:36:41:da:07:c7:5b:b3:b5:90:4c:
                    7b:6a:6b:98:5e:f6:7c:74:53:f9:cb:f4:e1:ad:04:
                    08:fd:e0:31:b6:c7:f3:39:2e:40:7a:25:14:b9:0f:
                    15:aa:7d:26:e0:0c:55:23:2c:cd:7b:0f:fa:07:83:
                    3f:10:a5:fe:01:89:f0:86:57:80:d5:ad:24:28:9d:
                    b3:03:4b:21:13:38:19:ce:d6:7e:be:38:5f:fe:89:
                    35:ce:91:4e:00:14:20:6b:8c:f4:47:3d:89:97:b0:
                    1f:be:c1:6e:a6:64:e5:92:e8:95:2e:1c:e1:da:a7:
                    fb:1e:7f:ba:60:26:94:4c:11:31:9d:65:aa:a0:42:
                    ed:ab:d3:4e:e8:3b:01:df:b8:7e:bc:f4:ad:7e:35:
                    cf:26:cf:9e:ef:cd:1a:9f:99:72:f4:9b:dd:ca:55:
                    0a:34:cd:5f:74:53:b3:eb:cb:aa:c6:2e:54:f0:fd:
                    26:3c:62:be:26:1f:59:94:d7:1a:71:6d:25:7a:cd:
                    99:83:7d:83:49:d9:08:99:16:66:f4:3b:73:4a:af:
                    26:d0:21:e5:5e:4a:32:9d:9f:80:94:04:6b:a1:37:
                    40:1d:4b:c4:8e:2e:a1:28:bd:a6:db:24:96:3a:16:
                    8a:4c:90:22:e1:77:43:c5:c4:7d:91:f9:80:f3:0e:
                    14:a9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.22177.300.1.1.4.3.5
                Policy: 1.3.6.1.4.1.22177.300.2.1.4.3.1
                Policy: 1.3.6.1.4.1.22177.300.1.1.4
                Policy: 1.3.6.1.4.1.22177.300.30
                Policy: 2.23.140.1.2.2

            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Subject Key Identifier:
                C8:0E:E6:B2:E9:FA:68:50:97:48:FF:0A:15:9E:E7:B6:61:3B:AA:A0
            X509v3 Authority Key Identifier:
                keyid:6B:3A:9B:8B:F9:F2:53:89:DA:E0:AD:B2:32:1E:09:1F:E8:AA:3B:74

            X509v3 Subject Alternative Name:
                DNS:www.thi.de, DNS:www.haw-ingolstadt.de, DNS:www.fh-ingolstadt.de, DNS:staging.thi.de, DNS:develop.thi.de
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://cdp1.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl

                Full Name:
                  URI:http://cdp2.pca.dfn.de/dfn-ca-global-g2/pub/crl/cacrl.crl

            Authority Information Access:
                OCSP - URI:http://ocsp.pca.dfn.de/OCSP-Server/OCSP
                CA Issuers - URI:http://cdp1.pca.dfn.de/dfn-ca-global-g2/pub/cacert/cacert.crt
                CA Issuers - URI:http://cdp2.pca.dfn.de/dfn-ca-global-g2/pub/cacert/cacert.crt

    Signature Algorithm: sha256WithRSAEncryption
         90:71:19:02:a9:d9:f3:db:8a:f1:1b:6b:bb:5d:e3:ef:2c:61:
         eb:ee:0e:0b:c8:f4:79:12:88:de:bd:5d:4c:25:72:5e:d1:9c:
         b6:bd:7d:49:b0:68:6e:74:e9:a1:da:9b:25:9e:b3:c5:07:d4:
         85:78:0d:5b:f8:56:18:7d:9a:fe:bb:23:d2:38:00:e9:a5:30:
         a7:3a:39:81:f3:c2:6e:93:7c:36:82:1b:7f:70:03:15:9e:69:
         a7:e4:25:f1:21:2b:53:24:bc:d6:92:fe:f6:fb:04:27:72:e8:
         73:ab:0b:06:0a:e3:eb:ba:77:6e:ab:5a:18:bf:6a:53:12:dc:
         fa:65:07:2c:02:fd:4b:ef:76:4e:f3:96:2c:a2:05:12:75:2d:
         f2:6c:f5:c6:0a:4b:63:50:8d:24:d8:5e:34:80:b4:47:5b:75:
         c0:49:00:27:e9:ec:92:40:65:3c:24:37:5d:a1:8d:76:f1:4b:
         72:55:40:aa:92:0d:8c:01:83:5c:21:57:ab:36:a6:d9:20:eb:
         1f:34:76:a3:ab:19:fa:bd:0a:f8:9b:d8:11:6d:2e:23:67:5e:
         a2:07:2d:38:99:f4:ee:a2:0c:24:b2:a1:60:96:c3:2a:4e:41:
         e8:80:7b:f1:c3:a8:e1:35:dd:85:12:0d:20:32:f1:3a:11:1e:
         04:71:03:3e
```

Bild D.1.11 *Zertifikat des Webservers der Technischen Hochschule Ingolstadt*

Bisher wurden nur Fälle betrachtet, in denen Zertifikate für mobile und intelligente Komponenten direkt von einer Zertifizierungsstelle ausgegeben werden. Es ist jedoch auch möglich, Zertifizierungsstellen hierarchisch zu organisieren, so dass eine Zertifizierungsstelle die Erstellung von Zertifikaten an andere Zertifizierungsstellen delegiert. Man spricht dann von einer Root-CA

(Wurzelzertifizierungsstelle), die die Aufgabe der Zertifikatserstellung an Sub-CAs (Unterzertifizierungsstellen) delegiert. Die Root-CA kann einer Sub-CA auch das Recht einräumen, selbst Sub-CAs zu bestimmen.

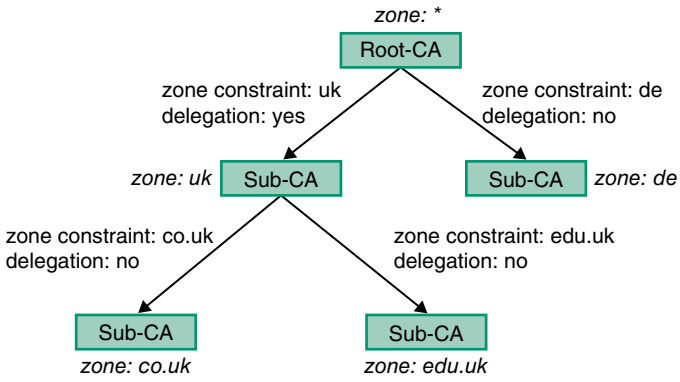

Bild D.1.12 *Beispiel hierarchisches Vertrauensmodell*

Bild D.1.12 zeigt ein Beispiel. In diesem Fall erfolgt die Delegation basierend auf DNS-Namen. Die Root-CA verwaltet alle DNS-Namen (zone:*). Sie delegiert alle DNS-Namen, die auf .uk enden (zone: uk), an die erste Sub-CA, und alle DNS-Namen, die auf .de enden (zone:de), an die zweite Sub-CA. Die de-CA hat dabei nicht das Recht erhalten, die Zertifikatserzeugung weiter zu delegieren. Die uk-CA hat das Recht zur Delegation erhalten und delegiert an eine Sub-CA für die DNS-Namen, die auf co.uk enden (zone:co.uk), sowie eine weitere Sub-CA für die DNS-Namen mit der Endung edu.uk (zone:edu.uk). Die Delegation wird jeweils in den Identitätszertifikaten der Zertifizierungsstellen dokumentiert, die von der übergeordneten Zertifizierungsstelle ausgestellt werden. Im Zertifikat ist verzeichnet, für welche DNS-Namen eine CA zuständig ist (zone constraint) sowie die Erlaubnis zur Delegation (delegation: yes). Bei der Zertifikatsprüfung müssen diese Einschränkungen überprüft werden. Ist einem Prüfer eines Zertifikats nur die Root-CA bekannt sowie ein Zertifikat, das eine Sub-CA ausgestellt hat, so muss der Prüfer einen Zertifikatspfad vom zu prüfenden Zertifikat über einen oder mehrere Sub-CAs bis zur Root-CA erstellen und überprüfen.

Die Verwendung von Zertifikatshierarchien wie in Bild D.1.12 zu sehen hat den großen Vorteil, dass damit sichere Identitäten bei einer Vielzahl von selbstverantwortlichen Teilnehmern an einer Industrie-4.0-Anwendung realisiert werden können. Das Delegationskonzept ermöglicht es, Industrie-4.0-Anwendungen über verschiedene Unternehmen hinweg bei maximaler Eigenständigkeit der einzelnen Unternehmen zu realisieren. Jedoch sind Zertifikatshierarchien in der Praxis meist schwierig zu verwalten. Die Tiefe der Hierarchie sollte auf ein absolutes Minimum reduziert werden. Da die Erstellung des Zertifikatspfades oft nicht ohne Weiteres möglich ist, sollten in Zertifikaten von mobilen und intelligenten Endgeräten auch die Zertifikate der Sub-CAs bis zur Root-CA enthalten sein. Selbst in diesem Fall ist die Überprüfung eines Zertifikats noch sehr aufwendig, da mehrere Zertifikate validiert werden müssen.

Zertifikate und die benötigten Private Keys müssen auf mobile und intelligente Komponenten installiert werden. Dies geschieht üblicherweise im Rahmen des Security Bootstrappings. Das Security Bootstrapping kann während der Herstellung geschehen, direkt auf dem Gerät erfolgen oder später über einen Verteildienst erfolgen. In der Praxis ist es oft aufwendig, ein geeignetes Security-Bootstrapping-Verfahren zu erzeugen.

Private Keys müssen auf einer mobilen und intelligenten Komponente sicher gespeichert werden (siehe dazu Abschnitt D.1.5.2). Da alle von einer bekannten Zertifizierungsstelle erzeugten Zertifikate akzeptiert werden, muss auch sichergestellt sein, dass ein Angreifer nicht die Liste der bekannten Zertifizierungsstellen und die zugehörigen Zertifikate manipulieren kann, d.h., die Integrität der Liste und der Zertifizierungsstellenzertifikate muss sichergestellt sein.

In Kürze

Dieses Kapitel gibt einen kurzen Überblick über Cyber Security für mobile und intelligente Komponenten von Industrie-4.0-Anwendungen. An den Komponenten sind insbesondere lokale Schnittstellen, Wartungs- und Administratorzugänge, die Datenspeicherung und die Netzwerkkommunikation zu schützen. Grundlegende Sicherheitsmaßnahmen umfassen den Schutz der ausgeführten Firmware und Software, den Schutz von kryptographischem Material, sichere Kommunikationsverbindungen sowie sichere Identitäten durch Identitätszertifikate. Eine große Herausforderung stellt eine effiziente und ressourcenschonende Implementierung von Sicherheitsmechanismen dar. Idealerweise wird zusätzliche Hardware, z.B. ein Trusted Platform Module, eingesetzt, um Sicherheitsmechanismen zu implementieren.

Lebensläufe

Dipl.-Ing. Heiko Adamczyk
Heiko Adamczyk studierte Elektrotechnik an der Otto-von-Guericke-Universität Magdeburg. Nach seiner Tätigkeit am ifak e.V. in Magdeburg und bei Knick Elektronische Messgeräte in Berlin ist er seit September 2016 ist er für die KORAMIS GmbH tätig und für den neu eröffneten Standort Potsdam/Berlin verantwortlich. Seine Aufgaben fokussieren dabei auf die Themen Security und Industrie 4.0. Herr Adamczyk leitete verschiedene Forschung- und Entwicklungsprojekte und hat darüber hinaus zahlreiche Publikationen herausgegeben. Er ist in der Arbeitsgruppe UK931.1 der DKE tätig. Im ZVEI gehört er dem Lenkungsausschuss «Security» an. Zudem er seit 2006 Obmann des Fachausschusses 5.22 «IT-Security» innerhalb der VDI/VDE-GMA und seit 2012 in dessen Beirat tätig.

Dr. rer. nat. Kemal Akman
Dr. Kemal Akman studierte Bioinformatik an der Ludwig-Maximilians-Universität. Nach seiner Promotion arbeitete er mehrere Jahre im Bereich Application Management in der Produktion bei Roche in Penzberg. Bereits vor dem Studium besaß er langjährige Berufserfahrung in den Bereichen IT-Sicherheit, sichere Softwareentwicklung und Kryptographie. Zu diesen Themenbereichen hat er bereits einige Artikel im c't Magazin sowie Whitepaper veröffentlicht. Nach seiner Tätigkeit als Manager bei Ernst & Young Deutschland im Bereich Cybersecurity, wo er schwerpunktmäßig Kunden im Bereich der Industrial Control Security beraten hat, wechselte er 2019 zur KPMG Deutschland Wirtschaftsprüfungsgesellschaft AG.

Prof. Dr. rer. nat. Frederik Armknecht
Prof. Dr. Frederik Armknecht studierte Mathematik an der Technischen Hochschule Karlsruhe. Nach seiner Promotion in Kryptographie über die Sicherheit bestimmter Verschlüsselungsverfahren arbeitete er bei NEC Europe Ltd. an der Sicherheit in unterschiedlichen Arten an Netzwerken. Später kehrte er an die Universitäten zurück und nach Zwischenstationen an der Ruhr-Universität Bochum und der Technischen Universität Darmstadt hat er nun einen Lehrstuhl für Dependable Systems Engineering an der Universität Mannheim inne. Sein Forschungsgebiet ist die Wahrung der Sicherheit und Privatsphäre im Kontext von sowohl bewusst als auch unbewusst herausgegebenen Daten.

Johannes Beckers, LL.B., M.Sc.
Johannes Beckers studierte Wirtschaftsrecht an der Rheinischen Fachhochschule in Köln und Versicherungswesen an der Fachhochschule Köln. Er schrieb seine Masterarbeit zum Thema Cyber-Versicherungen. Im Anschluss an sein Studium begann er als Financial Lines Underwriter und Produktentwickler für Cyber-Versicherungen bei einem Versicherungsassekuradeur. Seit 2017 arbeitet er beim AXA-Konzern als Cyber-Spezialist und -Underwriter. Im Rahmen seiner Cyber-Tätigkeit stand Herr Beckers bereits für diverse Interviews und Veröffentlichung zur Verfügung.

Daniel Conta, B.Sc.
Daniel Conta studierte Wirtschaftsinformatik an Hochschule für angewandte Wissenschaften Hamburg und Informatik an der Universität Hamburg. Über fünf Jahre wirkte er bei dem IT-Dienstleiser Diebold Nixdorf für die Finanzbranche am Aufbau eines hochpriviligierten Access Managements mit. Seit Beginn 2017 ist er als IT-Berater in der Gesundheitsbranche tätig und berät Kliniken, Praxen und Einrichtungen mit pflegerischem Schwerpunkt im Bereich Reputationsma-

nagement und bei der Digitalisierung von Arbeitsabläufen im organisatorischen und formalen Arbeitsalltag. Als Referent hält er für den Berufsverband für Orthopädie und Unfallchirurgie (BVOU) Vorträge auf Ärztekongressen (z.B. DKOU 2018 Berlin) und Webinars für den BVOU-Study Club.

Dipl.-Math. David Fuhr
David Fuhr studierte Mathematik, Informatik und Politikwissenschaft an der Freie Universität Berlin. Anschließend forschte er am Fraunhofer ISST und Fraunhofer IPK zu Wissensmanagement, Bilderkennung und digitaler Fälschungssicherung. Als Head of Research beim Berliner Security-Beratungsunternehmen HiSolutions verantwortet er Forschungsprojekte in Bereichen wie kritische Infrastrukturen, Incident Response, Industrie 4.0 und Katastrophenvorsorge. Seine Arbeitsgebiete umfassen Kryptographie, Standardisierung, Risikomanagement, maschinelles Lernen und die Vermittlung von Security-Fachwissen über Expertenkreise hinaus. David Fuhr ist Gestalt-Trainer und -Berater und als CISSP, CISA sowie ISO 27 001 Lead Auditor zertifiziert.

Dr. Dipl.-Phys. Christoph Glowatz
Dr. Christoph Glowatz studierte Physik an der Heinrich-Heine-Universität in Düsseldorf und promovierte dort in experimenteller Festkörperphysik. Im Anschluss trat er in die Dienste der Westdeutschen Landesbank und spezialisierte sich dort auf Planung und Aufbau hochverfügbarer Banken-Systeme unter UNIX. Später wechselte er in die Finance-Sparte von T-Systems, war dort mehrere Jahre im Bereich Security & Process-Management tätig und verantwortete Aufgaben im Operational Risk Management IT. Danach leitete er im Service Management der Bechtle AG den Aufbau und den Betrieb von Secured Managed IT Services für mittelständische Unternehmen und Behörden. Zuletzt übernahm er die Position des CISO an der Hochschule Düsseldorf.

Christian A. Gorke, M.Sc.
Christian Gorke studierte Mathematik an der Justus-Liebig-Universität Gießen. Praktische Erfahrung sammelte er während des Studiums bei Infineon Technologies AG in der Abteilung ChipCard & Security, wo er auch seine Masterarbeit mit Schwerpunkt Kryptographie und Security erarbeitete. Seit Abschluss des Studiums promoviert Christian Gorke an der Universität Mannheim bei Prof. Armknecht am Lehrstuhl Praktische Informatik: Dependable Systems Engineering. Dort forscht er in den Bereichen Cloud Security, Mobile Security, Web Security sowie angewandter IT-Security.

Dr.-Ing. Christian Haas
Dr. Christian Haas studierte Informatik an der Universität Karlsruhe (TH). Anschließend promovierte er am Karlsruher Institut für Technologie (KIT). Seit 2015 leitet er die Gruppe «Sichere vernetzte Systeme» in der Abteilung «Informationsmanagement und Leittechnik» am Fraunhofer IOSB. Seine wissenschaftlichen Schwerpunkte umfassen die Konzeption und Entwicklung von IT-Sicherheitsmechanismen für industrielle Produktionssysteme, die Weiterentwicklung des IT-Sicherheitslabors für die industrielle Produktion am Fraunhofer IOSB sowie die Projektleitung und Mitarbeit in industriellen Entwicklungs- und Forschungsprojekten im Themengebiet IT-Sicherheit für industrielle Produktionsanlagen/kritische Infrastrukturen.

Dipl.-Inf. Mark Hartmann
Mark Hartmann studierte Informatik an der Technischen Universität München. Durch unterschiedliche Tätigkeiten in den Bereichen Softwareentwicklung sowie Projekt- und Produktmanagement und als Datenschutzbeauftragter in kleinen, mittelständischen und großen Unternehmen verfügt er über eine mehr als 20-jährige Erfahrung zu unterschiedlichsten Aspekten der

IT-Sicherheit. Er arbeitet derzeit als Program Director IIoT & AI bei der Firma DriveLock SE an der Produktintegration von Machine Learning und Data Verification in Lösungen zum Schutz von Industrial-IoT-Systemen.

Peter Haufs-Brusberg, M.Sc.
Peter Haufs-Brusberg studierte Medieninformatik an der Hochschule Düsseldorf. Nach Abschluss des Bachelorstudiengangs, in dem er stark auf den Bereich der Informationssicherheit fokussierte und eine Bachelorarbeit in Kooperation mit einem Unternehmen erstellte, setzte er das Studium im Masterstudiengang fort. Nach Erstellung der Masterarbeit, in der ein Management-Informationssystem für Risiken der Informationssicherheit im Finanzsektor theoretisch entwickelt wurde, arbeitete er als wissenschaftlicher Mitarbeiter im Bereich der Informatik und IT-Sicherheit der Hochschule Düsseldorf. Bereits während des Studiums ging er einer selbstständigen Tätigkeit nach. Mit dem Wechsel zur Deutschen Bank Luxembourg arbeitete Peter Haufs-Brusberg anfangs als Risikoanalyst und hält heute die Rolle des Chief Information Security Officers.

Dipl.-Ing. Jens Hempel
Jens Hempel studierte Elektrotechnik an der Technischen Universität Budapest. Anschließend war er in verschiedenen mittelständischen sowie Großunternehmen in Deutschland und Asien tätig, zuletzt seit über 10 Jahren in der TÜV Rheinland Gruppe. Hier liegt sein Fokus derzeit auf der Entwicklung neuer Dienstleistungen und Projektleitung für Kommunikation und deren Sicherheit. Die bezogenen Themenfelder sind neben Smart Grid, Smart City, Smart Home, IIoT auch DSGVO, OT Cyberrisk und ISMS. Neben verschiedenen Arbeitskreisen der IEC und IECEE ist er auch bei der DKE tätig. Darüber hinaus wirkt er in der Wirtschaftsinitiative Smart Living des BMWi mit.

Prof. Dr. Nils Herda
Prof. Dr. Nils Herda studierte Wirtschaftsinformatik an der Otto-Friedrich-Universität Bamberg an der er anschließend promovierte. Nach einer beruflichen Karriere als Vorstandsassistent und Direktor für Direktbanking war er zehn Jahre bei der Excelsis Business Technology AG als Geschäftsführer für die deutsche und die Schweizer Ländergesellschaft tätig. Seit 2013 ist er als Professor für Wirtschaftsinformatik an der Hochschule Albstadt-Sigmaringen tätig und Co-Leiter des Instituts für IT-Governance, Risk and Compliance Management. Im Rahmen der angewandten Forschung hat er sich auf das Risikomanagement in IT-Anwendungssystemen sowie auf Digitale Plattformen in digitalin Ökosystemen spezialisiert.

Prof. Dr.-Ing. Hans-Joachim Hof
Prof. Dr. Hans-Joachim Hof studierte Informatik an der Universität Karlsruhe (TH). Nach seiner Promotion über Sicherheit für das Internet der Dinge führte Ihn sein beruflicher Werdegang über die Siemens AG (Research Scientist in der Corporate Technology) und die Hochschule München (Professor für Sichere Softwaresysteme) an die Technische Hochschule Ingolstadt, wo er als Professor für IT-Sicherheit eine Forschungsgruppe zur Sicherheit für Embedded Systems leitet. Professor Hof ist Vorsitzender des German Chapter of the ACM und Präsidiumsmitglied der Gesellschaft für Informatik.

Dr.-Ing. Lutz Jaenicke
Dr. Lutz Jaenicke studierte Elektrotechnik an der Technischen Universität Berlin. Anschließend promovierte er dort. Ab 2002 leitete er als CTO die Entwicklung der Innominate Security Technologies AG, jetzt Phoenix Contact Cyber Security AG. 2016 wechselte er in den Bereich Corporate Technology & Value Chain der Phoenix Contact GmbH & Co. KG und ist seitdem als

Product & Solution Security Officer tätig. In der Plattform Industrie 4.0 ist er Gründungsmitglied der Arbeitsgruppe «Sicherheit vernetzter Systeme» und mehrerer Unterarbeitsgruppen, von denen er zwei zum Thema «Sichere Kommunikation für Industrie 4.0» leitet. Er vertritt das Thema in verschiedenen Arbeitskreisen im ZVEI und VDMA. Darüber hinaus ist er stellvertretender Obmann der DKE Arbeitsgruppe DKE UK 931.1.

Dipl.-Inf. Michael Jochem
Michael Jochem studierte Informatik an der TU Darmstadt. Er startete seine berufliche Karriere bei der Robert Bosch GmbH in der Softwareentwicklung für CNC-Steuerungen. Über Fach- und Führungsaufgaben in der Entwicklung und dem Produktmanagement hat er viele Facetten der Automationsbranche kennengelernt. Seit 2016 ist er bei der Robert Bosch GmbH im Bereich Industrial Technology für IT-Security Governance & Services zuständig Er ist Leiter der Arbeitsgruppe «Sicherheit vernetzter Systeme» der Plattform Industrie 4.0 und Mitglied im Lenkungskreis der Plattform Industrie 4.0. Im ZVEI ist er als Vorsitzender des AK Cybersicherheit und Leiter der SG Sicherheit tätig. Darüber hinaus ist er im DKE Mitglied der Arbeitsgruppe UK 931.1.

Dipl.-Ing. (FH) Dirk Kalinowski
Dirk Kalinowski studierte Anlagen- und Verfahrenstechnik an der Fachhochschule Köln. Danach war er als Auditor für Verwertungs- und Entsorgungsbetriebe, QM- und UM-Systeme beim TÜV Rheinland tätig. 1999 wechselte er zur AXA Versicherung als Technischer Risikoberater im Bereich Haftpflicht und beschäftigte sich insbesondere mit Produktrisiken. Er arbeitete an verschiedenen Projekten im Bereich Risikomanagement mit u.a. in einer Arbeitsgruppe bei der DGQ. Seit 2015 arbeitet Herr Kalinowski als Senior Produktmanager im Bereich IT- und Cyber-Risiken im Industriekundengeschäft der AXA Versicherung. Er ist fachlicher Leiter der Kompetenzstelle Cyber und arbeitet in Arbeitsgruppen zur Informationssicherheit des eco Verbandes sowie der nrw-units mit.

Dr.-Ing. Tobias Kleinert
Dr. Tobias Kleinert studierte Maschinenbau an der Rheinisch-Westfälisch Technischen Hochschule Aachen. Seit der Promotion an der Ruhr-Universität Bochum arbeitet er für BASF u.a. in den Bereichen Advanced Process Control, Produktionstechnologie HPPO und der Technischen Expertise Automatisierung. Im Arbeitskreis 4.18 Automation Security der NAMUR Interessengemeinschaft Automatisierungstechnik der Prozessindustrie e.V. arbeitete er aktiv an der Entwicklung des Arbeitsblattes NA 163 Security for Safety mit.

Michael Krammel
Michael Krammel absolvierte eine Ausbildung zum Prozessleittechniker. In der Zeit von 1989 bis 1999 war er in einem Unternehmenskonzern verantwortlich für den Aufbau einer zentralen Leittechnik- und Automatisierungsabteilung. Nach seinem Wechsel 1999 zur KORAMIS GmbH übernahm er das Business Development «Digitale Fabrik» mit Schwerpunk Industrial Automation und seit 2005 auch Industrial Security (OT Security). Seit 2008 als Geschäftsführer steuert er diese nationale und internationale Geschäftsentwicklung, wirkt aktiv in Gremien, Fachverbänden und in der Arbeitsgruppe «Sicherheit vernetzter Systeme» der Plattform Industrie 4.0 mit. Dort leitet er eine eigene Unterarbeitsgruppe, welche sich mit den Herausforderungen der Industrie 4.0 Security für Mensch, Organisation und Qualifikation auseinandersetzt.

Erwin Kruschitz, M.Sc.
Erwin Kruschitz absolvierte eine Ingenieurausbildung in Klagenfurt und studierte Engineering Management an der TU Wien und der Oakland University. Vor der Gründung der anapur AG

arbeitete er als Automatisierungsingenieur für petrochemische und biopharmazeutische Prozesse. Seit 2006 befasst er sich mit OT-Security. Er leitet die Automation Security Arbeitskreise in NAMUR und DKE 931.1.

Dipl.-Ing. Thomas Leifeld
Thomas Leifeld studierte Elektrotechnik an der Technischen Universität Kaiserslautern und der University of Edinburgh. Im Anschluss forschte er an der Technischen Universität Kaiserslautern am Lehrstuhl für Automatisierungstechnik. Im Rahmen seiner Forschungstätigkeiten war er Mitglied der Ad-hoc-Arbeitsgruppe Security for Safety im Namur Arbeitskreis 4.18 Automation Security und wirkte unter anderem an der Entwicklung der Arbeitsblattes NA 163 IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen mit. Nach seiner Tätigkeit als Automation Engineer im Fachzentrum Automatisierungstechnik in der Fachgruppe Control Systems and Business Integration der BASF SE ist er seit 2019 wissenschaftlicher Mitarbeiter an der Technischen Universität Kaiserslautern.

Dipl.-Ing. Helmut Leopold, PhD
Helmut Leopold studierte Informatik an der Technische Universität Wien und absolvierte seinen Doktor an der Universität Lancaster in England. Anschließend war er 10 Jahre bei Alcatel-Lucent und weitere 10 Jahre bei Telekom Austria in verschiedenen Managementfunktionen tätig. Seit 2009 führt er am AIT Austrian Institute of Technology das Center for Digital Safety & Security. Aktuell leitet er verschiedene Cyber Security Expertengruppen wie die Task Force der Cyber Security Plattform (CSP) Austria des Österreichischen Bundeskanzleramtes als auch der Industrie 4.0 Plattform Austria und ist Präsident der Gesellschaft für Informations- und Kommunikationstechnik (GIT) im Österreichischen Verband für Elektrotechnik (OVE).

Dipl.-Inf. (FH) Jens Mehrfeld, M.Comp.Sc.
Jens Mehrfeld studierte Angewandte Informatik an der Hochschule Fulda und Fernhochschule Hagen. Seit 2007 ist er beim Bundesamt für Sicherheit in der Informationstechnik. Dort hat er sich unter anderem mit der Kommunikationssicherheit in Geschäftsprozessen beschäftigt. Derzeit ist er im Bereich Cybersicherheit in industriellen Anlagen. Er arbeitet dort Empfehlungen für Hersteller, Integratoren und Betreiber um sich vor Angriffen zu schützen. Er ist Mitglied der Arbeitsgruppe Sicherheit vernetzter Systeme der Plattform Industrie 4.0.

Sebastian Neef, B.Sc.
Sebastian Neef studiert gegenwärtig Informatik an der Technischen Universität Berlin. Seit seinem Abitur berät und hilft er unzähligen Unternehmen, wie z.B. Google, Facebook und Paypal, Sicherheitslücken aufzudecken und ihre Sicherheit zu verbessern. Als Mitbegründer des Internetprojekts «Internetwache.org» deckt er im Internet Schwachstellen und unsichere Systeme auf, um betroffene Betreiber zu informieren. Diese Arbeit, wie z.B. die Aufdeckung von ungesicherten Wasserwerken in Deutschland, wurde von diversen Behörden (BSI, US-Cert) und Medien (ARD, ZDF) aufgenommen. Seit 2018 ist er im Vorstand der studentischen Vereinigung AG Rechnersicherheit der Technischen Universität Berlin.

Prof. Dipl. El.-Ing. ETH Armand Portmann
Prof. Armand Portmann studierte Elektrotechnik an der Eidgenössische Technische Hochschule in Zürich. Danach arbeitete er als Entwicklungsingenieur und Projektleiter bei einem namhaften Schweizer Hersteller von Verschlüsselungsprodukten. Seit 2002 ist er im Bereich Informationssicherheit an der Hochschule Luzern – bis 2007 als wissenschaftlicher Mitarbeiter und danach als Dozent – tätig. Neben seinen Forschungsprojekten kamen später Unterrichtstätigkeiten im Bereich

Informationssicherheit in der Aus- und Weiterbildung dazu. Seit 2006 leitet er die Zertifikatslehrgänge Certificate of Advanced Studies in Information Security und seit 2013 auch den Master of Advanced Studies in Information Security.

Dipl.-Inf. (FH) Peter Rehäußer
Peter Rehäußer studierte Informatik an der Georg-Simon-Ohm Fachhochschule Nürnberg. Nach dem Studium begann er als IT-Sicherheitsberater bei CSC Ploenzke und übernahm später auch die Leitung der Cybersecurity Beratung für Zentral- und Osteuropa. Heute verantwortet er als Executive Director bei Ernst & Young die Beratungsleistungen für technische Cybersicherheit für den D-A-CH-Raum. Er berät nun seit fast 20 Jahren Großkonzerne und Bundesbehörden zu unterschiedlichsten Fragestellungen der Cybersicherheit.

Prof. Dr. Stefan Ruf
Prof. Dr. Stefan Ruf studierte Wirtschaftsinformatik an der Georg-August-Universität Göttingen und promovierte an der Eberhard-Karls-Universität Tübingen über Risikomanagementsysteme im Multi-Channel-Umfeld. Berufliche Stationen waren die Boston Consulting Group sowie die Landesbank Baden-Württemberg. Im Jahr 2010 erfolgte der Ruf als ordentlicher Professor für Betriebswirtschaftslehre an die Hochschule Albstadt-Sigmaringen mit dem Schwerpunkt Informationsmanagement. Aktueller Forschungs- und Lehrschwerpunkt ist die digitale Transformation von Wirtschaftsunternehmen im Kontext komplexer Anforderungen der Cybersicherheit.

Prof. Dr.-Ing. Holger Schmidt, Dipl.-Math.
Prof. Dr. Holger Schmidt studierte Mathematik an der Westfälischen Wilhelms-Universität in Münster. Anschließend arbeitete er an der Fakultät für Ingenieurwissenschaften der Universität Duisburg-Essen, wo seine Promotion zum Dr.-Ing. im Februar 2010 erfolgte. Neben seinen Lehr- und Forschungstätigkeiten an der Technischen Universität Dortmund und der Universität Duisburg-Essen folgten Beschäftigungen unter anderen bei der TÜV Informationstechnik GmbH, einem Unternehmen der TÜV Nord Group, in Essen. Seit August 2015 ist Holger Schmidt Professor für Informatik, insb. IT-Sicherheit am Fachbereich Medien der Hochschule Düsseldorf sowie freiberuflicher Berater für IT-Sicherheit. Seine Forschungsinteressen sind geprägt von der Integration der Informationssicherheit, des Faktor Mensch und Verfahren und Methoden des Software Engineering.

Dipl.-Ing. Thomas Schulz
Thomas Schulz studierte Maschinenbau an der Technischen Universität Budapest. Danach war er in verschiedenen mittelständischen sowie Großunternehmen tätig. Er verfügt heute über langjährige Erfahrung in Digitalisierungsprojekten bei der Einführung industrieller Software in der Fertigungs- und Prozessindustrie sowie der Cyber-Sicherheit zum Schutz von Maschinen und Anlagen. Als langjähriges Mitglied der Plattform Industrie 4.0 ist er Autor und Mitautor zahlreicher Publikationen. Derzeit zeichnet er verantwortlich für das Mittelstands- und Partnergeschäft in Mittel- und Osteuropa im Bereich GE Digital im Unternehmen General Electric (GE).

Dr. rer. pol. Frank Stummer
Dr. Frank Stummer studierte Wirtschaftswissenschaften an der Technischen Universität Bergakademie Freiberg. Anschließend promovierte er am Fraunhofer Institut für System- und Innovationsforschung FhG-ISI in Karlsruhe. Er ist Mitgründer mehrerer Unternehmen im Hochtechnologiebereich und arbeitet derzeit für die Rhebo GmbH und die Digital Forensics GmbH im Bereich von Sicherheitslösungen für industrielle Steuerungssysteme und der Analyse von Sicher-

heitsvorfällen. Frank Stummer ist aktiv in verschiedenen Arbeitskreisen u.a. zum Informationssicherheitsmanagement in Energieversorgungsunternehmen und Autor einer Reihe von Veröffentlichungen in diesem Bereich.

Paul Trompisch, MPP
Paul Trompisch studierte Wirtschaftswissenschaft an der Wirtschaftsuniversität Wien und Politikwissenschaft an der Hertie School of Governance in Berlin. Er arbeitete als Referent in der European Chamber of Commerce in Singapur und im Brüssel Büro der österreichischen Industriellenvereinigung. 2016 wurde er kurz nach der Gründung der Plattform Industrie 4.0 Österreich Teil der Geschäftsstelle und trug zur strategischen Konzeption, Aufbau und Etablierung der Plattform als zentraler Netzwerkknoten und Wissensträger im Bereich Industrie 4.0 bei. Als Senior Advisor ist er für die Themenbereiche Normen und Standards, Security und Safety und Mensch in der digitalen Fabrik verantwortlich.

Raphael Vallazza
Raphael Vallazza studierte Informatik an der Università dei Studi Milano-Bocconi. Durch seine Tätigkeit als Web-Entwickler während und nach dem Studium erkannte er den stetig wachsenden Bedarf an Security-Lösungen. 2003 gründete er Endian mit dem Ziel, ein virtuelles Open Source Unified Threat Management (UTM) zu entwickeln. Für diese Security-Lösung erhielt er 2008 den ersten «South Tyrol Free Software Award» (SFS Award) der Stiftung Südtiroler Sparkasse. Die prämierte UTM ist die Basis für die wegweisenden Industrie 4.0-Lösungen des Unternehmens. 2017 wurde Endian mit dem Digital Transformation Award der WEKA Fachmedien GmbH ausgezeichnet.

Prof. Dr.-Ing. Oliver Weissmann
Prof. Dr.-Ing. Oliver Weissmann studierte Technische Informatik an der Universität Siegen. Danach war er als Lehrbeauftragter für angewandte Kryptographie sowie für die Forschung und Lehre der Vorlesungen «Information Security Management» und das Praktikum «Kryptographische Verfahren und Anwendungen» dort tätig. In der Internationalen Standardisierungsorganisation wirkte er seit 1998 als Editor und Projektverantwortlicher. Die ISO/IEC 17799:1999, später ISO/IEC 27002:2005, betreute er als Editor bis hin zur letzten Überarbeitung im Jahr 2013 mit der Veröffentlichung als ISO/IEC 27002:2013. Er ist geschäftsführender Gesellschafter der xiv-consult GmbH und hält seit 2015 an der Hochschule Darmstadt die Professur für Informationssicherheit und lehrt in den Bereichen Security Management, sichere Software und IT Compliance.