HANSER

Leseprobe

zu

IT-Sicherheit

von Michael Lang (Hrsg.) und Hans Löhr (Hrsg.)

Print-ISBN: 978-3-446-47223-5
E-Book-ISBN: 978-3-446-47347-8
E-Pub-ISBN: 978-3-446-47511-3

Weitere Informationen und Bestellungen unter
https://www.hanser-kundencenter.de/fachbuch/artikel/9783446472235
sowie im Buchhandel

© Carl Hanser Verlag, München

Inhalt

Vorwort . . . . . **XIII**

1 IT-Sicherheit konsequent und effizient umsetzen **1**
Norbert Pohlmann

1.1 Einleitung 1
1.1.1 Chancen durch die Digitalisierung 1
1.1.2 Risiken durch die Digitalisierung 2
1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit 3
1.2 Beispiele von aktuellen Angriffsvektoren 4
1.3 IT-Sicherheitsstrategien 7
1.3.1 Vermeiden von Angriffen 8
1.3.2 Entgegenwirken von Angriffen 9
1.3.3 Erkennen von Angriffen 10
1.3.4 Reaktion auf Angriffe 11
1.4 Umsetzung eines angemessenen IT-Sicherheitslevels 12
1.5 IT-Sicherheitsmechanismen, die gegen Angriffe wirken 13
1.6 Die wichtigsten Punkte in Kürze 21
1.7 Literatur 22

2 Grundprinzipien zur Gewährleistung der IT-Sicherheit **23**
Hagen Lauer, Nicolai Kuntze

2.1 Einleitung 23
2.1.1 Trends 23
2.1.2 Herausforderungen 24
2.1.3 IT-Sicherheit vs. Sicherheit 25
2.1.4 Schutzziele 26
2.2 Grundprinzipien der IT-Sicherheit 31
2.2.1 Kenne die Bedrohungen 32
2.2.2 Sicherheit und Wirtschaftlichkeit 33
2.2.3 Keine „Security through Obscurity“ 34
2.2.4 Security by Design 34
2.2.5 Prinzip der geringsten Berechtigung 35
2.2.6 Trennung der Verantwortlichkeiten 36
2.2.7 Zugriffskontrolle 36

2.2.8 Defense in Depth . . . 37
2.2.9 Der Mensch als Faktor . . . 38
2.2.10 Design for Resilience . . . 39
2.3 Literatur . . . 41

3 Organisation des IT-Sicherheitsmanagements im Unternehmen . . 43
Markus Nauroth

3.1 Einführende Bemerkungen . . . 44
3.2 Imperative des IT-Sicherheitsmanagements . . . 45
3.2.1 Sicherheit ist aktiv und proaktiv . . . 45
3.2.2 Routine . . . 45
3.2.3 Sicherheit liegt in der Verantwortung eines jeden . . . 45
3.2.4 Worst-Case-Szenario . . . 46
3.2.5 Es bedarf vieler Unterstützer . . . 46
3.2.6 Denken wie ein Angreifer . . . 46
3.2.7 Mehrschichtige Verteidigung verwenden . . . 46
3.3 Grundlegende Pfeiler einer IT-Sicherheitsorganisation . . . 47
3.3.1 Gängige Organisationsstrukturen nach organisatorischem Reifegrad . . . 48
3.3.2 Das Information Technology Risk Council (ITRC) . . . 52
3.4 Die Rolle des CISO: Wie man eine Führungsrolle im Sicherheitsbereich gestaltet 54
3.4.1 Die richtige CISO-Rolle für Ihr Unternehmen entwerfen . . . 54
3.5 Finale Anmerkungen . . . 59

4 Rechtliche Rahmenbedingungen der IT-Sicherheit . . . 61
Thomas Jansen

4.1 Einleitung . . . 61
4.2 Vertrags- und haftungsrechtliche Risiken . . . 62
4.2.1 Allgemeine Sorgfaltspflichten . . . 62
4.2.2 Pflichten zur Gewährleistung der IT-Sicherheit . . . 63
4.2.3 Haftung für Verstöße gegen IT-sicherheitsrechtliche Anforderungen . . . 64
4.2.4 Anforderungen der DSGVO an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit . . . 65
4.2.5 Anforderungen des TKG und des TTDSG an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit . . . 66
4.2.6 Empfehlungen des BSI in Bezug auf technisch-organisatorische Maßnahmen . . . 67
4.3 Straf- und ordnungswidrigkeitsrechtliche Folgen bei der Verletzung der IT-Sicherheit . . . 68
4.3.1 Strafrechtliche Normen zum Schutz vor Cyberkriminalität . . . 68
4.3.2 Strafrechtliche Verantwortlichkeit der einzelnen Akteure . . . 70
4.4 Das IT-Sicherheitsgesetz (ITSiG 2.0) . . . 71
4.5 Die wichtigsten Punkte in Kürze . . . 73
4.6 Literatur . . . 74

5 Standards und Zertifizierungen 77
Thomas Lohre

5.1 Einleitung 77
5.2 Standards 79
5.2.1 Synergien zwischen Standards auflösen und nutzen 87
5.2.2 Zertifizierung/Testierung 89
5.3 Kompetenznachweise für Beteiligte der Informationssicherheit 92
5.4 Die wichtigsten Punkte in Kürze 96
5.5 Literatur 96

6 Datenschutz und Informationssicherheit: ungleiche Zwillinge 99
Stefan Karg

6.1 Einleitung 99
6.2 Rechtlicher Rahmen 101
6.3 Strategische/präventive Aspekte 103
6.3.1 Risikomanagement 103
6.3.2 Regelmäßige Überprüfung der Maßnahmen 104
6.3.3 Entwicklungsprozess 105
6.4 Operative Aspekte: technische und organisatorische Maßnahmen 107
6.4.1 Schutz der Vertraulichkeit 107
6.4.2 Schutz der Integrität 110
6.4.3 Schutz der Verfügbarkeit und Belastbarkeit 111
6.4.4 Vorfallsbehandlung (Incident Management) 111
6.5 Organisationsaspekte 113
6.6 Fazit 114
6.7 Literatur 114

7 Sicherheit durch Bedrohungs- und Risikoanalysen stärken 115
Daniel Angermeier

7.1 Einleitung 115
7.2 Nutzen und Mehrwert von Bedrohungs- und Risikoanalysen 116
7.3 Ablauf von Bedrohungs- und Risikoanalysen 118
7.4 Einbindung in Unternehmensprozesse 120
7.4.1 Anforderungsanalyse und Konzeptphase 120
7.4.2 Tests planen und priorisieren, Testergebnisse bewerten 124
7.4.3 Schwachstellen bewerten und behandeln 125
7.4.4 Laufende Systeme bewerten 126
7.5 Auswahlkriterien für geeignete Methoden 126
7.6 Die wichtigsten Punkte in Kürze 127
7.7 Literatur 127

8 Mittels Reifegradanalysen den IT-Security-Level nachhaltig und belastbar steigern 129
Martin Braun

8.1 Einleitung 129
8.2 Aufgabe und Wirkung einer Reifegradanalyse 130
8.2.1 Aufgabe der Reifegradanalyse 130
8.2.2 Die Reifegradanalyse hat unterschiedliche Aufgaben 130
8.2.3 Reifegradanalyse auch als Messinstrument der Belastbarkeit der Kernprozesse 131
8.2.4 Wirkung der Reifegradanalyse 132
8.3 Den Reifegrad des IT-Security-Prozesses ermitteln 134
8.3.1 Definition des IT-Security-Reifegrad-Levels 0: Initial 135
8.3.2 Definition des IT-Security-Reifegrad Level 1: wiederholbar 136
8.3.3 Definition des IT-Security-Reifegrad-Levels 2: definiert 137
8.3.4 Definition des IT-Security-Reifegrad-Levels 3: gemanagt 138
8.3.5 Definition des IT-Security-Reifegrad-Levels 4: optimiert 139
8.4 Durch eine kontinuierliche Reifegradmessung das IT-Risiko minimieren 140
8.4.1 Gesamtheitliche Betrachtung der Perspektiven 141
8.4.2 Perspektive Business 142
8.4.3 Perspektive Organisation und IT 144
8.5 Fazit 146

9 Der Chief Information Security Officer in der Praxis 147
Andreas Reisch

9.1 Einleitung 147
9.2 Business und IT, woher – wohin – mit wem? 148
9.3 Wozu gibt es nun den CISO? 149
9.4 Die persönliche Verantwortung des CISO 150
9.5 Verantwortung des Unternehmens 152
9.6 Das ISMS 153
9.7 Culture, Communication & Awareness 154
9.8 Assessments 156
9.9 Approvals und Information Security Consulting 157
9.10 Information Security Consulting 159
9.11 Lohnt sich das SOC? 160
9.12 IS-Operations 161
9.13 Fazit 162

10 Irgendwas ist immer – Informationssicherheit aus Sicht des CISO der Allianz Technology 163
Fabian Topp

10.1 Einleitung 163
10.2 Vernetzung – hilf mir, es selbst zu tun 165
10.3 Personal – die schlechten sind die teuersten Mitarbeiter 167
10.4 No Risk (no Privacy, no Audit, ...), no Fun. 171
10.4.1 Organisation ist ein Mittel, die Kräfte des Einzelnen zu vervielfältigen . . 172
10.4.2 Mehr als die Summe seiner Teile. 174
10.5 Ende gut, alles gut? 175

11 Entwicklung sicherer Software 177
Nicolai Kuntze, Hagen Lauer

11.1 Einleitung 177
11.2 Vorgehensmodelle der Softwareentwicklung 179
11.3 Secure Development Lifecycles 181
11.4 Requirements Engineering 182
11.5 Architektur und Entwurf. 183
11.6 Implementierung 184
11.7 Coding-Standards 184
11.8 Wahl der Programmiersprache. 186
11.9 Tests 188
11.10 Code Reviews 188
11.11 Static Code Analysis 189
11.12 Formale Analyse 189
11.13 Validierung 190
11.14 Maintenance 190
11.15 Die wichtigsten Punkte in Kürze 192
11.16 Literatur 192

12 Cybersicherheit in Produktion, Automotive und intelligenten Gebäuden 193
Marko Schuba, Hans Höfken

12.1 Einleitung 193
12.1.1 Automatisierungstechnik 194
12.1.2 Spezifische Anforderungen der Automatisierungstechnik 196
12.1.3 Spezifische Eigenschaften der Automatisierungstechnik 197
12.2 Schöne neue Welt – das Internet der Dinge 199
12.2.1 Internet der Dinge (IoT) 200
12.2.2 IoT-Chancen für die Automatisierungstechnik. 200
12.2.3 IoT-Risiken für die Automatisierungstechnik. 201

12.3 Was läuft schief? ... 201
12.3.1 Zu viel Vertrauen in andere ... 201
12.3.2 Zu wenig Management-Fokus ... 202
12.3.3 Sicherheits-Features zu teuer oder nicht genutzt ... 202
12.3.4 Es ist noch nie etwas passiert – und das bleibt auch so ... 203
12.3.5 Never change a running system ... 203
12.3.6 Sensibilisierung und Weiterbildung zu teuer/aufwendig ... 204
12.4 Was ist zu tun? ... 205
12.4.1 Cybersicherheit allgemein ... 205
12.4.2 Cybersicherheit in der Automatisierung ... 205
12.5 Praxisbeispiel: Einführung von Cybersicherheit in der Produktion (Orientierung an ISA/IEC 62443) ... 209
12.5.1 Audit ... 209
12.5.2 Festlegen eines Sicherheitslevels ... 210
12.5.3 Risikobeurteilung ... 210
12.5.4 Defense in Depth ... 211
12.5.5 Zonierung ... 212
12.5.6 Patchmanagement ... 213
12.5.7 Dienstleister ... 215
12.6 Zusammenfassung und Fazit ... 216
12.7 Literatur ... 216

13 Edge Computing: Chancen und Sicherheitsrisiken ... 219
Marcel Winandy

13.1 Einleitung ... 219
13.2 Was ist Edge Computing? ... 221
13.2.1 Das Internet der Dinge ... 221
13.2.2 Von der Cloud zur Edge ... 222
13.2.3 Impulsgeber für IoT Edge Computing ... 224
13.3 Chancen und Sicherheitsrisiken ... 225
13.3.1 Eröffnung neuer Möglichkeiten durch IoT Edge Computing ... 225
13.3.2 IoT Edge Computing bringt auch neue Sicherheitsrisiken ... 227
13.4 Entwicklung sicherer Edge-Computing-Plattformen ... 230
13.4.1 Security-by-Design-Prinzipien ... 230
13.4.2 Privacy-by-Design-Prinzipien ... 232
13.4.3 Spezielle Entwicklungsprinzipien für Edge Computing ... 233
13.5 Technologien für sichere Edge-Computing-Plattformen ... 234
13.5.1 Sicherheitskerne ... 235
13.5.2 Trusted Execution Environments ... 237
13.5.3 Kryptoagilität ... 237
13.6 Die wichtigsten Punkte in Kürze ... 238
13.7 Literatur ... 239

14 IT-Sicherheit in Vergabeverfahren 241
Jutta Pertenaïs

14.1 Einleitung 241
14.2 Vergabeverfahren in Deutschland 242
14.2.1 Grundsätze und Aspekte 243
14.2.2 Verfahrensarten 246
14.2.3 Elektronische Vergabeplattformen 249
14.3 IT-Sicherheit im Vergabeverfahren 249
14.3.1 TOM im Vergabeverfahren 249
14.3.2 Die Gestaltung der Vergabeunterlagen 251
14.3.3 Die Planung des Vergabeverfahrens 252
14.3.4 Die Verfahrensdurchführung 254
14.3.5 Die elektronische Kommunikation 254
14.3.6 Der Umgang mit Verschlusssachen 255
14.4 Kennzeichnen von Geschäftsgeheimnissen 256
14.5 Rechtschutzmöglichkeiten 258
14.6 Strafbarkeit im Vergabeverfahren 259
14.7 Bietertipps zum Umgang mit Vergabestellen und zur Erstellung von Angeboten 260
14.8 Die wichtigsten Punkte in Kürze 260
14.9 Literatur 261

15 Sicherheit in der Cloud 263
Christoph Skornia

15.1 Einleitung 263
15.2 Nutzungsmodelle 264
15.2.1 Servicemodelle 264
15.2.2 Bereitstellungsmodelle 265
15.3 Risiken des Cloud Computing 266
15.3.1 Überblick 266
15.3.2 Beispiele 268
15.4 Sicherheitsmaßnahmen 269
15.4.1 Sicherheitsrahmen 269
15.4.2 Zugangskontrolle 271
15.4.3 Datensicherheit 272
15.4.4 Monitoring und Überwachung 274
15.5 Zusammenfassung 276
15.6 Die wichtigsten Punkte in Kürze 277
15.7 Literatur 277

Herausgeber, Autorin und Autoren 279

Stichwortverzeichnis 285

Vorwort

Informationen sind die wertvollsten Güter für Unternehmen. Die zur Informationsverarbeitung eingesetzten IT-Systeme sind heutzutage zentraler Bestandteil jedes Unternehmens und bilden die Grundlage für nahezu alle Geschäftsprozesse. Ohne sie funktioniert fast nichts mehr.

Kommt es zu Störungen in der IT, kann dies im schlimmsten Fall das komplette Unternehmen zum Stillstand bringen und existenzbedrohend sein. Gleiches gilt, wenn Informationen des Unternehmens oder dessen Kunden verloren gehen, gestohlen werden, manipuliert werden oder nicht mehr verarbeitet werden können.

Daher ist es für Unternehmen existenziell bedeutend, die Sicherheit der Informationen, Systeme und Produkte zu gewährleisten. Dies trifft heute mehr denn je zu, denn mit zunehmender Vernetzung wächst auch die Angriffsfläche: Jedes vernetzte Gerät ist ein potenzielles Einfallstor für Gefährdungen, und das erhöht das Risiko zusätzlich.

Doch wie können Sie Ihr Unternehmen vor diesen Gefährdungen schützen und Sicherheit gewährleisten?

Die Antwort auf diese Frage – und viele hilfreiche Impulse und Best Practices zur Umsetzung – erhalten Sie in diesem Buch.

Wir freuen uns, dass dazu 16 ausgewiesene Experten/Expertinnen als Autoren/Autorinnen an diesem Buch mitgewirkt haben, um Ihnen die relevanten Aspekte zur IT-Sicherheit von Unternehmen zu beschreiben.

Wir wünschen Ihnen viel Spaß beim Lesen des Buches und viel Erfolg beim Umsetzen der dabei gewonnenen Erkenntnisse!

Ihre Herausgeber

Michael Lang und Hans Löhr

1 IT-Sicherheit konsequent und effizient umsetzen

Norbert Pohlmann

In diesem Beitrag erfahren Sie,

- welche Chancen und Risiken die fortschreitende Digitalisierung mit sich bringt,
- welche Angriffsvektoren heute für erfolgreiche Angriffe genutzt werden,
- welche IT-Sicherheitsstrategien helfen, Risiken zu reduzieren und mit verbleibenden Risiken umzugehen, und
- welche IT-Sicherheitsmechanismen gegen welche Angriffe wirken.

1.1 Einleitung

Wir befinden uns gerade in einer digitalen Transformation, die mit einer radikalen Umgestaltung unseres Alltags und unserer Arbeitswelt sowie aller Geschäftsmodelle und Verwaltungsprozesse einhergeht. Wirtschaftskraft und Wohlstand sowie die Leistungsfähigkeit unserer modernen Gesellschaft werden durch den gelungenen digitalen Wandel bestimmt.

1.1.1 Chancen durch die Digitalisierung

Die Digitalisierung eröffnet über alle Branchen und Unternehmensgrößen hinweg enorme Wachstumschancen und führt zu immer besseren Prozessen, die die Effizienz steigern und Kosten reduzieren. Die Digitalisierung beschleunigt auf allen Ebenen, und der Wertschöpfungsanteil der IT in allen Produkten und Lösungen wird immer größer (Pohlmann 2020) (siehe Bild 1.1, obere Kurve).

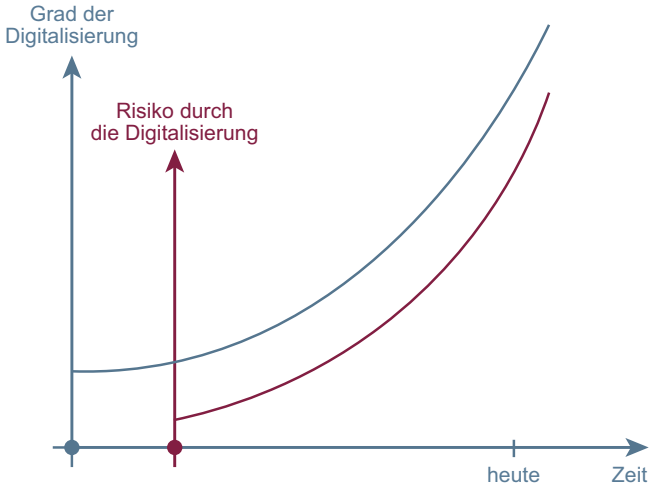


Bild 1.1 Entwicklung der Digitalisierung und des korrespondierenden Risikos

Mögliche Erfolgsfaktoren der Digitalisierung sind vielfältig:

- Mit 5G- und Glasfasernetzen erhöhen sich Kommunikationsgeschwindigkeit und -qualität, wodurch neue Anwendungen möglich werden.
- Smarte Endgeräte wie Smartwatches, Smartphones, PADs oder IoT-Geräte bringen viele neue sinnvolle Anwendungen mit sich.
- Zunehmend leistungsfähige zentrale IT-Systeme wie Cloud-Systeme, Edge-Computing oder Hyperscaler schaffen Innovationen mit großen Potenzialen.
- Da immer mehr Daten zur Verfügung stehen, ist die Verwendung von KI (ML ...) ein weiterer Treiber von neuen Geschäftsmodellen (Pohlmann 2019a).
- Moderne Benutzerschnittstellen, wie Sprache und Gestik, vereinfachen die Bedienung der smarten Endgeräte.
- Die Optimierung von Prozessen schafft ein enormes Rationalisierungspotenzial, das es zu heben gilt, um wettbewerbsfähig zu bleiben und Wachstumschancen zu nutzen.
- Neue Optionen wie Videokonferenzen und Cloud-Anwendungen ermöglichen, im Homeoffice zu arbeiten und damit die Personenmobilität zu reduzieren sowie letztendlich die Umwelt zu schonen.

1.1.2 Risiken durch die Digitalisierung

Wir müssen aber auch feststellen, dass seit Beginn der IT – sowie jetzt mit der zunehmenden Digitalisierung – die IT-Sicherheitsprobleme jedes Jahr größer werden und auf absehbare Zeit definitiv nicht abnehmen. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server, Netzkomponenten und zentralen IT-Dienstleistungen nicht sicher genug konzipiert und aufgebaut sind, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken. Die Vielzahl der lokalen und zentralen Anwendungen, die unterschied-

lichen Zugänge zum Internet, die Masse der IT-Systeme und IT-Infrastrukturen sowie die zunehmenden Abhängigkeiten innerhalb der Supply Chain machen die Komplexität der IT immer größer und damit auch die Anfälligkeit für bösartige Angriffe. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software zunutze machen, indem sie Malware installieren und damit Passwörter sowie Identitäten stehlen, Endgeräte ausspionieren oder die IT-Systeme verschlüsseln, um Lösegeld für die notwendigen Schlüssel zur Entsperrung zu erpressen. Aufgrund der generierten Datenmengen werden die Angriffsziele mit fortschreitender Digitalisierung kontinuierlich lukrativer.

Die Robustheit und Resilienz unserer IT-Systeme sind nicht hinreichend, und der Level an IT-Sicherheit entspricht nicht dem „Stand der Technik“. Mit dem höheren Grad an Digitalisierung steigt momentan das Risiko eines Schadensfalls (siehe Bild 1.1, untere Kurve). Daraus ergibt sich in der Konsequenz, dass durch Diebstahl, Spionage und Sabotage der deutschen Wirtschaft jährlich ein Gesamtschaden von mehr als 220 Milliarden Euro entsteht.

1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit

IT-Sicherheitsbedürfnisse sind Grundwerte der IT-Sicherheit, die mithilfe von IT-Sicherheitsmechanismen befriedigt werden können. IT-Sicherheitsbedürfnisse werden auch als IT-Sicherheitsziele bezeichnet.

- **Gewährleistung der Vertraulichkeit**
  Vertraulichkeit ist wichtig, damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.
- **Gewährleistung der Authentifikation**
  Mithilfe des IT-Sicherheitsmechanismus Authentifikation wird verifiziert, wer der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und Informationen zugreift.
- **Gewährleistung der Authentizität**
  Mithilfe des IT-Sicherheitsmechanismus Authentizität wird verifiziert, dass Informationen oder Identitäten echt sind.
- **Gewährleistung der Integrität**
  Beim IT-Sicherheitsbedürfnis „Gewährleistung der Integrität“ wird überprüft, ob Informationen, die übertragen werden oder gespeichert sind, unverändert, das heißt original, sind.
- **Gewährleistung der Verbindlichkeit**
  Das IT-Sicherheitsbedürfnis „Gewährleistung der Verbindlichkeit“ sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen auch verbindlich sind.
- **Gewährleistung der Verfügbarkeit**
  Dieses IT-Sicherheitsbedürfnis sorgt für die Gewissheit, dass die Informationen und Dienste auch zur Verfügung stehen.
- **Gewährleistung der Anonymisierung**/Pseudonymisierung
  Mit diesem IT-Sicherheitsbedürfnis wird gewährleistet, dass eine Person nicht oder nicht unmittelbar identifiziert werden kann.

1.2 Beispiele von aktuellen Angriffsvektoren

Im Folgenden werden exemplarisch relevante Beispiele von Angriffsvektoren mit den entsprechenden Angriffstechniken und Angriffswegen dargestellt.

1. **Malware-Infiltration über manipulierte Webseiten**
   Als Erstes wird mit einem gezielten Hacking-Angriff auf den Webserver die Platzierung von Angriffssoftware zur Durchführung eines Drive-by-Downloads unter Nutzung einer vorhandenen Schwachstelle auf dem Webserver umgesetzt. Um einen Nutzer (Opfer) zum Besuch der manipulierten Webseite zu motivieren, kann beispielsweise ein Phishing-/Social-Engineering-Angriff durchgeführt werden. Beim Zugriff auf die manipulierten Webseiten werden dann beim Drive-by-Download Sicherheitslücken des Browsers oder des Betriebssystems des Opfer-IT-Systems des Nutzers ausgenutzt, um Malware zu installieren. Mit der generalisierten installierten Malware kann dann der Angreifer spezielle Schadfunktionen nutzen, um das gekaperte IT-System gemäß seinem Ziel zu manipulieren.

2. **Malware-Infiltration über schadhafte E-Mail-Anhänge**
   Mithilfe von sozialen und Berufsnetzwerken werden die Vorlieben eines potenziellen Opfers analysiert. Mit diesen Kenntnissen wird dem Opfer eine persönliche Nachricht gesendet, die perfekt dazu verleitet, auf den Anhang der E-Mail zu klicken. Durch das Klicken wird ein Prozess ausgelöst, der ermöglicht, über vorhandene Schwachstellen eine Malware zu installieren. Damit ist die Übernahme der Kontrolle über das betroffene Opfer-IT-System umgesetzt. Anschließend nutzt der Angreifer entsprechende Schadfunktionen, um seine Ziele auf dem Opfer-IT-System umzusetzen.

3. **Mehrstufiger Angriff auf die IT-Infrastruktur von Unternehmen**
   Ein Angreifer verschafft sich einen ersten Zugang auf ein IT-System in einem Unternehmen, wie in den Beispielen 1 und 2 beschrieben. Dann sorgt der Angreifer mit der Schaffung einer individualisierten Malware dafür, dass er den Zugang etabliert, um sich im IT-System frei bewegen zu können und seine Spuren zu verwischen. Anschließend verschafft sich der Angreifer mit zusätzlichen Angriffstechniken mehr Administrationsrechte. Damit kann er die Kontrolle über weitere IT-Systeme bekommen und lateral in große Teile des Netzwerks gelangen. So sammelt der Angreifer umfangreiches Wissen über vorhandene Schwachstellen, Funktionen oder Werte auf den IT-Systemen des Unternehmens und kann darüber eine Strategie für den eigentlichen Angriff entwickeln und erfolgreich umsetzen. Diese Vorgehensweise wird auch als Advanced Persistent Threat (APT) bezeichnet.

4. **Man-in-the-Middle-Angriff (MITM)**
   Bei der Man-in-the-Middle-Angriffsmethode schleust sich ein Angreifer aktiv, aber heimlich – physisch oder logisch – in die Kommunikation zwischen mindestens zwei Kommunikationspartnern mit dem Ziel, Daten lesen oder manipulieren zu können. Die Kommunikationspartner bemerken diesen Eingriff nicht und gehen davon aus, dass sie direkt und vertraulich miteinander kommunizieren, da sich der Angreifer bei beiden Kommunikationspartnern jeweils als das wahrgenommene Gegenüber ausgibt. Durch einen Man-in-the-Middle-Angriff ist es möglich, Passwörter oder weitere wichtige Daten mitzulesen, Kommunikationsverbindungen zum Beispiel nach einer Authentifikation zu übernehmen oder Daten zu manipulieren.

5. **Angriff mithilfe eines Software-Updates (Supply-Chain-Angriff)**
   Bei einem Supply-Chain-Angriff oder Lieferketten-Angriff ist die prinzipielle Idee, dass ein vertrauenswürdiger Dienst (Software), der seit längerer Zeit bei einer Organisation/einem Unternehmen in Einsatz ist, irgendwann für einen Angriff verwendet wird. Als Angriffsvektor missbraucht der Angreifer ein legitimiertes Software-Update, das der vertrauenswürdige Softwarehersteller (Supplier) zur Verfügung stellt. Für die Durchführung dringt der Angreifer zuerst in das IT-System des vertrauenswürdigen Softwareherstellers ein und infiltriert ein Software-Update mit Malware. Voraussetzung für den eigentlichen Angriff ist, dass dieser Vorgang unbemerkt bleibt, daher muss er an einer bestimmten Prozessstelle umgesetzt werden. Nur so lässt sich sicherstellen, dass das manipulierte Software-Update offiziell als Hersteller-Update digital signiert wird, wodurch es mit einem autorisierten Code versehen ist und dadurch vom Kunden akzeptiert und eingespielt werden kann. Darauf basierend ist es dem Angreifer möglich, bei mehreren Tausend Organisationen gleichzeitig das Software-Update des Herstellers zu nutzen, um die eigentlichen Angriffe umzusetzen. Beispiele dieser Angriffsmethode sind: Kaseya und SolarWinds.
6. **Angriff auf die Verfügbarkeit von IT-Systemen (DDoS-Angriff, Distributed Denial of Service)**
   Der Angreifer nutzt die Schwachstelle aus, dass IT-Systeme nur begrenzte Ressourcen (Bandbreite, CPU, RAM ...) haben. Für den Angriff wird das IT-System gezielt mit einer großen Last spezieller Anfragen überflutet, dadurch überlastet und letztendlich lahmgelegt. Dies wird in der Regel unter Einsatz von Botnetzen, bei denen die Bots die Schadfunktion DDoS aktiviert haben, und weiteren Verstärkungsmechanismen wie Reflection und Amplification erfolgreich umgesetzt. Die Motivation der Angreifer ist vielfältig: Entweder soll ein IT-System für eine definierte Zeit lahmgelegt werden, um beispielsweise einen Wettbewerber zu behindern, oder es steckt eine erpresserische Absicht dahinter, um von dem angegriffenen Unternehmen eine bestimmte Summe verlangen zu können, damit der DDoS-Angriff gestoppt oder gar nicht erst durchgeführt wird.
7. **Missbräuchliche Ausnutzung einer Business-Beziehung mit einem High-Level-Phishing-Angriff**
   Ein Angreifer erlangt mithilfe eines Malware-Keyloggers den Zugang zu einem E-Mail-Konto im Unternehmen. In der Vorbereitungsphase analysiert der Angreifer kontinuierlich die E-Mails des angegriffenen Mitarbeiters dahingehend, welche Informationen für einen Angriff verwendbar sind. Das kann zum Beispiel eine hohe Rechnung an einen langfristigen Kunden sein. Sobald diese über das E-Mail-Konto versendet wird, beginnt der Angriff. Im ersten Schritt wird dafür diese E-Mail zusammen mit allen alten Inhalten kopiert, im zweiten Schritt dann in der PDF-Rechnung die Kontonummer verändert. Nach einer sehr kurzen Zeitspanne erfolgt dann der Versand dieser E-Mail zusammen mit einer E-Mail, in der der Angreifer nachfragt, ob die Rechnung bereits beglichen wurde. Der Zeitpunkt muss so gewählt sein, dass es sehr unwahrscheinlich ist, dass eine Bezahlung bereits stattgefunden hat. Denn nur so ist es möglich, das angegriffene Unternehmen dazu aufzufordern, die Rechnung an eine neue Kontonummer zu überweisen, zum Beispiel mit der Begründung, dies sei aufgrund aktueller Sicherheitsvorkehrungen notwendig geworden. Wichtig ist, dass diese E-Mail seitens des Angreifers von einem anderen E-Mail-Konto versendet wird, damit der Mitarbeiter – dessen E-Mail-Account kompromittiert wurde – den Vorgang nicht mitbekommt. Trotzdem ist bei dieser E-Mail der eigentliche Mitarbeiter als Absender angegeben (Mail-Spoofing). Als Return-Pfad

im E-Mail-Header ist jedoch eine andere E-Mail-Adresse angegeben, damit, falls der Empfänger eine Nachfrage hat, diese nicht bei dem Mitarbeiter des (angegriffenen) Unternehmens ankommt, denn in diesem Szenario ist es zwingend notwendig, dass der Angreifer diese (eventuelle) E-Mail erhält, damit er entsprechend reagieren kann. Dass der Empfänger glaubt, die E-Mail kommt von der altbekannten Kundenbeziehung, lässt sich dadurch erreichen, indem die Absenderadresse dieselbe ist und Fragmente älterer E-Mails integriert sind. Durch diese umfangreiche Vorarbeit ist sichergestellt, dass das angegriffene Unternehmen den geforderten Betrag auf das neue Konto überweist. Aufgrund längerer Zahlungsziele, zum Beispiel von sechs Wochen, fällt den beteiligten Unternehmen nicht rechtzeitig auf, dass sie einem Phishing-Angriff ausgesetzt waren. Daher ist die Verfolgung des Vorfalls sehr schwer bis unmöglich.

8. **Nutzung von homografischen Domänen für einen Angriff**
   Eine Ergänzung zum Angriffsvektor 7 im Business-Bereich ist, dass der Angreifer eine ähnliche Domäne, eine sogenannte homografische Domäne, eines Unternehmens registriert, um diese für einen Angriff zu nutzen. Dies ist möglich, da die homografische Domäne Zeichen enthält, die den Buchstaben der originalen Domäne ähnlich sind, etwa die Ziffer 0, die dem Buchstaben O ähnelt, oder die Buchstaben l (kleines L) und I (großes i). Beispiel für eine homografische Domäne: internet-sicherheit.de – im Original mit einem i am Anfang –, manipuliert mit einem kleingeschriebenen L, also lnternet-sicherheit.de.

   Der Angreifer kann diese Domäne für einen E-Mail-Dienst nutzen, um sich so fälschlicherweise als das eigentliche Unternehmen auszugeben, da der Empfänger die Täuschung mit hoher Wahrscheinlichkeit nicht bemerkt. Dadurch ist es dem Angreifer möglich, mit einer beliebigen falschen E-Mail-Adresse eine Kommunikationsbeziehung mit einem Mitarbeiter eines beliebigen Kunden von dem anvisierten Unternehmen aufzubauen, denn Kommunikationsinhalte sowie die richtigen Kommunikationspartner lassen sich leicht und strukturiert über Webseiten, Social-Media-Kanäle sowie Businessnetzwerke ermitteln. So ist es möglich, einen hohen Schaden anzurichten, beispielsweise bezüglich der Reputation: Aufkündigung von Verträgen oder Veränderung von Konditionen zuungunsten des Unternehmens.

9. **Die Geschichte eines erfolgreichen APT-Angriffs**
   Ein Steuerberater erhält per E-Mail die Mitteilung, dass über einen längeren Zeitraum eine Kopie seiner kompletten Mandantenkartei angefertigt wurde. In der gleichen E-Mail fordert der Angreifer den Steuerberater auf, 100.000 Euro zu zahlen, da er ansonsten den gesamten Datenbestand veröffentlichen würde. Zum Beweis, dass der Steuerberater nicht kontinuierlich zahlen müsse, übersendet der Angreifer, als Zeichen seiner Vertrauenswürdigkeit, eine Referenzliste. In dieser waren die Kontaktdaten derjenigen Steuerbüros aufgeführt, die aufgrund der Zahlung tatsächlich eine Veröffentlichung dauerhaft abgewendet haben. Interessant ist in diesem Fall auch die Frage bezüglich der Höhe des geforderten Betrags – also warum nicht 50.000 oder 250.000 Euro? Die Erklärung dafür lieferten im Weiteren die Experten, die der Steuerberater zu Hilfe holte. Diese fanden heraus, dass der Angreifer sich tief in die IT des Steuerberaters eingenistet hatte. Das ließ den Schluss zu, dass es sich nicht um Freizeit-Hacker handelte, sondern ein Profi mit einem langfristigen „Geschäftsmodell“ am Werk war, der die Lösegeldzahlung als einmalige und deshalb für die Opfer lohnenswerte Investition sieht. Zur Ermittlung der Summe hatte der Angreifer jahrelang jede digitale Bewegung beobachtet, geduldig die betriebswirtschaftliche Entwicklung des Steuerbüros verfolgt und dann zugeschlagen als das Geschäft für ihn einträglich, aber gleichzeitig für den Steuerberater wirtschaftlich verkraftbar war.

1.3 IT-Sicherheitsstrategien

Durch die steigende Digitalisierung wird das Risiko eines Schadens immer größer (siehe Bild 1.2, rote Kurve), weil dadurch nicht nur die Angriffsziele kontinuierlich lukrativer werden, sondern auch die Angriffsfläche zunehmend größer wird. Um diese Situation im Sinne der Unternehmen zu verbessern, werden grundsätzliche IT-Sicherheitsstrategien benötigt, die die IT-Sicherheitsrisiken strategisch reduzieren (siehe Bild 1.2, gestrichelte Kurve).

- **IT-Sicherheitsstrategien zur Reduzierung der Risiken**
  Die IT-Sicherheitsstrategien „Vermeiden von Angriffen“ und „Entgegenwirken von Angriffen“ helfen, den Level an verbleibenden Risiken so weit wie möglich zu verringern und zu halten. Die verbleibenden Risiken beschreiben die noch vorhandene Eintrittswahrscheinlichkeit eines Schadens, der trotz durchgeführter IT-Sicherheitsmaßnahmen zur Reduzierung der Risiken in Unternehmen auftreten kann, weil es keine hundertprozentige IT-Sicherheit gibt.
- **IT-Sicherheitsstrategien, um mit verbleibenden Risiken umzugehen**
  Da mit dem Einsatz der IT-Sicherheitsstrategien zur Reduzierung der Risiken keine hundertprozentige IT-Sicherheit erzielt werden kann, müssen weitere IT-Sicherheitsstrategien für die verbleibenden Risiken angewendet werden. Hier helfen die zwei IT-Sicherheitsstrategien „Erkennen von Angriffen“ und „Reagieren auf Angriffe“.

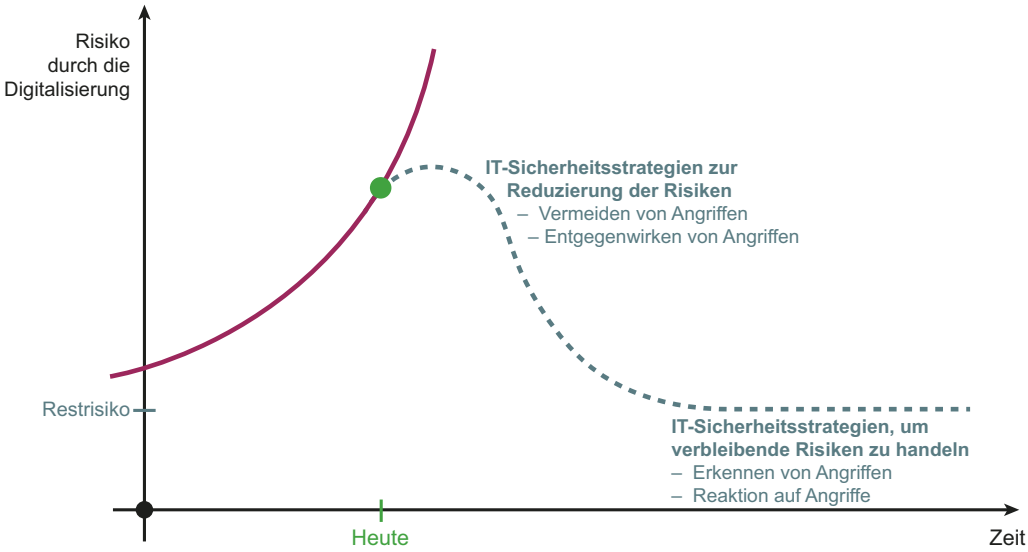


Bild 1.2 IT-Sicherheitsstrategien, um die Risiken der Digitalisierung zu managen

Im Folgenden werden die vier prinzipiellen IT-Sicherheitsstrategien beschrieben, die helfen können, IT-Sicherheitsmechanismen in strategische Ziele einzuteilen, um die Risiken der Digitalisierung zu managen. So können deren Wirkung auf Angriffe und den Schutz der Werte besser verstanden und geeignete IT-Sicherheitsstrategien ausgesucht sowie umgesetzt werden.

1.3.1 Vermeiden von Angriffen

Eine generelle IT-Sicherheitsstrategie zum Schutz der Werte eines Unternehmens ist die Idee, einen Schaden durch Angriffe zu vermeiden – die sogenannte Vermeidungsstrategie. Durch diese Vorgehensweise wird eine Reduzierung der Angriffsfläche und damit die Reduzierung der Risiken erreicht.

Im Folgenden werden unterschiedliche Prinzipien der Vermeidung erfolgreicher Angriffe aufgezeigt:

1. **Prinzip der Datensparsamkeit**
   Ein Aspekt der Vermeidungsstrategie ist das Prinzip der Datensparsamkeit, das heißt, so wenige wertvolle Daten generieren wie möglich und nur so viele wie nötig. Das Prinzip: Daten, die nicht auf IT-Systemen vorhanden sind, können nicht angegriffen werden. Daher sollten nur Daten gespeichert werden, die wirklich notwendig sind. Abgeleitete Daten, Zusammenfassungen und so weiter sollten nicht permanent erfasst, sondern bei Bedarf automatisiert neu berechnet werden.
2. **Nur sichere IT-Technologien, -Produkte und -Dienste verwenden**
   Ein weiteres Prinzip der IT-Sicherheitsstrategie Vermeiden von Angriffen ist: „Keine Technologien, Produkte und Dienste mit bekannten Schwachstellen verwenden“. Dazu müssen natürlich die entsprechenden Schwachstellen bekannt sein, damit ihnen begegnet werden kann. Beispiele von IT-Lösungen, bei denen dieses Prinzip umgesetzt werden kann, sind Browser, Betriebssysteme und Internet-Dienste. Hilfreich ist hier die Realisierung einer Zwei-Hersteller-Strategie beispielsweise bei Browsern. Diese ermöglicht, dass, wenn bei einem Browser Schwachstellen bekannt werden, unmittelbar der zweite Browser, ohne bekannte Schwachstelle, mit allen Einstellungen weiterverwendet werden kann.
3. **Fokussierung**
   Aus Studien ist bekannt, dass im Schnitt circa fünf Prozent aller vorhandenen Daten in Unternehmen besonders schützenswert sind. Welche Daten zu den fünf Prozent gehören und von daher besonders schützenswert sind, wissen die Verantwortlichen in der Regel nicht genau. Generell sind dies unter anderem Daten, die dem Unternehmen einen hohen Schaden verursachen, wenn sie in die Hände des Wettbewerbs fallen würden, also beispielsweise das geistige Eigentum des Unternehmens, Kalkulationsdaten oder Kundendaten. Aus diesem Grund ist eine Schutzbedarfsanalyse notwendig, um diese unternehmenskritischen Daten auf den vorhandenen IT-Systemen zu identifizieren und deren IT-Schutzbedürfnisse genau zu kennen. Mit dem exakten Wissen, welche Daten für das Unternehmen besonders schutzbedürftig sind, werden die Verantwortlichen in die Lage versetzt, sich auf möglichst wenige IT-Systeme zu konzentrieren und diese besonders zu schützen. So sind zum Beispiel, wie in Bild 1.3 aufgezeigt, nur auf dem IT-System in der Mitte besonders sicherheitsrelevante Werte gespeichert sind, die schlussfolgernd der IT-Schutzbedürfnisse spezifisch und besonders geschützt werden müssen.
4. **Reduzierung von IT-Möglichkeiten**
   Die Reduzierung der IT-Möglichkeiten ist ein weiteres Prinzip zur Vermeidung von Angriffen. Nicht notwendige Software vom IT-System entfernen, nicht verwendete Funktionen einer Anwendung deaktivieren oder Kommunikationsmöglichkeiten zum Beispiel mithilfe von Routern und Firewall-Systemen reduzieren, all diese Maßnahmen helfen, die potenziellen Angriffsflächen zu verringern.

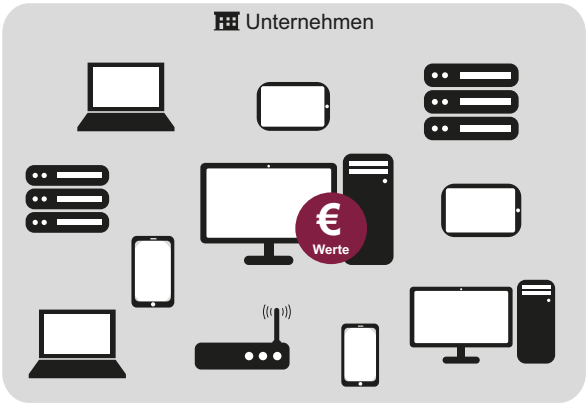


Bild 1.3 Idee der Fokussierung

5. **Sicherheitsbewusste Mitarbeiter**
   Security Awareness, also das Vorhandensein eines Sicherheitsbewusstseins, ist ein weiterer wichtiger Punkt der Vermeidungsstrategie. Sicherheitsbewusstsein setzt sich aus Wissen und einer bestimmten Einstellung der Mitarbeiter zusammen, beides dient dazu, die IT mit all ihren Werten zu schützen. Das relevante Wissen erstreckt sich hierbei über die Werte eines Unternehmens, die zu schützen sind, den Schutzbedarf dieser Werte sowie die Bedrohungen, die auf diese Werte wirken; aber auch unter anderem darüber, welche organisatorischen Regelungen einzuhalten sind, oder die richtige Nutzung von IT-Sicherheitsmaßnahmen zum Schutz der Werte. Mit der Einstellung ist gemeint, dieses Wissen zu verinnerlichen und zum Schutz des Unternehmens aktiv umzusetzen.
6. **Bewertung der Vermeidungsstrategie**
   Das Vermeiden von Angriffen ist die beste IT-Sicherheitsstrategie, um Schäden zu reduzieren. Leider ist die Vermeidungsstrategie jedoch praktisch nur eingeschränkt umsetzbar, da eine bestimmte Anzahl an IT-Systemen und Daten benötigt wird, um die gewünschten digitalen Aktivitäten umzusetzen. Das Vermeiden von Angriffen reduziert zwar die Angriffsfläche, aber für die gewollten IT-Anwendungen und -Dienste sowie die erforderliche Kommunikation etwa mit Kunden oder Dienstleistern muss eine weitere IT-Sicherheitsstrategie, wie das Entgegenwirken von Angriffen, zum Einsatz kommen, um die vorhandenen Risiken weiter zu minimieren.

1.3.2 Entgegenwirken von Angriffen

Das Entgegenwirken von Angriffen ist die meistverwendete IT-Sicherheitsstrategie, um das vorhandene Risiko zu minimieren und damit Schäden zu vermeiden. Dazu werden IT-Sicherheitsmechanismen verwendet, die eine hohe Wirkung gegen bekannte Angriffe zur Verfügung stellen. Die Stärke der Wirkung eines IT-Sicherheitsmechanismus hängt prinzipiell von unterschiedlichen Aspekten ab. Außerdem müssen die Fachkenntnisse, Gelegenheit und Ressourcen der Angreifer bei der Diskussion der Wirksamkeit betrachtet werden. Da Angriffe immer ausgefeilter, komplexer und intelligenter werden, müssen IT-Sicherheitsmechanismen kontinuierlich optimiert werden, um die notwendige Wirkung aufrechtzuhalten (Pohlmann 2019b).

IT-Sicherheitsmechanismen, die gegen spezielle Angriffe wirken, sind zum Beispiel:

- **Verschlüsselung**
  (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL/TLS ...)
  Die Verschlüsselung sorgt dafür, dass keine unerlaubten Informationen im Klartext gelesen werden können.
- **Multifaktor-Authentifikationsverfahren**
  Mithilfe einer Multifaktor-Authentifikation wird verhindert, dass unerlaubte Nutzer Zugriff auf das IT-System oder den IT-Dienst erhalten.
- **Anti-Malware-Lösungen**
  Anti-Malware-Lösungen sorgen dafür, dass illegales Aufspielen und kriminelles Nutzen von Malware auf IT-Systemen nicht umgesetzt werden können.
- **Anti-DDoS-Verfahren**
  Mithilfe von Anti-DDoS-Verfahren wird die erfolgreiche Umsetzung von DDoS-Angriffen verhindert.
- **Signaturverfahren**
  Die Nutzung von Signaturverfahren ermöglicht es zu verhindern, dass digitale Handlungen geleugnet werden können.
- **Hardware-Sicherheitsmodule**
  Mithilfe von Hardware-Sicherheitsmodulen (Smartcards, TPMs, High-Level Security Modules) wird der unerlaubte Zugriff auf Sicherheitsinformationen und die unerlaubte Nutzung von Kryptografie-Funktionen mit Schlüssel unterbunden.

Da Angreifer zunehmend schneller mehr, aber auch neue Angriffsmethoden entwickeln und umsetzen sowie die potenziellen Ressourcen für Angriffe immer leistungsstärker werden, müssen die IT-Sicherheitsmechanismen, die diese abwehren sollen, kontinuierlich und zeitnah verbessert werden.

Bewertung des Entgegenwirkens

Die IT-Sicherheitsstrategien „Entgegenwirken von Angriffen“ ist eine naheliegende Vorgehensweise, digitale Werte angemessen zu schützen. IT-Sicherheitsmechanismen sollten dem Stand der Technik genügen, um mittels einer hohen Wirkung einen angemessenen IT-Sicherheitslevel zu erzielen. Momentan stehen nicht genügend, beziehungsweise nicht schnell genug, wirkungsvolle IT-Sicherheitstechnologien, -lösungen und -produkte gegen die immer intelligenteren Angriffe zur Verfügung oder werden nicht angemessen und vollumfänglich genug eingesetzt. Das dokumentiert die Vielzahl der professionell durchgeführten und daher erfolgreichen Angriffe. Da es keine hundertprozentige IT-Sicherheit gibt und somit immer ein Restrisiko bleibt, muss mit weiteren IT-Sicherheitsstrategien gegen die verbleibenden Risiken vorgegangen werden.

1.3.3 Erkennen von Angriffen

Wenn Angriffen mithilfe von IT-Sicherheitsmechanismen nicht angemessen oder vollständig entgegengewirkt werden oder eine Vermeidung die Angriffsfläche nicht ausreichend redu-

zieren kann, bleibt noch die Strategie, Angriffe erkennen und zu versuchen, den Schaden so schnell wie möglich zu minimieren.

In diesem Bereich spielen prinzipiell Frühwarn- und Lagebildsysteme eine besondere Rolle, da sie Lagebilder erstellen und Warnungen erzeugen, wenn die Bedrohungslage ungewöhnlich groß ist und gerade umgesetzte Angriffe erkannt werden.

Hier ist die Idee, dass in einem definierten Bereich (etwa IT- und Kommunikationsinfrastruktur, Endgeräte oder Server) nach Angriffssignaturen oder Anomalien gesucht wird. Bei Erkennen eines Angriffs werden die Hintergründe analysiert und adäquate Gegenmaßnahmen eingeleitet, um weitere Schäden zu verhindern oder zumindest zu reduzieren.

Bewertung des Erkennens

Die IT-Sicherheitsstrategie „Erkennen von Angriffen“ ist sehr hilfreich, hat aber definierte Grenzen, da es keine hundertprozentige Erkennungsrate gibt. Aus diesem Grund wird es in der Zukunft wichtig, auf diesem Gebiet durch mehr und bessere Sensoren sowie einen unternehmensübergreifenden Austausch viele sicherheitsrelevante Informationen verfügbar zu machen, aber auch durch den Einsatz von KI-Systemen die Erkennungsraten so weit wie möglich zu steigern. Zudem ist es wichtig, schnell und angemessen zu reagieren. Daher müssen die IT-Sicherheitsstrategien „Erkennen von Angriffen“ und „Reaktion auf Angriffe“ zusammen betrachtet werden.

1.3.4 Reaktion auf Angriffe

Wenn Angriffe erkannt werden, gilt es, so schnell wie möglich mit passenden Aktionen zu reagieren.

1. **Automatisierte Reaktion**
   Wenn ein Angriff erkannt wird, können zum Beispiel sofort und (halb-)automatisiert Firewall-Regeln oder E-Mail-Server-Regel so reduziert werden, dass nur noch die wichtigen Prozesse für das Unternehmen aufrechterhalten bleiben. Durch die Reduktion der Angriffsfläche lassen sich die potenziellen Schäden so gut wie möglich verringern.
2. **Definition von Befugnissen, Informationsflüssen, Entscheidungsprozessen und Kommunikationsstrategien**
   Für das gesamte Abschalten der Internetverbindung oder die Notwendigkeit des Herunterfahrens vieler IT-Systeme, etwa bei großen Ransomware-Angriffen, müssen in der Regel die Verantwortlichkeiten sowie die damit verbundenen Rechte definiert sein. Um schneller handeln zu können, ist es notwendig, die erforderlichen Informationsflüsse und Reaktionsmöglichkeiten exakt ausgearbeitet und vereinbart zu haben. Wichtig für ein angegriffenes Unternehmen sind somit ein sehr kurzer Entscheidungsprozess, effiziente Pfade für die Informationsverteilung sowie klar definierte Befugnisse der Akteure, um im Notfall schnell und verantwortungsvoll reagieren zu können. Zudem muss die Kommunikationsstrategie bezüglich Mitarbeitern, Kunden, Regulierungsbehörden und Medien sorgfältig geplant sein, um einen hohen Imageschaden zu vermeiden.
3. **Digitale Forensik**
   Grundsätzlich ist die digitale Forensik eine streng methodisch vorgenommene Datenanalyse auf Datenträgern und von IT-Systemen und Kommunikationsnetzwerken zur

Aufklärung von Vorfällen durch forensische Sicherung von digitalen Beweisen sowie zur Analyse der digitalen Beweismittel. In Sinne einer Reaktion lässt sich durch die Analyse eines Angriffes gewährleisten, dass eventuell vorhandene Lücken geschlossen, vorhandene IT-Sicherheitsmaßnahmen optimiert oder weitere integriert werden, damit das Unternehmen zukünftig besser geschützt ist.

4. **Notfallplanung**
   Wichtig ist auch, dass es bereits getestete Reaktionskonzepte (Notfallplanungen) gibt, in denen die richtige Vorgehensweise im Krisenfall definiert ist, aber auch welche Personen die Rechte haben, die entsprechenden Reaktionen auszulösen. Besonders relevant ist dabei, alle definierten Abläufe in ausreichendem Maße mit allen Mitarbeitern zu trainieren, damit im Ernstfall die adäquaten Reaktionen schnell und erfolgreich umgesetzt werden können.

Bewertung der Reaktion

Die IT-Sicherheitsstrategie „Reagieren auf Angriffe“ hilft, Schäden zu vermeiden oder zu minimieren. Es kann jedoch nur reagiert werden, wenn Angriffe erkannt werden. Notwendig ist, die Reaktionskonzepte vorher definiert sowie getestet zu haben, um im Ernstfall schnell und wirkungsvoll reagieren zu können.

1.4 Umsetzung eines angemessenen IT-Sicherheitslevels

Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme, um ein gesetzliches IT-Sicherheitsziel zu erreichen (TeleTrusT 2021).

Das Technologie- und IT-Sicherheitsniveau „Stand der Technik“ ist angesiedelt zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung“ und dem bewährten Technologiestand „allgemein anerkannte Regeln der Technik“ (siehe Bild 1.4).

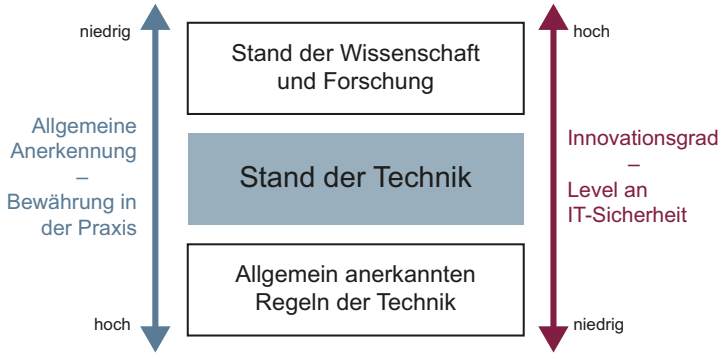


Bild 1.4 Angemessener IT-Sicherheitslevel durch den Stand der Technik

Stand der Technik Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme, um das entsprechende IT-Sicherheitsziel zu erreichen. IT-Sicherheitslösungen, die dem Stand der Technik genügen, bieten einen angemessenen Level an IT-Sicherheit für den aktuellen Grad der Digitalisierung.

Stand der Wissenschaft und Forschung Technische IT-Sicherheitsmaßnahmen im Stadium „Stand der Wissenschaft und Forschung" haben einen hohen Innovationsgrad sowie IT-Sicherheitslevel, sind sehr dynamisch in ihrer Entwicklung und gehen mit der Erreichung der Marktreife (oder zumindest mit ihrer Markteinführung) in das Stadium „Stand der Technik" über. Dort nimmt die Dynamik ab, etwa durch die Standardisierung der Prozesse.

Allgemein anerkannte Regeln der Technik Auch technische Maßnahmen im Stadium „allgemein anerkannte Regeln der Technik" sind am Markt verfügbar. Ihr Innovationsgrad ist geringer, sie haben sich jedoch in der Praxis bewährt und werden oftmals in den entsprechenden Standards beschrieben. Jedoch ist im Stadium „allgemein anerkannte Regeln der Technik" das Entgegenwirken von innovativen Angreifern nicht mehr so wirkungsvoll. Einige Beispiele hierfür sind: Die Nutzung von Passwörtern für die Authentifikation oder die Nutzung von nicht mehr sicheren Kryptografie-Algorithmen etwa bei Signaturen, Authentifikation oder Verschlüsselung. Aber ebenso Anti-Malware-Lösungen, die überwiegend auf der Basis der Signaturerkennung funktionieren, oder Firewall-Systeme, die keine sicheren Regeln nutzen oder umsetzen können, gehören – in Anbetracht der aktuell sehr dynamischen Digitalisierung – in diese nicht mehr angemessene Kategorie.

Verfügbare Bestleistung einer IT-Sicherheitsmaßnahme Unter anderem im „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" und in der „EU-Datenschutz-Grundverordnung (DSGVO)" ist vorgeschrieben, dass sich die IT-Sicherheitsmaßnahmen an dem Stand der Technik orientieren. Daher kommt diesem eine hohe Bedeutung zu, auch aus der Sicht der Haftung im Schadensfall.

1.5 IT-Sicherheitsmechanismen, die gegen Angriffe wirken

Im Folgenden werden einige IT-Sicherheitsmechanismen beschrieben, die gegen Angriffe wirken (Pohlmann 2019b).

1. Verschlüsselung

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Nutzer dennoch verwendbar bleiben, muss es diesem jedoch möglich sein, durch Anwendung einer inversen Transformation daraus wieder die Originaldaten zu generieren (siehe Bild 1.5).

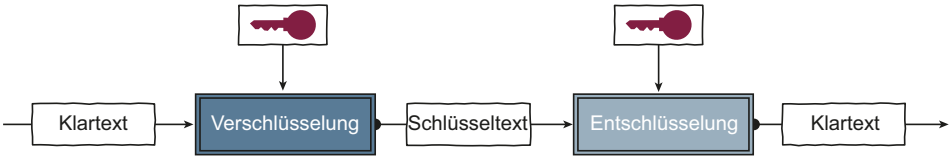


Bild 1.5 Verschlüsselung

Die Verschlüsselung wird zur Übertragung und Speicherung vertraulicher Daten verwendet, die nur dem legitimen Empfänger/Besitzer zugänglich sein sollen. Anwendungsfälle sind unter anderem: Datei-, Festplatten-, E-Mail-Verschlüsselung, IPSec-Verschlüsselungssysteme, SSL/TLS-Absicherung.

Im Bereich Verschlüsselung gibt es bei den meisten Unternehmen noch einen großen Nachholbedarf. Aus diesem Grund sollte ein Konzept erarbeitet werden, wie die Verschlüsselung und eine dazu notwendige IT-Sicherheitsinfrastruktur umgesetzt werden können.

Kryptoagilität Beim Einsatz von Verschlüsslungssystemen sollte auf die Kryptoagilität geachtet werden. Die Kryptoagilität ermöglicht es einem IT-Sicherheitssystem, auf ein alternatives neues Kryptosystem (unter anderem bezüglich kryptografischer Algorithmen, Schlüssellänge, Schlüsselgenerierungsverfahren, technischer Umsetzung) sehr schnell umzuschalten, ohne wesentliche Änderungen am IT-System oder IT-Sicherheitssystem (wie Systemarchitekturen oder Protokolle) vorzunehmen. Damit kann garantiert werden, dass ein IT-Sicherheitssystem kontinuierlich ein Mindestniveau an IT-Sicherheit halten kann.

In Bezug auf die wichtigsten Angriffsvektoren, wie Man-in-the-Middle (MITM), hilft Verschlüsselung, diese zu verhindern.

2. Authentifikationsverfahren

Authentifikation bezeichnet einen Prozess, in dem überprüft wird, ob der Nutzer (Mitarbeiter, Kunde und andere Personen), der gerade auf ein IT-System zugreifen möchte, echt ist. Bei der Authentifikation wird mit der Erbringung eines oder mehrerer Nachweise bestätigt, ob es sich um den Nutzer mit der angegebenen und behaupteten digitalen Identität handelt (siehe Bild 1.6).

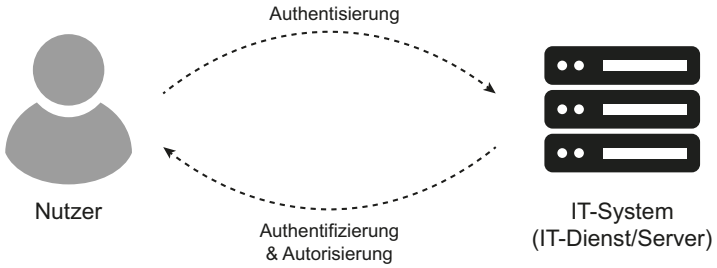


Bild 1.6 Authentifikation, Authentisierung & Autorisierung

- **Authentisierung (Sichtweise Nutzer):**
  Der Nutzer authentisiert sich gegenüber einem IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud), indem er einen Nachweis über seine digitale Identität erbringt, zum Beispiel den Nutzernamen.

- **Authentifizierung (Sichtweise IT-System):**
  Das IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud) überprüft den Nachweis, um die Echtheit der digitalen Identität eines Nutzers im Rahmen der Authentifizierung festzustellen.
- **Autorisierung (Sichtweise IT-System):**
  Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud) dem Nutzer definierte Rechte einräumen.

Klassen von Authentifizierungsverfahren Es werden verschiedene Klassen von Authentifizierungsverfahren unterschieden, bei denen unterschiedliche Aspekte eine Rolle spielen und diverse Charakteristika berücksichtigt werden müssen.

1. *Wissen:* Bei dieser Klasse von Authentifizierungsverfahren wird über einen Nachweis der Kenntnis von Wissen die Echtheit eines Nutzers überprüft. Beispiele von Wissen sind: Passwort, PIN oder Antwort auf eine bestimmte Frage (Sicherheitsfrage).
2. *Besitz:* Verwendung eines Besitztums für das Authentifizierungsverfahren ist eine weitere Klasse. Beispiele für Besitz sind: Neuer Personalausweis, SIM-Karte im Smartphone und weitere Hardware-Sicherheitsmodule, wie Smartcard oder USB-Stick. In der Regel wird in diesem Bereich der Besitz von geheimen Schlüsseln mithilfe von Challenge-Response-Verfahren nachgewiesen, die in den Hardware-Sicherheitsmodulen sicher gespeichert sind.
3. *Sein:* Bei dieser Klasse von Authentifizierungsverfahren muss der Nutzer gegenwärtig sein. Beispiele von Sein sind: Biometrische Merkmale wie Fingerabdruck, Gesichtsgeometrie oder Iris.
4. *Weitere unterstützende Faktoren (Reputation, Standort, Zeit, Technologie):* Es können noch weitere unterstützende Faktoren für die Beurteilung der Echtheit des Nutzers herangezogen werden. Beispiele sind: Vergangene Transaktionen des Nutzers (Reputation), verwendete Endgeräte und Software des Nutzers (Technologie), Standort und Zeit des Authentisierungsprozesses.

Multifaktor-Authentifizierung Stand der Technik heute ist die Multifaktor-Authentifizierung. Mit einer Multifaktor-Authentifizierung (MFA) kann flexibel agiert und mit einer höheren Vertrauenswürdigkeit authentifiziert werden. Ein Beispiel für eine Multifaktor-Authentifizierung ist: Es wird als Basis eine digitale Signatur einer Zufallszahl mithilfe eines Hardware-Sicherheitsmoduls (etwa Smartcard, USB-Stick oder Sicherheitsmodul im Smartphone) umgesetzt, das mit einem Passwort oder PIN aktiviert werden muss. Um den Nutzerbezug zu verstärken, muss der Nutzer noch mithilfe eines Fingerabdrucks oder der Gesichtserkennung seine Gegenwärtigkeit zusätzlich verifizieren lassen.

Konzept der risikobasierten und adaptiven Authentifizierung Die adaptive Authentifizierung entscheidet auf der Basis der Vertrauenswürdigkeit des zugreifenden Nutzers, der Kritikalität der konkreten Anwendung/Aktion und der Rahmenbedingungen des aktuellen Zugriffs, welche Klassen von Authentifikationsverfahren zum Einsatz kommen sollen. Dieser risikoorientierte Ansatz erhöht das allgemeine Sicherheitsniveau und vermindert die Anzahl nicht notwendiger starker Authentifizierungen. Es wird das Optimum zwischen Sicherheit und Komfort angestrebt. Umgesetzt werden Konzepte der adaptiven Authentifizierung mithilfe von Mehrfaktor-Authentifizierung (MFA), die flexibel, in Abhängigkeit vom gerade notwendigen Sicherheitsniveau oder von Risiken, die passenden Klassen von Authentifikationsverfahren auswählt.

3. Firewall-Systeme

Ein Firewall-System sichert und kontrolliert den Übergang von einem zu schützenden Netz zu einem unsicheren Netz, wie dem öffentlichen Internet. Ein Firewall-System lässt erlaubte Kommunikation durch (grün) und blockiert nicht gewünschte (orange, siehe Bild 1.7). Die grundsätzliche Idee ist, zwischen verbundenen Netzen durch Regulierung und Kontrolle Sicherheitsdomänen mit unterschiedlichem Schutzbedarf zu schaffen. Durch eine Reduzierung von Kommunikationsmöglichkeiten über ein Firewall-System werden die Angriffsfläche und dadurch das Risikopotenzial minimiert.

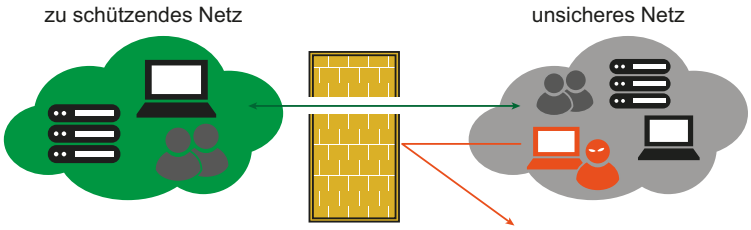


Bild 1.7 Firewall-System

Unternehmen müssen auswerten sowie entscheiden, welche Protokolle und Methoden sie über das Firewall-System zu welchen Zeiten und welchen Mitarbeitern möglich machen wollen, damit die notwendigen Aufgabenstellungen umgesetzt werden können. Diese müssen aktiv eingestellt und regelmäßig überwacht werden, damit die Reduzierung der Möglichkeiten und damit der Angriffsfläche immer optimal umgesetzt werden kann. Außerdem sollten die eingesetzten Firewall-Systeme eine hohe Qualität haben, damit durch eine ausreichende Tiefe der Analyse gewährleistet ist, dass Angriffe erkannt und darauf reagiert werden kann.

4. Zero Trust-Konzept

Das Zero Trust-Modell ist ein IT-Sicherheitskonzept, das auf dem Prinzip basiert, weder dem IT-System noch einem Nutzer, IT-Dienst, Netzwerk zu vertrauen und ebenfalls keiner IT-Anwendung, IT-Infrastruktur – allgemein IT-Entität – innerhalb oder außerhalb des eigenen Netzwerks (Zero Trust). Das bedeutet, sämtliche Kommunikation zwischen den IT-Entitäten wird kontrolliert sowie auf Angriffe untersucht, und alle IT-Entitäten müssen sich authentifizieren.

Herkömmliche IT-Sicherheitskonzepte wie die Perimeter-Sicherheit stufen lediglich externe Kommunikation als gefährlich ein und vertrauen sämtlichen internen IT-Entitäten. Diese IT-Sicherheitskonzepte haben den Nachteil, dass, sobald jemand in das Unternehmensnetz eingedrungen ist oder von innen angreift, kaum noch IT-Sicherheitsmaßnahmen zur Verfügung stehen, um gegen diese Angriffe vorgehen zu können.

Daher hat das Zero Trust-Konzept beachtliche Auswirkungen auf die IT-Sicherheitsarchitektur eines Unternehmens, weil alle IT-Entitäten mit zusätzlichen IT-Sicherheitsmaßnahmen ausgestattet werden müssen anstatt nur die Sicherung der Netzwerkgrenzen. Durch die zusätzliche Umsetzung der minimalen Rechte auf allen IT-Entitäten werden die Möglichkeiten für Angreifer stark eingeschränkt und somit ein höherer Level an IT-Sicherheit erreicht. Mit dem Zero Trust-Konzept (vgl. Bild 1.8) werden zum Beispiel mehrstufige Angriffe/Advanced Persistent Threats (APT) verhindert.

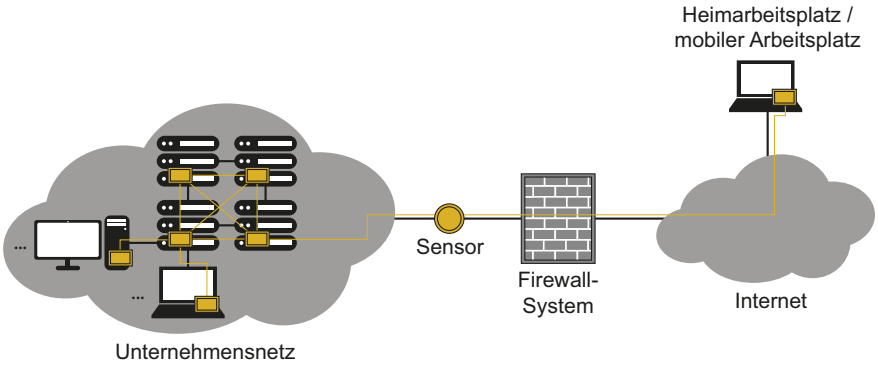


Bild 1.8 Zero Trust-Konzept

5. Blockchain-Technologie (Vertrauensdienst)

Mithilfe der Blockchain-Technologien werden zusätzlich zu PKIs Vertrauensdienste angeboten, die neue Möglichkeiten im Rahmen der Digitalisierung für mehr Sicherheit und Vertrauenswürdigkeit anbieten. Insbesondere im Bereich der Verifizierung etwa von Bescheinigungen, Berechtigungen, Beglaubigungen oder Qualifikationen wird es in der nahen Zukunft viele Anwendungen geben, die die Digitalisierung von Unternehmensprozessen vertrauenswürdig und sicher möglich machen. Ein weiterer wichtiger Anwendungsbereich der Blockchain-Technologie ist eine vertrauenswürdige und automatisierte Zusammenarbeit zwischen verschiedenen Organisationen, die Prozesse sehr viel schneller effizienter und kostengünstiger umsetzen lässt.

Unterschiedliche Sichtweisen auf die Blockchain-Technologie Die verschiedenen Disziplinen können die Blockchain-Technologie aus sehr unterschiedlichen Blickwinkeln betrachten und bewerten (siehe Bild 1.9).

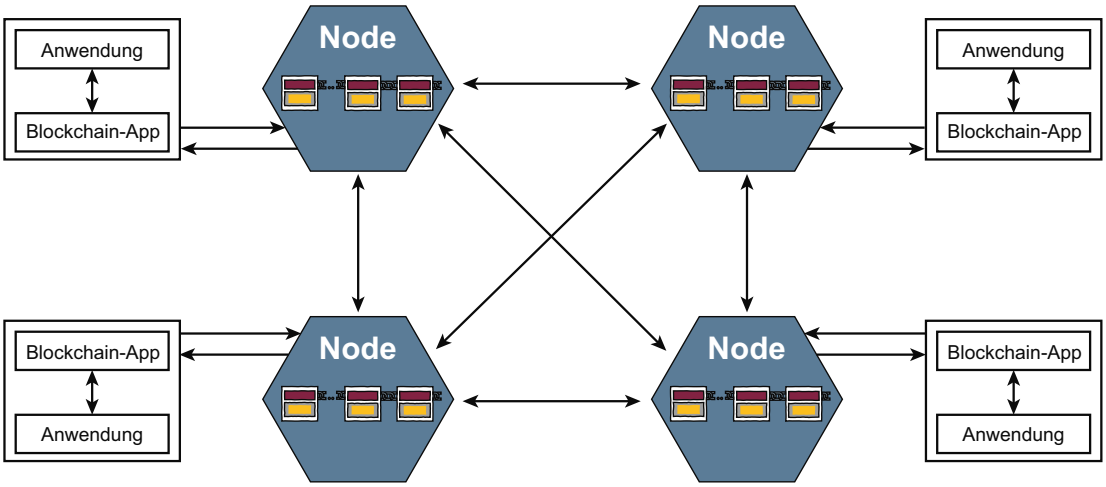


Bild 1.9 Blockchain-Technologien

Für einen Informatiker produziert die Blockchain-Technologie eine einfache Datenstruktur, die Blockchain, die Daten als Transaktionen in einzelnen Blöcken verkettet und in einem verteilten Peer-to-Peer-Netz redundant verwaltet. Die Alternative wäre eine konventionelle Datenbank, die kontinuierlich von allen Teilnehmern repliziert wird.

Für die IT-Sicherheitsexperten hat die Blockchain-Technologie den Vorteil, dass die Daten als Transaktionen in den einzelnen Blöcken manipulationssicher gespeichert werden können, das heißt, die Teilnehmer der Blockchain sind in der Lage, die Echtheit, den Ursprung sowie die Unversehrtheit der gespeicherten Daten (Transaktionen) zu überprüfen. Die Alternative wäre hier zum Beispiel ein PKI-System als zentraler Vertrauensdienstanbieter.

Für den Anwendungsdesigner bedeutet die Nutzung der Blockchain-Technologie eine vertrauenswürdige Zusammenarbeit zwischen verschiedenen Organisationen, ohne die Einbindung einer zentralen Instanz etwa eines PKI-Systems oder Notars. Die Alternative könnte hier ein kostenintensiver Treuhänder sein, der die Zusammenarbeit und Eigentumsübertragung zwischen den verschiedenen Organisationen verwaltet und verifiziert.

Da die Blockchain-Technologie dies automatisiert macht, werden durch die vertrauenswürdige Zusammenarbeit die Prozesse sehr viel schneller und effizienter. Das macht einen Vertrauensdienst auf der Basis einer Blockchain-Technologie preisgünstiger, und das Vertrauen verteilt sich auf die Node-Betreiber.

6. Trusted Computing (moderne IT-Sicherheitsarchitektur)

Trusted Computing ist eine IT-Sicherheits- und Vertrauenswürdigkeitstechnologie. Mithilfe von Trusted Computing stehen moderne und intelligente IT-Sicherheitsarchitekturen, -konzepte und -funktionen zur Verfügung, die es ermöglichen, IT-Systeme mit einer höheren Robustheit sowie einem höheren IT-Sicherheitslevel umzusetzen. Der besondere Schwerpunkt liegt dabei auf der Verifikation der Integrität eines IT-Systems, wodurch einige große IT-Sicherheitsprobleme wie Softwarefehler und Malware in ihrer Wirkung deutlich eingeschränkt werden können.

Trusted Computing basiert auf einem Hardware-Sicherheitsmodul und arbeitet mit einem kleinen Sicherheitskern (sichere Betriebssysteme) und Virtualisierung (siehe Bild 1.10). Auf dieser Basis können mit Trusted Computing Funktionen in dem Trusted Software-Layer Software- und Hardware-Konfigurationen messbar im Sinne der Vertrauenswürdigkeit machen und mit einer starken Isolation Anwendungen mit ihren Daten separiert werden. Der IT-Sicherheitsaspekt der Modularisierung ist eine Möglichkeit, Anwendungen, die zusammengehören, in einer virtuellen Maschine laufen zu lassen, und Anwendungen, die getrennt sein sollten, in unterschiedlichen virtuellen Maschinen zu positionieren. Dieser IT-Sicherheitsaspekt offeriert einen interessanten Gestaltungsspielraum, mit dem sich ein sehr hoher Grad an IT-Sicherheit erzielen lässt, weil für verschiedene IT-Sicherheitslevel von Anwendungen verschiedene virtuelle Maschinen genutzt werden können. Beispiel: Das Office-Paket läuft in einer virtuellen Maschine, das Design-Paket für die Business-Anwendung in einer anderen, und der Browser hat eine separate virtuelle Maschine.

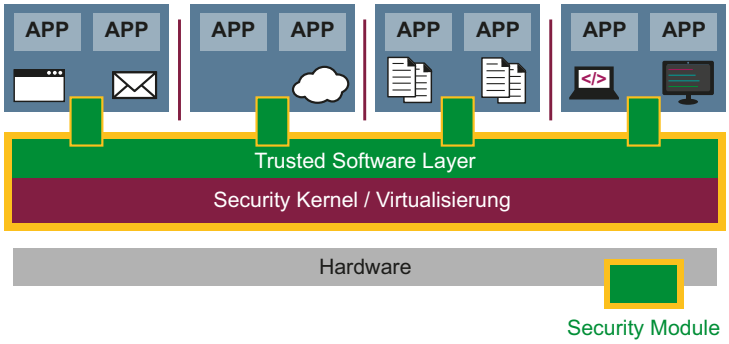


Bild 1.10 Trusted Computing (moderne IT-Sicherheitsarchitektur)

7. Anti-Malware-Lösungen

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde usw. Angreifer (kriminelle Organisationen, politisch und wirtschaftlich orientierte Spione, Terroristen, Strafverfolger usw.) nutzen Softwareschwachstellen und menschliche Unzulänglichkeiten aus, um Malware auf IT-Systemen zu installieren. Über E-Mail-Anhänge oder unsichere Webseiten mithilfe von sogenannten Drive-by-Downloads wird Malware hauptsächlich in IT-Endgeräte unbemerkt eingeschleust. Ein Botnetz ist eine Gruppe von IT-Endgeräten, die unter zentraler Kontrolle eines Angreifers stehen und von ihm für Angriffe genutzt werden.

Ein Angreifer kann die Malware aus der „Ferne“ mit verschiedenen Schadfunktionen bespielen. Dadurch können Angreifer unterschiedliche Arten von Angriffen durchführen, wie Informationen von IT-Systemen mithilfe von Keyloggern und Trojanern auslesen, IT-Systeme für die Spam-Verteilung und DDoS-Angriffe nutzen sowie mit Ransomware Daten verschlüsseln und Lösegeld für die Entschlüsselung verlangen. Bei Ransomware verschlüsseln die Angreifer mithilfe der Malware wichtige Daten auf dem IT-System und verlangen vom Besitzer zum Beispiel einige Tausend Euro für die Herausgabe des Schüssels, mit dem die Daten wieder entschlüsselt werden können.

Anti-Malware-Lösungen haben das Ziel, Malware zu erkennen und damit entsprechende Angriffe zu verhindern.

Herkömmliche Anti-Malware-Lösungen haben heute bei Massenangriffen mit 75 bis 95 Prozent eine zu schwache Erkennungsrate. Bei gezielten direkten Angriffen auf ein ausgewähltes IT-System liegt die Erkennungsrate im Schnitt sogar nur bei 27 Prozent. Hintergrund dieser Entwicklung ist, dass signaturbasierte Erkennungen bei gezielten Angriffen ihre Wirkung verlieren, da keine Signaturen mehr erstellt und verteilt werden, aber auch weil Signaturen bei einem direkten Angriff individuell sind (siehe Bild 1.11).

Moderne Anti-Malware-Lösungen arbeiten mit intelligenten Sensoren in den IT-Endpunkten wie Smartphone, Notebooks oder IoT-Geräten, die ihre Daten an ein zentrales System in der Cloud senden. Im zentralen System werden die Daten mithilfe von KI-Systemen analysiert, eine globale Sichtweise aufgebaut, mit Threat Intelligent Informationen abgeglichen und dann eine geeignete Reaktion umgesetzt, falls ein Angriff erkannt wird. Eine passende Reaktion kann zum Beispiel die Isolierung eines oder mehrerer Notebooks sein. Mit modernen Anti-Malware-Lösungen können die am häufigsten verwendeten Angriffsvektoren verhindert werden.

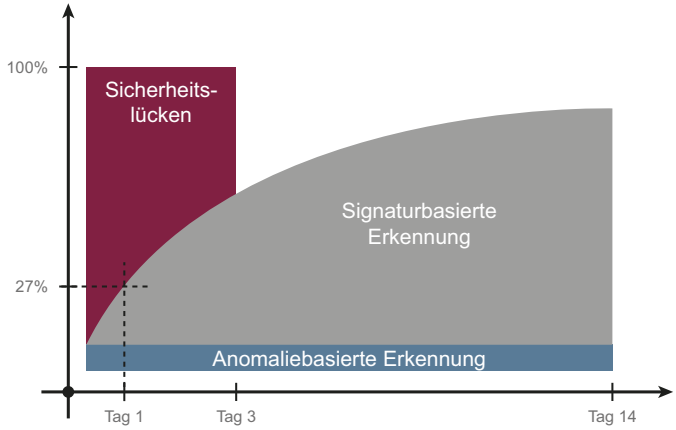


Bild 1.11 Anti-Malware-Lösungen

8. IT-Sicherheit-Frühwarn- und Lagebildsystem

Alle Organisationen sind zunehmend von der Verfügbarkeit der eigenen und öffentlichen IT-Infrastruktur im Cyber-Raum abhängig. Ausfälle und Störungen der weltweiten Kommunikation, der angebotenen Dienste und digitalen Geschäftsprozesse können zu unkalkulierbaren Schäden führen. Ein IT-Sicherheit-Frühwarn- und Lagebildsystem hilft, die IT-Sicherheitslage aktuell aufzuzeigen, möglichst früh Angriffspotenziale sowie reale Angriffe zu erkennen, und dient dazu, rechtzeitig Warnhinweise zu geben, damit Schäden auf IT-Systemen und IT-Infrastruktur minimiert oder verhindert werden können. Ein IT-Sicherheit-Frühwarn- und Lagebildsystem hilft, Sicherheit und Vertrauenswürdigkeit von IT-Systemen und IT-Infrastruktur nachhaltig zu erhöhen und diese widerstandsfähiger zu gestalten.

Aus diesem Grund sollten Unternehmen eine Vielzahl von Sensoren einsetzen, damit möglichst viele digitalen Aktivitäten beobachtet werden können, um einen kontinuierlichen Status der gesamten IT des Unternehmens zu haben, um die Angriffspotenziale und reale Angriffe identifizieren zu können (siehe Bild 1.12).

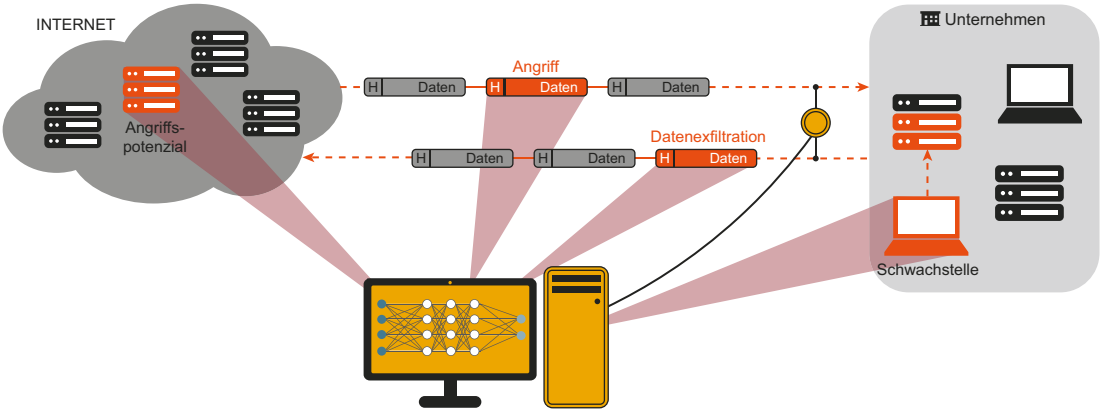


Bild 1.12 IT-Sicherheit-Frühwarn- und Lagebildsystem

Weitere IT-Sicherheitsmechanismen sind zum Beispiel, Anti-DDoS-Verfahren, Signaturverfahren, Enterprise Identity and Access Management, E-Mail-Sicherheit usw. (Pohlmann 2019b)

1.6 Die wichtigsten Punkte in Kürze

- Die IT-Sicherheitsrisiken eines Unternehmens steigen mit dem Grad der Digitalisierung.
- IT-Systeme müssen in Zukunft mit einer möglichst umfassenden Angriffsresilienz ausgestattet werden. Das bedeutet, die notwendige IT, die im Rahmen der Digitalisierung sowieso innoviert wird, mit IT-Sicherheitsarchitekturen und -mechanismen im Sinne Security by Design/Security by Default auszustatten, die eine deutlich höhere Wirkung gegen Angriffe aufzeigen, optimalerweise automatisch funktionieren und eine hohe Qualität besitzen.
- Die Verantwortlichen für die IT-Sicherheit in Unternehmen sollten verschiedene IT-Sicherheitsstrategien umsetzen, um das Risiko von Schäden zu reduzieren.
- Die IT-Sicherheitsstrategie „Vermeiden von Angriffen“ hilft, das Schadenspotenzial zu reduzieren, hat jedoch Grenzen in der Umsetzung und Wirkung, weil die geforderten digitalen Aktivitäten ohne Einschränkung zur Verfügung stehen müssen.
- Die IT-Sicherheitsstrategie „Entgegenwirken von Angriffen“ ist sehr naheliegend und erfolgsversprechend. Wichtig ist jedoch, dass hier IT-Sicherheitslösungen und -Maßnahmen gemäß Stand der Technik eingesetzt werden, um einen hohen Wirkungsgrad gegen intelligente Angriffe zu erreichen.
- Die verbleibenden Risiken sollten mit der IT-Sicherheitsstrategie „Erkennen von Angriffen“, also durch das Identifizieren von aktuell stattfindenden Angriffen, unter Kontrolle gebracht werden.
- Mit der IT-Sicherheitsstrategie „Reaktion auf Angriffe“ kann ein Schaden entweder vollständig verhindert oder zumindest reduziert werden.
- Im Prinzip sind alle Voraussetzungen gegeben, um den Kampf gegen professionalisierte Angreifer oder Cyberkriminelle zu gewinnen. Wichtig ist hierbei auch, dies mit allen Stakeholdern (Anbieter- und Anwenderwirtschaft, Wissenschaft, Politik und Staat) gemeinsam umzusetzen, um aufgrund der erzeugten Synergien noch effizienter vorgehen zu können.
- Selbstverständlich wird es ohne IT-Sicherheit keine nachhaltige Digitalisierung geben können – daher steht der Bedarf hinsichtlich des weiteren Fortschritts und nachweislicher Erfolge in der IT-Sicherheit vollkommen außer Frage.

1.7 Literatur

Pohlmann, Norbert: *Wertschöpfung der Digitalisierung sichern – Vier Cybersicherheitsstrategien für den erfolgreichen Wandel in der IT*. In: IT-Sicherheit – Mittelstandsmagazin für Informationssicherheit und Datenschutz, DATAKONTEXT-Fachverlag, 1/2020, S. 60–65

Pohlmann, Norbert: *Künstliche Intelligenz und Cybersicherheit – Unausgegoren, aber notwendig*. In: IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 1/2019, S. 56–63

Pohlmann, Norbert: *Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer-Vieweg Verlag, Wiesbaden 2019

Bundesverband IT-Sicherheit – TeleTrusT: *Handreichung zum Stand der Technik technischer und organisatorischer Maßnahmen*, Berlin 2021 *https://www.teletrust.de/publikationen/broschueren/stand-der-technik/*

Herausgeber, Autorin und Autoren

Die Herausgeber

Prof. Dr. Michael Lang
ist Professor für Wirtschaftsinformatik an der Technischen Hochschule Nürnberg. Seine Forschungs- und Lehrschwerpunkte liegen in den Bereichen Digitale Transformation, Business Analytics und IT-Management. Zu diesen Themen hat er zudem 25 Fachbücher veröffentlicht. Vor seiner aktuellen Tätigkeit war Herr Prof. Dr. Lang in diversen Fach- und Führungspositionen beschäftigt und zugleich Lehrbeauftragter für Projekt- und IT-Management an verschiedenen Hochschulen. Zuletzt war er als Führungskraft bei einem der größten IT-Dienstleistungsunternehmen Europas tätig.

Prof. Dr. Hans Löhr
ist Professor für Informatik mit Schwerpunkt in den Bereichen IT-Sicherheit und Kryptografie an der Technischen Hochschule Nürnberg Georg Simon Ohm. Zuvor wurde er am Horst-Görtz-Institut für IT-Sicherheit der Ruhr-Universität Bochum promoviert. Daraufhin war er langjährig in der zentralen Konzernforschung der Robert Bosch GmbH und danach bei der SUSE Software Solutions Germany GmbH tätig. Dabei beschäftigte er sich unter anderem mit innovativen Sicherheitslösungen und -konzepten für zukünftige Produkte, Software Security und der Entwicklung und Zertifizierung von sicheren Produkten.

Autorin und Autoren

Daniel Angermeier
ist stellvertretender Abteilungsleiter am Fraunhofer AISEC. Als Diplom-Informatiker beschäftigt er sich seit einem Jahrzehnt mit Fragestellungen der sicheren Systementwicklung in Kunden- und Forschungsprojekten.

Martin Braun
ist Geschäftsführender Gesellschafter der CyberSecurity manufaktur GmbH und zertifizierter KRITIS- und ISO 27001-Auditor. Seine Wurzeln hat er im Bereich internationale Rechenzentrums- und Infrastrukturleitung, bevor er 2011 den Schritt in die Selbstständigkeit wagte. IT-Security begleitet ihn seit dem Jahr 2000 und berät seither Inhaber und Geschäftsführer generalistisch in den Themen CyberSecurity, Security-Strategie und Riskmanagement. Er ist ein Verfechter der Reifegradmethodik zur Verbesserung des unternehmensweiten Security-Levels.

martin.braun@cybersecurity-manufaktur.de

Diplom-Ingenieur Hans Höfken
ist Geschäftsführer bei @-yet Industrial IT Security. Er studierte Elektrotechnik und arbeitete als Automatisierer in der Papierindustrie, ehe er zur IT-Sicherheit kam. Hier beschäftigt er sich seit über zehn Jahren mit IT-Forensik, Informationssicherheit und Hacking. Seit 2015 liegt sein Schwerpunkt auf der OT-Sicherheit im industriellen Umfeld.

hans.hoefken@add-yet-iis.de

Dr. Thomas Jansen
ist Rechtsanwalt und Partner im Münchner Büro der Sozietät HEUKING KÜHN LÜER WOJTEK. Er ist seit mehr als 25 Jahren spezialisiert auf die Beratung von deutschen und internationalen Mandanten in technologiebezogenen Transaktionen aller Art, insbesondere bei komplexen Projektverträgen und Joint Ventures. Den Schwerpunkt seiner Tätigkeit bilden IT-Projekte und Outsourcing-Vorhaben, komplexe Kooperationsvereinbarungen sowie Lizenz- und Vertriebsvereinbarungen. Darüber hinaus berät Herr Dr. Jansen zu Rechtsfragen der Virtualisierung, insbesondere zu Rechtsfragen um die Cloud sowie im nationalen und internationalen Datenschutzrecht, speziell zu Fragen der grenzüberschreitenden Datenübermittlung und des Direktmarketings.

Stefan Karg
studierte Elektro- und Informationstechnik an der TU-München und ist heute als Sachverständiger, Auditor und Berater mit Schwerpunkt technischer Datenschutz und Informationssicherheit tätig. Aus dem Einsatz an der Schnittstelle zwischen Technik und Recht ist er mit den praktischen Herausforderungen in mittleren und großen Unternehmen vertraut.

infosec@itk-experts.de

Prof. Nicolai Kuntze
ist seit über 15 Jahren in der IT-Sicherheit in verschiedenen Rollen am Fraunhofer-Institut für Sichere Informationstechnologie SIT, Huawei, der Trusted Computing Group und seit 2017 an der Hochschule Mainz aktiv. Hierbei hat er verschiedene Projekte im Bereich der sicheren Entwicklung und Verteilung von Software, Einsatz von Trusted Computing und der Digitalisierung von Prozessen aktiv gestaltet.

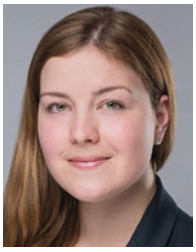
Dr. Hagen Lauer
ist Wissenschaftler am Fraunhofer-Institut für Sichere Informationstechnologie (SIT) und forscht dort an verschiedenen Themen zu Trusted Computing und Sicherheit in kritischen Infrastrukturen. Am Fraunhofer SIT leitet er die Abteilung „Cyber-Physical Systems Security“ und koordiniert den Forschungsbereich „Open and Sustainable IoT Security (OPSIS)“ im Nationalen Forschungszentrum für angewandte Cybersicherheit (ATHENE). Zudem ist er Vorsitzender der Arbeitsgruppe „Virtualisierung“ in der Trusted Computing group und lehrt IT-Sicherheit an der Hochschule Darmstadt. Er schloss sein Master-Studium in Informatik in Gießen ab und promovierte an der Monash University in Melbourne.

Dr. Thomas Lohre
ist diplomierter Kaufmann und Wirtschaftsinformatiker und hat zum Thema „IT-Risikomanagement in Unternehmen“ promoviert. Etliche in seinem Artikel beschriebenen Personenzertifizierungen hat er erfolgreich absolviert. Aktuell ist er Senior Consultant bei der DATEV eG im Bereich „Strategy & Certifications“ und beschäftigt sich dort mit der Etablierung integrierter Managementsysteme sowie deren Zertifizierungen und der Erstellung Multi-Normen Security and Privacy Frameworks.

thomas.lohre@datev.de

Prof. Dr. Markus Nauroth
ist Assistant Professor für Cyber Security am Lehrstuhl für Computer Management and Information Systems (CMIS) Department der Southern Illinois University Edwardsville, USA, sowie Professor für Wirtschaftsinformatik an der Hochschule Mainz. Er studierte Technische Informatik an der Berufsakademie Mannheim und bei der IBM Deutschland sowie Physik an der Universität Mainz und promovierte in Theoretischer Physik an der Technischen Universität München. Prof. Dr. Nauroth arbeitete mehrere Jahre als Berater für die internationale Unternehmensberatung Booz Allen & Hamilton in New York (heute PWC Strategy+) sowie im Bereich Global Business Services der IBM in London, bevor er an die Universität wechselte. Seit 2020 ist er zudem Senior Lecturer am Swiss Cyber Institut in Zürich.

markus@nauroth.com



Jutta Pertenaïs
ist selbstständige Rechtsanwältin und Senior Consultant einer Technologie- und Managementberatung (Valora Consulting GmbH) in Berlin. Ihr Schwerpunkt liegt im IT-Recht und Vergaberecht. Sie ist eine absolute Technik-Enthusiastin und studiert derzeit nebenberuflich Informationstechnologie und Recht (LL.M.) an der Universität des Saarlandes.

info@kanzlei-pertenais.de und

jutta.pertenais@valora-consulting.com

Prof. Dr. Norbert Pohlmann
ist Informatikprofessor für Informationssicherheit und geschäftsführender Direktor des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

pohlmann@internet-sicherheit.de

Andreas Reisch
studierte Elementarteilchen- und Laser-Physik an der Universität in Mainz. Nach Stationen als Senior Consultant und IT-Leiter verantwortete er als CISO bei MAN Truck & Bus in München die Information Security der Volkswagen AG. Seit Januar 2022 ist er selbstständiger Interim Manager und Business Coach (IHK).

andreas@reisch.coach

Prof. Dr. Marko Schuba
war mehr als zehn Jahre bei Ericsson tätig, bevor er 2010 für das Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik an die FH Aachen berufen wurde. Als aktiver Gesellschafter der Unternehmen Schuba & Höfken GbR und @-yet Industrial IT Security GmbH kennt er die aktuellen Cybersicherheitsprobleme der Industrie. Er kooperiert u. a. mit dem LKA NRW, deutschen Sicherheitsbehörden sowie Interpol.

schuba@fh-aachen.de

Prof. Dr. Christoph Skornia
hat Mathematik sowie Physik im Lehramt für Gymnasien studiert und nach wissenschaftlicher Arbeit am Max-Planck-Institut für Quantenoptik promoviert. Im Anschluss fokussierte er sich auf die IT-Sicherheit und war in diesem Bereich in verschiedenen Führungspositionen für Softwareunternehmen tätig. Seit Februar 2012 ist er Professor und Leiter des Labors für Informationssicherheit an der OTH Regensburg und dort aktuell Dekan der Fakultät Informatik und Mathematik.

Fabian Topp
ist Chief Information Security Officer (CISO) der Allianz Technology SE. Er ist mit ISO 27001 Lead Implementer, Lead Auditor und CISM zertifiziert und hat sowohl in den USA als auch in China gelebt und gearbeitet. Er besitzt Universitätsabschlüsse in Politologie wie auch Rechtswissenschaften.

Fabian.topp@allianz.com

Dr.-Ing. Marcel Winandy
hilft Menschen, innovativ zu sein und die Ideen zu maximieren, für die sie sich begeistern. Seit 2003 arbeitet und forscht er im Bereich IT-Sicherheit, insbesondere zu Betriebssystemen und IoT. Aktuell ist er als Cyber Security Architect bei E.ON und als Technology Advisor bei Kaspersky tätig. Zuvor war er Security Technologist bei Huawei. Er ist diplomierter Informatiker und hat in IT-Sicherheit an der Ruhr-Universität Bochum promoviert.

marcel@winandy.de

Stichwortverzeichnis

A

Agile Methoden 179
Agile Vorgehensmodelle 179
Allianz Cyber Defence Center (ACDC) 172
Anforderungen (Softwareentwicklung) 181
Anforderungsanalyse 182
Anforderungsaufnahme 182
Anforderungserhebung 182
Anforderungsmanagement 182
Anforderungsspezifikation 182
Anforderungsvalidierung 182
Angriff 27
Angriffsvektoren 4
Anlagensicherheit 56
Anonymisierung 3
Anti-Malware 19
Approval (Freigabe) 157
Architektur (Softwareentwicklung) 181
ARM TrustZone 237
Assessment 156
Audit 91
– Automatisierungstechnik 209
Auditing 30
Ausschluss (Vergabeverfahren) 254
Authentifikation 3, 14
Authentifizierung 15, 29
Authentisierung 14
Authentizität 3
Automatisierungstechnik 194
Autorisierung 15, 30
Availability 29
Awareness 9

B

Bedrohungen 27
– analysieren 119
– Edge Computing 227
Berechtigungen 35
Bericht (Audit) 91
Betriebsgeheimnisse 69
Blockchain 17
Bring-your-own-Key (BYOK) 274
Bundesamt für Sicherheit in der Informationstechnik (BSI) 67
Business-Continuity-Management-System 67

C

C5 Cloud Computing 84
CCSP 93
Challenge-Response 29
Charter of Trust 165
CIA-Triade 26
CISA 94
CISIS12 84
CISM 94
CISO (Chief Information Security Officer) 47, 54, 150
– Profile 57
– Schwerpunktbereich 56
– Verantwortlichkeiten 55
CISSP 93
Cloud Computing 219, 263
Code Review 188
Coding-Standards 184
Common Criteria 87
Community Cloud 265
Compliance-Pflichten 63
Computerbetrug 69

Computersabotage 69
Confidentiality 27
Container-as-a-Service (CaaS) 264
Control-flow Integrity 37
CRISC 94
Cyberkriminalität 68
Cyber-Physical Systems 25
Cyberphysische Systeme 193
Cyber Security Framework (NIST) 205

D
Data-at-Rest 272
Data-in-Transit 273
Data-in-Use 273
Datenschutz
– Begriff 100
– betroffene Person 100, 101, 112
– Blickwinkel 100
– Edge Computing 224
– personenbezogene Daten 100
– Privacy by Design 101, 106
– Sicherheit der Verarbeitung 102
– Verantwortlicher 102
Datenschutzbeauftragter 102, 113
– Beteiligung Entwicklung 106
Datenschutzvorfall 112
Datenschutz-Zertifikat 86
Datenspeicher (Cloud Computing) 274
Datenveränderung 69
DDoS 5, 29
Defense in Depth 37, 211
Deutsche Cyber-Sicherheitsorganisation (DCSO) 166
DevOps 180
DevSecOps 191
Dienstleistungsmodell 264
Distributed-Denial-of-Service 29
DSGVO 65, 99
Dynamische Analyse 190

E
Echtheit 29
Echtzeitfähigkeit 196
Edge Computing 220, 222
– Grundmodell 225
Einflussmessgrößen 134
End-of-Life (EoL) 191
Energieverbrauch (Edge Computing) 224
Entgegenwirken (IT-Sicherheitsstrategie) 9
Entscheidungshilfe (Vergabeverfahren) 243
Entwicklungsprozess 179
Entwurf (Softwareentwicklung) 181
Environment, Social, Governance (ESG) 169
Erkennen von Angriffen (IT-Sicherheitsstrategie) 10
Exploit Database 203
eXtreme Programming 188

F
Fail-Safe 39
Fernmeldegeheimnis 66
Fernwartung 208
Firewall 16, 37
Forensik 11
Formale Analyse 189
Freigabe (Approval) 157
Function-as-a-Service (FaaS) 265
Funktionale Sicherheit 194
Fuzzing 190

G
Gefahr 27
Gefährdung 27
Geheimhaltung 27
Geräteheterogenität 230
Gleichbehandlungsgrundsatz 245

H
Hackerparagraph 68
Haftung 64, 65
Hybrid Cloud 266

I
ICS Security Kompendium (BSI) 207
Implementierung (Softwareentwicklung) 181
Information Security Consulting 159
Information Security Governance 172
Information Security Management System (ISMS) 153
Information Security Operations 161

Information Security Steering Board (ISSB) 173
Informationssicherheit
– Beauftragter *siehe* ISB
– Begriff 100
– Schutzziele 101
Informationssicherheits-Managementsysteme *siehe* ISMS
Informationssicherheits-Managementsystem (ISMS) 205
Information Technology Risk Council 47, 52
Infrastructure-as-a-Service (IaaS) 264
Innentäter (ICS) 208
Innovationspartnerschaft 248
Integrität 3, 28, 110
Intel SGX 237
Internet der Dinge (IoT) 200, 221
Internet of Things (IoT) 200
Intrusion Detection 37
IoT-Gateway 236
ISA99 207
ISAE 3402 82
ISA/IEC 62443 207
ISB 102, 113
ISMS 102, 107, 205
ISO 15408 87
ISO 27001 80
ISO 31000 82
Isolierte Bereiche 233
ISO/SAE 21434 207, 208
IT-Compliance-Standards 72
IT-Grundschutz 67, 83
IT-Grundschutz-Kompendium 67
IT-Sicherheit
– Begriff 100
– Schutzziele 107
– Security by Design 106
IT-Sicherheitsgesetz (ITSiG 2.0) 71
IT-Sicherheitsstrategien 7
IT-Sicherheitsziele 3

K
Kanban 180
Katastrophenschutz 32
Kerkhoffs, Auguste 34
Kerndimensionen der Informationssicherheitskultur 154
Kleine und mittlere Unternehmen 49
Komplexität, reduzierte 233
Konnektivität (Edge Computing) 224
kontinuierliche Verbesserung 141
Korruptionsbekämpfung 259
Kosten (Edge Computing) 224
Kritische Infrastrukturen (KRITIS) 71
Kritische Komponenten 72
Kryptoagilität 14, 237

L
Latenz (Edge Computing) 224
Lead Auditor (ISO 27001) 95
Lebenszyklus 177
Leistungsbeschreibung 253
Live-Migration (Edge Computing) 227
Lock-in-Effekte 270

M
Maintenance 191
Malware 19
Man-in-the-Middle 4
Markterkundung 252
Maßnahmen 123
Mehrschichtige Verteidigung 46
Memory Safety 37, 186
Mikrokern 235
Mindestanforderungen (Vergabeverfahren) 252
Mitre Att&ck Framework 183
Modularität 234
MS STRIDE 183
Multifaktor-Authentifizierung 15

N
Need-to-know (Sicherheitsprinzip) 273
Nichtdiskriminierungsgrundsatz 245
Nicht offenes Verfahren (Vergabeverfahren) 247
Notfalleinsätz 56

O
Offenes Verfahren (Vergabeverfahren) 247

Onlinebanking 32
OpSec 179
Organisationsstruktur
(Sicherheitsorganisation) 47
Organisations- und Führungsmessgrößen 134
OWASP Threat Modeling 183

P
Patches 213
PCI-DSS 86
Penetration Testing 190
Personal 167
Personalauswahl 168
Personenzertifizierungen 93
Platform-as-a-Service (PaaS) 265
Post-Quanten-Kryptografie 238
Prinzip der geringsten Berechtigung 35
Privacy by Design 232
Private Cloud 265
Privatheit 31
Produktentwicklung 178
Programmiersprache 186
Programmmanagement 56
Protokollierung 274
Prozesslenkung 141
Prozessmessgrößen 134
Pseudonymisierung 3
Public Cloud 265

Q
Quanten-Kryptografie 238

R
Reaktion auf Angriffe 11
Regelung 194
Reifegradanalyse 131
Reifegrad-Level 134
Reifegradmessung 134
– kontinuierlich 142
Requirements Engineering 182
Resilience 39
Richtlinien-Framework 88
Risiko
– analysieren 119
– betroffene Person 112
– Datenschutz 104
– IT 104
– Überprüfung 105
– Unternehmen 104
Risikobehandlung 116
Risikoeinschätzung 33
Risk Committee (RiCo) 173
Routine 45

S
Safe Arithmetic 187
Safety 194
Safety Integrity Level (SIL) 197
Schutzbedarf feststellen 118
Schutzziele 27, 107
– Integrität 110
– Verfügbarkeit 111
– Vertraulichkeit 107
Schwachstelle 27, 125
Scrum 179
Secure Boot 236
Security-Anforderungen 120
Security by Design 34, 177, 230
Security Operations Center (SOC) 56, 160
Security-Prozesse 38
Security-Storys 180
Security-Tests 124
Security through Obscurity 34
SEI CERT-Coding-Standard 184
Separation Kernel 235
Serverless-Computing 265
Sicherheitsbeauftragte 48
Sicherheitskern 235
Sicherheitslevel 210
Sicherheitsmodell (Cloud Computing) 271
Sicherheitstechnik 56
Sicherheitsvorfall 112
Signaturerkennung (Virenerkennung) 37
Smart Grid 32
Social Engineering 38
Software-as-a-Service (SaaS) 265
Sorgfaltspflichten 62
Sprint 179
Stand der Technik 12
Start-up 48

Statische Codeanalyse 189
Steuerung 194
Strafbarkeit (Vergabeverfahren) 259
Strafrechtliche Normen 68
Strafrechtliche Verantwortung 70
Supply-Chain 5
Systemmodellierung 182

T
Technische Richtlinien (BSI) 87
Technische und organisatorische Maßnahmen (TOM) 249 *siehe* TOM
Telekommunikation 66
Telekommunikations-Gesetz (TKG) 66
Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) 66
Telemediengesetz 66
Testat 91
Testen (Softwareentwicklung) 182
Tests (Sourcecode) 188
Thread Safety 187
Threat Modeling 32
TISAX 84
TISP 94
TOM 101, 107
– Eingabekontrolle 110
– Protokollierung 110
– Pseudonymisierung 110
– Transportkontrolle 109
– Trennung nach Zwecken 107
– Verschlüsselung 110
– Weitergabekontrolle 109
– Zugangskontrolle 109
– Zugriffskontrolle 109
– Zutrittskontrolle 109
Top-Level-Leadership 47
Trennung von Verantwortlichkeiten 36
Trusted Computing 18
Trusted Execution Environment (TEE) 237
Trusted Platform Module (TPM) 235
Type Safety 187

U
Überprüfbarkeit 30
Überprüfung (Assessment) 156
Untersuchungsgegenstand modellieren 118
Updates 191

V
Validierung 190
Verantwortlichkeiten (Cloud Computing) 267
Verantwortung (CISO) 150
Verbindlichkeit 3, 30
Verfahrensart (Vergabeverfahren) 246
Verfügbarkeit 3, 29, 111
Verhältnismäßigkeitsgebot 245
Verhandlungsverfahren 248
Verifikation 189
Vermeidungsstrategie 8
Verschlüsselte Dateisysteme 273
Verschlüsselte Übertragung der Daten 273
Verschlüsselung 13
– auf Applikationsebene 273
Verschlusssachen (Vergabeverfahren) 255
Vertragsbedingungen (Einkauf) 242
Vertraulichkeit 3, 107
V-Modell 179
Voraudit 90
Vorfallsmanagement 56
Vorgehensmodell 179
Vorstand (Verantwortlichkeit) 62
Vulnerability 27
Vulnerability Scanner 190

W
Wettbewerblicher Dialog 248
Wettbewerbsgrundsatz 244
Wirtschaftlichkeitsgrundsatz 245
Worst-Case-Szenario 46

Z
Zero Trust 16
Zertifikat 91
Zertifizierung (Vorgehen) 89
Zone 212
Zugangskontrolle (Cloud Computing) 271
Zugriffskontrolle 36, 109, 234