

# Inhaltsverzeichnis

<b>Vorwort</b> .....	V
<b>Abkürzungsverzeichnis</b> .....	XVII
<b>1. Einführung und Grundlagen</b> .....	1
1.1. Ziele dieses Buchs .....	1
1.2. Was dieses Buch enthält .....	1
1.3. Was sind ISB/IT-SiBe? .....	2
1.4. Überblick über die Aufgaben .....	5
1.5. Wie wird man ISB/IT-SiBe? .....	7
1.6. Erwartungen an die Beaufragten .....	10
<b>2. Technische Grundlagen</b> .....	13
2.1. Betriebssicherheit und Sicherheit gegen Angriffe .....	13
2.2. Ziele der IT-Sicherheit .....	14
2.2.1. Vertraulichkeit .....	14
2.2.2. Integrität .....	14
2.2.3. Authentizität .....	15
2.2.4. Authentifizierung .....	15
2.2.5. Nicht-Abstreitbarkeit .....	16
2.2.6. Zutrittskontrolle .....	16
2.2.7. Zugangskontrolle .....	16
2.2.8. Zugriffskontrolle .....	16
2.2.9. Schutz der Privatsphäre .....	17
2.2.10. Verfügbarkeit .....	17
2.2.11. Kontroll- und Ausblickfragen .....	17
2.3. Technische Maßnahmen .....	18
2.3.1. Verschlüsselung .....	18
2.3.1.1. Steganographie .....	18
2.3.1.1.1. Covert Channels .....	19
2.3.1.1.2. Polyglotte Dateien .....	19
2.3.1.2. Kryptographie .....	20
2.3.1.2.1. Symmetrische Kryptographie .....	21
2.3.1.2.1.1. Cäsar Schiebealgorithmus und vergleichbare Verfahren ...	21
2.3.1.2.1.2. Vignère und Co. ....	22
2.3.1.2.1.3. Moderne Verfahren wie DES, 3DES und AES .....	23
2.3.1.2.1.4. Zwischenfazit .....	24
2.3.1.2.2. Asymmetrische Kryptographie .....	25
2.3.1.2.2.1. Diskrete Exponentiation und diskreter Logarithmus .....	25
2.3.1.2.2.2. Primfaktorzerlegung .....	26

## Inhaltsverzeichnis

2.3.1.2.2.3.	RSA als Beispiel	26
2.3.1.2.2.4.	Zwischenfazit RSA	27
2.3.1.2.2.5.	Post-Quantum – Elliptic Curve	27
2.3.1.2.2.6.	Fazit asymmetrische Kryptographie	28
2.3.1.2.3.	Hybride Kryptographie	28
2.3.1.2.4.	Homomorphe Verschlüsselung	29
2.3.1.2.5.	Key-Exchange mit Diffie Hellman	29
2.3.1.2.5.1.	Mathematischer Hintergrund	30
2.3.1.2.5.2.	Praktische Bedeutung	31
2.3.1.2.5.3.	Praxisbeispiel	31
2.3.1.2.6.	Perfect Forward Secrecy	32
2.3.1.2.6.1.	Exkurs: Heartbleed	32
2.3.1.2.6.2.	Perfect Forward Secrecy und Heartbleed	34
2.3.1.2.7.	Kryptographie Buzzword-Bingo	34
2.3.1.2.7.1.	Ende-Zu-Ende- und Transportverschlüsselung	34
2.3.1.2.7.2.	Transportverschlüsselung und Plattenverschlüsselung wären Vollverschlüsselung	36
2.3.1.2.7.3.	ETSI Enterprise Transport Security	37
2.3.1.2.7.4.	Staatliche Eingriffe in Verschlüsselung	38
2.3.1.2.8.	Relevante Implementierungen	39
2.3.1.2.8.1.	FileVault & Co.	39
2.3.1.2.8.2.	TrueCrypt und VeraCrypt	42
2.3.1.3.	Prüfsummen	43
2.3.1.3.1.	Einfache Prüfsummen	43
2.3.1.3.2.	Hashing	45
2.3.1.3.3.	Kryptographisch sichere Hashes	45
2.3.1.3.4.	Hash-Chains und Block-Chains	47
2.3.1.3.5.	Robustes Hashing	48
2.3.1.4.	Digitale Signatur	49
2.3.1.4.1.	Technische Umsetzung	49
2.3.1.4.2.	Grenzen digitaler Signaturen	49
2.3.1.4.3.	Digitale Signaturen in der EU	50
2.3.1.4.3.1.	Einfache elektronische Signatur	50
2.3.1.4.3.2.	Fortgeschrittene elektronische Signatur	52
2.3.1.4.3.3.	Qualifizierte elektronische Signatur	52
2.3.1.5.	Zertifikate	53
2.3.1.5.1.	Ziel: Vermeiden von Man-In-The-Middle-Angriffen	53
2.3.1.5.2.	Certificate Authorities	54
2.3.1.5.3.	Zertifikatsklassen	57
2.3.1.5.3.1.	Domain Validated	57
2.3.1.5.3.2.	Individual Validated und Organisation Validated	57
2.3.1.5.3.3.	Extended Validation	57

## Inhaltsverzeichnis

2.3.1.5.4.	eIDAS 2.0 und die Sicherheit .....	58
2.3.1.6.	Implementierungen .....	59
2.3.1.6.1.	SSL/TLS .....	59
2.3.1.6.2.	PGP/GnuPG .....	61
2.3.1.6.3.	S/MIME .....	62
2.3.1.6.4.	SEPP-Mail/DATEV .....	62
2.3.1.6.5.	TeamDrive, Wire & Co. ....	63
2.3.1.6.6.	Praktische Anwendungen-FAQ .....	65
2.3.1.6.6.1.	Was mache ich, wenn der Empfänger keinen Key hat? ...	65
2.3.1.6.6.2.	Komplizierte Mathematik, also ist verschlüsseln kompliziert? .....	65
2.3.1.6.6.3.	Muss ich verschlüsseln? .....	66
2.3.1.6.6.4.	Was mache ich, wenn ein Mitarbeiter ausscheidet? .....	67
2.3.1.7.	Fazit Kryptographie .....	68
2.3.2.	Fehlererkennung und -behebung .....	69
2.3.2.1.	Fehlererkennung .....	69
2.3.2.2.	Fehlerbehebung .....	70
2.3.2.3.	Fazit .....	71
2.2.3.	Authentizität .....	71
2.3.3.	Nicht-Abstreitbarkeit .....	71
2.3.4.	Authentifizierung .....	72
2.3.4.1.	Passwörter .....	72
2.3.4.1.1.	Passwortkomplexität .....	73
2.3.4.1.2.	Passwortregeln .....	74
2.3.4.1.3.	Gültigkeitsdauer von Passwörtern .....	75
2.3.4.1.4.	Compliance bei Passwörtern .....	75
2.3.4.1.5.	Passwortspeicher .....	76
2.3.4.1.6.	Alternativen .....	77
2.3.4.1.7.	Zurücksetzen von Passwörtern .....	78
2.3.4.2.	Biometrie .....	79
2.3.4.3.	Besitz .....	80
2.3.4.4.	One-Time-Password .....	80
2.3.4.5.	Multifaktorauthentifizierung .....	80
2.3.4.6.	WebAuthN und Fido2 .....	81
2.3.4.7.	Fazit Authentifizierung .....	82
2.3.5.	Zutrittskontrolle .....	82
2.3.6.	Zugriffskontrolle .....	84
2.3.6.1.	Rollen- und Zugriffskonzepte .....	84
2.3.6.2.	Beispiel Unix-Rechte .....	86
2.3.6.3.	Beispiel ACL .....	86
2.3.6.4.	Verschlüsselung als Zugriffskontrolle .....	87
2.3.7.	Schutz der Privatsphäre .....	88

## Inhaltsverzeichnis

2.3.7.1.	Pseudonymisierungsverfahren .....	88
2.3.7.2.	Anonymisierungsverfahren für Daten .....	89
2.3.7.3.	Anonymisierung im Internet .....	90
2.3.7.3.1.	IPv4 .....	90
2.3.7.3.2.	IPv6 .....	90
2.3.7.3.3.	TOR .....	91
2.3.7.3.3.1.	Zugriffe aus dem TOR-Netz als Sicherheitsrisiko? .....	91
2.3.7.3.3.2.	TOR für die eigene Geheimhaltung .....	92
2.3.7.3.3.3.	Funktionsweise und Grenzen .....	92
2.3.7.3.3.4.	VPN-Anbieter und Open-Proxies als Alternativen? .....	93
2.3.8.	Verfügbarkeit .....	93
2.3.8.1.	Störungen der Verfügbarkeit .....	94
2.3.8.1.1.	dDoS .....	94
2.3.8.1.1.1.	Akzidentielle dDoS-Situationen .....	94
2.3.8.1.1.2.	SYN-Flooding .....	96
2.3.8.1.1.3.	Amplification-Angriffe .....	97
2.3.8.1.1.4.	Fazit dDoS .....	98
2.3.8.1.2.	Individuelle DoS-Angriffe .....	98
2.3.8.1.2.1.	Erzeugen von Abstürzen .....	98
2.3.8.1.2.2.	Angriffe auf Router .....	99
2.3.8.1.2.3.	Reverse Tar Pit .....	100
2.3.8.1.2.4.	Fazit Individuelle DoS-Angriffe .....	101
2.3.8.1.3.	Sicherheitslücken .....	101
2.3.8.2.	Maßnahmen zur Verfügbarkeit .....	102
2.3.8.2.1.	Stromversorgung und Internetversorgung .....	102
2.3.8.2.2.	Redundanz .....	103
2.3.8.2.3.	Load-Balancing .....	104
2.3.8.2.4.	Backups .....	105
2.3.8.2.5.	RAID-Array .....	105
2.4.	Schwachstellen und Angriffe .....	107
2.4.1.	Ursachen von Schwachstellen .....	107
2.4.2.	Typische Schwachstellen in Web-Anwendungen .....	107
2.4.2.1.	HTML-Injection .....	107
2.4.2.2.	Cross-Site-Scripting (XSS) .....	108
2.4.2.3.	Vertrauen in Nutzereingaben .....	109
2.4.2.4.	SQL-Injection .....	109
2.4.2.5.	Remote Command Injection .....	110
2.4.2.6.	Alte oder schwachstellenbehaftete Komponenten .....	111
2.4.2.7.	Security Misconfiguration .....	111
2.4.2.8.	Vorhersagbarkeit von Zufallszahlen .....	111
2.4.2.9.	Fazit Schwachstellen in Web-Anwendungen .....	112
2.4.3.	Typische Schwachstellen in compilierten Anwendungen ..	113

## Inhaltsverzeichnis

2.4.3.1.	Buffer-Overflow	113
2.4.3.1.1.	Programme Counter	113
2.4.3.1.2.	Stack	114
2.4.3.1.3.	Overflow	114
2.4.3.1.4.	Ausnutzen des Overflows	115
2.4.3.1.5.	Gegenmaßnahmen	115
2.4.3.2.	Format-String-Vulnerability	116
2.4.3.2.1.	Spezialitäten	116
2.4.3.2.2.	Ausnutzen	117
2.4.3.2.3.	Folgen	117
2.4.3.2.4.	Gegenmaßnahmen	117
2.4.3.3.	Off-By-One	118
2.4.3.4.	Fazit Schwachstellen in compilierten Anwendungen	118
2.4.4.	Typische Behauptungen von Herstellern	119
2.4.5.	Gegenmaßnahme: Qualitätssicherung	122
2.4.5.1.	Schulung	123
2.4.5.2.	Coding Standards	124
2.4.5.3.	Code-Reviews	124
2.4.5.4.	Statische und dynamische Code-Analyse	125
2.4.5.5.	Testing	126
2.4.5.6.	Penetrationstest	126
2.4.5.7.	Abnahme	127
2.4.5.8.	Fazit	128
2.4.6.	Schadsoftware	128
2.4.6.1.	Transportmechanismus	128
2.4.6.1.1.	Virus	128
2.4.6.1.2.	Wurm	130
2.4.6.1.3.	Trojaner	131
2.4.6.2.	Schadfunktion	133
2.4.6.3.	Gegenmaßnahmen	134
2.5.	UCE und UBE	136
2.5.1.	Spam	137
2.5.1.1.	IP-Filter	137
2.5.1.2.	Inhaltsfilter	138
2.5.1.3.	Kollaborative Filter	139
2.5.1.4.	Robuste Hashwerte	140
2.5.1.5.	Filtern über SPF, DomainKey und DMARC	140
2.5.1.6.	Kombinierte Filter	140
2.5.1.7.	Zurückweisen, markieren oder in den Spam-Ordner?	140
2.5.1.8.	Zulässigkeit von Filtern	141
2.5.1.9.	Greylisting	142
2.5.1.10.	Tricks der Spammer	143

## Inhaltsverzeichnis

2.5.1.11.	Fazit zu Anti-Spam	144
2.5.2.	Filtern weiterer Massenmailings	144
2.6.	Human Factors, OSINT und Social Engineering	145
2.6.1.	Human Factors	145
2.6.2.	Open Source Intelligence – OSINT	146
2.6.3.	Social Engineering	147
2.7.	Technische Gegenmaßnahmen	150
2.7.1.	Datenträger	150
2.7.1.1.	Datenträgerverschlüsselung	150
2.7.1.2.	Sicheres Löschen	151
2.7.1.2.1.	Festplatten	151
2.7.1.2.2.	Solid-State-Disks	152
2.7.1.3.	Angriffe über USB	153
2.7.2.	Netzwerksicherheit	155
2.7.2.1.	Reconnaissance	155
2.7.2.2.	Firewalling	156
2.7.2.2.1.	Firewall-Architekturen	156
2.7.2.2.2.	Stateless Filtering	157
2.7.2.2.3.	Stateful Filtering	158
2.7.2.2.4.	Reaktion auf unerwünschte Pakete	158
2.7.2.2.5.	Filterrichtung	159
2.7.2.2.6.	Application-Level-Firewalls	159
2.7.2.2.7.	Mythen zu Firewalls	161
2.7.2.2.7.1.	NAT braucht keine Firewalling	161
2.7.2.2.7.2.	Firewalls sind selbst sicher	162
2.7.2.2.7.3.	Personal Firewalls schützen	162
2.7.2.2.7.4.	Firewalls sind unumgänglich	163
2.7.2.2.7.5.	Firewalls können alle Protokolle filtern	163
2.7.2.2.7.6.	Je mehr Firewalls, desto besser	164
2.7.2.2.7.7.	Firewall schützt vor Schadsoftware	164
2.7.2.2.8.	Firewalls umgehen	164
2.7.2.2.8.1.	Tunneling	165
2.7.2.2.8.2.	Covert Channels	166
2.7.2.2.9.	Fazit Firewalls	166
2.7.2.3.	Intrusion Detection und Prevention	167
2.7.2.3.1.	Host Intrusion Detection Systeme	167
2.7.2.3.1.1.	Rootkits und Backdoors	167
2.7.2.3.1.2.	Dateisystemänderungen	168
2.7.2.3.1.3.	Rootkit-Detektion	169
2.7.2.3.1.4.	Schadsoftware erkennen	169
2.7.2.3.1.5.	Analyse von Log-Files	169
2.7.2.3.1.6.	Kombinierte Systeme	170

2.7.2.3.2.	Network Intrusion Detection Systeme	170
2.7.2.3.3.	Fazit NIDS und HIDS	171
2.7.2.3.4.	Teergruben und Honeypots	172
2.7.2.3.5.	Intrusion Prevention System	173
2.7.2.4.	Security Information and Event Management (SIEM)	173
2.7.2.5.	Virtual Private Networks	174
2.7.2.5.1.	Technische Grundlagen	174
2.7.2.5.2.	Varianten	174
2.7.2.5.2.1.	IPSec	175
2.7.2.5.2.2.	Wireguard VPN	176
2.7.2.5.2.3.	OpenVPN	176
2.7.2.5.3.	Risiken und Grenzen	177
2.7.2.5.4.	Alternativen	177
2.7.2.5.5.	Fazit VPN	177
2.7.2.6.	WLAN-Sicherheit	178
2.7.3.	Physische Sicherheit	179
<b>3.</b>	<b>Rechtliche Grundlagen</b>	<b>181</b>
3.1.	Gesetzliche Grundlagen	181
3.1.1.	IT-SiBe und ISB als Governance-Element für privat-rechtliche Unternehmen und öffentliche Stellen	181
3.1.2.	§ 166 TKG – die Blaupause des IT-SiBe	183
3.1.3.	ISB/IT-SiBe in KRITIS-Organisationen bzw. besonders wichtigen Einrichtungen (BSIG)	186
3.1.4.	ISB bei Anbietern digitaler Dienste, Unternehmen im besonderen öffentlichen Interesse bzw. wichtigen Einrichtungen (BSIG)	194
3.1.5.	Sicherheitskataloge für Betreiber von Strom- und Gasnetzen und von Energieanlagen, § 11 EnWG (einschließlich Kernkraft)	197
3.1.6.	Finanz- und Versicherungsunternehmen und deren Dienstleister (inklusive DORA)	198
3.1.7.	Elektronische Gesundheitsdienste einschließlich Telematik	203
3.1.8.	ISB/IT-SiBe in Organisationen des Bundes (Bundesrepublik Deutschland)	205
3.1.9.	ISB/IT-SiBe in Organisationen der Länder und Kommunen	206
3.2.	Vertragliche Grundlagen	210
3.2.1.	Vertragliche Gestaltung der Aufgaben und Position des ISB/IT-SiBe	210
3.2.2.	Interner ISB/IT-SiBe	215

## Inhaltsverzeichnis

3.2.3.	Externer ISB/IT-SiBe .....	221
3.3.	Untergesetzliche Normen und Standards .....	226
3.3.1.	Rechtliche Einordnung .....	226
3.3.2.	IT-Grundschutz des BSI .....	229
3.3.3.	ISO/IEC 27001 und Normenfamilie ISO/IEC 27000 .....	234
3.3.4.	TISAX .....	237
3.3.5.	CoBiT .....	238
3.3.6.	ITIL .....	238
3.3.7.	VdS-Richtlinien .....	239
3.3.8.	PCI-DSS .....	240
3.3.9.	NIST Cybersecurity Framework .....	240
3.4.	Rechtliche Verantwortung und Haftung des ISB/IT-SiBe, Versicherungsfragen .....	240
<b>4.</b>	<b>Zuständige Behörden und öffentliche Stellen zur IT-Sicherheit .....</b>	<b>247</b>
4.1.	EU-Institutionen und ihre Aufgaben .....	247
4.1.1.	ENISA .....	247
4.1.2.	EDSA/EDPB .....	247
4.1.3.	ACER .....	248
4.1.4.	ENTSO-E und ENTSO-G .....	248
4.1.5.	EMSA .....	249
4.1.6.	CERT-EU .....	249
4.1.7.	ETSI .....	250
4.2.	Nationale Behörden und Einrichtungen und ihre Aufgaben .....	250
4.2.1.	Im Bereich der Bundes- und Landesinnenministerien. ....	250
4.2.1.1.	BSI .....	250
4.2.1.2.	Landesbehörden zur Informations- und IT-Sicherheit (LSIs, Cyberagenturen) .....	251
4.2.1.3.	Bundesamt für Verfassungsschutz und Landesämter für Verfassungsschutz .....	253
4.2.1.4.	Bundeskriminalamt .....	253
4.2.1.5.	Nationales Cyber-Abwehrzentrum .....	253
4.2.1.6.	Zentrale Stelle für Informationstechnik im Sicherheits- bereich (ZITiS) .....	253
4.2.1.7.	Landespolizeien mit LKAs .....	253
4.2.2.	Bundesnachrichtendienst .....	254
4.2.3.	IT-Sicherheit in der Organisation des Bundesverteidi- gungsministeriums .....	254
4.2.3.1.	Abteilung Cyber/IT (CIT) im Verteidigungsministerium ..	254
4.2.3.2.	Kommando Cyber- und Informationsraum (CIR) .....	255

4.2.3.3.	Cyberinnovationhub Bw (CIHBw) . . . . .	256
4.2.3.4.	Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) . . . . .	256
4.2.3.5.	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr . . . . .	257
4.2.3.6.	BWI GmbH . . . . .	257
4.2.4.	IT-Sicherheit im Bereich weiterer Bundes- und Landes- ministerien . . . . .	257
4.2.4.1.	BaFin . . . . .	258
4.2.4.2.	Bundesnetzagentur . . . . .	258
4.2.4.3.	Aufsichtsbehörden nach dem AtomG . . . . .	259
4.2.5.	Weitere Einrichtungen . . . . .	259
4.2.5.1.	Gematik . . . . .	259
4.2.5.2.	Bundes- und Landesdatenschutzbeauftragte und Daten- schutzaufsichtsbehörden . . . . .	259
<b>5.</b>	<b>Abgrenzung zu weiteren Verantwortungsträgern . . . . .</b>	<b>263</b>
5.1.	Unternehmens- und Behördenleitung . . . . .	263
5.2.	Datenschutzbeauftragte . . . . .	264
5.3.	Betriebsrat . . . . .	267
5.4.	IT-Abteilung/externe Administratoren . . . . .	269
<b>6.</b>	<b>Die To-dos: Wie organisiert sich ein ISB/IT-SiBe? . . . . .</b>	<b>271</b>
6.1.	Voraussetzungen schaffen . . . . .	271
6.2.	Leitlinie Informationssicherheit . . . . .	273
6.3.	Ermittlung und Inventarisierung der Schutzobjekte/ Information Assets . . . . .	276
6.4.	Risikoanalyse und Risikobehandlung – Statement of Applicability (SoA)/Sicherheitskonzept . . . . .	277
6.5.	Umsetzung und kontinuierliche Verbesserung: Plan, Do, Check, Act . . . . .	280
6.6.	Bewältigung von Sicherheitsvorfällen . . . . .	281
6.6.1.	Wahrnehmung des Sicherheitsereignisses . . . . .	282
6.6.2.	Sofortmaßnahmen . . . . .	282
6.6.3.	Alarm/Eskalation/Meldeverfahren . . . . .	282
6.6.4.	Einrichtung und Aufnahme des Notbetriebs; Wieder- anlauf des Normalbetriebs . . . . .	283
6.6.5.	Kommunikation und Dokumentation . . . . .	283
6.6.6.	Nacharbeit . . . . .	284
6.6.7.	Analyse und Bewertung der Bewältigung . . . . .	284
6.6.8.	Vorsorgemaßnahmen . . . . .	284
6.6.9.	Training . . . . .	284

## Inhaltsverzeichnis

6.7.	Information und Beratung der Organisationsleitung . . . . .	285
6.8.	Information und Sensibilisierung der Beschäftigten/ IT-Nutzer . . . . .	286
6.9.	Projektbegleitung . . . . .	287
6.10.	Branchenspezifische Sonderanforderungen . . . . .	287
7.	<b>Anhang</b> . . . . .	289
	<b>Weiterführende Literatur</b> . . . . .	309