



# Stichwortverzeichnis

3DES 208

## A

Accountability 42  
 Address Resolution Protocol 279  
 AEAD 213, 229  
 AES 129, 208, 209, 212, 241, 242, 275, 276, 306  
 Allianz für Cybersicherheit 194  
 AlphaGo 357  
 Android 306  
 Angriffserkennung 55, 61, 84, 189, 322, 323  
 Angriffserkennungssystem 93, 322–325  
 Anonymisierung 283, 312  
 APT28 327  
 Archivierung 258, 263, 264  
 Assetmanagement 174  
 Audit 55  
 Auftragskontrolle 147  
 Ausfallsicherheit 146, 265–267  
 Authenticator 253, 277, 278, 317, 339  
 Authentifizierung 81, 87, 253, 289, 340  
 Authentizität 35, 42, 69, 225, 226, 229, 275, 340  
 Availability *siehe* Verfügbarkeit  
 Awareness 197, 198

## B

Backup 41, 52, 136, 143, 147, 173, 257, 307, 308, 352  
 BDSG 52, 65–67, 73, 131–135, 141, 143, 146–148, 248  
 Bedienbarkeit 127, 174  
 Bedrohungsanalyse 169  
 Belastbarkeit 45, 59, 60, 145  
 Benutzbarkeit 43  
 Benutzermanagement 141  
 Berechtigung 180, 183  
 Betriebskontinuitätsmanagement, 146

Betriebsrat 142, 222  
 Bitcoin 356  
 Bitlocker 50, 305, 306  
 Bitlocker To Go 308  
 Blockchain 355, 356  
 Blockverschlüsselung 209–211  
 Bluebugging 288  
 Bluejacking 288  
 Bluesnarfung 288  
 Bluetooth 267, 284, 286–288  
 Braktooth 288  
 BS7799 95  
 BSI 27, 36, 44, 51, 52, 54, 55, 194  
 BSI-Gesetz 36, 38, 47, 49, 52, 54, 55, 81, 82, 85, 90, 92, 94  
 BSI-ITSiKV 78  
 BSI-Kritisverordnung 77, 82, 85  
 Bundesamt für Sicherheit in der Informationstechnik *siehe* BSI  
 Bundesdatenschutzgesetz *siehe* BDSG  
 Bundesnetzagentur 52, 54, 55, 93  
 Bundesverfassungsgericht 68  
 Bußgeld 52

## C

Caesar-Chiffre 203  
 CBC 116, 210, 211, 214, 275, 276  
 CBC-MAC 222  
 CCM 213  
 CDO 156  
 CERT 158, 159, 194  
 Chatham House Rule 195  
 Chatserver 344  
 Chipkarte 80, 125, 232, 233, 249–252, 304  
 CIO 156  
 Ciphertext *siehe* Geheimtext  
 CISO 156  
 Cloud-Dienst 298  
 Cloud-Firewall 299  
 Common Criteria 95, 251

Common Vulnerability Enumeration 333  
 Common Vulnerability Scoring System 333  
 Compliance 44  
 Computer Emergency Response Team *siehe* CERT  
 Computerviren 286  
 Confidentiality *siehe* Vertraulichkeit  
 Containerverschlüsselung 307, 308  
 CSIRT 158  
 Cybersicherheit 35, 38, 39, 76, 77, 81, 84  
 Cyphersuite 275

## D

Daktyloskopie 246  
 Data Encryption Key 304  
 Data Encryption Standard *siehe* DES  
 Dateiverschlüsselung 112, 309  
 Datenkategorien 321  
 Datenminimierung 114  
 Datenschutz 44  
 Datenschutzaufsicht 55  
 Datenschutzbeauftragte 131, 157, 166, 186, 320  
 Datenschutzgrundverordnung *siehe* DS-GVO  
 Datenschutzverletzung 186  
 Datensicherung 251, 257–264, 326  
 Datenträgerverschlüsselung 134, 304–306  
 Datenverschlüsselung 275  
 Deduplizierung 135, 136  
 Demilitarisierte Zone *siehe* DMZ  
 Deming-Kreis 155, 163, 164  
 Denial of Service *siehe* DoS  
 DES 208  
 66398 145  
 66399 145  
 EN 1627 132





## 380 Stichwortverzeichnis

DES 208  
 DLIES 229  
 dm-crypt 305, 306  
 DMZ 294, 298  
 DoS 288  
 DS-GVO 47, 50, 52, 54–56, 59,  
 60, 67, 155, 157, 303  
 Dual\_EC\_DRBG 217

### E

E2E-Verschlüsselung *siehe*  
 Ende-zu-Ende-  
 Verschlüsselung  
 ECC 117, 227, 229  
 ECIES 229  
 eIDAS-Verordnung 43, 79, 80,  
 232  
 Eingabekontrolle 141  
 Einmalpasswort 252, 253,  
 338  
 Eintrittswahrscheinlichkeit 49,  
 49, 59, 60  
 Einwegverschlüsselung  
 336  
 Elliptische-Kurven-  
 Kryptographie *siehe*  
 ECC  
 Ende-zu-Ende-Verschlüsselung  
 310, 344, 347, 348  
 ENISA 38, 77, 198  
 Erpressung 109  
 Ethereum 356  
 Ethernet 270, 279  
 European Union Agency for  
 Cybersecurity *siehe* ENISA  
 Evil-Maid-Angriff 305

### F

Fachkunde 55, 330  
 Faktorisierung 240, 241  
 Fancy Bear *siehe* APT28  
 Fernmeldegeheimnis 93  
 Festplattenverschlüsselung 50,  
 71  
 FileVault 2, 305  
 Fingerabdruck 237, 243, 246,  
 247  
 Firewall 132, 175, 191, 276,  
 291–299, 313  
 FIRSAT 194  
 Forensik 191, 246

### G

GCM 213  
 Gefährdungsanalyse 108  
 Gefährdungspotenzial 55, 89,  
 93, 322  
 Geheimchutz 192  
 Geheimtext 207, 209, 211, 212,  
 213, 215, 216, 220  
 Geschäftsgeheimnis 86  
 Geschäftsgeheimnisgesetz 86  
 Geschäftsprozess 107  
 Gesichtserkennung 244, 247,  
 248, 339, 340  
 Gewährleistungsziel 74, 114,  
 141  
 GnuPG 237, 311

### H

Hackerangriff 82  
 Hash 129, 222, 336  
 Hashfunktion 142, 221, 222,  
 254, 275, 276, 336  
 Hashwert 139, 142, 143,  
 221–223, 225, 230, 251, 330,  
 336,  
 355, 356  
 Hintertür 208  
 Hybridverschlüsselung 220,  
 221, 225

### I

IDEA 208  
 Identitätsmanagement 157,  
 180, 184, 341  
 Implementierungskosten 59,  
 60, 70, 72  
 Informationssicherheits-  
 ausschuss 159  
 Informationssicherheits-  
 beauftragter 155–157, 161,  
 320  
 Informationssicherheits-  
 management-System *siehe*  
 ISMS  
 Informationssicherheits-  
 richtlinie 128  
 Initialisierungsvektor 212  
 Integrität *siehe* Integrität  
 Integrität 36–38, 41–43, 45,  
 114, 123, 141, 147,  
 165–168

Interessenabwägung 264  
 Intervenierbarkeit 62, 73, 114  
 Inventarverzeichnis 171, 172  
 iPad 306  
 iPhone 306  
 Iris-Scan 247  
 ISMS 98, 100–102, 105, 106,  
 110, 120, 121, 125, 164, 320  
 ISO 95  
 9001 99  
 14001 99  
 27000 96–98, 100, 101  
 IT Infrastructure Library *siehe*  
 ITIL  
 IT-Grundschutz 101, 115, 119,  
 125, 175  
 IT-Sicherheitsbeauftragter 157  
 IT-Sicherheitsgesetz 75, 81  
 IT-Sicherheitsgesetz 2.0 78  
 IT-Sicherheitskonzept 156  
 IT-Sicherheitsvorfall 158  
 ITIL 130, 172  
 ITSEC 95

### K

Key Encryption Key 304  
 Key Performance Indicators  
 319  
 Key Wrapping 304  
 Keylogger 191  
 Klartext 207, 209, 210, 212,  
 213, 216, 220–222, 224, 226  
 Konfigurationsmanagement  
 178–180  
 Korrektheit 41, 141, 143, 349  
 Kreuzreferenztabellen 111  
 Krisenstab 107  
 KRITIS 36, 85, 92  
 Kritische Infrastruktur *siehe*  
 KRITIS  
 Kryptoanalyse 204  
 Kryptodebatte 206  
 Kryptografie 139, 203, 204,  
 206, 217, 219, 228

### L

Löschfristen 145  
 Löschkontrolle 144, 303  
 Löschprozess 260  
 Lieferantenbeziehungen 147  
 Lizenzmanagement 176





## Stichwortverzeichnis 381

### M

Mallory 215  
 Malware *siehe* Schadsoftware  
 Mandantentrennung 135  
 MD4 222, 223  
 MD5 222, 223  
 Meldepflicht 50, 52, 53, 186,  
 187, 303  
 Memcached 282  
 Mindeststandard 86  
 MISP 195  
 Missbrauch 71, 108, 109, 112  
 Missbrauchsrisiko 294

### N

Nachrichtenschlüssel 344  
 Nachweispflichten 133  
 Nameserver 271  
 National Institute of Standards  
 and Technology *siehe* NIST  
 Near Field Communication  
*siehe* NFC  
 Netzwerkadresse 174  
 Netzwerksan 173  
 Netzwerksicherheit 69  
 Netzwerkzugang 267, 284  
 NFC 252, 289  
 Nichtabstreitbarkeit 43  
 Nichtverkettbarkeit 73, 135  
 Nichtverkettung 114  
 NIS-2-Richtlinie 77, 158  
 NIS-Richtlinie 38, 47, 53, 60,  
 75–77, 82  
 NIST 130, 145, 184, 198, 199,  
 217, 242, 336, 337  
 nmap 149  
 Notfallmanagement 106, 107  
 Notfallpläne 107  
 NSA 208

### O

OATH 253  
 OFB 211  
 Once-Only-Prinzip 157  
 Onlinezugangsgesetz *siehe*  
 OZG  
 OpenPGP 231, 234–236, 311,  
 345  
 Orange Book 95  
 OZG 87, 88

### P

Packet Filter 294, 295  
 Padding 224, 225  
 Partitionsverschlüsselung  
 307  
 Passwort 243, 252, 278, 285,  
 306–308, 317, 335–340  
 Passworhash 336  
 Passworrichtlinie 335  
 PDCA-Zyklus 98, 163, 164,  
 166, 169  
 Penetrationstest (Pentest) 87,  
 151, 349  
 PGP *siehe* OpenPGP  
 Phishing 199, 328  
 Post-Quantenkryptografie 242  
 Prüfsumme 142, 213, 316  
 Primfaktoren 218, 227  
 Privatsphäre 272, 276, 284,  
 287, 289, 296  
 Protokolldateien 168, 190, 296  
 Pseudonymisierung 59, 60, 84,  
 137–139

### Q

Qualität 44  
 Quantencomputer 237,  
 240–242

### R

RAID 265, 266  
 Ransomware 40, 186, 258, 261,  
 326, 327  
 Rechenschaftspflicht 144  
 Rechtmanagement 144, 182,  
 183  
 Rechtsakt zur Cybersicherheit  
 77  
 Redundanz 41, 146, 264  
 Reifegradmodell 87, 88  
 Resilienz 44  
 RFID 249, 289, 290  
 RIPEMD 222, 223  
 Risiko 49–52, 59, 60, 67, 72, 78,  
 89, 97, 101, 189, 233  
 Risikoanalyse 48, 105,  
 107, 110  
 Risikokarte 49  
 Risikoklasse 49  
 Risikomanagement 48, 75, 101,  
 107, 124

Rollenkonzept 114, 180  
 Rutkowska, Joanna 305

### S

S/MIME 311, 345  
 Sabotage 212  
 Sandbox 328, 329  
 Schadenshöhe 49, 49, 60  
 Schadsoftware 40, 41, 128, 186,  
 292, 293, 296, 326–329, 346  
 Schlüsselerzeugung 216, 285  
 Schlüssellänge 208, 209, 227,  
 241, 275  
 Schlüsselmanagement 126,  
 304, 309, 311, 349, 353  
 Schlüsselpaar 229, 233, 251,  
 253, 254, 344  
 Schlüsselstrom 209  
 Schlüsselvereinbarung 214,  
 215, 242, 275, 343, 344  
 Schutzbedarfsanalyse 321  
 Schutzziele 36, 37, 39, 44, 45,  
 48, 49, 65, 69, 74, 91,  
 165–167, 262, 263  
 Schwachstellenscan 151  
 Schwachstellenscanner 149  
 SDG-Verordnung 81  
 Secure Boot 304  
 Security Incident and Event  
 Monitoring *siehe* SIEM  
 SGB V 47, 88  
 SHA-1 222  
 SHA-2 222  
 SHA-3 222, 223  
 sha1 223  
 SHA256 222, 223  
 Sicherheitsüberprüfungsgesetz  
 192  
 Sicherheitsarchitektur 277  
 Sicherheitseinstellungen 44  
 Sicherheitskonzept 93, 139  
 Sicherheitsvorfall 52, 77  
 SIEM 190  
 Signatur  
 digitale 43, 79, 142, 143, 225,  
 234, 243  
 einfache 79  
 elektronische 43, 79  
 fortgeschrittene 79  
 qualifizierte 80  
 Signaturerstellungsdaten 79  
 Signaturerstellungseinheit 80





## 382 Stichwortverzeichnis

- Signaturerstellungseinheit 80  
 Single-Sign-on 340  
 Smartcard 251  
 Social Engineering 48  
 Softwareinventarisierung 175  
 Sozialgesetzbuch V *siehe* SGB V  
 Speicherchipkarte 251  
 Spinnennetzdiagramm 320, 321  
 Spionage 168  
 Stand der Technik 67  
 Standard-Datenschutzmodell 113  
 Stromverschlüsselung 209, 210  
 Substitutionsverschlüsselung 203
- T**
- TCP/IP 268–270  
 TCSEC 95  
 Technisch-organisatorische Maßnahmen *siehe* TOM  
 Telekommunikationsgesetz *siehe* TKG  
 Telekommunikation-  
   Telem Medien-  
   Datenschutzgesetz *siehe* TTDSG  
 Telematik-Infrastruktur 90  
 Telemediengesetz *siehe* TMG  
 TISAX 119, 123  
 TKG 47, 52, 55, 67, 92–94, 157
- TLS 115–117, 129, 140, 149, 213, 272–276, 283, 314, 315  
 TMG 92–94  
 TOM 21, 59, 131, 148, 149  
 TOTP 253  
 Traffic Light Protocol 193  
 Transparenz 114  
 Transport Layer Security *siehe* TLS  
 Transportverschlüsselung 116, 272, 310, 343, 347, 349, 351  
 Trennungskontrolle 135  
 TrueCrypt 305  
 Trust on First Use 237  
 TTDSG 67, 92–94
- U**
- Umsetzungsplan Bund 82  
 USV 146
- V**
- VeraCrypt 305  
 Verantwortlichkeit 42, 43, 94  
 Verbindlichkeit 44  
 Verfügbarkeit 39–41, 45, 48, 50, 52, 59, 61, 114, 145–147, 166–168  
 Verfügbarkeitskontrolle 146  
 Verschlüsselung *siehe auch* Kryptografie  
   asymmetrische 214  
   Betriebsarten 210  
   homomorphe 238  
   symmetrische 208  
 Verschlusssache 192  
 Verschlusssachenanweisung 192  
 Vertrauensdiensteanbieter 80  
 Vertraulichkeit 36, 38, 42, 50, 69, 80, 114, 131, 141, 145, 166, 167  
 Virtual LAN *siehe* VLAN  
 Virtual Private Network *siehe* VPN  
 Virus *siehe* Schadsoftware  
 VLAN 280  
 VoIP 141  
 VPN 29, 140, 277, 311, 312, 314  
   OpenVPN 315  
   Wireguard 317
- W**
- Web of Trust 235  
 WebSSL 314  
 Weitergabekontrolle 143  
 Wireguard 317
- Z**
- Zertifizierung 56  
 Zufallszahlen 139, 212, 217, 220  
 Zugangskontrolle 133  
 Zugangssteuerung 133  
 Zugriffskontrolle 134  
 Zutrittskontrolle 132  
 Zuverlässigkeit 44

