



Sebastian  
Kübeck

# Web-Sicherheit

Wie Sie Ihre Webanwendungen  
sicher vor Angriffen schützen

# Stichwortverzeichnis

## Numerisch

3COM 201  
3DES 91

## A

Abbild 193  
Abbruchbedingung 176  
Abdecken 116, 120  
Abdeckfunktion 116, 120,  
136  
Abdeckmechanismus 136  
Abfrage 108  
Abhängigkeiten 256  
Abkürzungen 68  
Ablaufdatum 56  
Abmelden 154  
Abmeldeseite 234  
Absender 97  
Absicherung 41, 203, 282  
Absicherungstechnik 155  
Absturz 168  
Active Server Pages siehe  
ASP  
Adapterklasse 294  
Administrationsoberfläche  
62, 188  
Administrationswerkzeug  
188  
Administrationszugang 61,  
62, 163  
Administrator siehe System-  
administrator  
Adobe 145  
Adressraum 168  
Advanced Encryption Stan-  
dard siehe AES  
Advanced Research Projects  
Agency siehe ARPA  
AES 91  
AJAX  
Anwendungen 128, 137

Akronym 77  
Aktenvernichter 76  
Aktien 57  
Akustikkoppler 25, 26  
Alarm 104  
Anlage 65  
System 65  
Alert-Fenster 124  
Alice 82  
Allheilmittel 16, 59, 62  
Altair 8800 24  
Alternative 182  
Analyse 199, 230  
Anführungszeichen 281  
Angreifer 15, 36, 62  
Angriff 205  
Angriffserkennung 66  
Angriffsfläche 21, 62, 187,  
239, 248  
Angriffsmöglichkeit 65, 187,  
232, 239  
Angriffsmuster 171  
Angriffspunkt 250  
Angriffssignatur 206  
Angriffsszenario 65  
Angriffstechnik 21, 26, 76,  
77, 79, 81, 197  
Angriffsvektor 206, 261,  
281, 285  
Angriffsversuche 51  
Anmeldeformular 207  
Anmeldeseite 234  
Anmeldung 126  
Annotation 257  
Anthropologie 14  
Anti-Phishing Phil 37  
Antivirus-Software siehe  
Virens Scanner  
Antivirus-Software siehe  
Virens Scanner  
Anweisung 236

Anwender 197  
Anwendung 150, 197  
Anwendungslogik 109  
Anzeige 73  
Apache  
Webserver 97  
Apache Tomcat  
siehe Tomcat  
Apache-Webserver 190, 194  
AppCodeScan 235  
Apple I, II 24  
Applets 145  
Appliance 104  
Applikationsebene 140  
AppScan 236  
Archetyp 82  
Armband 70  
ARPA 28, 29  
NET 28, 29  
Array 130, 228  
ASCII 249  
Askimet 273  
ASP 191  
ASP.NET 106  
Asymmetrie 62  
Attribut 153, 215, 220  
Aufrechterhaltung 68  
Aufteilung 63  
Aufteilungsprinzip 63  
Aufwand 59  
Ausdruck 181  
Ausführungsstrang siehe  
Thread  
Ausführungszeit 184  
Ausgabedokument 223  
Ausgabesequenz 222  
Auskunftsfreude 189  
Auslesen 110  
Ausprobieren 112  
Auswahl 113  
Auswahlliste 205, 248

- Ausweis 69  
 Auswirkung 52, 241  
 Authentifizierung 14, 69, 140, 149, 151, 232  
 Authentifizierungsverfahren 75, 79, 149, 152  
 Authentisieren 70  
 Autofahren 67  
 Autohersteller 49  
 Autoindustrie 50, 53  
 Automat 181  
 Automatisierung 203, 254  
 Autoproduzent 50  
 Autorisierung 14, 69, 157, 232
- B**
- Back Door siehe Hintertür  
 Backslash 163, 165  
 Backup 192  
     Datei 202  
 Bank 127, 137  
 Bankkunde 126  
 Barrierefreie Webseite 78  
 BASH 119  
 Basic Authentication 150  
 Basistechnologie 152  
 Batch-Betrieb 21  
 Bauchgefühl 52  
 BBS 25  
 Bedienungsfehler 197  
 Bedrohung 52, 67  
 Bedrohungslage 103  
 Bedürfnisse 59  
 Behörde 69  
 Behörden 56  
 Benutzer 120, 137, 138  
     Aktivitäten 154, 184  
     Anfrage 62  
     Daten 114, 166, 220  
     Eingabe 116  
     Freundlichkeit 66  
     Konto 61, 62, 76, 200  
     Name 109  
     Sitzung siehe Session  
 Berechnung 171  
 Berechtigung 69  
 Bereich 168  
 Bericht 203  
 Beruhigung 67
- Beschaffenheit 201  
 Bestimmungen 52  
 Betriebsarten 91  
 Betriebsgeheimnis 39  
 Betriebssystem 50, 88, 177, 184, 188, 192, 202  
     Hersteller 58  
     Kern 168  
     Prozess 184  
     Shell 164  
 Bewusstsein 52  
 Bibliotheken 106  
 Bildschirm 22  
 Biologie 14  
 Biometrische Verfahren 70  
 Black Box Test 217  
 Black-Box-Methode 237  
 Black-Hats 24  
 Blaster 31  
 Blind-SQL-Injection 111, 112  
 Blockchiffren 91  
 Blog 36, 120, 260, 273  
     Anwendung 128  
     Kommentar 250  
     Post 175  
 Blowfish 91  
 Bluetooth 79  
 Blurp-Suite 199  
 Bob 82  
 Body-Element 147  
 Bonneau, Joseph 79, 155  
 Börse 57  
 Bot  
     Netz 31, 32  
 Bot-Netzbetreiber 175  
 bouncycastle 97  
 Bourne-Shell 119  
 Brain-Virus siehe Pakistani-Virus  
 Browser 123, 128, 137, 138, 142, 144, 150, 161, 169, 206  
     Erweiterung 146  
     Fenster 144  
     Hersteller 147  
     Interaktion 274  
     Plugin 145  
     Version 138  
 Browser Security Handbook 138
- Brute-Force-Attacke 76, 150, 153, 234  
 BSI  
     Grundschutz 46  
 BTX (Bildschirmtext) 27  
 Bücher 194  
 Buffer Overflow 167  
 Bulletin Board Systems  
     siehe BBS  
 Bundesinnenministerium  
     44  
 Bush, George W. 57  
 Bytecode 236
- C**
- C (Programmiersprache) 13, 167  
 C# 13, 167, 253  
 C++ 13, 167, 171  
 Cache 152, 158  
 Cambridge 79  
 CAPCHAS 77  
 Carriage Return 249  
 Cascading Style Sheets siehe CSS  
 C-Bibliothek 168  
 CCC (Chaos Computer Club) 24, 27, 71  
 Center for Internet Security  
     siehe CIS  
 CFB 91  
 CGI-Skript 171  
 Change-Root-Mechanismus 165  
 Chaos Computer Club siehe CCC  
 Checkbox 205  
 Chiffre 81  
     symmetrisch 153  
 Chip 88  
 Chipkarte 85  
 Choke Point 62  
 Chrome 184  
 Chuck 82  
 Cipher Feedback siehe CFB  
 CIS 194  
 Cisco 201  
 Clausewitz 14  
 Clickjacking 142  
 Client-Zertifikat 97, 139

- CMS 97  
Code  
    Bestandteil 253  
    Red 30  
    Review 171, 217, 285  
    Scan 237  
    Scanner 236  
Cohen, Fred 105  
Command and Control  
    Server siehe Steuerungs-  
    server  
Command-Injection-  
    Schwachstelle 117  
Commodore 64 24  
Compartmentalization  
    siehe Aufteilungsprinzip  
Compiler 188  
Compliance 15  
Computer 21, 23  
Computer Security Resource  
    Center siehe CSRC  
Computer-Hacker siehe  
    Hacker  
Computerkriminalität 21, 25  
Computerprogramm 88  
Computersystem 52  
Conficker-Wurm 33  
Connection  
    Pool 179  
Cookie 142, 153, 166  
    Einstellungen 153  
Counter siehe CTR  
Cracker 24  
Cracklib 77  
Cross-Site-Request-Forgery-  
    Angriffe 76  
Cross-Site-Request-Forgery-  
    Schwachstelle 137, 139,  
    203  
Cross-Site-Scripting 57  
    Angriff 76  
    Schwachstelle 107, 123,  
    142, 203, 206,  
    217, 222, 241,  
    252  
Cryptographic Message  
    Syntax siehe CMS  
C-Shell 119  
CSRC 194  
CSRF-Token 140, 232
- CSS 104, 123, 136  
CTR 91  
CumbaJohnny 43  
CVS 253
- D**  
Data Encryption Standard  
    siehe DES  
Data Execution Prevention  
    siehe DEP  
Data-Segment 168  
Datei 236  
    Endung 165  
    Name 163  
    Pfad 159  
    Separator 163  
    Streams 178  
    System 88, 162, 163,  
    232  
Daten 55, 66, 157, 167  
    öffentlich 55  
    veränderbar 55  
    vertraulich 55  
Datenbank 105, 108, 117, 158,  
    161, 206, 218, 221, 251, 256  
    Abfrage 113  
    Anfrage 218  
    Firewall 105, 120, 180  
    Inhalt 110  
    Kommando 259  
    Objekt 287  
    Produkt 108, 111, 114,  
    281  
    Schema 111, 180, 257,  
    276  
    System 104, 110, 121,  
    180  
    Tabelle 287  
    Team 218  
    Typ 281  
    Verbindung 178, 215,  
    220, 287  
    Versionsnummer 110  
    Zeile 109  
    Zugriff 180, 215, 222,  
    287  
Datenbehälter 94  
Datenfluss 236  
Datenflussanalyse 217, 223,  
    239
- Datenquelle 230  
Datensatz 87, 206  
Datenschutz 55  
Datenspeicherung 84  
Datentyp 171, 239, 248  
Datenverlust 192, 198  
DDoS-Angriff 175  
DDoS-Attacke 30, 43, 44, 58  
Debian 61  
Defense In-Depth siehe Tief-  
    greifende Verteidigung  
dekodieren 239  
Delete  
    Anweisung 109  
Demoralisieren 180  
Demozugang 234  
Denial-of-Service-Schwach-  
    stelle siehe DoS-Schwach-  
    stelle  
DEP 170  
DES 91  
Dieb 64  
Diebstahl 50, 82  
Dienst 78, 188  
Dienstleister 136  
Digest Authentication 150  
Digitale Signatur 93  
Digitales Zertifikat 94  
Diskette 24, 25  
Distributed Denial of Ser-  
    vice-Attacke siehe DDoS-  
    Attacke  
DIV-Element 143  
Django 106  
Dijkstra, Edsger 197  
DNS 202  
    Server 188  
Dokument 161, 234  
Dokumentname 159  
Domain 42  
Domäne siehe Domain  
Dominoeffekt 78  
DoS-Angriff 175  
DoS-Schwachstelle 175  
Drahtlose Netzwerke 153  
Drop-Zone 38  
dual control 61  
Dumpster Diving 76

**E**

ECB 91  
 Eclipse 222, 257  
   Plugin 236  
 Eigenimplementierung 85  
 Eigenschaft 130  
 Einarbeitungszeit 199  
 Einbetten 117  
 Einbruch 65  
 Einfallstor 64  
 Eingabedaten 107, 181, 206, 239  
 Eingabefeld 127, 152, 166, 205, 279  
 Eingabelänge 182  
 Eingabeparameter 119  
 Eingabepuffer 167  
 Eingang 69  
 Einladung 189  
 Einsatz 79  
 Einsatzdauer 87  
 Einsatzzweck 188  
 Einschleusen 113  
 Einstellungen 187  
 Eintrittskarte 69  
 Eintrittspunkt 217  
 Eisbrecher 59  
 EJB QL 119  
 Electronic Codebook siehe ECB  
 Element 142  
 Eltern-Verzeichnis 165  
 E-Mail 26, 31, 34, 36, 97  
   Adresse 265  
   Client 97  
   Server 188  
   Verschlüsselung 97  
 Embedded-Prozessor 168  
 Empfehlung 87, 194  
 Endlosschleife 176  
 Endpunkt 217  
 Engressia, Joe 22  
 Enron 57  
 Enterprise Security API siehe ESAPI  
 Entschädigung 158  
 Entwicklung 191  
 Entwicklungsplattform 114

Entwicklungsumgebung 198, 253  
 Ergebnis 109, 257  
 Ergebnisliste 234  
 Erkennungsmechanismus 203  
 Erkennungsrate 105  
 Ernstfall 52  
 Ersatzsystem 45  
 ESAPI 106, 118, 136, 162, 284  
   Bibliothek 133, 150  
 ESAPI-Bibliothek 165  
 Estland 43  
 Ethernet 25  
 Event 69  
 Evolution 48  
 evolutionsbiologisch 48  
 Exit-Strategie 59  
 Exklusiv-Oder-Funktion 90

**F**

Fabrikat 201  
 Facebook 57, 78, 79  
 Fahrzeug 49, 50  
 Fahrzeughersteller 50  
 fail  
   safe 60  
   secure 60  
 Falsch-Positiv 64, 72, 202, 237  
 fälschungssicher 70  
 false positive siehe Falsch-Positiv  
 Fehlalarm 65  
 Fehlbedienung 197  
 Fehler 197, 262  
 Fehlercode 203  
 Fehlerinformation 191  
 Fehlermeldung 111, 158, 191, 248  
 Fehlschlag 63  
 fehlschlagen 60  
 Feld 205  
 Fernadministration 189  
 Ferngespräch 22  
 Fernwartung 189  
 Festplatte 82, 193  
 Filter 215, 220  
 Filtermechanismus 103, 105  
 FindBugs 180  
 Fingerabdruck 70, 71, 87  
   Sensor 71  
 Firefox 96, 169, 184  
 Firesheep 153  
 Firewall 50, 62, 63, 104, 159, 189  
   Konfiguration 63  
 Fishing 36  
 Flash 138  
   Plugin 145  
 Fliegen 67  
 Flughafen 68  
 Flugverkehr 67  
 Flugzeugabsturz 67  
 Folgeangriff 189  
 Folgefehler 254  
 Follower 61, 125  
 Forenbetreiber 57  
 Forensic-Team 45  
 Format 249  
 Formular 126, 140, 205, 249, 280  
 formularbasiert 150  
 Fortify 236  
 Forum 36, 57  
 Foto 69, 72  
 Fragezeichen 115  
 Frame 138  
   Hierarchie 146  
 Framebusting 145  
 Frameworks 106  
 Fremdbibliothek 171  
 Fremdsoftware 53  
 Frequenz 22  
 Führerschein 69  
 Funktion 88, 228, 230  
 Funktionalität 63, 187  
 Funktionsaufruf 228  
 Funktionsdefinition 139  
 Funktionstest 197  
 Funktionsweise 200  
 Fun-Virus 25  
 Fuzzer 178, 184

**G**

Garagentoröffner 70  
 Gastbetriebssystem 193

- Gästebücher 57  
 Gegenreaktion 58  
 Gegenstand 72  
 Geheimdienst 39, 40  
   Apparat 39  
 Geheimhaltung 55, 56, 60  
 Geheimhaltungsstrategie 56  
 Geldausgabeautomat 73, 76  
 Gericht 57  
 Geschäftsführung 16  
 Gesicht 70, 72  
 Gesichtserkennung 72  
 GET-Anfrage 137  
 Git 253  
 Glied 61  
 Globalisierung 38  
 Gmail 138  
 GNU Privacy Guard siehe  
   GnuPG  
 GnuPG 98  
 Google 57, 78, 138, 157, 183,  
   188, 198, 199  
   Hacking 157  
   Suchmaschine 113  
 Grauzone 57  
 Gray-Hats 24  
 GreenSQL 105  
 Grey Box Test 217  
 Größerzeichen 134, 281  
 Gruppieren 182  
 Gruyere 198  
 Gültigkeit 56, 69, 136, 154  
 Güter 49, 51, 65
- H**
- Hacker 21, 23, 24, 26, 34, 40,  
 57, 60, 61, 79, 81, 113, 157,  
 163, 170  
   Aktivitäten 30  
   Angriffe 50  
   Community 23, 24  
   Gruppe 22  
   Sprache 163  
   Szene 22  
 Hackers – Im Netz des FBI  
 24  
 HackThisSite 198  
 Halteproblem 177  
 Handlungsbedarf 51, 187  
 Handshake 96
- Hardware 51, 74, 104, 192  
 Hardware-Token 74  
 Härten 193  
 Hash  
   Algorithmus 84  
   Funktion 87  
   Wert 87  
 Hashwert 150  
 Hauptspeicher 193, 256  
 Hausschlüssel 70, 73  
 Header-Element 146  
 Heap 169, 178  
 Helpdesk 65  
   Mitarbeiter 75  
 Hersteller 49, 192, 194  
 Herunterladen 232  
 Heuristik 52  
 hexadezimal 134  
 Hilfsklassen 287  
 Hintertür 32, 63  
 Hinweis 111  
 HMAC 92  
 Hochkomma 108, 116  
 Hochladen 232  
 hostbasiert 104  
 HP 201  
 HQL 119  
 HSQL-Datenbank 256  
 HSQLDB 287  
 HTML 104, 123, 131, 136, 215,  
   227, 281, 282  
   Code 129, 282  
   Element 125, 128, 130  
   Inhalte 132  
   Sprachelement 57  
 HTML-Element-Objekt 128,  
 227  
 HTML-kodiert 251  
 HTML-Kodierung 252  
 HTTP 104, 189, 202, 265  
   Client 129, 138  
   Header-Element 146,  
   205, 216  
   Protokoll 94, 137, 152  
   Proxy 200  
   Status-Code 150  
 HTTP-Anfrage 292  
 HTTPS 94, 151, 189, 202,  
 265  
 HTTPUnit 253, 274
- Hydra 77  
 Hyperlink 57  
 Hyper-V 193
- I**
- IBM PC 24  
 ICMP 104  
 ICQ 32  
 IDEA 91, 257  
 Identifikation 69  
 Identifikationsmerkmal 72  
 Identifikationsnummer 159,  
 161  
 Identifizieren 149  
 Identität 62  
 IDS 104, 186  
 IETF 103  
 IFrame 127, 143  
 IIS 30  
 Image 193  
 Implementierung 85, 200,  
 257  
 Inbetriebsetzung 188  
 Index 180  
 Indikator 160, 281  
 Industriespionage 39  
 Information 112, 157, 159  
 Informationssicherheit 13,  
 55, 57, 60  
 Informationstechnologie 17,  
 50  
 Infrastrukturkomponente  
 257  
 Inhalt 143, 199, 221, 234  
 Injection  
   Schwachstelle 107, 117,  
   119, 132, 203  
 Injection-Angriff 164  
 Input-Tag 281  
 Insert-Statement 249, 287  
 Installation 188, 193  
 Instant-Messaging-Software  
 32  
 Integer 113  
 Integer Overflow 167  
 Integer-Überlauf 171, 203  
 Integrationstest 253, 274  
 Integrität 56  
 Interface 293  
 Interne Anwendung 79, 139

- Internes Netzwerk 63
  - Internet 26, 27, 28, 29, 30, 38, 62, 63, 199
    - Kriminalität 38
    - Krimineller 38
    - Recherche 202
  - Internet Engineering Task Force siehe IETF
  - Internet Explorer 169, 184
  - Internet Information Server siehe IIS
  - Internet Relay Chat siehe IRC
  - Internetcafé 73
  - Intitalisierungsvektor 97
  - Intrusion-Detection-System siehe IDS
  - Intrusion-Prevention-System siehe IPS
  - Intrusion-Prevention-System siehe IPS
  - Investitionen 53, 59
  - IP 104
    - Adresse 30, 43, 62, 76, 104, 176, 189, 200, 201, 265
  - IPS 104, 201
  - IRC 32
  - Iris 70
    - Scanner 72
  - ISO 10646 134
  - ISO 27001 16
  - IT 15, 75, 120
    - Dienstleister 50, 51, 52
    - Infrastruktur 46
    - Sicherheit 50
    - System 11, 194
    - Systeme
  - iTAN 36
  - IT-Grundschutz 16
- J**
- Java 13, 97, 106, 128, 167, 178, 191, 253, 256, 265, 293
    - EE 15
    - IDE 257
    - VM 177
  - Java Native Interface siehe JNI
  - Java-Anwendung 235
  - Java-EE-Dokumentation 220
  - Java-Plugin 138, 145
  - JavaScript 13, 104, 106, 123, 128, 136, 153, 206, 227, 253
    - Bibliothek 132, 218
    - Code 57, 125, 138, 145, 205, 274
    - Implementierung 183
    - Inhalt 130
    - Keylogger 127
    - Teil 232
  - JDBC 115
  - JDBC-Statement 178
  - JMeter 180
  - JNI 167
  - John The Ripper 77
  - JSON 128
    - Bibliothek 135
    - Daten 136
    - Format 129, 230
  - json\_parse 135
  - JSP 163
    - Skript 123, 125, 159, 166, 218, 274
  - JsUnit 253, 257, 274
  - JUnit 253, 255, 274
  - Junk siehe Spam
  - JVM 13
- K**
- Kamera 145
  - Kanäle 206
  - Kanalisierung 62
  - Kartenleser 73
  - Katastrophe 59
  - Kerberos 140
  - Kerckhoffs, Auguste 85
  - Kerckhoffs-Prinzip 85
  - Kette 61
  - Keylogger 41, 127
  - Kind-Prozess 118, 165
  - Klartext 81
  - Klasse 210, 257
  - Klassenpfad 256, 287
  - Kleinerzeichen 134
  - Klick 142
  - Kodierung 97, 132, 239, 249
  - Kodierungsfunktion 134, 282
  - Kodierungslogik 252
  - Kodierungsmechanismus 118
  - Kodierungsvorschrift 90
  - Kollision 88
  - Kollisionsfreiheit 88
  - Kombination 182
  - Kommando 118
  - Kommandozeile 117, 118
  - Kommandozeilenwerkzeug 236
  - Kommentar 109, 120, 130, 234, 259
  - Kommunikation 79, 81, 151, 200
  - Kommunikationsnetzwerk 21
  - Komplexität 63, 199, 250
  - Kompromiss 59, 148
  - Kompromittierung 45
  - Konfiguration 187, 191, 193
  - Konfigurationsdatei 190
  - Konkurrenz 50
  - Konstruktor 287
  - Kontoinformationen 234
  - Kontrolle 63
  - Konvertierung 173
  - Kopierschutz 26
  - Kosten 17, 59, 68, 192
  - Kreditkarten 45, 46, 56
    - Daten 38, 43, 45, 56, 66, 158, 234
    - Gesellschaft 45, 158
    - Informationen 41
    - Nummer 56
  - Kriminelle 21
  - Kristallstruktur 88
  - Kryptoanalyse 60
  - Kryptoanalytiker 85
  - Kryptografie 81
    - Funktionen 97
  - Kryptografisches Token 73
  - Kryptografisches Verfahren 84
  - Kunden 49
  - Kundenwünsche 187
  - Kunststoffleiste 71
  - Kunstwerk 49

**L**

Ländercode 215, 246, 248  
 Länge 282  
 LAPSE 235  
 Lasttest 180  
 Laufzeit 236, 248  
 LDAP 119  
 least knowledge 61  
 Leerstring 265  
 Leerzeichen 249  
 Leistungsfähigkeit 81  
 Lesegerät 73  
 Line Feed 249  
 Link 123, 157, 160, 184, 200  
 Linux 61, 104, 119, 165, 184,  
 194  
 Liste 260  
 Literatur 194  
 Lochkarten 21  
 Log-Datei 191, 254  
 Login  
     Mechanismus 61, 62,  
     63, 234

**M**

MAC 84, 92  
 Mafia 38  
 Magnetstreifen 56, 74  
 Mailbox 25, 26, 27, 30  
 Mail-Filter 138  
 Mailserver 42  
 Make-up 72  
 Management 16  
 Mängel 207  
 Mängelbehebung 207  
 manipuliert 112  
 Marketingabteilung 50  
 Marktanteil 51  
 Marktplatz 38  
 Maschinencode 167  
 Mashup-Seite 134, 138  
 Massenepidemien 30  
 Maßnahme 52, 68  
 Mausinformationen 88  
 Mechanismus 88, 140  
 Mehrdeutigkeiten 185  
 Mehrfachkodierung 132  
 Mehrwert 191  
 MeinVZ 79  
 Meldung 190

Member 249  
 Mercury 253  
 Message Authentication  
     Code siehe MAC  
 Metazeichen 116, 282  
 Methode 163, 215, 227, 257,  
 287  
 Microblogging 125  
     Dienst 57  
 Microsoft Messenger 32  
 Microsoft-Homepage 194  
 Mifare  
     Hack 60  
 Migrationsprojekt 191  
 Mikeyy 57  
 Minimale Angriffsfläche 62  
 Minimum 250  
 Minimum Attack Surface  
     Area siehe Minimale  
     Angriffsfläche  
 Misstrauen 68  
 MIT 22, 93  
 Mitnick, Kevin 23  
 Mobile Endgeräte 148  
 mod\_security 104  
 Modem 25, 26  
 Modul 104  
 Modulo-Funktion 171  
 Monat 113  
 Monitor 145  
 Monty Python's Flying Cir-  
     cus 34  
 Moorsches Gesetz 86  
 Morris, Robert 29  
 Morris-Wurm 29, 30, 167  
 MS-DOS 25  
 MS-SQL-Server 189  
 mTAN 36  
 Müll 76  
 Museum 65  
 Muster 182, 222  
 MySpace 79  
 MySQL 105  
     Datenbank 110, 116  
 mysql\_real\_escape\_string  
     116

**N**

Nachrichten 81  
 Nachrichtenübermittlung 81

National Institute of Stan-  
 dards and Technology sie-  
 he NIST  
 Nebeneffekt 263  
 Nebenwirkungen 198  
 Nessus 193, 201  
 .NET 106, 128, 178, 191  
 Netbeans 257  
 Netbook 83, 145, 168  
 .NET-Runtime 13  
 Netz 63  
 Netzwerk 81, 192, 200  
     Komponente 201  
     Scan 201  
     Scanner 200  
     Segment 176  
     Verkehr 62, 79  
     Zone 62, 63  
 Netzwerkbandbreite 176  
 netzerkbasierend 104  
 Netzwerkverkehr 104, 176  
 Netzwerkzugang 176  
 Neu verschlüsseln 84  
 Neuumplementierung 191  
 Newsgroup 26, 36  
 Nimda 31  
 NIST 88, 91, 194  
 nmap 193, 201  
 Norton Ghost 193  
 Notebook 82, 145, 168  
 Notepad 118  
 Notfall-Patch 254  
 Notfallplan 46, 254  
 NTLM 140  
 NTP-Server 188  
 Nuklearrakete 62  
 NUnit 253, 257  
 Nutzentheorie 47  
 Nutzungsrecht 49  
 Nutzwert 47, 48  
 NXP 60

**O**

Obama, Barack 61  
 Oberflächliche Verteidigung  
     60  
 Objekt 159  
 Objektreferenz 159, 161  
 OFB 91  
 Öffentlicher Schlüssel 92

- Öffentlichkeit 56
  - OK-Button 143
  - ökonomisch 49
  - Onlinebanking
    - Anwendung 41
  - Onlinespiele 26
  - OpenID 78
  - Open-Source 187
    - Anwendung 183
    - Datenbanksystem 180
    - Framework 183
    - Implementierung 155
    - Produkte 191
    - Software 51
  - OpenSSL 61
  - Oracle
    - Datenbank 110, 273
  - Organisation 254
  - Organisierte Kriminalität 38
  - Outlook 97
  - Output Feedback siehe OFB
  - OWASP
    - Foundation 103, 198
    - Guide 155, 194
    - Top Ten 103
- P**
- P2P 42
  - Padding 91
  - Pakistani-Virus 25
  - Panik 52
  - Pantoffelnetzwerk 24
  - Parameter 114
    - Nummer 115
  - Paros 199
  - Password 36
    - Cracker 24
    - Safe 78
    - Sniffing 79
  - Password 56, 64, 65, 70, 75, 77, 78, 82, 109, 138, 149, 152, 157
    - Authentifizierung 75, 80
    - Cracker 163
    - Datei 163
    - Eingabe 76, 152
    - eingabe 77
    - Komplexität 75
    - Sicherheit 75
  - Passwortauthentifizierung
    - 106, 234
  - passwortgeschützt 200
  - Patch 61, 191, 202
    - Management 192
  - Path-Traversal-Schwachstelle 120, 232
  - Path-Traversal-Verwundbarkeit 162
  - PC 82, 168
  - PC siehe auch Personal Computer
  - PCI DSS 45
  - PDP-1 22
  - Peer to Peer siehe P2P
  - Pen Test siehe Penetrationstest
  - Pendant 170
  - Penetration Test siehe Penetrationstest
  - Penetrationstest 205, 217, 241, 285
  - Penetrationstester 205
  - Perfekte Sicherheit 59
  - Perl 13
  - persistent 131
  - Person 56
  - Personal Computer 24
  - Personal Identification
    - Number siehe PIN
  - Personalausweis 69
  - Personenbezogene Daten
    - 43, 45
  - Personengruppe 55
  - Pfad 163, 181, 236
  - Pfadbestandteil 284
  - PGP 98
  - Phisher 37, 42
  - Phishing 36
    - Angriff 166
    - Mail 37, 38, 42, 123, 125, 166
  - PHP 13, 106, 116, 128, 163, 164, 167, 177, 194, 215, 248, 253
    - Interpreter 13
    - Shell 164
    - Skript 236
  - PHPUnit 253, 257
  - Phreaker 22, 23, 26
    - Szene 22
  - PIN 75, 126, 137, 234
    - Eingabe 76
  - Pixy 236
  - Plugin 138, 145
  - Pointer-Operation 172
  - Politikwissenschaft 34
  - Ponemon-Institute 45
  - Port 201
  - POST-Anfrage 138
  - Postleitzahl 216, 249
  - Preibusch, Sören 79, 155
  - Prepared-Statement 114, 216, 263
    - Parameter 249
  - Pretty Good Privacy siehe GPG
  - Prinzipien 58
  - Privater Schlüssel 93
  - Problembhebung 253
  - Problembewusstsein 51
  - Produkt 49, 189, 202, 276
  - Produktivbetrieb 191
  - Produktivsetzung 254
  - Produktivsystem 198
  - Produktivumgebung 253
  - Produktversion 191, 192
  - Profil 125
  - Programm 56, 168
  - Programmbibliothek 181, 183
  - Programmcode 168
  - Programmierbibliothek 192
  - Programmierer 52
  - Programmiersprache 167
  - Prospect-Theorie 47
  - Protection Space siehe Schutzbereich
  - Protokoll 104, 189, 265
  - protokollieren 273
  - Proxy 200
  - Prozentkodierung siehe URL-Kodierung
  - Prozess 168, 177
  - Prozessor 88, 168
  - Prüfen 114
  - Prüfnummer 56
  - Prüfsumme 87, 170

- Pseudo-Verzeichnis 163  
Pseudozufallszahlengenerator 73, 89  
Psychologie 14, 47  
Public Key Infrastructure  
siehe PKI  
Puffer 167  
Grenze 167  
Größe 170  
Pufferüberlauf 30, 167, 203  
Schwachstellen 103  
Python 13, 167
- Q**  
quadratisch 182  
Qualitätssicherung 197  
Qualitätssicherungsmaßnahme 171  
Quellcode 133, 163, 207, 215, 217, 222, 253, 254  
Segment 222  
Verwaltung 253, 254  
Quelle 217, 222, 236  
Quellen 194  
Quelltext siehe Quellcode  
Query 115  
Quiz 37
- R**  
Rauschen 88  
Raw-Device 104  
RC4 90  
RDP 62, 189  
Rechenleistung 66  
Rechenoperation 173  
Recherchen 187  
Rechnernetze 21  
Rechtliche Situation 49  
ReDoS-Schwachstelle 180  
Referenz 159, 165, 232  
Regel 239, 249  
Regelsätze 235  
Regierungsorganisationen 43  
Reguläre Ausdrücke 180  
mehrdeutig 182  
Regular-Expression-DoS-Schwachstelle siehe ReDoS-Schwachstelle
- Regular-Expression-Injection-Schwachstelle 186  
Reisepass 69  
Reiter 184  
Rekursion 176  
Relationales Datenbanksystem 107, 189  
Release-Zyklus 191  
Relevanz 103  
Remote Desktop Protocol  
siehe RDP  
Ressource 177, 178  
Return Oriented Programming 170  
Risiko 48, 52, 61, 66  
Router 140, 188, 201  
RSA 93  
Ruby 13, 167  
Ruby on Rails 106  
Rücksprungadresse 169, 170  
rückwärtskompatibel 86  
Rückwärtsreferenz 181  
Rufschaden 41
- S**  
S/MIME 97  
Sachbeschädigung 50  
Salted Hashes 150  
Salt-Wert 150  
Same Origin Policy 138  
Sarbanes-Oxley Act 57  
Scan 217  
Methode 203  
Resultat 201  
Signatur 201  
Scareware 32, 33, 37, 38  
Schadcode siehe Schadsoftware  
Schaden 49, 154  
Schadroutine 30  
Schadsoftware 24, 25, 29, 30, 40, 64, 66, 74, 83, 125, 131  
Schattenwirtschaft 38  
Schäuble 71  
Schloss 73  
Schlüssel 61  
Anhänger 73  
Länge 86  
Paar 93  
Schneier, Bruce 65, 66
- Schutz 55  
Schutzbereich 151  
Schwachstellen 12, 24, 29, 34, 50, 58, 61, 103, 217, 253  
Analyse 205  
Datenbank 202  
Scanner 201  
Schwächstes Glied 61  
Schwarze Bretter 26  
Screenshot 144  
Script-Tag 128, 138, 281  
Secure Shell siehe SSH  
Secure Socket Layer siehe SSL  
Secure-Shell 163, 189  
Security Token siehe Token  
Seed 89  
Segment 168  
Seitenaufruf 146, 292  
Seitenbetreiber 51, 148  
Seiteninhalte 158  
Selbstschutz 66  
Select  
Anweisung 108  
Selenium 253, 274  
Semikolon 108  
Senke 217, 236  
Sensor 71  
serverfault 194  
Serversoftware 192  
Servlet 142, 160, 162, 176, 210, 215, 228, 231, 241, 250, 255  
Session 140, 152, 234  
Hijacking 152  
Management 149, 151, 152  
Mechanismus 151, 232  
Session-Fixation-Angriff 234  
Session-Fixation-Attacke 154  
Session-ID siehe Sitzungsschlüssel  
Shell 117, 188  
Befehle 118  
Kommando 107  
Sicherheit 14, 15, 197  
Sicherheitsanforderungen 152  
Sicherheitsberater 52

- Sicherheitseinstellungen 194
- Sicherheitsexperte 15, 55, 75
- Sicherheitshinweise 194
- Sicherheitskontext 138
- Sicherheitslösung 59
- Sicherheitslücke 24, 197
- Sicherheitslücke siehe Schwachstelle
- Sicherheitsmaßnahme 51, 52, 58, 59, 65, 66, 67
- Sicherheitsmechanismus 36, 63
- Sicherheitsnetz 263
- Sicherheitsniveau 105
- Sicherheits-Patches 254
- Sicherheitspersonal 68
- Sicherheitsprinzipien 65, 187
- Sicherheitsproblem 11, 14, 15, 51, 52, 53, 197, 218, 239
- Sicherheitsprodukt 68
- Sicherheitsssituation 50, 51, 58, 66, 68
- Sicherheitssoftware 50
- Sicherheitspezialist 50
- Sicherheitsstandard 16, 17
- Sicherheitsstrategie 58, 61, 66, 84
- Sicherheitssystem 59, 63
  - aktiv 63
  - passiv 63
- Sicherheitstechnologie 50
- Sicherheitstest 197
- Sicherheitstester 198
- Sicherheitsstheater 66, 105
- Sicherheitsüberlegungen 52
- Sicherheitsüberprüfung 52, 199, 218
- Sicherheits-Update 50
- Sicherheitsvorfall 46
- Sicherheitsvorschrift 16, 68
- Sicherheitswerkzeug 15
- Sicherheitszertifizierung 17
- Signatur 84, 93, 166, 201
- simulieren 52
- Single-Sign-On 80
  - Lösungen 78
  - Mechanismus 139
- Sitzungsdaten 151
- Sitzungsschlüssel 137, 152
- Skript 124, 137, 142, 177
- Skriptsprache 188
- Slammer-Wurm 189
- Slash 165
- Smartcard 73
- Smartphone 73, 82, 145
- Sneakers 24
- Sniffing 153
- SNMP 202
- Snort 104
- Social Engineering 33, 34, 76, 82
- Socket 178
- Software 49, 51, 82, 192
- Softwareaktualisierung 191, 192
- Softwareentwickler 15
- Softwarehersteller 49, 50, 52, 187, 191
- SonicWall 37
- Soziale Netzwerke 14, 57
- Spalten 221
- Spaltenüberschrift 281
- Spam 34, 57, 251
  - Aktivitäten 36
  - Attacken 42
  - Filter 40, 251, 273
  - Mail 34, 35, 42
  - Nachricht 36
  - Sketch 34
  - Versender 42
- Spammer 34, 35, 158, 273
- Spam-Produzent siehe Spammer
- Speicher 168
- Speicherleck 178
- Speichern 149
- Speicherplatz 193
- Speicherung 81
- Speicherzugriff 171
- Spickzettel 75
- Spider 198, 200, 205
  - Lauf 200
- Spiel 188
- Spionage
  - Aktivitäten 39
- Sputnik 28
- Spyware 40
- SpywareProtect2009 33
- SQL 13
  - Abfrage 107
  - Bestandteil 249
  - Code 107, 108, 114, 120, 215, 241
  - Dialekt 273
  - Fragmente 205
  - Funktion 216
  - Operator 110
  - Syntax 109
- SQL-Injection
  - Schwachstelle 107, 120
- SQL-Injection-Angriff 218, 241
- SQL-Injection-Schwachstelle 206, 215, 216, 217, 248
- sqlmap 110
- SQL-Slammer 31
- SSH 62
- SSL 74, 79, 127, 132
  - Protokoll 94
  - Protokollversionen 96
- Stack 168
- Standardeinstellungen 188
- Standardisierung 193
- Standardkonfiguration 187
- Standardkonformität 15
- Stapel 168, 177
  - Überlauf 178
- Stapelgrenze 168
- Startwert 89
- Status-Code siehe HTTP-Status-Code
- Statuszeile 216
- Stellenanzahl 171
- Steuerungsserver 32
- Steuerzeichen 249, 265, 282
- Stillstand 180
- Stillstandszeit 192
- Stored Procedure 218
- Stromchiffre 90
- Studie 79, 155
- Style-Anweisung 147
- Style-Eigenschaft 147
- Subnetz 200
- Suchbegriff 157
- Suche 235
- Suchmaschine 57, 157, 183, 188, 199
- Suchmechanismus 234

- Suchmuster 227, 276, 282  
Suchoperator 157  
Suchoperatoren 199  
Support-Mitarbeiter 125  
SVN 253  
System 55, 61, 62, 187  
    Administrator 16, 52,  
        193, 194  
    Ebene 168  
    Funktion 171  
    Partition 193  
    Tabelle III, 281
- T**  
Tabelle III, II2, 180, 222,  
    230, 252, 256, 259  
Tabelleninhalt 281  
Tabellenname II2  
Tag 137  
TAN 36  
Tarnung 143  
Task-Manager 184  
Tastatur 88  
Tastendruck 127  
Tasteneignis 127  
Täuschung 33, 34, 68, 123,  
    166  
Täuschungsmanöver 76, 77  
TCP/IP 104  
Tech Model Railroad Club  
    22  
Technik 14  
Teile und herrsche 63  
Teilsystem 61  
Telebanking 66  
Telefonhörer 26  
Telefonnetz 21, 22, 26  
Telefonsystem 22  
Telnet 189  
Terminal 22  
Terroranschlag 67  
Tesafilm 71  
Test 197, 257  
    Daten 260  
    Double siehe Testimp-  
        lementierung  
    Implementierung 257,  
        293  
    Methode 53, 198  
    Runner 257
- System 192  
Umgebung 198, 253,  
    254, 259  
Verfahren 197  
Werkzeug 274  
Tester 197, 205  
Text 280  
    Nachrichten 90  
    Segment 168  
Theorie 82  
Thread 176  
Thunderbird 97  
Ticket  
    System 60  
Tiefgreifende Verteidigung  
    60  
Time-Sharing 22  
Tippfehler 197  
Titanic 59  
TJX 46  
TLS siehe SSL  
Token 70, 72, 140  
Tomcat 151, 188  
Totalausfall 192  
Trainingsseite 198  
Trainingswerkzeug 198  
Transaktionsnummer siehe  
    TAN  
Transport Layer Security sie-  
    he SSL  
Trap-Funktion 215  
Trennung 63  
Trojaner 32  
Trustworthy Computing Ini-  
    tiative 50  
TSL  
    Protokoll siehe SSL  
Tunnel 94  
Twitter 57, 61, 62, 78, 125  
Two Factor Authentication  
    siehe Zwei-Faktor-  
    Authentifizierung  
Twofish 91
- U**  
Überprüfen 113  
Überprüfung 161  
übertragbar 69  
Überwachung 62  
Überzug 71
- U-Boot 61  
UDP 104  
UI-Redressing siehe Clickja-  
    cking  
Umgebung 187  
Umwandeln 113, 114  
Umwandlung 220, 239  
Unachtsamkeiten 197  
Unfälle 50  
Unicode-Steuerzeichen 249  
Unicode-Zeichen 249  
union 110  
Unit Test 186, 253, 274, 294  
Unix 119, 184  
    Derivate 165  
Untergrundaktivitäten 23  
Unternehmensdaten 57  
Unternehmenserfolg 51  
Unterprogramm 169  
Update-Statement 287  
Upgrade 191  
Upload-Mechanismus 164  
Urheber 40  
URL 152, 153, 157, 166, 222,  
    265, 284  
    kodierte 127, 216  
    Kodierung 123  
Ursache 254  
USB-Stick 40
- V**  
validieren 239  
Validierung 180, 239  
Validierungsfunktion 206  
Variable 221, 228  
VB.NET 191  
Veranstaltung 69  
Verantwortung 158  
Verarbeitung 217, 221, 224  
Verarbeitungsdauer 181  
Verdacht 222  
Vereinigung 110  
Verfahren 65, 218  
Verfügbarkeit 59  
Verhalten 256  
Verhindern 136  
Verkehrsunfall 67  
Vermittler 139  
Vernetzung 81  
Vernunft 52

- Veröffentlichen 158  
 Verschleierung 60, 85  
 Verschleierungstaktik 77, 189  
 Verschlüsseln 79  
 Verschlüsselung 60, 81  
 Verschlüsselungsmechanismus 60  
 Verschlüsselungsverfahren 60  
     asymmetrisch 90, 92  
     symmetrisch 90  
 Version 158, 189, 202  
 Versionsnummer 202, 281  
 Verteidiger 62  
 Verteidigungslinie 60, 105  
 Verteidigungsstrategie 66  
 Verträge 52  
 Verwaltung 151  
 Verwundbarkeit 22, 63  
 Verzeichnis 162  
 Verzeichnispfad 165  
 Videotext 27  
 Vier-Augen-Prinzip 61  
 VIP 70  
     Loge 70  
 Viren 25, 27  
     Befall 32  
     Scanner 33, 37, 50, 64, 65, 105, 171, 203  
 Virtual Private Network  
     siehe VPN  
 Virtualisierungstechnik 192  
 Virus 24, 25, 83, 167  
 Virus Construction Kit 25  
 VISA 46  
 Visual Basic 191  
 VMWare 193  
 VNC 189  
 Volltextsuche 157  
 Vollversion 37  
 VPN 189  
  
**W**  
 Wachpersonal 65  
 WAF 104, 120, 132, 162, 180, 186, 205  
 WAN 25  
 Warez 27  
 WarGames 23  
 Wärmeentwicklung 88  
 Warnmeldung 64  
 Wartezeit 175  
 Wartungszugang 79, 164  
 WASC 103  
 Weakest Link siehe  
     Schwächstes Glied  
 Web Application Firewall  
     siehe WAF  
 Web Application Security  
     Consortium siehe WASC  
 Webanwendung 103, 217  
 Webapplikation 11, 12, 13, 14, 58, 106, 107, 253  
 Webauftritt 165  
 Webbenutzer 165  
 Webbrowser siehe Browser  
 Web-Crawler siehe Web-Spider  
 Webdesigner 132  
 Webentwicklung 15  
 Web-Framework 140, 192  
 WebGoat 198  
 Web-IDS 105  
 Weblog siehe Blog  
 Weboberflächen 140  
 Webpräsenz 147  
 Web-Proxy 147  
 WebScarab 199  
 Webseite 41, 42, 51, 137, 143, 199  
 Webseitenbetreiber 57, 132, 157  
 Webserver 22, 41, 104, 188, 200  
 Webservice 120  
 Web-Spider 158, 199  
 Webtechnologien 106  
 Weiterleitung 165, 166  
 Weiterleitungsmechanismus 166  
 WEP-Protokoll 90  
 Werbebotschaft 57  
 Werbe-E-Mail 34  
 Werbung 158  
 Werkzeug 197, 205  
 Wertebereich 171  
 Wettbewerb 88  
 Wettbewerbssituation 58  
 Wettbewerbsvorteil 50  
 White Box Test 217  
 White-Hats 24  
 White-Listing 166  
 Wiederholung 182, 185  
 Wiki 36, 57  
 Windows 184, 193, 194  
 Windows NT 30  
 Wirtschaft 14  
 Wirtschaftswissenschaften 47  
 Wirtsrechner 30  
 Wirtssystem 30  
 Wissenschaftler 81  
 WLAN 79, 81, 153  
 WLAN-Treiber 188  
 World Wide Web 31  
 Worldcom 57  
 Wörterbuchattacke 77, 234  
 Wurm 29, 30, 57, 83, 167  
  
**X**  
 XEN 193  
 Xerox 25  
 X-FRAME-OPTIONS 146  
 XHR 138, 228  
 XHR siehe HTTP-Client  
 XING 79  
 XML 104, 119, 128  
     Firewall 180, 186  
 XML-Firewall 105, 120, 164  
 XPath 119  
 XQuery 119  
 XSS siehe Cross-Site-Scripting  
 XSS-Schwachstelle siehe  
     Cross-Site-Scripting-Schwachstelle  
  
**Y**  
 Yahoo 78  
 YouTube 112  
  
**Z**  
 Zahlencode 70, 87  
 Zahlendarstellung 173  
 Zahlenfolge 89  
 Zähler 241  
 Zahlungsbestätigung 143

- Zeichenkette 181  
Zeilenumbruch 249  
Zeitfenster 56  
Zertifikat 74  
Zertifizierung siehe Sicherheitszertifizierung  
Zertifizierungsstelle 94, 154  
Zeus 32  
Zielformat 239  
Ziel-URL 166  
Zombie 32, 175
- Zombie-Rechner 30  
Zufall 89  
Zufallszahl 150  
Zufallszahlengenerator 84, 88, 153  
Zugang 55, 61, 62, 76, 78, 189  
Zugangsdaten 61, 66, 76, 78, 79, 127, 131, 137, 142, 151, 152, 188
- Zugangsmechanismus 56, 64, 149  
Zugriff 58  
Zugriffsfehler 171  
Zugriffsverfahren 120  
Zurücksetzen 65, 79  
Zusammensetzen 115  
Zuse, Konrad 21  
Zuständigkeitsproblem 218  
Zwei-Faktor-Authentifizierung 70, 79, 154, 189