

# **Faszination Cybercrime**

Das umfassende  
Cybercrime & -security  
Kompendium

Band 1

A bis O



Copyright: 2024

Klaus-Peter Baumdick  
c/o COCENTER  
Koppoldstr. 1  
86551 Aichach

Text:

Libreoffice Writer 7.3.4.2

Coverdesign:

Klaus-Peter Baumdick

Grafik:

aitubo.ai

Erste Auflage

ISBN:

978-3-384-27289-8





# Inhaltsverzeichnis

|                                           |    |
|-------------------------------------------|----|
| Verzeihung.....                           | 19 |
| Cybercrime & -security – Ein Vorwort..... | 21 |
| Disclaimer.....                           | 29 |
| 16Shop.....                               | 31 |
| 2600.....                                 | 34 |
| Acid Rain.....                            | 34 |
| Acrylic WiFi.....                         | 37 |
| Acunetix.....                             | 40 |
| Ad Fraud.....                             | 44 |
| Adobe Angriff.....                        | 46 |
| Adrian Lamo.....                          | 47 |
| Advanced IP Scanner.....                  | 49 |
| Advanced Persistent Threats (APTs).....   | 51 |
| Advanced Threat Protection.....           | 54 |
| AIDE.....                                 | 57 |
| Aircrack-ng.....                          | 60 |
| Airgeddon.....                            | 61 |
| AiTM Angriffe.....                        | 61 |
| Albert Gonzalez.....                      | 62 |
| Amap.....                                 | 64 |
| AndroRAT.....                             | 64 |
| Angriffserkennungssysteme.....            | 66 |
| Angriffsvektoren.....                     | 68 |
| Angry IP Scanner.....                     | 68 |
| Anomali.....                              | 71 |
| Anomalieerkennung.....                    | 72 |
| Anonsurf.....                             | 75 |
| Anonymous.....                            | 78 |
| Anthem Hack.....                          | 79 |
| Antiviren Software.....                   | 81 |
| Apache Struts-Sicherheitslücke.....       | 81 |
| APKTool.....                              | 83 |

|                                            |     |
|--------------------------------------------|-----|
| Application Security.....                  | 85  |
| Approved Scanning Vendor.....              | 88  |
| APT1 (Unit 61398).....                     | 91  |
| APT28 (Fancy Bear).....                    | 92  |
| APT29 (The Dukes).....                     | 93  |
| APT33.....                                 | 94  |
| APT41.....                                 | 95  |
| ARP-Spoofing.....                          | 96  |
| Ashley Madison Hack.....                   | 98  |
| Attack Trees.....                          | 100 |
| Aurora Angriff von 2009.....               | 103 |
| Aurora Hacks von 2011.....                 | 103 |
| Authentifizierungstechnologien.....        | 104 |
| Automobile hacken.....                     | 106 |
| Autopsy.....                               | 111 |
| Avalanche Botnet.....                      | 114 |
| Ave Maria Rat.....                         | 116 |
| Awareness-Schulungen.....                  | 118 |
| Ayyıldız Tim.....                          | 120 |
| BackOrifice.....                           | 120 |
| BadUSB.....                                | 122 |
| Barnaby Jack.....                          | 123 |
| Bedrohungsanalyse.....                     | 125 |
| Bedrohungsmodellierung.....                | 130 |
| BeEf (Browser Exploitation Framework)..... | 133 |
| BEEFHooked.....                            | 135 |
| Bernstein-Breaking.....                    | 138 |
| Betrug.....                                | 139 |
| BGP-Angriffe.....                          | 141 |
| BigFish.....                               | 148 |
| Biometrie.....                             | 148 |
| BitPaymer.....                             | 150 |
| Black Hat Hacker.....                      | 151 |
| BlackEnergy.....                           | 152 |

|                                   |     |
|-----------------------------------|-----|
| BlackShades.....                  | 154 |
| Blockchain.....                   | 155 |
| BlueBorne.....                    | 161 |
| Bluejacking.....                  | 162 |
| Bluesnarfing.....                 | 163 |
| BLUFFS.....                       | 165 |
| BMW i3 Hack.....                  | 168 |
| BO2k.....                         | 169 |
| Botnets.....                      | 171 |
| BPDU Flooding.....                | 173 |
| BPDU Manipulation.....            | 177 |
| Brain Virus.....                  | 184 |
| BredoLab.....                     | 185 |
| British Airways Hack.....         | 187 |
| Browser-Sicherheit.....           | 189 |
| Brute Force.....                  | 191 |
| Brutus.....                       | 196 |
| Bumblebee.....                    | 197 |
| Burp Suite.....                   | 199 |
| Business Continuity Planning..... | 201 |
| BYOD-Sicherheit.....              | 203 |
| Cain and Abel.....                | 205 |
| Carbanak.....                     | 207 |
| Cash-Trapping.....                | 208 |
| Cdorked.....                      | 209 |
| CeWL.....                         | 211 |
| Chaos Computer Club (CCC).....    | 213 |
| Chris Tarnovsky.....              | 214 |
| Ciphey.....                       | 214 |
| CISA.....                         | 217 |
| Clickfraud.....                   | 220 |
| Clickjacking.....                 | 222 |
| Cloud Security.....               | 223 |
| Cobalt Strike.....                | 226 |

|                                              |     |
|----------------------------------------------|-----|
| Code Injection.....                          | 227 |
| Code-Analysen.....                           | 229 |
| Code-Red-Wurm.....                           | 231 |
| CommView.....                                | 231 |
| Compliance.....                              | 233 |
| Condor.....                                  | 236 |
| Content Security Police.....                 | 237 |
| Conti.....                                   | 240 |
| Cookie Theft.....                            | 242 |
| Credential Dumping.....                      | 243 |
| Credential Harvester Attack Method.....      | 244 |
| Credential Harvesting.....                   | 246 |
| Credential Phishing.....                     | 248 |
| Credential Stuffing.....                     | 250 |
| Crimson Tide.....                            | 251 |
| Cross-Site Request Forgery (CSRF).....       | 251 |
| Crowbar.....                                 | 253 |
| Cryptographie (Kryptographie).....           | 255 |
| Cryptojacking.....                           | 260 |
| CSIRT.....                                   | 261 |
| Cuckoo Sandbox.....                          | 264 |
| Cult of the Dead Cow.....                    | 265 |
| Cyber Terrorists.....                        | 266 |
| Cyber-Sabotage.....                          | 268 |
| Cyber-Spionage.....                          | 270 |
| Cyberabwehr (Abwehr von Cyberangriffen)..... | 272 |
| Cyberangriffe.....                           | 275 |
| Cyberbedrohungen.....                        | 276 |
| Cyberhygiene.....                            | 279 |
| Cyberkriminalität.....                       | 280 |
| Cybersecurity Consultants.....               | 282 |
| Cybersicherheitsrichtlinien.....             | 286 |
| Cyberwarfare (Cyberkriegsführung).....       | 288 |
| DarkHotel.....                               | 291 |

|                                           |     |
|-------------------------------------------|-----|
| Darknet.....                              | 292 |
| DarkTequila.....                          | 294 |
| Data Exfiltration.....                    | 295 |
| Data Manipulation.....                    | 298 |
| Dateeinschluss-Schwachstellen.....        | 300 |
| Datendiebstahl.....                       | 306 |
| Datenschutz-Folgenabschätzung (DSFA)..... | 308 |
| Datenschutz.....                          | 310 |
| Datenschutzgrundverordnung.....           | 313 |
| DCSync-Angriff.....                       | 317 |
| DDoS Angriffe.....                        | 318 |
| Deep Web.....                             | 320 |
| DEF CON.....                              | 321 |
| Denial-of-Service (DoS).....              | 323 |
| Diavol.....                               | 325 |
| Digitale Forensik.....                    | 327 |
| DirBuster.....                            | 328 |
| DKIM.....                                 | 331 |
| DLL Injection.....                        | 333 |
| DMARC.....                                | 334 |
| DNS Amplification Attack.....             | 336 |
| DNS Tunneling.....                        | 337 |
| DNS-Hijacking.....                        | 339 |
| DNS-Spoofing.....                         | 340 |
| Domain Hijacking.....                     | 342 |
| DoublePulsar.....                         | 344 |
| Dragonfly.....                            | 345 |
| DREAD.....                                | 348 |
| Dridex.....                               | 353 |
| Drive-by-Downloads.....                   | 354 |
| dsniff.....                               | 356 |
| dSploit.....                              | 358 |
| Dumpster Diving.....                      | 360 |
| Duqu.....                                 | 363 |

|                                         |     |
|-----------------------------------------|-----|
| E-Mail-Phishing.....                    | 365 |
| Eavesdropping.....                      | 367 |
| Ebury.....                              | 369 |
| Email Security (E-Mail-Sicherheit)..... | 370 |
| Emergency Response.....                 | 371 |
| Empire.....                             | 374 |
| Encryption.....                         | 376 |
| Encryption Key Management.....          | 379 |
| Endpoint Security.....                  | 381 |
| ENISA.....                              | 383 |
| Equifax-Datenleck.....                  | 386 |
| EternalBlue.....                        | 388 |
| EternalRomance.....                     | 389 |
| Ethical Hacking.....                    | 390 |
| Ettercap.....                           | 392 |
| Event Logging.....                      | 394 |
| Evil Corp.....                          | 396 |
| Evil Twin-Angriff.....                  | 397 |
| EvilGinx2.....                          | 399 |
| Exploit.....                            | 401 |
| Exploit-Kits.....                       | 403 |
| ExploitDB.....                          | 405 |
| Fancy Bear.....                         | 406 |
| Fern Wifi Cracker.....                  | 407 |
| File Integrity Monitoring.....          | 408 |
| Fileless Malware.....                   | 410 |
| FIN7.....                               | 412 |
| Firewall-Management.....                | 413 |
| Firmware Hacking.....                   | 415 |
| Firmware-Angriff.....                   | 417 |
| Firmware-Sicherheit.....                | 419 |
| Flame.....                              | 420 |
| Fluxion.....                            | 423 |
| Forensische Analyse.....                | 424 |

|                                    |     |
|------------------------------------|-----|
| Formjacking.....                   | 426 |
| Fping.....                         | 427 |
| Fraud Detection.....               | 429 |
| FTK Imager.....                    | 431 |
| Fuzzdb.....                        | 434 |
| Fuzzing.....                       | 437 |
| Gary McKinnon.....                 | 438 |
| Gefahrenabwehr.....                | 439 |
| Gefahrenanalyse.....               | 442 |
| Geheime Schlüssel.....             | 443 |
| Geldkarten.....                    | 444 |
| Generierung von Zufallszahlen..... | 446 |
| Geräteverwaltung.....              | 448 |
| Geschäftsprozesskontrolle.....     | 450 |
| Ghidra.....                        | 452 |
| Ghost Phisher.....                 | 455 |
| Google Dorks.....                  | 458 |
| Gophish.....                       | 461 |
| Governance.....                    | 463 |
| GPS Hacking.....                   | 465 |
| Gray Hat Hacker.....               | 467 |
| Gruppenrichtlinien.....            | 469 |
| GSM Spoofing.....                  | 470 |
| GSM-Jamming.....                   | 472 |
| Hacker.....                        | 473 |
| Hackerethik.....                   | 476 |
| Hacktivists.....                   | 478 |
| Hardware-Sicherheit.....           | 480 |
| Hash Identifier.....               | 482 |
| Hashcat.....                       | 483 |
| Hashfunktionen.....                | 485 |
| Hashpump.....                      | 487 |
| Havij.....                         | 490 |
| Heartbleed.....                    | 491 |

|                                           |     |
|-------------------------------------------|-----|
| Heuristische Analyse.....                 | 492 |
| HIPAA.....                                | 494 |
| HOIC (High Orbit Ion Cannon).....         | 498 |
| Honeypot.....                             | 499 |
| Host-basierte Sicherheit.....             | 502 |
| Hping.....                                | 504 |
| HTML Smuggling.....                       | 506 |
| HTTP Flooding.....                        | 507 |
| Hulk.....                                 | 509 |
| Human Factors in Cybersecurity.....       | 510 |
| Hybrid Cloud Security.....                | 511 |
| Hydra.....                                | 512 |
| I2P.....                                  | 514 |
| IAM.....                                  | 515 |
| IcedID.....                               | 518 |
| Ich bin James Bond.....                   | 520 |
| ICMP Flooding.....                        | 525 |
| Ida Pro.....                              | 527 |
| Identitätsdiebstahl.....                  | 529 |
| Immunity Debugger.....                    | 531 |
| Impacket.....                             | 533 |
| Incident Response.....                    | 535 |
| Informationsbeschaffung durch Hacker..... | 538 |
| Informationsbeschaffung.....              | 541 |
| Insider-Bedrohung.....                    | 545 |
| InSSIDer.....                             | 546 |
| Intrusion Detection Systems (IDS).....    | 550 |
| IoT Device Compromise.....                | 552 |
| IoT.....                                  | 553 |
| IP Spoofing.....                          | 555 |
| IVRE.....                                 | 557 |
| ISO 27001 und 270xx Familie.....          | 560 |
| Jackpotting.....                          | 570 |
| Java Applet Attack Method.....            | 573 |

|                                                    |     |
|----------------------------------------------------|-----|
| Java Security.....                                 | 575 |
| JavaScript Security.....                           | 577 |
| Jeep Cherokee Hack.....                            | 579 |
| Jeff Moss.....                                     | 580 |
| John Draper.....                                   | 581 |
| John the ripper.....                               | 581 |
| Jonathan James.....                                | 583 |
| JSON Security.....                                 | 584 |
| Kali Linux.....                                    | 586 |
| Kerberos-Angriff.....                              | 587 |
| Kerberos-Tickets.....                              | 589 |
| Kerberos.....                                      | 591 |
| Kernel Security.....                               | 593 |
| Kevin Poulsen.....                                 | 594 |
| Key Management.....                                | 595 |
| Keylogging.....                                    | 597 |
| Kill Chain.....                                    | 599 |
| Kim Schmitz.....                                   | 601 |
| Kingpin.....                                       | 603 |
| Kismet.....                                        | 603 |
| Known Vulnerabilities.....                         | 605 |
| Krack.....                                         | 606 |
| KRITIS.....                                        | 608 |
| L0pht Heavy Industries.....                        | 608 |
| L0phtCrack.....                                    | 610 |
| Lastenausgleich.....                               | 612 |
| Lateral Movement.....                              | 614 |
| Layered Security.....                              | 615 |
| Least Privilege.....                               | 617 |
| Leckage von Informationen.....                     | 619 |
| Legal Compliance.....                              | 620 |
| Lifecycle-Management von Sicherheitsprodukten..... | 622 |
| LINDDUN.....                                       | 624 |
| Lizard Squad.....                                  | 629 |

|                                                 |     |
|-------------------------------------------------|-----|
| Log-Management.....                             | 630 |
| Logic Bomb.....                                 | 631 |
| LOIC (Low Orbit Ion Cannon).....                | 633 |
| Löschung von Daten.....                         | 634 |
| LSASS-Dumping.....                              | 635 |
| Lynis.....                                      | 637 |
| Machine Learning in Cybersecurity.....          | 639 |
| Magecart.....                                   | 641 |
| Mailbomben.....                                 | 643 |
| Make money fast.....                            | 644 |
| Maltego.....                                    | 645 |
| Malvertising.....                               | 648 |
| Malware-Analyse.....                            | 649 |
| Malware-as-a-Service (MaaS).....                | 651 |
| Malware.....                                    | 653 |
| Man-in-the-Browser (MitB).....                  | 655 |
| Man-in-the-Middle-Angriff (MitM).....           | 656 |
| Managed Security Service Provider.....          | 658 |
| Mandiant.....                                   | 661 |
| Mark Abene.....                                 | 662 |
| Maskprocessor.....                              | 663 |
| Masscan.....                                    | 667 |
| Medusa.....                                     | 669 |
| Memory Corruption.....                          | 670 |
| Memory-Dumping.....                             | 672 |
| Metadaten-Sicherheit.....                       | 675 |
| Metagoofil.....                                 | 676 |
| Metasploit Browser Exploit Method.....          | 678 |
| Metasploit.....                                 | 680 |
| Meterpreter.....                                | 684 |
| Mimikatz.....                                   | 687 |
| Mirai Botnet.....                               | 688 |
| Mitarbeiter-Schulung und -Sensibilisierung..... | 689 |
| MITRE ATT&CK.....                               | 690 |

|                                                 |     |
|-------------------------------------------------|-----|
| Mobbing.....                                    | 693 |
| Mobile Device Management (MDM).....             | 694 |
| Mobile Sicherheit.....                          | 695 |
| Multi-Faktor-Authentifizierung (MFA).....       | 696 |
| Nation-State Hacker.....                        | 698 |
| Nationale Cybersicherheitsstrategien.....       | 700 |
| Nessus.....                                     | 701 |
| NetStumbler.....                                | 703 |
| Netzwerkforensik.....                           | 706 |
| Netzwerkintrusionserkennungssysteme (NIDS)..... | 708 |
| Netzwerksegmentierung.....                      | 710 |
| Netzwerksicherheit.....                         | 713 |
| Netzwerksicherheitsrichtlinien.....             | 714 |
| Neue Bedrohungen in der Cybersicherheit.....    | 717 |
| Next-Generation Firewalls.....                  | 718 |
| NFC Angriff.....                                | 720 |
| NFC Scanner.....                                | 721 |
| Ngrep.....                                      | 724 |
| Nikto.....                                      | 726 |
| NIS2.....                                       | 727 |
| NIST Cybersecurity Framework.....               | 730 |
| nmap.....                                       | 732 |
| Notfallmanagement in der Cybersicherheit.....   | 734 |
| NotPetya.....                                   | 735 |
| Obfuscation Techniques.....                     | 737 |
| Offensive Cybersicherheit.....                  | 739 |
| OllyDbg.....                                    | 741 |
| On-Demand Security.....                         | 743 |
| Online Privacy (Online-Datenschutz).....        | 745 |
| Open Source Security.....                       | 747 |
| OpenVAS.....                                    | 749 |
| Operating System Security.....                  | 751 |
| Operation Aurora.....                           | 753 |
| Operation Blackout 2015.....                    | 755 |

|                                      |     |
|--------------------------------------|-----|
| Operation Ghost Secret.....          | 757 |
| Operation Pawn Storm.....            | 759 |
| Operation Tovar (GameOver Zeus)..... | 761 |
| Operation Windigo.....               | 763 |
| Operational Technology Security..... | 766 |
| Ophcrack.....                        | 767 |
| Organisationale Cybersicherheit..... | 768 |
| OSSEC.....                           | 770 |
| Outsourcing der Cybersicherheit..... | 774 |
| Over-the-air Security.....           | 777 |
| OWASP ZAP (Zed Attack Proxy).....    | 779 |

# Verzeihung

Als junger Computerhacker tat ich mehr als einmal Prof. Dr. Klaus Brunnstein Unrecht, weil ich als Black Hat Hacker mit Anfang 20 seinen Gedanken auf meine Weise folgte und nicht in der Weise, wie er es gemeint hatte.

Prof. Dr. Klaus Brunnstein galt als erster Informatiker von akademischem Rang in Deutschland, der es in den frühen 1980er Jahren zu seiner Mission machte, den Datenschutz und die Sicherheit der Informationstechnologie in die öffentliche Diskussion zu bringen.

Dadurch lag es in der Natur an sich, dass wir verschiedener Meinung waren und wir sind mehr als einmal böse aneinander gerasselt.

Heute bin ich über 50, habe mehr als 30 Jahre in der Computersicherheit, aber auch in der Computerkriminalität hinter mir, bin seit mehr als 10 Jahren politisch interessiert und aktiv und kann jetzt erst seine Gedanken nachvollziehen.

Leider kann meine Entschuldigung Prof. Dr. Brunnstein nicht mehr erreichen, denn er verstarb schon vor fast auf den Tag dieser Niederschrift genau vor 9 Jahren, am 19. Mai 2015.

Trotzdem sage ich, es tut mir leid. Ich konnte damals Ihre Gedanken nicht erkennen. Das ist heute anders, Sie haben in vielem, was Sie mir gesagt haben, recht gehabt.



# Cybercrime & -security – Ein Vorwort

Die Stelleninserate sind voll mit tollen Angeboten für Quereinsteiger im Bereich Cybersecurity. Gerade eben habe ich wieder Werbung bekommen von einer Firma, die mir gleich anbietet, ich könne einen Ausbildungsschein vom Arbeitsamt bekommen und dann bei denen Hacker werden. Ein kurzer Check und ich bin von der Firmenlocation begeistert. Es ist eine Imbissbude namens Chicken & More. Ich schäme mich für diesen Laden. Denn machen wir uns mal nichts vor, da draußen tobt ein Krieg. Und da sollen es jetzt arbeitslose Webdesignerassistenten und erfolglose Influencer mit ein paar Monaten Grundausbildung in Cybersecurity mit den Besten der Besten der Welt aufnehmen? Das ist absolut lächerlich. Wenn ich die Inserate lese und sehe die Aufgaben, die diese arbeitslosen Arbeitslosenassistenten bald übernehmen sollen, dann sehe ich, dass auch die Chefs von diesen Cybersecurity Consultants in spe nicht den Hauch einer Ahnung haben. Penetrationstests, SIEM und ISO 27001 sind die Schlagworte, die tonnenweise ins Rennen geschickt werden. Als Penetrationstest versteht man Angriffe auf das eigene System zur Feststellung, ob Sicherheitslücken vorhanden sind. Ja, ok, das kann man machen und es macht auch Sinn. Zumindest zur Abwehr von Botnets, Viren und Trojanern. Doch kaum ein Hacker, der etwas auf sich hält, greift ein Netzwerk frontal an. Weil es im Regelfall einfach sinnlos ist. Um in Netzwerke einzudringen, kommt man von innen. Sozusagen wie ein Krebsgeschwür, welches sich von in-