**Informationssicherheit – IT-Security**

**Glossar – Glossary**



**Inhaltsverzeichnis / Table of Contents**

1 Scope 4

1.1 Identification 4

1.2 Overview 4

1.3 Document Overview 4

2 Definitions 5

3 Abbreviations 6

**Abbildungsverzeichnis / List of Figures**

[Figure 4‑1 text 2 3](#_Toc465690028)

**Tabellenverzeichnis / List of Tables**

[Table 2‑1: Referenced Documents 3](#_Toc465690029)

[Table 4‑1 text 3](#_Toc465690030)

# Scope

## Identification

This document contains a collection of definitions and abbreviations that can be found in the area of IT security.

## Overview

…

## Document Overview

The content of this document is divided into the following chapters:

Chapter 1 Identifies this document

Chapter 2 Contains definitions

Chapter 3 Contains abbreviations

Chapter 4 Lists documents and links to web resources

# Definitions

|  |  |
| --- | --- |
| **Certified Information Systems Security Professional** | Der Certified Information Systems Security Professional (CISSP) ist eine Zertifizierung, die vom International Information Systems Security Certification Consortium, Inc. (auch: (ISC)²) angeboten wird. Es handelt sich bei dem Zertifikat um einen international anerkannten Weiterbildungsstandard auf dem Gebiet Informationssicherheit.  <https://www.isc2.org/Training/Self-Study-Resources> |
| **Classless Inter-Domain Routing** | **Classless Inter-Domain Routing** ([**CIDR**](https://de.wikipedia.org/wiki/Classless_Inter-Domain_Routing)) beschreibt ein Verfahren zur effizienteren Nutzung des bestehenden 32-Bit-[IP-Adress](https://de.wikipedia.org/wiki/IP-Adresse)-Raumes für [IPv4](https://de.wikipedia.org/wiki/IPv4).  Beispiel: 10.43.8.67/28 entspricht der Adresse 10.43.8.67 mit der Netzmaske 255.255.255.240: In [binärer](https://de.wikipedia.org/wiki/Dualsystem) Schreibweise ist die Netzmaske 11111111.11111111.11111111.11110000 – es gibt also 3 · 8 + 4 = 28 gesetzte Bits, wieder genau wie im Suffix angegeben. Das IPv4-Netz, in dem der Host 10.43.8.67 liegt, geht somit von 10.43.8.64 bis 10.43.8.79 und wird kurz als 10.43.8.64/28 notiert, wobei nur 10.43.8.65 bis 10.43.8.78 für Hosts genutzt werden können. Die Broadcast-Adresse ist 10.43.8.79, die Netz-Adresse 10.43.8.64 und das Subnetz kann 14 Hosts adressieren. |
| **Common Body of Knowledge (CBK)** | CISSP – 8 high-level disciplines of any enterprise security program:   * Security and Risk Management * Asset Security * Security Architecture and Engineering * Communication and Network Security * Identity and Access Management * Security Assessment and Testing * Security Operations * Software Development Security |
| **Common Criteria** | The Participants in this Arrangement share the following objectives:   * to ensure that evaluations of Information Technology (IT) products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles; * to improve the availability of evaluated, security-enhanced IT products and protection profiles; * to eliminate the burden of duplicating evaluations of IT products and protection profiles; * to continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation\* process for IT products and protection profiles. |
| **Cookie** | Ein Cookie ist eine Textinformation, die im Browser auf dem Computer des Betrachters jeweils zu einer besuchten Website (Webserver, Server) gespeichert werden kann. Der Cookie wird entweder vom Webserver an den Browser gesendet oder im Browser von einem Skript (JavaScript) erzeugt. Der Webserver kann bei späteren, erneuten Besuchen dieser Seite diese Cookie-Information direkt vom Server aus auslesen oder über ein Skript der Website die Cookie-Information an den Server übertragen.  Name – Value Pairs  [RFC 6265](https://tools.ietf.org/html/rfc6265) |
| **Cyber-Sicherheit** | Unter dem Begriff Cyber-Sicherheit werden alle Maßnahmen der nationalen Cyber-Sicherheitsstrategie für  Deutschland (siehe Bezug Anlage 11.18 (LfdNr. 41)) sowie die in der Enhanced NATO Policy on Cyber Defence (siehe Bezug Anlage 11.18 (LfdNr. 25)) enthaltenen Vorgaben subsumiert.  Aus A 960/1. |
| **DNS spoofing** | … |
| **Distributed Denial-of-Service (DDoS)** | … |
| **DMARC** | Domain-based Message Authentication, Reporting and Conformance (DMARC) ist eine Spezifikation, die entwickelt wurde, um den Missbrauch von E-Mails zu reduzieren, wie er etwa bei Mail-Spoofing vorkommt. |
| **Datenschutz Grundverordnung** | Seit Mai 2018 in Kraft  (siehe https://www.superoffice.ch/service/artikel/was-ist-gdpr/)  GDPR – DSGVO  1. Das Recht auf Zugang  2. Das Recht, vergessen zu werden  3. Das Recht auf Datenportabilität  4. Das Recht informiert zu werden  5. Das Recht, dass Informationen korrigiert werden  6. Das Recht, die Verarbeitung zu beschränken  7. Der Widerspruch  8. Das Recht, benachrichtigt zu werden. |
| **IKT-Minimalstandard** | Framework zum Schutz der IT-Infrastruktur des Bundesamts für wirtschaftliche Landesversorgung BWL.  106 Massnahmen gegliedert nach dem fünf Themenbereichen:   * Identifizieren (Identify) * Schützen (Protect) * Detektieren (Detect) * Reagieren (Respond) * Wiederherstellen (Recover)   Verwendet   * CCS CSC 1 * COBIT 5 * ISA 62443-3:2013 * ISO 27001:2013 * NIST-SP-800-53 Rev. 4 * BSI 100-2 |
| **Informationssicherheits-managementsystem (ISMS)** | Mit PDCA-Lebenszyklus   * Plan - Planung von Sicherheitsmassnahmen * Do - Umsetzung der Massnahmen * Check - Erfolgskontrolle, Überwachung der Zielerreichung * Act - Beseitigung von Defiziten, Verbesserung |
| **Mail-Spoofing** | … |
| **Malware** | wie Viren und Trojaner |
| **Multi-Factor Authentication** | **Multifactor authentication** (MFA) is a security system that requires more than one method of **authentication** from independent categories of credentials to verify the user's identity for a login or other transaction.  Users who enable multi-factor authentication (MFA) for their accounts will end up blocking 99.9% of automated attacks.  <https://www.zdnet.com/article/microsoft-using-multi-factor-authentication-blocks-99-9-of-account-hacks/> |
| **Open Source Intelligence (OSINT)** | Open Source Intelligence ist ein Begriff aus der Welt der Nachrichtendienste, bei dem für die Nachrichtengewinnung Informationen aus frei verfügbaren, offenen Quellen gesammelt werden, um durch Analyse der unterschiedlichen Informationen verwertbare Erkenntnisse zu gewinnen.  [https://osintframework.com](https://osintframework.com/) |
| **PDCA-Lebenszyklus** | … |
| **Ransomware** | Ransom malware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.  Beispiele: WannaCry, Petya (2017) |
| **Red Team** vs. **Blue Team** | See <https://securitytrails.com/blog/cybersecurity-red-blue-team>  **Red teams** are focused on penetration testing of different systems and their levels of security programs. They are there to detect, prevent and eliminate vulnerabilities.  A red team imitates real-world attacks that can hit a company or an organization, and they perform all the necessary steps that attackers would use. By assuming the role of an attacker, they show organizations what could be backdoors or exploitable vulnerabilities that pose a threat to their cybersecurity.  A common practice is to hire someone outside the organization for red teaming — someone equipped with the knowledge to exploit security vulnerabilities, but unaware of the defenses built into the organization’s infrastructure.  A **blue team** is similar to a red team in that it also assesses network security and identifies any possible vulnerabilities.  But what makes a blue team different is that once a red team imitates an attacker and attacks with characteristic tactics and techniques, a blue team is there to find ways to defend, change and re-group defense mechanisms to make incident response much stronger.  Like a red team, a blue team needs to be aware of the same malicious tactics, techniques and procedures in order to build response strategies around them. And blue team activity isn’t exclusive to attacks. They’re continuously involved to strengthen the entire digital security infrastructure, using software like an IDS (intrusion detection system) that provides them with an ongoing analysis of unusual and suspicious activity.  Some of the steps a blue team incorporates are:   * Security audits, such as a DNS audit * Log and memory analysis * pcap * Risk intelligence data analysis * Digital footprint analysis * Reverse engineering * DDoS testing * Developing risk scenarios |
| **Resilienz** | **Resilienz** (von lateinisch resilire „zurückspringen, abprallen“) steht für:  die Fähigkeit von technischen Systemen, bei einem Teilausfall nicht vollständig zu versagen (Ingenieurwissenschaften).  Siehe IKT-Minimalstandard und Wikipedia. |
| **Tracking Pixels** | … |
| **Trojaner** | Ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.  Beispiele: Emotet, Trickbot |
| **Viren** | … |
| **White Hats** | See <https://securitytrails.com/blog/ode-white-hats-ethical-hacking>  There are three kinds of hackers – white hats, gray hats and black hats.  White hats are ethical hackers who find vulnerabilities with authorized access and use them to help people; black hats are malicious hackers who, with unauthorized access, steal and compromise data; and grey hats, who don’t have authorized access but use the information they obtain for a good cause. |
| **Zero-Day-Exploit** | A **Zero-day** (also known as **0-day**) vulnerability is a [computer-software](https://en.wikipedia.org/wiki/Computer_software) [vulnerability](https://en.wikipedia.org/wiki/Vulnerability_(computing)) that is unknown to, or unaddressed by, those who should be interested in mitigating the vulnerability (including the vendor of the target software). Until the vulnerability is mitigated, [hackers](https://en.wikipedia.org/wiki/Hacker) can [exploit](https://en.wikipedia.org/wiki/Exploit_(computer_security)) it to adversely affect computer programs, data, additional computers or a network. An exploit directed at a zero-day is called a **zero-day exploit,** or **zero-day attack.** |

# Abbreviations

The following abbreviations are used:

|  |  |
| --- | --- |
| **A** | |
| ARP | Address Resolution Protocol |
| ASLR | Address Space Layout Randomization |
| ASN.1 | Abstract Syntax Notation One |
| ASP | Application Service Provider |
|  | |
| **B** | |
| BCM | Business Continuity Management |
| BCP | Business Continuity Plan |
| BDSG | Bundesdatenschutzgesetz (D) |
| BEDO DRAM | Burst EDO DRAM |
| BIA | Business Impact Analysis |
| BIOS | Basic Input/Output System (see also coreboot, UEFI) |
| BMVg | Bundesministerium der Verteidigung (D) |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
|  | |
| **C** | |
| CA | Certificate Authority |
| CBK | Common Body of Knowledge (CISSP) |
| CC | Common Criteria |
| CERTBw | Computer Emergency Response Team der Bundeswehr (D) |
| CIA | confidentiality, integrity und availability  (deutsch: Vertraulichkeit, Integrität, Verfügbarkeit) |
| CIDR | Classless Inter-Domain Routing |
| CIO | Chief Information Officer |
| CIS | Center for Internet Security (https://www.cisecurity.org/) |
| CISO | Chief Information Security Officer |
| CISSP | Certified Information Systems Security Professional |
| COBIT | Control Objectives for Information and Related Technology |
| CRL | Certificate Revoke List |
| CSIRT | Computer Security Incident Response Team |
| CSR | … (certificates) |
| CSSL | Cyber Security Service Line (NCI Agency) |
| CVE | Common Vulnerabilities and Exposures |
|  | |
| **D** | |
| DDoS | Distributed Denial-of-Service |
| DDR SDRAM | Double Data Rate SDRAM |
| DMARC | Domain-based Message Authentication, Reporting and Conformance |
| DNS | Domain Name System |
| DoH | DNS-over-HTTPS |
| DoS | Denial-of-Service |
| DRAM | Dynamic RAM |
| DRP | Disaster Recovery Plan |
| DSGVO | Datenschutz Grundverordnung (GDPR) |
|  | |
| **E** |  |
| EDO DRAM | Extended Data Out DRAM |
| EEPROM | Electrically Erasable Programmable ROM |
| EFI | Extensible Firmware Interface (BIOS, UEFI) |
| ENISA | European Union Agency for Network and Information Security |
| EPROM | Erasable Programmable ROM |
|  | |
| **F** | |
| FIRST | Forum of Incident Response and Security Teams |
| FTP | File Transfer Protocol |
|  | |
| **G** | |
| GDPR | General Data Protection Regulation (DSGVO) |
| GPL | GNU General Public License |
| GUI | Graphical User Interface |
|  | |
| **H** | |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
|  | |
| **I** | |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| ICMP | Internet Control Message Protocol |
| ICS | Industrial Control System (NIST, BSI) |
| IDPS | Intrusion Detection and Prevention System |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force (run by nerds) |
| IKT | Informations- und Kommunikationstechnik (CH) |
| IP | Internet Protocol |
| IRC | Internet Relay Chat |
| IS | Informationssicherheit (BSI) |
| ISB | Informationssicherheitsbeauftragter (BSI) |
| (ISC)2 | International Information Systems Security Certification Consortium |
| ISMS | Informationssicherheitsmanagementsystem (BSI) |
| ISO | Inernational Organization for Standardization |
| ISOC | Internet Society |
| ISP | Internet Service Provider |
| IT | Information Technology |
| ITIL | IT Infrastructure Library |
| ITSEC | Information Technology Security Evaluation Criteria  (alt, ersetzt durch Common Criteria) |
| IT-SiBeBw | IT-Sicherheitsbeauftragter der Bundeswehr (D) |
| ITU | International Telecommunication Union |
| IV | [Initialization Vector](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjAlfLlit3mAhWwyqYKHeyOCNYQFjADegQIBhAB&url=https%3A%2F%2Fgerardnico.com%2Fsecurity%2Fkey%2Fiv&usg=AOvVaw1w6Z8aYHTgD10zF1ASH-xS) |
|  | |
| **J** | |
| JS | Java Script |
| JSON | JavaScript Object Notation |
|  | |
| **K** | |
| … | … |
|  | |
| **L** | |
| LAN | Local Area Network |
| LPI | Linux Professional Institute |
| LPIC | Linux Professional Institute Certification |
|  | |
| **M** | |
| MAC | Media Access Control |
| MFA | Multi-Factor Authentication |
| MPTD | Maximum Period Time of Disruption |
| MTD | Maximum Tolerable Downtime |
|  | |
| **N** | |
| NAT | Network Address Translation |
| NCI Agency | NATO Communications and Information Agency |
| NCIRC | NATO Computer Incident Response Capability |
| NDA | Non-Disclosure Agreement |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NTP | Network Time Protocol |
| NVD | National Vulnerability Database |
|  | |
| **O** | |
| OCSP | Online Certificate Status Protocol (certificates, [RFC 6960](https://tools.ietf.org/html/rfc6960)) |
| OS | Operating System |
| OSCP | Offensive Security Certified Professional (Kali) |
| OSINT | Open Source Intelligence |
| OSSTMM | Open Source Security Testing Methodology Manual |
| OWASP | Open Web Application Security Project |
|  | |
| **P** | |
| PAP | Password Authentication Protocol |
| PDCA | Plan – Do – Check – Act (BSI) |
| PIN | Personal Identifiable Information |
| PKI | Public-Key-Infrastructure (Crypto) |
| PROM | Programmable ROM |
| PTES | Penetration Testing  <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines> |
|  | |
| **Q** | |
| … | … |
|  | |
| **R** | |
| RAM | Random Access Memory |
| RFC | Request for Comment |
| ROM | Read-Only Memory |
| RPO | Recovery Point Objective |
| RSA | Rivest, Shamir und Adleman (asymmetrische Verschlüsselungsverfahren) |
| RTO | Recovery Time Objective |
|  | |
| **S** | |
| SaaS | Software-as-a-Service |
| SDL | Secure Development Lifecycle |
| SDRAM | Synchronous DRAM |
| SHA | Secure Hash Algorithm |
| SLA | Service Level Agreement |
| SNMP | Simple Network Management Protocol |
| SOP | Standard Operating Procedure |
| SRAM | Static RAM |
| SSH | Secure Shell |
| SSL | Secure Sockets Layer (neu TLS) |
|  | |
| **T** | |
| TCP/IP | Transmission Control Protocol / Internet Protocol |
| TCSEC | Trusted Computer System Evaluation Criteria (a.k.a. Orange Book) |
| tl;dr | Too long; didn't read. |
| TLS | Transport Layer Security (Verschlüsselungsprotokoll) |
| TPM | Trusted Platform Module |
|  | |
| **U** | |
| UDP | User Datagram Protocol |
| UEFI | Unified Extensible Firmware Interface |
| URL | Uniform Resource Locator |
|  | |
| **V** | |
| VM | Virtual Machine |
| VoIP | Voice Over Internet Protocol |
| VPN | Virtual Private Network |
|  | |
| **W** | |
| WAN | Wide Area Network |
| WLAN | Wireless Local Area Network |
| WSC | World Standards Cooperation |
|  | |
| **X** | |
| XML | Extensible Markup Language |
|  | |
| **Y** | |
| … | … |
|  | |
| **Z** | |
| ZETA | Zero Day Exploit Attack |

# Links

The following links and resources may be useful:

|  |  |
| --- | --- |
| https://www.commoncriteriaportal.org | Common Criteria |
| https://www.osstmm.org | Open Source Security Testing Methodology Manual |
| https://insider.fortscale.com | Fortscale Insider Blog |
| https://www.cisecurity.org/ | Center for Internet Security |
| https://www.isc2.org/ | International Information Systems Security Certification Consortium, Inc. auch: (ISC)², |
| https://www.isc2chapter-germany.org/ |  |
| https://ISECOM.org | Test Lab |
| https://www.hackerhighschool.org | Tutorial |
| https://phrack.org | Phrack Zine |
| https://throwawaymail.com | Create an e-mail account |
| https://freeshell.org | Free shell for education |
| https://exploit-db.com | Exploit Database |
| https://vxheaven.org | Viruses |
| http://www.pentest-standard.org | PTES Technical Guidelines |
| https://nvd.nist.gov/ | National Vulnerability Database |
| http://www.cnnvd.org.cn/ | China National Vulnerability Database of Information Security |
| <https://www.first.org/resources/guides/reference.html> | FIRST (2010) |

**Germany:**

|  |  |
| --- | --- |
| https://cir.bundeswehr.de/ | Cyber- und Informationsraum (Bundeswehr) |
| https://www.bsi.bund.de/ | Bundesamt für Sicherheit in der Informationstechnik |
| https://www.bsi-fuer-buerger.de |  |
| https://www.bmwi.de | Bundesministerium für Wirtschaft und Energie |
| https://www.isc2chapter-germany.org/ | siehe (ISC)2 |
| https://www.it-sicherheit-in-der-wirtschaft.de/ | BMWi Sicherheitsnavigator |
| https://www.itzbund.de | Informations Technik Zentrum Bund (IT-Dienstleistungen für die öffentliche Verwaltung) |
| https://www.allianz-fuer-cybersicherheit.de | Cybersicherheit |

**Switzerland:**

|  |  |
| --- | --- |
| https://www.bwl.admin.ch | IKT-Minimalstandard des Bundesamt für wirtschaftliche Landesversorgung BWL |
| https://ictswitzerland.ch/themen/cyber-security/ | Umbrella Organisation for the Digital Economy |
| https://www.cybersecurity-check.ch | ICTswitzerland Cybersecurity-Schnelltest für KMU |

**Tools:**

|  |  |
| --- | --- |
| https://www.kali.org | Penetration testing distribution based on Linux |
| https://www.hiren.info | Hiren's BootCD with a lot of tools and Windows XP |
| https://www.lpi.org/de/ |  |

**Linux:**

|  |  |
| --- | --- |
| https://www.lpi.org/de/ | Linux Professional Institute |

**Microsoft:**

|  |  |
| --- | --- |
| https://www.microsoft.com | Microsoft |

**NATO:**

|  |  |
| --- | --- |
| [https://www.ncia.nato.int](https://www.ncia.nato.int/) | NATO Communications and Information Agency |