InfoSurance

G l o s s a r

Erläuterungen zum Thema
Sicherheit der Informationsinfrastruktur

eine Dienstleistung der

Stiftung Infosurance Badenerstr.551 8048 Zürich
Tel: 01 - 433 39 39 Fax: 01 - 433 38 78
E - mail: mail@infosurance.ch
http://www.infosurance.org

Glossarinhalte der *Stiftung InfoSurance*

Stand Februar 2001 (ca. 115 Begriffe)

Alarmorganisation
Authentifizierung / Authentisierung
Authentizität
Autorisierung
Backup
Bedrohung
bps, bit pro sekunde
Byte, Kilobyte, Megabyte, Gigabyte, Terabyte
Chiffrierung
Client
Computerkriminalität
Computersicherheit
Cracker, Cracking
Cyberwar(fare)
Daten
Datenbank
Datendiebstahl
Datensicherheit
Diebstahl von Informationen
Digitalisierung
E-Business
E-Commerce
E-Government
E-mail
EDV
Electronic War(fare)
Erkennung
Firewall
Flooding
Fraud
Frühwarnung
Gefährdung
Geschäftskritische Informationen
Hacker, Hacking
Host
HTML
Hyperlink
Identifizierung
Industriespionage
Informatiksicherheit
Information Assurance
Information War
Information(en)
Informations-Infrastruktur
Informationsgesellschaft
Informationskrieg
Informationssicherheit
InformationsTechnologie, IT
Informationstyp
Integrität
Intelligence
Intrusion
ISDN
IT

Know-How
Kommunikationssicherheit
Kommunikationstechnologie(n)
Kritische Informationen
Kryptografie
Kryptologie
Logische Bombe
Makro
Manipulation von Informationen
Modem
Netzwerke
Offene Kommunikationsnetze
Öffentliches Netzwerk
Physische Sicherheit
PKI
PGP
Prävention
Privates Netzwerk
Protokoll
Risiken
Risikoanalyse
Sabotage
Schaden (Informationssicherheit)
Schwachstelle
Schwachstellenanalyse
Sensitive Informationen
Server
Sicherheitskonzept
Sicherheitspolitik (Information)
Sicherheitsziel
(Digitale) Signatur
Smart-Cards
Spionage
Spoofing
Standortqualität
Störung
Systemsicherheit
TCP/IP
Trojanisches Pferd
Unversehrtheit (integrity)
Verfügbarkeit (availability)
Verlässlichkeit
Verlust von Informationen
Vertical Integration
Vertrauenswürdigkeit (Rechnersystem)
Vertraulichkeit (confidentiality)
Verwundbarkeit
Virtueller Krieg
Virus
Vorbeugung
Wissen
Wurm
WWW
XML (Extensible Markup Language)
Zugangsschutz

Erklärungen in alphabetischer Reihenfolge

Alarmorganisation	Organisation, die Benutzer vor akuten Gefahren für die Informationssicherheit ihrer Systeme warnt, zur Zeit nur in bestimmten Bereichen der IT-Technologie etabliert, eine nationale Organisation ist in der Schweiz geplant
Authentifizierung / Authentisierung	Identifizierung eines Nutzers zur Erteilung der Zutrittsberechtigung. Wird z. B. zur Sicherung von Rechnern und Daten vor unbefugtem Zugriff durchgeführt mittels Kennwort, Passwort, Signatur (Chipkarte oder biometrisch, z.B. Fingerabdruck, Iris-Erkennung)
Authentizität	Die Echtheit von Daten und Informationen und ihrer Identität, Bestandteil der → Informationssicherheit, durch geeignete Kontrollmassnahme wird sichergestellt, dass Daten und Informationen wirklich aus der angegebenen Quelle stammen bzw. dass die Identität eines Benutzers oder eines angeschlossenen Systems (z. B. Netzwerk) korrekt sind.
Autorisierung	Erteilung der Zutrittsberechtigung auf Dienste, Programme und Daten eines Netzwerks und / oder Computersystems
Backup	„den Rücken decken“, Datensicherung, Vorgang zur Speicherung von Daten auf einem separaten Datenträger, sollte zur Vermeidung hoher Kosten beim Defekt eines Computersystems in jeder kommerziell genutzten Informatik-Anwendung regelmässig vorgenommen werden, wird aber im Umfeld kleiner, kommerziell genutzter Rechnersysteme oft vernachlässigt
Bedrohung	**alt**: Feindliches Verhalten und Massnahmen eines Gegners gegen einen Staat, Einrichtungen und Personen im militärischen Sinn **neu**: Ausdehnung auf das gesamte Umfeld moderner Kommunikations- und → Informations-Technologien mit dem Ziel, Informationen und Informationssysteme aktiv oder passiv anzugreifen
bps, bit pro sekunde	Mass für die Übertragungsgeschwindigkeit digitaler Daten, 1 bit entspricht einer logischen NULL oder EINS z. B. im digitalen → ISDN Telefonsystem 64.000 bps (siehe auch → Byte)
Byte **Kilobyte** **Megabyte** **Gigabyte** **Terabyte**	digitales Datenformat, 1 Byte enthält normalerweise 8 bit, Kilobyte = KB = 1000 Byte, Megabyte = MB = 1 Mio Byte Gigabyte = GB = 1000 Megabyte, Terabyte = TB = 1 Mio Megabyte
Chiffrierung	Veränderung von → Informationstypen durch einen „Schlüssel“ (normalerweise ein mathematischer Algorythmus), der Daten bzw. Informationen für dritte nicht mehr zugänglich macht, siehe auch → Signatur
Client	„Klient, Kunde“ , Arbeitsplatzrechner, der in einem Computernetzwerk normalerweise auf Daten und Programme eines → Servers zugreift

Computerkriminalität	Erzeugen wirtschaftlicher Schäden bei normalerweise persönlicher Vorteilnahme durch → Manipulation, →Sabotage und →Datendiebstahl von Daten und Informationen in Computersystemen, siehe auch →Fraud, → Industriespionage, früher auf lokale Systeme beschränkt, durch die neuen → Kommunikationstechnologien sind neue Möglichkeiten entstanden und sie hat stark an Bedetung zugenommen
Computersicherheit	Bestandteil der → Informatiksicherheit, technische Massnahmen, die bei einem Computer den Schutz der Daten und Informationen gegen Verlust und Manipulation gewährleistet
Cracker, Cracking	Kriminelle Form des → Hacking durch unberechtigtes Eindringen in Computersysteme mit dem Ziel des → Datendiebstahls (Informationen und Passwörter), der → Sabotage durch Datenmanipulation (Löschung, Veränderung), der Bereicherung oder des Erschleichens kostenpflichtiger Leistungen der Computer-Infrastruktur. Code-Cracking: Voraussetzung für die Softwarepiraterie zum unbefugten Kopieren lizenzpflichtigen geistigen Eigentums
Cyberwar(fare)	„Krieg(sführung) im virtuellen Raum“, irreführender Begriff aus dem Science Fiction Bereich, bezeichnet eine reale Form der Kriegsführung mit dem Ziel, die Sicherheit von Informations-Infrastrukturen des Gegners zu verletzen oder zu zerstören, siehe auch → Informationskrieg bzw. → Electronic War, Cyberwar reduziert sich **nicht** auf den militärischen Bereich, sondern kann auch im zivilen IT - Bereich angewendet werden
Daten	Wertvollste Ressource des „Informationszeitalters“, deren Kosten (und Wert) für ihre Erzeugung und Verwaltung normalerweise nicht erfasst werden, sind wichtigste Grundlage einer → Informations-Infrastruktur und bestehen aus einer dokumentierten bzw. digitalisierten Form von Informationen
Datenbank	Rechneranwendung für die strukturierte „Aufbewahrung“ von Daten und Informationen auf Computersystemen
Datendiebstahl	Diebstahl → Sensitiver Informationen, die im IT- Zeitalter meist in digitaler Form vorliegen (Inhalte von Datenbanken, Passwörter, etc.). Fällt unter → Computerkriminalität, kann auch als → Sabotage ausgeführt werden, wenn dadurch die Funktion des „bestohlenen“ Rechners beeinträchtigt wird
Datensicherheit	Aufwand und Umfang von Massnahmen, die zur Sicherung und Sicherheit der Daten auf Computersystemen dienen, um → Angriffe, → Sabotage, → Diebstahl, → Verlust etc. zu vermeiden, siehe auch → Computersicherheit und → Informatiksicherheit
Diebstahl von Informationen	Ist keineswegs auf die → Informationstechnologie beschränkt sondern umfasst sämtliche Formen des unberechtigten Aneignens von Informationen durch Softwarepiraterie, → Datendiebstahl, → Spionage, (illegale) → Intelligence, → Vertical Integration etc.
Digitalisierung	Umwandlung jeglicher Daten (Texte, Zeichnungen etc.) sowie elektrischer Signale, die analog erzeugt werden (z. B. Mikrofon, Telefon) in ein digitales Datenformat
E-Business	Jede Form einer Geschäftstätigkeit, die mit Hilfe der modernen elektronischen Medien durchgeführt wird (Internet, Fernsehen, Telefon)

E-Commerce	Handel mit Waren und Dienstleistungen, die mit Nutzung der modernen elektronischen Medien unmittelbar durchgeführt werden
E-Government	Dienstleistungen, die von der öffentlichen Hand (Gemeinden, Städte, Kantone, Staat) den Bürgern mit Hilfe der modernen elektronischen Medien angeboten werden
E-mail	„Elektronische Post“, Internet - und Netzwerk Dienst, der mit einem eigenen → Protokoll (SMTP / POP3) für den Austausch von Texten und Bildern verwendet wird, dazu werden spezielle Server (Mail Exchange Server) verwendet, die diesen Dienst bereitstellen
EDV	**E**lektronische **D**aten**V**erarbeitung, Historischer Begriff, der auf die Strukturen und Anwendungen alter Computersysteme (ca. 1960 bis gegen Ende der Achtziger Jahre) zurückgeht und normalerweise die neuen Kommunikationstechnologien nicht berücksichtigt
Electronic War(fare)	„Elektronische Kriegsführung“, Kriegsmethodik, die sich nicht auf die Informationstechnologien beschränkt, sondern grundsätzlich die Verletzung oder Zerstörung aller elektronischen Systeme des Gegners beabsichtigt
Erkennung	siehe → Authentifizierung und → Identifizierung
Firewall	„Feuermauer“, Sicherheitseinrichtung eines Computersystems, um das unberechtigte Eindringen (→ Intrusion) in geschützte Bereiche von Rechnersystemen zu verhindern
Flooding	„Überfluten“ eines Computersystems →(Servers) oder eines Netzwerks mit grossen Datenmengen. Dabei wird die Verabeitungskapazität des Systems weit überschritten und seine Dienste und Funktionen sind nicht mehr verfügbar, Form der → Sabotage
Fraud	„Betrug, arglistische Täuschung, Schwindel“, eine Form der → Computerkriminalität, die speziell durch → Datendiebstahl (Schlüssel, Passwörter) ermöglicht wird, z. B. Umleitung beim Zahlungsverkehr auf Konten des Betrügers, Bestellung von Waren mit fremden Kreditkartennummern etc.
Frühwarnung	Eine generell volkswirtschaftlich wünschenswerte Einrichtung, um die hohen Schäden durch erfolgreiche Angriffe auf die Informationssicherheit zu vermeiden. In der Praxis ist durch die überraschenden Formen der Angriffe und die hohe Ausbreitungsgeschwindigkeit (Internet) eine effektive Frühwarnung schwierig umzusetzen, siehe auch →Alarmorganisation
Gefährdung	Aktive Bedrohung der Informationssicherheit, deren Stärke von der Form eines Angrifftyps (Intrusion, Datendiebstahl, Viren, Trojanisches Pferd, etc.), der Häufigkeit seines Auftretens, den Ressourcen des Angreifers und seiner Motivation sowie von den eigenen Schwachstellen bestimmt wird
Geschäftskritische Informationen	siehe → Kritische Informationen und → sensitive Informationen
Hacker, Hacking	Software - Spezialist, der seine Kenntnisse und Fähigkeiten zum Aufspüren sicherheitsrelevanter Schwachstellen in einer Software und / oder einem Computersystem ohne Absicht der persönlichen Bereicherung einsetzt, Gegensatz → Cracker, Cracking

Host	„Gastgeber, Wirt“, Bezeichnung für ein Computersystem, das Dienstleistungen zur Verfügung stellt, z. B. Webhost ist ein Rechnersystem, das die Daten eines Internet-Auftritts enthält und diese Daten im Internet allgemein zugänglich macht
HTML	**H**yper **T**ext **M**arkup **L**anguage, Bezeichnung für die Programmsprache zur Übertragung von Dokumenten. Wird im Internet verwendet und von den Browsern so ausgewertet (interpretiert), dass die Daten (leider nicht immer identisch) auf dem Bildschirm dargestellt werden können
Hyperlink	„Sprungverbindung“, wichtige Funktion der HTML Sprache, ermöglicht durch Anklicken die Verbindung zu einem anderen Dokument im eigenen Auftritt oder im gesamten Internet
Identifizierung	Erkennen einer Berechtigung für den authorisierten Zugang, im IT Bereich durch Kennwort, Passwort, Signatur etc.
Industriespionage	Unberechtigtes Aneignen → sensitiver und → kritischer Informationen eines Unternehmens, z.B. Know-How, Technologien, Forschungs- / Entwicklungspläne / -ergebnisse, Daten, etc. Ausmass, Häufigkeit und Methoden werden allgemein stark unterschätzt. Siehe auch → Spionage und → Vertical Integration
Informatiksicherheit	Vermeidung von Schäden an Informatik-Systemen (Computer, Netzwerke, Software) durch ein umfassendes Massnahmenpaket wie Sicherheit von → Authentizität, → Authentifizierung / Authentisierung, durch → Backup, → Firewall, Zugangsschutz, Virenscanner etc. siehe auch → Computersicherheit und → Informations-sicherheit
Information Assurance	„Informationssicherheit“, siehe dort
Information War	„Informationskrieg“, siehe dort)
Information(en)	Wertvollste Ressource des „Informationszeitalters“, deren Kosten (und aktiver Wert) für die Erzeugung und Verwaltung normalerweise nicht erfasst werden, sie sind die wichtigste Grundlage einer → Informations-Infrastruktur und bestehen im IT- Bereich üblicherweise aus digitalisierten Daten, neben dem IT- Bereich gehören dazu bei Personen verfügbares oder durch Personen dokumentiertes und vermitteltes → Wissen, → Kenntnisse (Know-how), etc.
Informations-Infrastruktur	Die Infrastruktur (Netzwerke, Systeme und Einrichtungen) für die Verfügbarkeit, Erzeugung, Verwaltung und Sicherung von → Informationen bei öffentlichen und privaten Organisationen und Unternehmen, der Schutz dieser Bereiche ist das Hauptziel der Stiftung InfoSurance
Informationsgesellschaft	Soziologische Bezeichnung der aktuell dominanten Grundlagen der Weltwirtschaft, die durch die extremen Fortschritte in den → Kommunikations- und Computertechnologien entstanden sind. In der Vergangenheit: „Industriegesellschaft“
Informationskrieg	Reale Form sowohl ziviler wie auch militärischer Form der Kriegsführung mit dem Ziel, die Sicherheit von Informations-Infrastrukturen des Gegners zu verletzen oder zu zerstören, siehe auch → Electronic War, Informationskrieg reduziert sich also **nicht** auf den militärischen Bereich, sondern wird auch im zivilen Bereich angewendet → Computerkriminalität

Informationssicherheit	Aufwand und Umfang aller Massnahmen, die zur Sicherung und Sicherheit sensitiver → Informationen in Unternehmen und Organisationen dienen
InformationsTechnologie, IT	Sammelbezeichnung für Techniken, Methoden, Systeme und Werkzeuge, die für unterschiedliche Arten von Informationen, den Zugang sowie die → Verfügbarkeit von Informationen verwendet werden
Informationstyp	Begriff für die Form, in der Information vorliegt z. B. Schrift, Druck, analoge oder digitale Daten etc.
Integrität	Die Sicherstellung der Korrektheit von Daten (Datenintegrität) und der korrekten Funktion von Computersystemen (Systemintegrität), Bestandteil der → Informatiksicherheit
Intelligence	Gezieltes Vorgehen, das zu „Erkenntnissen“, Kenntnissen und Informationen führt, um für den eigenen Vorteil, zur Vermeidung eigener Nachteile oder auch zum direkten Nachteil des Informationslieferanten verwendet zu werden, Massnahmen und Methoden der Sammlung von Erkenntnissen können legal oder illegal → Spionage, → Vertical Integration sein
Intrusion	Normalerweise unberechtigtes „Eindringen“ in Daten- und Computernetzwerke mit dem Ziel, durch → Sabotage oder → Diebstahl einen → Schaden zu verursachen
ISDN	**I**ntegrated **S**ervices **D**igital **N**etwork, digitales Fernmeldenetz zur einheitlichen Übertragung von Telefon, Fax und Daten, durch die Form der Digitalisierung sind Übertragungsraten von 64.000 bzw. 128.000 bit pro Sekunde möglich, im Vergleich mit der analogen Technik verbesserte Übertragungs-Qualität und -Sicherheit
IT	**I**nformations**T**echnolgie, siehe dort
Know-How	„Wissen wie“, eine bereits verifizierte oder praktizierte, jedoch undokumentierte Form von Wissen, ist → Information, wenn verfügbar, dokumentiert, publiziert oder sonst kommuniziert wird, kann daher auch den → sensitiven Informationen zugeordnet werden, und ist dann Bestandteil der → Informationssicherheit, wird in seiner Schutzwürdigkeit und Bedeutung oft unterbewertet
Kommunikationssicherheit	Sicherheit und Schutz von Informationen während der Übertragung und Übermittlung auf drahtlosem Weg (Funk), über Kabel (Netzwerkkabel, Telefonleitungen, etc.) und über optische Medien (z. B. Glasfaser). Sie bezieht sich sowohl auf mögliche Zugriffe auf das Übertragungssystem wie auch auf die Vermeidung von systembedingten Übertragungsfehlern. Hauptziel ist die → Integrität der übermittelten Daten und Informationen

Kommunikationstechnologie(n)	Sammelbezeichnung für Techniken, Methoden, Systeme und Werkzeuge, die für verschiedene Varianten der Kommunikation verwendet werden, z. B. Satellitennavigation (Verkehr), Internet, Videokonferenzen, Handy (NATEL), Telefon, Fax etc. Durch die enormen Fortschritte in Technik und Technologien während der vergangenen 50 Jahre in den Bereichen Digital-, Computer-, Halbleiter-, Nachrichten- und Verfahrenstechnik (Fertigung) sind Grundlagen für diese neuen Anwendungen bei gleichzeitig enormer Steigerung der übertragenen und verfügbaren Daten und Informationen geschaffen worden. Gleichzeitig stehen die modernen Kommunikationstechnologien in den industrialisierten Ländern wegen der extremen Reduzierung der Kosten praktisch allen zur Verfügung
Kritische Informationen	siehe →Sensitive Informationen
Kryptografie	Wissenschaft der Geheimhaltung von Nachrichten
Kryptologie	Wissenschaft der „Verschlüsselung“ von Informationen, in der Kommunikationstechnik wird dabei das Signal (analog oder digital) mit einem mathematischen Algorythmus verknüpft: → Chiffrierung
Logische Bombe	Programmierte → Bedrohung für ein Rechnersystem. Eine versteckte Funktion (z. B. in einem Trojanischen Pferd), die im Normalfall einen erhebliche Schaden an der → Informationssicherheit hervorruft, wenn ein bestimmter Zustand des Systems erreicht wird, siehe → Zeitbombe und vgl. → Wurm und → Virus
Makro	Programm, das in Verbindung mit einem Anwendungsprogramm (z. B. MS Word) zusätzliche anwendungsspezifische Funktionen und Programmabläufe ermöglicht, kann aber auch als (Makro-)Virus in einer Datei versteckt sein wie beispielsweise beim „I love you“ Virus
Manipulation von Informationen	Gezielte Veränderung von Daten, die als sensitive und relevante Informationen die korrrekte Funktion von Computersystemen gewährleisten, moderne Form der → Sabotage im Informationszeitalter
Modem	**Mo**dulator / **Dem**odulator, Elektronisches System, das zur Aufbereitung und / oder Umwandlung elektrischer Signale für Senden und Empfang in Kommunikations-Netzwerken verwendet wird
Netzwerke	Drahtlose, elektrische oder optische (Glasfaser) Verbindung von → öffentlichen / privaten Systemen mit Sendern und Empfängern → Modems, die zur Kommunikation und Übertragung von Daten verwendet werden, z.B Telefonnetz, Internet etc.
Offene Kommunikationsnetze	siehe → Öffentliches Netzwerk
Öffentliches Netzwerk	Kommunikations- und Datenverbindungen, die von Netzwerkbetreibern allen Nutzern öffentlich zugänglich gemacht werden (Telefonnetz, ISDN, Internet etc.). Eindringen (→ Intrusion) und unberechtigter Zugang zu privaten Informations-Infrastrukturen erfolgt meist über öffentliche Netzwerke.
Physische Sicherheit	Schutz von Computersystemen gegen Schäden durch Bedrohungen wie Stromausfall, Feuer, Einbruch und Diebstahl

PKI	„**P**ublic **K**ey **I**nfrastructure“, sicherer Datenaustausch durch die Verwendung eines privaten und öffentlichen kryptografischen Schlüsselpaares z. B. beim Geldverkehr über das Internet, an einer Standardisierung wird z. Zt. gearbeitet.
PGP	„Pretty Good Privacy“, ein verbreitetes Programm zum Austausch sicherer E-Mails und zur Datei - Verschlüsselung. Der nicht-kommerzielle Gebrauch ist kostenlos: http://www.pgp.com/downloads/default.asp
Prävention	Vorbeugendes und umfassendes Massnahmenpaket zur Informationssicherheit. Hinweise finden Sie in unserem „Leitfaden für Führungskräfte“.
Privates Netzwerk	Kommunikations- und Datenverbindungen, die von Netzwerkbetreibern ausschliesslich einem einzelnen Nutzer vermietet werden (Standleitungen, Mietleitungen) oder Netzwerke (Kabel, Glasfaser), die vom Anwender eigenständig erstellt und betrieben werden. Sehr wichtige Voraussetzung für → Informations- und → Informatiksicherheit
Protokoll	Standard, der die kontrollierte Übermittlung von Daten festlegt. Enthält Konventionen mit formalen Regeln für die Datenkommunikation zwischen Rechnern in einem Netzwerk, die beispielsweise die Datenstruktur, den Aufbau der Datenpakete und die Codierung der Daten festlegen. Ausserdem können in Protokollen Steuerungsbefehle sowie Hard- und Software-Anforderungen spezifiziert sein. Man unterscheidet prinzipiell Anwendungs-, Transport- und Vermittlungsprotokolle
Risiken	Die Wahrscheinlichkeit oder relative Häufigkeit einer Schädigung der → Informationssicherheit z. B. durch die Ausnutzung von Schwachstellen.
Risikoanalyse	Systematische Erfassung der realen und ideellen Werte von Inhalten und Daten eines Rechnersystems bei gleichzeitiger Berücksichtigung der Schwachstellen des Systems sowie der Bedrohungen und Gefährdungen dieser Werte
Sabotage	**Alt**: Vorgang, bei dem durch einzelne oder mehrere verdeckte Massnahmen dem Ziel / Gegner ein unmittelbarer Schaden an Sachen, Material und Personen zugefügt wird **Neu**: wie oben, jedoch erweitert auf die → Informationstechnologie mit völlig neuartigen Methoden durch → Manipulation oder Diebstahl von Daten mittels berechtigtem oder unberechtigtem Eindringen → (Intrusion) in Rechnersysteme
Schaden (Informationssicherheit)	Durch Mängel bei der Sicherheit von Informations-Infrastrukturen entstehen weltweit Schäden in ungeheuren Grössenordnungen. Durch → Computer-Kriminalität und die Verletzbarkeit von → Informations-Infrastrukturen durch Schwachstellen ist hier ein extremes Wachstum zu verzeichnen. Aber auch weniger komplexe Schadensformen, wie Datenverlust durch Fehlbedienung oder Defekte an Computersystemen sind von grosser Bedeutung. Sie werden aber meist nicht erfasst und daher unterschätzt. Die Mehrheit der Schadensformen lässt sich nicht durch Versicherungen abdecken und belastet letztlich das einzelne Unternehmen oder die gesamte Volkswirtschaft.

Schwachstelle	Möglichkeiten des unbefugten Zugangs durch Umgehung, Täuschung → (Fraud) oder Manipulation der Sicherheitsfunktionen eines Informationssystems, nicht nur auf den IT-Bereich beschränkt, sondern schliesst auch Personen ein, siehe auch → Vertical Integration, → Intelligence
Schwachstellenanalyse	Systematische Methode, um die finanziellen und ideellen Werte sensitiver Informationen (z. B. ein Rechnersystem mit seiner gesamten Infrastruktur) zu erfassen und die Bedrohung und Risiken dieser Werte mit allen Sicherheits-Schwachstellen zu korrelieren
Sensitive Informationen	Informationen, die eine ökonomische Bedeutung für eine Organisation oder ein Unternehmen aufweisen. Sie bestehen nicht nur aus Computerdaten, sondern schliessen auch dokumentiertes und undokumentiertes Wissen (→ Know-how) und Personen ein. Vor allem geschäftskritische Informationen, die reibungslose Geschäftsabläufe bestimmen, sind besonders sensitiv und daher durch ein konsequentes → Sicherheitskonzept zu schützen
Server	Computer, der seine Hardware- und Software-Ressourcen in einem Netzwerk anderen Rechnern →(Clients) zugänglich macht z. B Applikations-, Daten-, Web-, Mail-Server
Sicherheitskonzept	Planung und Erarbeitung der Massnahmen, die für die Sicherheit von Informationen und Daten, Computersystemen sowie der gesamten Informations-infrastruktur eines Unternehmens, einer Organisation oder eines Landes erforderlich sind
Sicherheitspolitik (Information)	Richtlinien, Massnahmen und ihre aktive Durchführung, die zur Herstellung, Gewährleistung und Verbesserung der Sicherheit von Informationen und Daten, Computersystemen sowie der gesamten Informations-Infrastruktur eines Unternehmens, einer Organisation oder eines Landes dienen
Sicherheitsziel	Festlegung über Art und Umfang von Schutzmassnahmen für die unterschiedlichen Sicherheitsstufen → sensitiver Informationen unter ökonomischen Gesichtspunkten
(Digitale) Signatur	Sicherstellung der → Authentizität und → Integrität einer elektronischen Nachricht. Verschlüsselungsverfahren, das die eindeutige Identifikation eines Absenders sicherstellt und eine nachträgliche Manipulation verhindert.
Smart-Cards	Karte, die im Gegensatz zur herkömmlichen Magnetstreifen - Karte Informationen enthält, die mittels neuer Technologien über Funktionen verfügt, die eine eindeutige Identifikation des Besitzers ermöglicht und / oder den Zugang zu interaktiven Dienstleistungen (Telefon, Geldverkehr) ermöglicht

Spionage	**alt**: Aneignen sensitiver und wichtiger Informationen eines Gegners, meist im militärischen und später auch im industriellen Bereich (Industriespionage) verwendet, wurde unmittelbar durch Personen ausgeführt **neu**: Unberechtigtes Aneignen sensitiver und kritischer Informationen durch Nutzung der modernen Kommunikationstechnologien. Dadurch ist eine neue Qualität der Spionage durch mittelbare Methoden möglich, wie → Datendiebstahl und Diebstahl von → Know-How, Technologien, Forschungs- und Entwicklungsplänen / -ergebnissen, etc. Ausmass, Häufigkeit und Methoden werden allgemein stark unterschätzt
Spoofing	„beschwindeln, verulken“, Form der → Computerkriminalität, um beispielsweise unter Vortäuschung der Identität die Herausgabe von sensitiven Daten und Informationen veranlassen oder um die Sicherheit eines Systems zu verletzen (Herausgabe von Kennwörtern für den Zugang zu Online - Dienstleistungen), siehe auch → Fraud
Standortqualität	Allgemeiner Begriff für den Standard einer Volkswirtschaft mit einer Vielfalt von Qualitätskriterien, heute spielt dabei die Sicherheit der → Informationsinfrastruktur eine wesentliche Rolle für den wirtschaftlichen Erfolg einer Volkswirtschaft
Störung	Zeitlich begrenzte Fehlfunktion oder Ausfall eines Informations (Informatik) - Systems. Bei angestrebter hoher → Verfügbarkeit eines Systems sind für die Ausarbeitung eines → Sicherheitskonzepts die sehr vielfältigen Möglichkeiten von Störungen und ihrer Ursachen zu berücksichtigen und die erforderlichen Vorkehrungen und Massnahmen zur Vermeidung zu definieren, weitere Hinweise finden Sie in unserem „Leitfaden für Führungskräfte“.
Systemsicherheit	Bestandteil der → Informatiksicherheit, technische Massnahmen, die sämtliche Bestandteile eines Computersystems (incl. Netzwerk) einschliesst und den Schutz der Daten und Informationen gegen Verlust und Manipulation gewährleistet, siehe auch → Computersicher-heit
TCP/IP	**T**ransmission **C**ontrol **P**rotocol / **I**nternet **P**rotocol, Protokoll - Konzept, das 1983 standardisiert wurde. Bestimmt den Aufbau der Datenstruktur zur Übertragung in miteinander verbundenen, individuellen Netzwerken (routing -fähiges Protokoll). Als Router bezeichnet man die Rechner, die Daten von einem Netzwerk zum nächsten übermitteln. **TCP** bestimmt die Form der Datenpakete während **IP** die Eigenschaften der Netz- und Rechneradressen (IP-Adresse, MAC) festlegt. Das TCP/IP -Protokoll bildet eine wesentliche Grundlage des heutigen Internet
Trojanisches Pferd	Nicht erkennbares Programm oder eine Datei, die das Trojanische Pferd mit einem → Virus oder → Wurm enthält. Wird üblicherweise als Bestandteil einer E-mail, beim Herunterladen einer Datei oder durch → Intrusion unbemerkt auf dem Rechner abgespeichert. Unter vorgegebenen Voraussetzungen starten sie auf dem befallenen Computer mit unzulässiger Sammlung und Diebstahl, Manipulation und der Zerstörung von Daten. Moderne Form von → Spionage und → Sabotage

Unversehrtheit (integrity)	Eigenschaften von Daten und Informationen, bei Übertragung, Speicherung und Verwendung ihre Inhalte ohne Veränderung durch unterschiedliche Einflüsse und → Bedrohungen in der ursprünglich korrekten Form zur Verfügung zu stellen, Bestandteil von → Informations- und → Informatiksicherheit,
Verfügbarkeit (availability)	Verhältnis von gesamter Einsatzzeit mit ungehindertem und störungsfreien Zugang eines berechtigten Benutzers zu den Komponenten eines Rechnersystems (Peripherie, Programme und Daten) zu Ausfallzeit und Fehlfunktion (→ Störung) eines Computersystems, Angabe in Prozent. Ein scheinbar hoher Wert von 99,9% bedeutet bei ganzjährigem Betrieb eines Systems eine Ausfallzeit von ca. 8,7 Stunden, also etwa einen ganzen Arbeitstag !
Verlässlichkeit	Bestandteil von → Informations- und → Informatiksicherheit, bezieht sich auf Daten und Systemfunktionen (Hard- und Software) siehe auch →Vertrauenswürdigkeit, → Unversehrtheit
Verlust von Informationen	Seine Vermeidung und Verhinderung ist wichtigster Bestandteil der → Informations- und →Informatiksicherheit, konnte früher im → EDV- Bereich hauptsächlich durch angepasste Datensicherungs - Massnahmen (→Backup) verhindert werden, entsteht aber auch durch Entlassung und Weggang von Mitarbeitern. Durch die neuen → Kommunikationstechnologien in Verbindung mit neuen Formen und Qualitäten der → Computerkriminalität sind zusätzliche Möglichkeiten (→ Datendiebstahl etc.) für den Verlust von Informationen entstanden. Er ist normalerweise nur mit einem hohen Zeit- und Kostenaufwand wieder auszugleichen, wird aber oft buchungstechnisch nicht und häufig in seiner ökonomischen Bedeutung zu wenig berücksichtigt
Vertical Integration	Moderne Form der → Industriespionage mit dem Ziel, durch „vertikale Integration“ als angeblicher Mitarbeiter mittels Telefonaten, Belauschen von Gesprächen etc. sensitive und / oder kritische Informationen zu erhalten, siehe auch → Intelligence
Vertrauenswürdigkeit (Rechnersystem)	Eigenschaft eines Systems oder Produkts, mit einem bestimmten Grad der Zuverlässigkeit realen oder angenommenen → Bedrohungen wirksam zu widerstehen, seine Funktionen fehlerfrei auszuführen und den Zugriff auf verlässliche Daten in unterschiedlichen Sicherheitskategorien zu ermöglichen
Vertraulichkeit (confidentiality)	Klassifizierung von → sensitiven Informationen, die nur bestimmten Personen zugänglich sind
Verwundbarkeit	Bestandteil der → Informationssicherheit, ihre Grössenordnung wird durch die Anzahl und Art der → Schwachstellen in einem Informations- / Rechnersystem / -netzwerk sowie von der eingesetzten Betriebs- und Anwendungssoftware bestimmt, auch ein scheinbar ideales Sicherheitsdispositiv garantiert allerdings keine Unverwundbarkeit der Informationssicherheit
Virtueller Krieg	Deutsch für → Cyberwar(fare), Krieg(sführung) im virtuellen Raum, irreführender Begriff aus dem Science Fiction Bereich, bezeichnet eine reale Form der Kriegsführung mit dem Ziel, die Sicherheit von Informations-Infrastrukturen des Gegners zu verletzen oder zu zerstören, siehe auch → Informationskrieg bzw. → Electronic War

Virus	Versteckter Programmteil einer Datei, der Daten- und komplette Netzwerkstrukturen zerstört. Kann durch jede Form der Datenübernahme (Internet, Disketten, ZIP-Laufwerke, CD-ROMS, Netzwerke etc.) übertragen und verbreitet werden. Vermeidung nur durch gesamthaftes Massnahmenpaket im Rahmen der → Informatiksicherheit
Vorbeugung	Massnahmenpaket, um Schäden durch Beeinträchtigung, Verletzung, Aufhebung oder Zerstörung der → Informations-sicherheit zu vermeiden
Wissen	Vernetzte Information, zunächst personenbezogen. In der Elektronik und Computertechtechnik besteht Wissen aus (analogen und digitalen) einzelnen Daten, die in Dateien Informationen enthalten. In Datenbanken und vollständigen Systemen ist also grundsätzlich Wissen verfügbar. Daher geht es bei der → Informationssicherheit im eigentlichen Sinn um den Schutz von Wissen
Wurm	(Von einer Datei) unabhängiges Programm, das sich selbst (meist unter Ausnutzung von Schwachstellen) durch Kopieren von einem Rechnersystem oder -netzwerk zum nächsten ausbreitet. Meistens enthält ein Wurm (wie ein Virus) Befehle, die Daten direkt zerstören oder die Systemleistung beeinträchtigen
WWW	**W**orld **W**ide **W**eb, „Weltweites (Spinnen)-Netzwerk“, Elektrische und elektronische Verbindung von Computersystemen für die Datenkommunikation, die Übermittlung der Daten beruht auf dem HTTP - Protokoll, für andere Dienste (z. B. E-mail, FTP) werden andere Protokolle und Server verwendet, jedoch wird prinzipiell das gleiche Netzwerk benutzt
XML (Extensible Markup Language)	Weiterentwicklung der Programmsprache → HTML, die eine wesentliche Verbesserung und Ausweitung der Möglichkeiten und Funktionen im Internet gestattet, setzt voraus, dass der Browser diese Funktionen versteht und auch richtig interpretiert, bisher nur (teilweise) im Internet Explorer 5
Zugangsschutz	Bestandteil der → Informationssicherheit, Massnahme, um den unberechtigten Zugang zu Programmen, Informationen und Daten in einem Rechensystem zu verhindern, siehe auch → Authentisierung und → Autorisierung