Harald Haider

IT-Security - Sicher unterwegs in digitalen Welten

Reihe Hintergründe

Bestellnummer 12-025-238

- Vorschau -
IT-Security - Sicher unterwegs
12-025-238 © 2012
www.LehrerSelbstVerlag.de

Zum Autor

Harald Haider arbeitet als Psychotherapeut in freier Praxis und als Lehrer für Deutsch, Informatik und Bewegung und Sport mit 20-jähriger Berufserfahrung. Er ist auch in der Lehrerfortbildung an Pädagogischen Hochschulen tätig.

IT-Security - Vorschau - Sicher unterwegs
12-025-238 © 2012
www.LehrerSelbstVerlag.de

Alle Rechte vorbehalten. All rights reserved.
Nachdruck, auch auszugsweise, vorbehaltlich der Rechte,
die sich aus § 53, 54 UrhG ergeben, nicht gestattet.

Lehrerselbstverlag
Sokrates & Freunde GmbH, Bad Honnef (Germany) 2012
www.lehrerselbstverlag.de

Lektorat und Layout: Josephine Mahler
Druck: docupoint GmbH, Magdeburg

INHALTSVERZEICHNIS

VORWORT **6**

1. WIE FUNKTIONIERT DAS INTERNET? **7**

1.1 Das „Netz der Netze“ **7**
1.2 Dienste im Internet **8**
1.3 Gefahren **9**
1.4 Linkliste **9**
Summary I: Wie funktioniert das Internet? **10**

2. DATEN, INFORMATIONEN UND DATENSCHUTZ **11**

2.1 Aus Daten werden Informationen **11**
2.2 Daten lauern vielfältige Gefahren **11**
2.3 Die drei Hauptziele der Datensicherheit **12**
2.4 Rechtliche Grundlagen des Datenschutzes **13**
2.5 Links **15**
Summary 2: Daten und Datenschutz **16**
Test: Grundlagen und Datenschutz **17**

3. GRUNDLEGENDE MÖGLICHKEITEN DES DATENSCHUTZES – DEN DATENSCHATZ HÜTEN **19**

3.1 „Sesam öffne dich“ – Wie sieht ein sicheres Passwort aus? **19**
3.2 Lang leben die Daten! Backups **21**
3.2.1 Tipps und tricks für Backups **21**
3.2.2 Sicherungsarten **22**
3.2.3 Backup-Methoden **23**
3.3 Daten endgültig vernichten **27**
3.4 Links **28**
Summary 3: Grundlegende Möglichkeiten des Datenschutzes **29**
Test: Datenschutz **30**

4. ANGRIFFSZENARIEN AUS DEM INTERNET **31**

4.1 Identitätsdiebstahl – social engineering **31**
4.2 Malware **33**
4.3 Weitere Angriffsszenarien **35**
4.4 Links **37**
Summary 4: Angriffsszenarien aus dem Internet **38**
Test: Angriffsszenarien aus dem Internet **39**

5. SCHUTZMAßNAHMEN **41**

5.1 Was sagt der Hausverstand? **41**
5.2 Links **42**
5.3 Sicherheitseinstellungen im Browser – das „Tor zur Welt“ sichern **42**
5.4 Personal Firewall **55**
5.5 Anti-Malware-Programme **58**
Summary 5 - Schutzmaßnahmen im Internet **65**
Test: Firewall, Anti-Malware-Programme & Co **67**

IT-Security - Sicher unterwegs - Vorschau
12-025-238 © 2012
www.LehrerSelbstVerlag.de

6. E-MAILS – SCHNELL UND SICHER ... 68

6.1 Wie funktionieren E-Mails? ... 68
6.2 Gefahren ... 69
6.2.1 Das „Abhören“ von E-Mails ... 69
6.2.2 Die missbräuchliche Verwendung der E-Mail-Adresse ... 70
6.2.3 Infizierte E-Mail-Anhänge ... 71
6.2.4 Spam- und Werbemails ... 71
6.3 Links ... 73
Summary 6: E-Mails – schnell und sicher ... 74
Test: E-Mails – schnell und sicher ... 75

7. SICHERHEIT IN NETZWERKEN ... 76

7.1 Netzwerkgrundlagen ... 76
7.2 Sicherheit in Netzwerken ... 77
7.3 Links ... 81
Summary 7: Sicherheit in Netzwerken ... 82
Test: Sicherheit in Netzwerken ... 83

8. SICHER UNTERWEGS IM WEB 2.0 ... 84

8.1 Das Mitmach-Web ... 84
8.2 Gefahren im Web 2.0 ... 85
8.3 Web 2.0-Tipps ... 87
8.4 Links ... 88
Summary 8: Sicher unterwegs im Web 2.0 ... 89
Test: Sicher unterwegs im Web 2.0 ... 90

9. FACEBOOK ... 91

9.1 Ein paar Fakten rund um Facebook ... 91
9.2 Sicherheits- und Privatsphäreeinstellungen ... 92
9.3 Links ... 97
Summary 9: Facebook ... 98
Test: Facebook ... 99

10. SAFER SHOPPING – EINKAUFEN IM NETZ ... 100

10.1 Schöne neue Einkaufswelt ... 100
10.2 Tipps und Tricks rund ums Online-Shoppen ... 100
10.3 Auktionen ... 104
10.4 Abzocke im Internet ... 105
10.5 Links ... 105
Summary 10: Online-Shopping ... 106
Test: Online-Shopping ... 107

- Vorschau - IT-Security - Sicher unterwegs 12-025-238 © 2012 www.LehrerSelbstVerlag.de

11. HANDYSPAß OHNE RISIKO 108

11.1 Kostenfallen **108**
11.2 Sicherheitstipps rund ums Handy **112**
11.3 Links **114**
Summary 11: Kostenfallen und Sicherheitsrisiken rund ums Handy **115**
Test: Handyspaß ohne Risiko **116**

12. CYBER MOBBING – KEIN KAVALIERSDELIKT 117

12.1 Was ist Cyber Mobbing? **117**
12.2 Gesetzliche Rahmenbedingungen – „Mit einem Fuß im Kriminal ..." **119**
12.3 Was tun bei Cyber-Mobbing? **119**
12.4 Linkliste **121**
Summary 11: Cyber-Mobbing **122**
Test: Cyber Mobbing **123**

ERGÄNZENDE LITERATUR 124

LÖSUNGEN ZU DEN ÜBUNGSAUFGABEN 124

IT-Security - Sicher unterwegs - Vorschau
12-025-238 © 2012
www.LehrerSelbstVerlag.de

VORWORT

Moderne Medien und das Internet in all seinen Anwendungsformen sind mittlerweile fixer Bestandteil des gesellschaftlichen und schulischen Lebens geworden. PC, Smartphone und Internetanschluss gehören zur „Standardausrüstung" der meisten Jugendlichen. Als „digital natives" benutzen Kinder und Jugendliche moderne Medien mit einer Selbstverständlichkeit und „angeborenen" Kompetenz. Mit fast „schlafwandlerischer Sicherheit" surfen Jugendliche im Internet, nutzen die vielfältigen Funktionen von Smartphones, präsentieren sich in sozialen Netzwerken und machen immer schnellere Entwicklungen mühelos mit.

Echten Nachholbedarf gibt es allerdings, was Sicherheitsthemen betrifft. Besonders Kindern, aber auch vielen Jugendlichen ist nicht bewusst, welche vielfältigen Gefahren die Nutzung von Computern, Handys und Internet bergen.

Auch IT-Sicherheit will gelernt sein. Dieses Buch ist daher als Lehrbuch gedacht und beschreibt alle aktuell relevanten Themen „von der Pike" auf. Der Bogen wird von Grundlagenthemen (z. B. Datenschutz, Browsereinstellungen) bis zu Anwendungsthemen (z. B. Online-Shopping, sicherer Umgang mit dem Smartphone) gespannt.

Um „nachhaltiges Lernen" zu ermöglichen, wird jedes Kapitel in folgende Abschnitte gegliedert:

	Grundlegende Informationen
	Gefahren und Risiken
	Tipps und Tricks
	Check up (Lernzielkontrolle)
	Summary (Kopiervorlage)

Zu jedem Kapitel werden nützliche Links angegeben. Die gesamte Liste kann zusätzlich bei www.lehrerselbstverlag.de heruntergeladen werden.

Dieses Buch eignet sich auch gut zur Vorbereitung auf den ECDL (Modul 8, IT-Security).

IT-Security - Sicher unterwegs - Vorschau - 12-025-238 © 2012 www.LehrerSelbstVerlag.de

1. WIE FUNKTIONIERT DAS INTERNET?

„EDV-SYSTEME VERARBEITEN, WOMIT SIE GEFÜTTERT WERDEN. KOMMT MIST REIN, KOMMT MIST RAUS.“ (ANDRE KOSTOLANY)

1.1 DAS „NETZ DER NETZE“

Das Internet (= interconnected network) ist ein **weltweites Netzwerk** von Computern, genauer gesagt: von Computernetzwerken. Jeder einzelne PC ist Teil eines größeren Netzwerkes: Wenn sich z. B. ein Heimcomputer ins Internet einwählt, wird er Teil des Netzwerks des Internetproviders (= einer Firma, die den Zugang ins Internet ermöglicht). Dieses ist wiederum Teil eines größeren Netzwerks, usw. Zwischen den Netzwerken bestehen verschiedene Verbindungswege, vergleichbar mit Städten, die durch verschiedene Straßen und Wege mit anderen Städten verbunden sind. Die meisten Netzwerke sind untereinander durch **Glasfaserkabel** verbunden, die eine große Verarbeitungskapazität und Übertragungsgeschwindigkeit gewährleisten.

Man kann sich diese **Verbindungen** ungefähr so vorstellen: Im Prinzip kann jeder Computer mit jedem anderen auf der ganzen Welt verbunden werden und Daten austauschen. Ein grundlegendes Prinzip beim Datenaustausch (z. B. Bilder, Dokumente, E-Mails) ist das **Client-Server-Prinzip**: Es kommunizieren **immer genau zwei Computer** miteinander, wobei der eine Partner, der **Server**, Informationen zur Verfügung stellt, die der andere, der **Client**, abrufen kann. Jemand, der von seinem Gerät aus (Computer, Notebook, iPhone) eine bestimmte Seite im Web aufruft, ist also der Client, der Computer, der die Seite zur Verfügung stellt, wird als Server bezeichnet.

Da das Netz Millionen von Computern und Netzwerken und unzählige Verbindungswege umfasst, stellt sich natürlich die Frage, **wie** man von seinem Computer aus **genau den gewünschten Server anwählen** kann. Eine reibungslose Verbindung und Kommunikation zwischen zwei Computern basiert auf folgenden Eckpunkten:

- **IP-ADRESSE:**

Jeder Computer im Internet kann durch eine bestimmte Adresse **eindeutig identifiziert** werden. Diese IP-Adresse ist vergleichbar mit der Postanschrift im realen Leben: Wenn man einen Brief verschicken möchte, braucht man einen Absender und einen Adressaten. Da Computer mit Zahlen am besten umgehen können, bestehen die IP-Adressen aus vier Zahlen zwischen 0 und 255, wie z. B. 188.52.34.8. Da es für uns Menschen sehr schwierig wäre, sich die Zahlen der IP-Adressen zu merken, gibt es einen Dienst, der das Eingeben der richtigen Adresse erheblich erleichtert: der **Domain Name Service** (DNS). Wird eine Webadresse wie z. B. wikipedia.de eingegeben, dann übersetzt der DNS den Namen in die Zahlen der IP-Adresse und ermöglicht die Verbindung zur richtigen Seite.

IT-Security - Sicher unterwegs
12025-238 © 2012
www.LehrerSelbstVerlag.de
- Vorschau -

- **DIE „SPRACHE“ DER COMPUTER**
  Möchte man sich mit jemandem unterhalten, benötigt man eine **gemeinsame Sprache**, die beide Geprächspartner verstehen. Auch im Internet ist es notwendig, dass es gewisse Grundregeln gibt, die alle Computer, gleich welcher Bauart und mit welchem Betriebssystem, verstehen und einhalten können, damit Daten problemlos von A nach B übertragen werden können. Diese „gemeinsame Sprache“ nennt man **Protokolle**, durch die genau festgelegt wird, wie die Kommunikation zwischen Computern ablaufen soll. Die wichtigsten Protokolle werden unter dem Namen **TCP/IP** (= Transmission Control Protocol/Internet Protocol) zusammengefasst.

- **„POSTÄMTER“ IM INTERNET – DIE ROUTER**
  Werden Daten im Internet übertragen, so werden nicht alle auf einmal gesendet, sondern in **kleine Datenpakete** zerlegt und auf verschiedenen Transportrouten versandt. Dass diese Pakete auch an der richtigen Adresse ankommen, dafür sorgen sogenannte **Router**. Router sind Geräte, die man sich als Postämter vorstellen kann: Es werden (Daten-)Pakete angeliefert. Dann wird kontrolliert, wohin sie weiterverschickt werden sollen und wenn ein günstiger Weg gefunden worden ist, werden sie in Richtung Ziel gesendet.

1.2 DIENSTE IM INTERNET

Das Internet als Verbindung von unzähligen Computern und Netzwerken kann für verschiedenste Zwecke verwendet werden. Die am häufigsten genutzten Dienste sind:

- **WWW (World Wide Web)**
  Das WWW besteht aus unzähligen Websites, die vor allem Texte, Bilder und Videos enthalten. Um diese ansurfen und betrachten zu können, benötigt man einen Browser.
- **E-Mail**
  Die „elektronische Post“ ermöglicht das Versenden und Empfangen von Nachrichten in Sekundenschnelle.
- **ftp (file transfer protocol)**
  ftp dient zum Austausch und Kopieren von Dateien von einem Computer auf den anderen.
- **newsgroups**
  Newsgroups sind so etwas wie „Anschlagtafeln“ im Internet. So kann jemand zu einem bestimmten Thema seine Meinung kundtun (posten), innerhalb kürzester Zeit kann dieser Beitrag von Usern aus der ganzen Welt gelesen und kommentiert werden.
- **telnet**
  telnet ermöglicht den Fernzugriff vom eigenen auf andere Computer, die sich im selben Netzwerk befinden. Dadurch ist es z. B. möglich, von Zuhause auf das Netzwerk seiner Firma zuzugreifen und von seinem Heimarbeitsplatz aus zu arbeiten.
- **Web 2.0**
  Im „Mitmachweb“ ist man Produzent und Konsument zugleich, es bietet eine Vielzahl an Möglichkeiten (z. B. Wikis, soziale Netzwerke, Blogs).

IT-Security. Sicher unterwegs - Vorschau
12-025-238 © 2012
www.LehrerSelbstVerlag.de

1.3 GEFAHREN

Aus dieser kurzen Einführung lassen sich bereits drei potenzielle Gefahren ableiten, die für das Thema **Sicherheit im Internet** von grundlegender Bedeutung sind:

- **Anonymität** im Internet gibt es nicht. Egal, was du im Internet machst, du hinterlässt **Spuren** verschiedenster Art. Viele denken, dass sie anonym sind, weil gleichzeitig so viele Surfer unterwegs sind – doch das Gegenteil stimmt: Die Technik macht es möglich, Surfprofile anzulegen, Verhaltensweisen auszukundschaften und besuchte Webseiten herauszufinden. Wenn es sein muss (z. B. bei illegalen Handlungen, Cybermobbing, etc.) ist es genau möglich, herauszufinden, wer an welchem Computer was gemacht hat. In diesem Zusammenhang spricht man vom **digitalen Fußabdruck**: Alles, was du im Internet tust, hinterlässt Spuren. Das können Bilder, die du von dir auf Facebook präsentierst, Postings in Foren, Downloads von Spielen, E-Mails, die du schreibst, u.v.m. sein.

- Alle Daten bewegen sich auf verschiedensten Wegen durch das Netz. Dadurch ist es möglich, diese Daten „abzuhören". Jemand, der mit dem nötigen Know-How ausgestattet ist, kann **ungeschützte Daten abfangen und auslesen**. Das kann den Inhalt von E-Mails genauso betreffen wie sensible Daten (z. B. Kreditkartennummern, Kontodaten).

- Jedes Gerät (Computer, iPhone, etc.) wird zum Teil eines riesigen Netzwerkes und kann im Prinzip von anderen Netzteilnehmern **ausspioniert und angegriffen** werden. Je schlechter ein PC geschützt ist, desto höher ist die Wahrscheinlichkeit, angegriffen zu werden.

Das Internet ist ein weltweites Netzwerk von Computern und unterschiedlich großen Netzwerken. Jeder Computer, der sich mit dem Internet verbindet, erhält eine IP-Adresse und ist damit nicht mehr anonym. Die gemeinsame „Sprache" sind Protokolle, das wichtigste wird TCP/IP genannt. Daten werden im Internet in Pakete zerlegt und über verschiedene Wege versandt. Bekannte und häufig genutzte Dienste im Internet sind www, E-Mail, ftp und web 2.0.

1.4 LINKLISTE

www.internet-abc.de	Grundlegende Infos über das Internet
www.internauten.de	Spiele und Tipps rund um das Internet
www.klicksafe.de	Umfangreiche Seite rund ums Internet
www.saferinternet.at	Wissen rund ums Internet
http://www.youtube.com/saferinternetat	Videos zu Internet-Themen
http://a1internetfüralle.at/campus/kidsjugendliche	Kostenlose Schulungen rund ums Internet

IT-Security - Vorschau - Sicher unterwegs 12-025-238 © 2012 www.LehrerSelbstVerlag.de

SUMMARY I: WIE FUNKTIONIERT DAS INTERNET?

1. Was ist das Internet?

Das Internet (=**interconnected network**) ist ein **weltweites Netzwerk von Computern**, genauer gesagt: von Computernetzwerken. Wenn du dich mit deinem Computer oder Smartphone ins Internet einwählst, wirst du mit einem größeren Netzwerk (meist das eines Providers) verbunden. Dieses Netzwerk ist wiederum Teil eines größeren. Zwischen den Netzwerken bestehen verschiedene **Verbindungswege**, meist Glasfaserkabel.

Ein grundlegendes Prinzip der Verbindung im Internet ist das **Client-Server-Prinzip**.

2. Wie funktioniert die Verbindung zwischen zwei Computern?

Damit unter Millionen Computern **genau zwei** reibungslos miteinander in Verbindung treten können, braucht es folgende Unterstützung:

- **IP-Adresse:** Jeder PC verfügt über eine IP-Adresse, die so etwas wie eine Postadresse darstellt. Damit kann jeder Computer eindeutig identifiziert werden.
- **TCP/IP:** Damit PCs miteinander „sprechen" können, brauchen sie eine **gemeinsame „Sprache"**, die Protokoll genannt wird. Unter dem Namen TCP/IP werden die wichtigsten Protokolle zusammengefasst.
- **Router:** Damit die **Datenpakete** auch den richtigen und einen freien Verbindungsweg benutzen, werden sie über „Postämter", sogenannte Router, verschickt.

3. Dienste im Internet

Die wichtigsten Dienste im Internet sind das **WorldWideWeb, E-Mail, ftp, Newsgroups telnet** und das **Web 2.0.**

Bei all dem dürfte schon eines klar geworden sein: **Anonymität** beim Surfen gibt es nicht! Im Prinzip kann alles, was du tust, nachverfolgt werden (= **digitaler Fußabdruck**).

IT-Security - Vorschau - Sicher unterwegs
12-025-238 © 2012
www.LehrerSelbstVerlag.de

2. DATEN, INFORMATIONEN UND DATENSCHUTZ

„NICHT JEDER SCHATZ BESTEHT AUS SILBER UND GOLD."

2.1 AUS DATEN WERDEN INFORMATIONEN

Unter **Daten** wird alles verstanden, was **in digitaler Form** gespeichert werden kann. Das können Zahlen, Programmcode, Buchstaben, Symbole und Grafiken sein. Damit aus Daten **Informationen** werden, müssen sie in einen **Bedeutungszusammenhang** gestellt werden, d. h. sie müssen für den, der sie betrachtet oder verarbeitet, einen Sinn ergeben. So sagt die Zahl 027423532 noch nichts über ihre Bedeutung aus, sie ist lediglich ein **Datensatz**. Wird diese Zahl aber als Telefon-, Konto- oder Bestellnummer erkannt und behandelt, wird sie zur **Information** für denjenigen, der ihre Bedeutung versteht.
Daten sind sozusagen der „**Rohstoff**" für Information. Wer Daten richtig lesen kann, erhält Informationen. Von **personenbezogenen Daten** spricht man dann, wenn Daten einer Person zugeordnet werden können. Zu den persönlichen Daten gehören z. B. der Name, das Geburtsdatum, die E-Mail-Adresse, die Telefonnummer, die Kontonummer und die Wohnadresse.

2.2 DATEN LAUERN VIELFÄLTIGE GEFAHREN …

Daten sind in vielen Fällen **wertvolles Gut** und müssen geschützt werden. Unter wichtige, schützenswerte Daten fallen beispielsweise: die neuesten technischen Entwicklungen einer Firma, die Krankenakte einer Person, die Daten von Behörden, personenbezogene Daten (Kreditkartennummer, E-Mail-Adresse) und auch urheberrechtlich geschützte Musik und Filme fallen unter diese Kategorie.

WICHTIGEN DATEN DROHEN VIELFÄLTIGE GEFAHREN:

a) Cybercrime

Cybercrime ist ein **Sammelbegriff** für verschiedenste Formen der Internetkriminalität. Dazu zählen Internetbetrug, Kinderpornografie, die Verbreitung von extremem politischen Gedankengut (z. B. rechtsradikale Inhalte), Urheberrechtsverletzungen (z. B. das illegale Downloaden von Musik). Häufige kriminelle Handlungen im Zusammenhang mit dem **Ausspähen und dem Diebstahl von Daten sind**:

- der Betrug mithilfe finanzieller Daten (z. B. gestohlene Kreditkarteninformationen oder Kontodaten)
- das Ausspähen von persönlichen Daten (z. B. die E-Mail-Adresse für Werbezwecke, Spam)
- die Verbreitung von illegal kopierter Software (Softwarepiraterie)
- das bewusste Manipulieren oder Vernichten von Daten
- das Ausspähen von wertvollen Informationen im industriellen und wirtschaftlichen Bereich (z. B. Industriespionage)

IT-Security - Sicher unterwegs
Vorschau
12 026 238 © 2012
www.LehrerSelbstVerlag.de

b) Datenverlust durch „höhere Gewalt“

Datenverlust droht auch durch unvorhergesehene Ereignisse wie Feuer, Erdbeben oder Hochwasser. Auch in Krisen- und Kriegszeiten können wichtige Daten leicht zerstört werden oder verloren gehen.

c) Menschliche Fehler

Ein häufig vorkommender Grund für Datenverlust liegt schlicht und einfach in **Bedienungsfehlern**, die durch mangelnde Kompetenz oder Unaufmerksamkeit von Mitarbeitern verursacht werden. So können Daten versehentlich gelöscht oder nicht gespeichert, sensible Daten irrtümlich an die falsche Adresse versendet oder Datenbestände durch falsche Bearbeitung ganz oder teilweise vernichtet werden. Gelegentlich kommt es auch vor, dass unbefugte Personen Zugriff auf Dateien erhalten, die nicht für sie bestimmt sind. Wenn z. B. ein Schulnetzwerk schlecht gesichert ist, kann es sein, dass Schüler Zugriff auf Daten bekommen, die eigentlich nur für Lehreraugen bestimmt sind. Es kann auch passieren, dass Mitarbeiter einfach **schlampig oder fahrlässig** handeln: Passwörter werden auf Zettel geschrieben und für alle gut sichtbar auf den Monitor geklebt, USB-Sticks mit wichtigen Daten gehen verloren, usw.

2.3 Die drei Hauptziele der Datensicherheit

Damit Daten **möglichst sicher verwahrt** werden, sollen **drei Grundprinzipien** der Datensicherheit eingehalten werden:

- **Vertraulichkeit**
  Das **erste Ziel der Datensicherheit** besteht darin, dass nur diejenigen Personen vertrauliche Daten sehen können, die auch dazu **berechtigt** sind. In einem Schulnetzwerk sollen nur Lehrer Zugriff auf die Daten der Schüler (z. B. Adressen, familiäre Verhältnisse und Noten) haben. In einem Krankenhaus dürfen die Patientendaten nur von berechtigten Personen eingesehen werden. E-Mails, die einen vertraulichen Inhalt haben, sollten nur von den Personen gelesen werden können, an die geschrieben wurde.

- **Integrität**
  Das **zweite Ziel der Datensicherheit** zielt darauf ab, dass Daten **unverändert** und **korrekt** bleiben. Es soll sicher gestellt werden, dass Daten nicht versehentlich, absichtlich oder durch einen technischen Fehler verändert werden. In der **Schule** muss das System so weit abgesichert sein, dass kein Unbefugter (z. B. ein Schüler) die Zeugnisnoten beliebig verändern kann. Auch Daten von **Behörden** müssen korrekt sein: Wenn z. B. jemand durch einen technischen Fehler für tot erklärt wird, wird er das schmerzhaft spüren: seine Pension wird eingestellt.
  Eng im Zusammenhang mit dem Ziel der Integrität steht der Begriff der **Authentizität**: Es soll gewährleistet sein, dass man nachvollziehen kann, **woher Daten stammen**. Ein Beispiel dafür kann eine E-Mail mit wichtigen Inhalten sein: Man kann dem Inhalt nur vertrauen bzw. sich darauf berufen, wenn der Absender der E-Mail **eindeutig** feststeht. Das kann z. B. durch eine digitale Unterschrift gewährleistet werden, die genauso gilt wie die eigenhändige Unterschrift auf Papier.

IT-Security - Vorschau - Sicher unterwegs
12-025-228 © 2012
www.LehrerselbstVerlag.de

- **Verfügbarkeit**
  Als **drittes Ziel der Datensicherheit** soll sicher gestellt sein, dass der Zugriff auf Daten **dauerhaft gewährleistet** ist. Das technische System muss so **sicher** sein, dass man auf benötigte Daten, Informationen und Dienste zuverlässig zugreifen kann. Systemausfälle sollen nach Möglichkeit verhindert werden. In beinahe jedem Bereich unseres Alltags sind wir in erheblichem Ausmaß auf Computersysteme angewiesen. Wenn z. B. das Stromnetz nur für ein paar Stunden ausfällt, kann das enorme Schäden nach sich ziehen. Um Verfügbarkeit zu gewährleisten, müssen Computersysteme auf verschiedene Art und Weise **abgesichert** werden:
  - Server (="Gehirne" von Netzwerken) müssen **gegen Feuer und Wasser** abgesichert sein.
  - Server müssen gegen einen plötzlichen **Stromausfall** abgesichert sein (z. B. durch unterbrechungsfreie Stromversorgung)
  - Das System muss **gegen unbefugten Zugriff** geschützt sein.
  - Wichtige Daten müssen noch an einem anderen Ort gespeichert werden (**Backups**).

2.4 Rechtliche Grundlagen des Datenschutzes

a) Datenschutzgesetz

Personenbezogene Daten sind alle Daten, die sich mit einer bestimmten Person in Verbindung bringen lassen (Name, Adresse, Telefonnummer, E-Mail-Adresse, Sozialversicherungsnummer, Geburtsdatum, Konto- und Kreditkartendaten, Krankenakte, u. v. m.) Diese Daten werden durch **Gesetze** geschützt. In Österreich zeichnen sich das **Datenschutzgesetz** (DSG 2000) und das **Telekommunikationsgesetz**, in Deutschland das **Bundesdatenschutzgesetz** und das **Telekommunikationsgesetz** dafür verantwortlich. Diese Gesetze legen vor allem folgende Richtlinien fest:

- Prinzipiell hat jedermann Anspruch darauf, dass seine personenbezogenen Daten **geheim gehalten** werden. Es gibt allerdings **Ausnahmen**, z. B. für Behörden (z. B. Meldeamt, Finanzamt) und wenn ein Gericht die Offenlegung von Daten fordert.
- Das **Grundrecht auf freie Entfaltung der Persönlichkeit** legt fest, dass das Individuum gegen eine unbegrenzte Erhebung, Speicherung, Weitergabe und Verwendung seiner Daten **geschützt** werden muss. Im Klartext heißt das, dass für jede Erhebung oder Verarbeitung von personenbezogenen Daten eine rechtliche Grundlage bestehen muss und das Schutzbedürfnis des Individuums dadurch nicht verletzt werden darf.
- Personenbezogene Daten dürfen **ohne ausdrückliche Erlaubnis** im Online-Bereich nicht erhoben, gespeichert oder verarbeitet werden. Andere dürfen Daten nur für einen Zweck verwenden, der mit dir ausdrücklich vereinbart wurde oder wenn es per Gesetz erlaubt ist. Es gilt der **Grundsatz der informierten Einwilligung:** Will jemand (z. B. eine Firma oder Dienstleister) Daten über eine Person speichern, so muss diese **ausdrücklich einwilligen** – das geschieht meist über eine **Datenschutzerklärung** auf den Internetseiten. Firmen sind natürlich an deinen Daten interessiert, z. B. für Werbung. Daher wird es dem Nutzer leicht gemacht, einzuwilligen: Man muss lediglich einen „Haken" setzen.

IT-Security - Sicher unterwegs - Vorschau
ISBN 978-3-902525-238 © 2012
www.LehrerSelbstVerlag.de

- Behörden und Ämter, die personenbezogene Daten verarbeiten, müssen dafür Sorge tragen, dass diese Daten **ausreichend geschützt werden** und nicht missbräuchlich verwendet werden können. Mitarbeiter dieser Behörden unterliegen der **Verschwiegenheitspflicht**, d. h. sie dürfen diese Daten nicht an Dritte weitergeben bzw. Auskunft darüber erteilen.
- Werden Daten von Ämtern, Behörden oder auch Firmen gespeichert, dann hat man das **Recht** …
  - über Umfang und Zweck der Datenspeicherung informiert zu werden,
  - Auskunft darüber zu verlangen, welche Daten gespeichert werden,
  - falsch gespeicherte Daten berichtigen zu lassen,
  - unrechtmäßig gespeicherte Daten löschen zu lassen,
  - jederzeit zu verbieten, dass Daten weiterhin verwendet werden. Das gilt allerdings nicht, wenn die Verwendung der Daten gesetzlich erlaubt ist (z. B. in Polizeiakten oder beim Meldeamt).

b) Das Urheberrecht

Nicht nur die eigenen persönlichen Daten werden vom Gesetz geschützt, auch **geistiges Eigentum** soll durch das Urheberrecht vor Missbrauch bewahrt werden. Als geistiges Eigentum versteht man eigenständige (inviduelle, originelle) geistige Schöpfungen, die sich in folgende **Kategorien** einteilen lassen:

- Literatur: Romane, Erzählungen, Gedichte, …
- Musik: Pop-Songs, Schlager, Musicals, …
- Bildende Kunst: Gemälde, Kunstwerke, …
- Filmkunst: Videos, Kinofilme, Werbespots, …

Das Urheberrecht **verbietet**, fremdes geistiges Eigentum zu verwenden. Ein paar typische **Urheberrechtsverletzungen** sind beispielsweise:

- Bilder aus dem Internet kopieren und in die eigene Website einfügen
- kommerzielle Videos (z. B. Kinofilme) und Musikfiles zum Download anbieten
- Kopieren von DVDs und Musik-CDs und diese an Freunde und Bekannte weitergeben
- Musik kostenlos aus illegalen Quellen downloaden
- Texte aus Büchern einscannen und verbreiten
- Seiten aus Schulbüchern kopieren und diese austeilen

Verletzungen des Urheberrechts sind keine Kavaliersdelikte und können **teuer** kommen. Besonders problematisch sind **Tauschbörsen** für Musik und Videos, denn gerade hier werden Urheberrechtsverletzungen von der Unterhaltungsindustrie rigoros verfolgt. Wenn man z. B. Musikfiles auf Tauschbörsen wie eDonkey oder BitTorrent „shared“ (=zum Download bereitstellt), begeht man auf jeden Fall eine Urheberrechtsverletzung. Wer auf Nummer sicher gehen möchte, sollte auf alle Fälle legale Dienste wie www.itunes.com/de oder www.musicload.de nutzen.

Das Urheberrecht schützt aber auch dich als **Individuum** und zwar durch …

- **Das Recht am eigenen Bild**
  Wenn von dir Fotos oder Aufnahmen mit Webcams oder Digitalkameras gemacht werden, hast du das Recht, **darüber zu entscheiden**, ob diese Ablichtung veröffent-

IT-Security - Sicher unterwegs - Vorschau - 12-025-238 © 2012 www.LehrerselbstVerlag.de

licht werden darf. Das spielt eine große Rolle auf sozialen Netzwerken, wie z. B. facebook. Es darf also niemand von jemandem ein Foto oder eine Videoaufnahme online stellen, wenn „**berechtigte Interessen**“ verletzt werden. Das betrifft vor allem Fotos und Videos, die jemanden **in nachteiliger Weise zeigen oder bloßstellen** (z. B. Fotos in betrunkenem Zustand). Entdeckt man im Internet ein nachteiliges Foto oder Video, hat man das Recht, diese Aufnahme löschen zu lassen.

Daten umfassen alles, was digital gespeichert werden kann. Werden Daten in einen Bedeutungszusammenhang gestellt, werden sie zu Informationen. Daten müssen geschützt werden, da damit Missbrauch in verschiedensten Formen betrieben werden kann (cybercrime). Die Hauptziele der Datensicherheit lauten Vertraulichkeit, Integrität (Authentizität) und Verfügbarkeit. Der Schutz personenbezogener Daten und geistigen Eigentums wird im Datenschutzgesetz und im Urheberrecht geregelt.

c) Creative Commons–Lizenz

Im Internet gibt es aber auch Unmengen an sogenannten „**Open contents**“: Das sind Inhalte (Fotos, Videos, Software, …), deren Nutzung von den Urhebern ausdrücklich **gestattet** wurde. Autoren und Urheber, die ihre Werke frei zugänglich machen möchten, veröffentlichen diese unter einer **Creative-Commons-Lizenz**. Jede Creative-Commons-Lizenz erlaubt das Kopieren, Verteilen und Benutzen eines Werkes, solange die Bedingungen, die vom Autor vorgegeben werden, eingehalten werden. Es gibt verschiedene **Einschränkungen**: So kann z. B. vom Autor verlangt werden, dass sein Name genannt wird oder das Werk darf nicht zur kommerziellen Nutzung verwendet werden. Es kann auch sein, dass zwar das Verbreiten und Verwenden eines Werks erlaubt, die Bearbeitung und Veränderung allerdings verboten ist. Genaue Informationen zu den Lizenzierungsarten findest du unter http://creativecommons.org.

2.5 LINKS

http://www.surfen-ohne-risiko.net/daten-schuetzen/	Grundlegende Informationen zum Datenschutz
http://www.klicksafe.de/themen/datenschutz/	Datenschutz auf klicksafe
http://www.klicksafe.de/themen/datenschutz/	Quiz zum Thema Datenschutz
http://www.panopti.com.onreact.com/swf/index.htm	Interaktive Präsentation zum Thema Datenschutz
www.handysektor.de	Handy und Datenschutz, Menü: Tipps
www.datenparty.de	Infos und Tipps
www.saferinternet.at	Thema: Datenschutz
www.irights.info	Genaue Informationen zum Urheberrecht
http://freemusicarchive.org/ www.jamendo.de, www.ccmixter.org	Freie Musik im Internet
http://creativecommons.org	Informationen zu Creative Commons
http://search.creativecommons.org	Suchmaschine für CC-Werke

IT-Security - Sicher unterwegs - Vorschau - 12-025-238 © 2012 www.LehrerSelbstVerlag.de

SUMMARY 2: DATEN UND DATENSCHUTZ

1. Was sind Daten und Informationen?

Unter Daten wird alles verstanden, was in digitaler Form gespeichert werden kann (Zahlen, Buchstaben, Programmcode, Grafiken, Symbole). Werden Daten in einen Bedeutungszusammenhang gebracht, werden sie zur **Information**. Daten, die einer Person zugeordnet werden können (Adresse, Telefonnummer, Kontodaten, etc.) nennt man **personenbezogene Daten.**

2. Gefahren für Daten

Daten sind ein wertvolles Gut und müssen geschützt werden. Sie werden durch drei Hauptgefahren bedroht: **Cybercrime, Datenverlust durch „höhere Gewalt“** und **menschliche Fehler.**

3. Die drei Hauptziele des Datenschutzes

Damit Daten möglichst sicher verwahrt werden, müssen drei Grundprinzipien eingehalten werden: **Vertraulichkeit, Integrität und Verfügbarkeit.**

4. Rechtliche Grundlagen des Datenschutzes

Bestimmte Daten werden auch gesetzlich geschützt, zwei Gesetze sind dafür maßgeblich:

a) **Datenschutzgesetz**
Dieses Gesetz schützt vor allem personenbezogene Daten. Es legt fest, dass Daten prinzipiell geheim gehalten werden müssen.

b) **Urheberrecht**
Durch dieses Gesetz wird **geistiges Eigentum** geschützt: Musik, Filme, Texte, etc., die du nicht selbst hergestellt hast, dürfen von dir auch nicht verwendet, kopiert, heruntergeladen u. Ä. werden. Zum Urheberrecht gehört auch das **Recht am eigenen Bild.**

IT-Security - Vorschau - Sicher unterwegs
12-025-238 © 2018
www.LehrerSelbstVerlag.de

TEST: GRUNDLAGEN UND DATENSCHUTZ

1. Wofür steht die Abkürzung Internet?

a.	international network	
b.	interconnected network	
c.	interrupt network	
d.	interpretation network	

2. Was ist das Internet?

a.	ein weltweites Netzwerk von Computern und Netzwerken	
b.	ein europaweites Netzwerk	
c.	eine Verbindung von Netzwerken zwischen Europa und Übersee	
d.	eine weltweite Verbindung von Einzelcomputern	

3. Das grundlegende Prinzip bei der Datenübertragung im Internet nennt sich:

a.	peer-to-peer-connection	
b.	server-server-Prinzip	
c.	client-server-Prinzip	
d.	computer-connection	

4. Wodurch kann ein Computer im Internet eindeutig identifiziert werden?

a.	Postanschrift	
b.	Seriennummer	
c.	Telefonnummer	
d.	IP-Adresse	

5. Damit Computer miteinander kommunizieren können, brauchen sie eine gemeinsame „Sprache". Wie nennt man diese?

a.	TCP/IP-Protokoll	
b.	ftp	
c.	www	
d.	Standardprotokoll	

6. Welche Aussage ist richtig? (drei richtige Antworten)

a.	Im Internet kann man ohne Bedenken anonym surfen.	
b.	Daten werden über das Internet in getrennten Paketen verschickt.	
c.	Mit der richtigen Software kann man fremde Daten „mitlesen".	
d.	Je ungeschützer ein Computer ist, desto leichter kann er von außen angegriffen werden.	

7. Welcher Dienst ist kein Internetdienst?

a.	telnet	
b.	www	
c.	ftp	
d.	usb	

8. Wie lauten die drei Hauptziele der Datensicherheit? (drei richtige Antworten)

a.	Vertraulichkeit	
b.	Geheimhaltung	
c.	Integrität	
d.	Verfügbarkeit	

IT-Security - Sicher unterwegs - Vorschau
978-3-7025-238 © 2012
www.LehrerSelbstVerlag.de

9. Wie hängen Daten und Informationen zusammen?

a.	Daten und Informationen sind im Prinzip dasselbe.	
b.	Informationen erhält man, indem man Daten interpretieren kann.	
c.	Daten sind Zahlen, Informationen sind Buchstaben.	
d.	Alles, was man an technischen Zusammenhängen verstehen kann, sind Informationen, der Rest sind Daten.	

10. Wie lautet der Sammelbegriff für kriminelle Handlungen im Internet?

a.	cyborg	
b.	cyberactivities	
c.	cybercrime	
d.	cybercriminal	

11. Was versteht man unter personenbezogenen Daten? (zwei richtige Antworten)

a.	Alle Daten, die man mit einer Person in Zusammenhang bringen kann.	
b.	Adresse, E-Mail-Adresse, Telefonnummer ein und derselben Person	
c.	urheberrechtlich geschützte Musikdateien	
d.	Fotos auf der Schulwebsite	

12. Welche Aussage zum gesetzlich geregelten Datenschutz ist richtig? (drei richtige Antworten)

a.	Im Online-Bereich dürfen Daten ohne ausdrückliche Zustimmung nicht gespeichert und verarbeitet werden.	
b.	Jeder Bürger hat prinzipiell das Recht, dass seine Daten geheim gehalten werden.	
c.	Falsch gespeicherte Daten müssen berichtigt werden.	
d.	Behörden dürfen jederzeit auf Daten zugreifen.	

13. Was schützt das Urheberrecht?

a.	Alle Musikdateien, die im Internet verfügbar sind.	
b.	Alle Fotos, die im Internet verfügbar sind.	
c.	die persönlichen Rechte von Autoren	
d.	geistiges Eigentum wie Romane, Kinofilme, Kunstwerke	

14. Wie nennt man das Recht, Bilder oder Videoaufnahmen von sich selbst nicht veröffentlichen zu lassen?

a.	Recht an der eigenen Person	
b.	Recht am eigenen Bild	
c.	Recht am eigenen Video	
d.	Recht zur Selbstbestimmung	

15. Durch welche menschlichen Fehler können Daten ganz oder teilweise vernichtet oder versehentlich preisgegeben werden? (drei richtige Antworten)

a.	Bedienungsfehler	
b.	Fahrlässigkeit im Umgang mit Passwörtern	
c.	fehlerhaftes Speichern	
d.	zu lange Kaffeepausen	

GESAMTPUNKTZAHL: 24 P. **DEINE PUNKTEZAHL: _____**

IT-Security - Sicher unterwegs - Vorschau
12.025.238 © 2012
www.LehrerSelbstVerlag.de